Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 6, No. 4, August 2025, Page. 1745-1768
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4835

Ambidextrous AI Governance Model for Advancing State-Owned Bank in Indonesia Digital Transformation Through COBIT 2019 Traditional and DevOps

Rama Putra Ramdani*[1], Rahmat Mulyana[2], Taufik Nur Adi[3]

[1,3] Information Systems, Faculty of Industrial Engineering, Telkom University, Indonesia
[2]Department of Computer and Systems Science, Stockholm University, Sweden

Email: [1]ramaputra@student.telkomuniversity.ac.id

Received: Jun 6, 2025; Revised: Jun 24, 2025; Accepted: Jun 24, 2025; Published: Aug 18, 2025

Abstract

Integrating artificial intelligence into the banking sector accelerates digital transformation, but it also presents governance challenges, particularly in striking a balance between innovation and regulatory compliance, risk management, and operational control. This research proposes an ambidextrous AI governance model by combining two distinct yet complementary mechanisms from COBIT 2019: the structured, control-oriented Traditional framework and the agile, adaptive DevOps Focus Area. This dual approach enables organizations to pursue innovation and maintain governance stability simultaneously. The study investigates BankCo's, a state-owned bank in Indonesia that is undergoing a systemic digital transformation and applies the Design Science Research (DSR) methodology with a case study approach. Collecting data through five semi-structured interviews with key IT Governance, Risk, and Compliance stakeholders and triangulated with internal policy documents, annual reports, and audit trails. The analysis identified two prioritized Governance and Management Objectives (GMOs), MEA03 (Managed Compliance with External Requirements) and APO12 (Managed Risk), based on design factors, regulatory alignment (POJK No. 11/2022 and SOE Minister Regulation No. PER-2/MBU/03/2023), and agile governance needs. A maturity gap analysis revealed areas for improvement across people, process, and technology dimensions, with the proposed model raising governance capability from 3.55 to 3.95. The proposed model applies multidimensional prioritization through Resource-Risk-Value (RRV) analysis. This study presents a practical and auditable approach to ethical AI governance that strikes a balance between innovation and accountability. The model supports digital transformation in banks and contributes to information systems governance by linking the ethical use of AI with agile yet compliant practices in regulated environments.

Keywords: *Ambidextrous AI Governance, Banking, Case Stud, COBIT 2019, Compliance, Design Science Research, DevOps, Digital Transformation, Risk Management.*

1. INTRODUCTION

The Fourth Industrial Revolution has altered the global banking sector, compelling conventional financial institutions to accelerate digital transformation (DT) in response to ever-changing market demands [1], [2]. Preferences for mobile banking, electronic payments, and tailored financial services are being used to describe digital-native client behavior [3], [4]. These changes have made DT a vital survival strategy for banks looking to compete with fintech and big-tech enterprises that are technologically nimble and innovative [5], [6]. Simultaneously, financial institutions face more demanding regulatory compliance standards, as demonstrated by Indonesia's Otoritas Jasa Keuangan (OJK), highlighting the necessity of prudent risk management in technology deployment [7]. As one of Indonesia's largest commercial banks, BankCo has the difficult task of integrating new digital technology into its current infrastructure in a safe, compliant, and scalable manner [8].

Vol. 6, No. 4, August 2025, Page. 1745-1768
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4835

Emerging as a pillar of DT in the banking industry, artificial intelligence (AI) provides real-time data analytics, automated credit scoring, predictive risk modelling, and tailored consumer interactions via AI-powered chatbots [9], [10]. However, with these developments come serious governance problems like algorithmic bias, data privacy violations, cybersecurity vulnerabilities, and ethical questions [11], [12]. These difficulties have driven an increasing demand for strong AI governance systems guaranteeing responsible AI use and regulatory alignment [13]. Despite growing scholarly interest, there is a notable gap in research addressing how AI governance can be operationalized within the DT agendas of banks, particularly in developing economies where regulatory landscapes are evolving rapidly [14], [15]. This study fills this gap by operationalizing an ambidextrous AI governance model in state-owned financial institutions under regulatory pressure.

In this context, BankCo must develop and adopt a governance model capable of managing technological complexity and public accountability while maintaining compliance with national policies and industry standards [16]. To meet these governance challenges, this research proposes the ambidextrous approach to AI governance design with the two mechanisms of COBIT 2019 Traditional, which is more structured, and COBIT 2019 DevOps, which is a more flexible, agile, adaptive approach, allows organizations to optimize the potential for innovation while maintaining control over operational stability [17], [18]. With the ambidextrous combination of COBIT 2019 Traditional and DevOps, BankCo can design AI governance that is agile, but secure and trustworthy. COBIT 2019 provides the structure needed for effective planning and management, while DevOps enables integration between development and operations, supporting AI deployment quickly and efficiently [19], [20], [21]. This ambidextrous approach is well-suited for the banking sector, where operational stability must be balanced with the demands of rapid technological change [22], [23]. Nevertheless, integrating both models within a single organization introduces unique challenges, including alignment across cultural and process dimensions and adherence to governance standards in a highly regulated environment [24].

BankCo provides a case study for this study to look at the actual use of AI governance in a technologically evolving bank. Showing strategic intent to use intelligent technologies, BankCo has used AI for credit approval and customer relationship management [25], [26]. However, the absence of a unified governance structure poses a risk to long-term compliance and operational consistency [27]. Regulatory mandates such as POJK No.11/2022 and SOE Minister No. 2/2023 further necessitate the establishment of structured governance mechanisms that oversee AI implementation and usage [28], [29]. To capture ground-level insights, this study applies a qualitative research methodology using semi-structured interviews with stakeholders from BankCo's IT, risk management, and audit functions.

This study addresses this research question: How can an AI governance model based on COBIT 2019 Traditional and DevOps be developed to support digital transformation in BankCo? The objective is to explore current governance practices, design an integrated model that leverages the strengths of both COBIT 2019 framework approaches, and assess its potential impact on DT outcomes. The study contributes theoretically by extending the literature on ambidextrous IT governance and AI risk management [30], [31]. While offering a replicable governance framework that aligns AI innovation with ethical standards, regulatory compliance, and sustainable value creation. In the context of informatics and computer science, this study also addresses the urgent need to embed ethical principles within AI deployment through structured IT Governance mechanisms-particularly in highly regulated environments such as Indonesia's banking sector, where mandates like POJK No. 11/2022 intersect with AI-based digital initiatives [28], [32], [33]. Prior research underscores that effective governance significantly enhances risk oversight and ethical behavior [34], yet ethical alignment remains underdeveloped in AI practices across emerging economies [35]. By proposing a ambidextrous AI governance model grounded in COBIT 2019 and DevOps, this research contributes to the field of

Vol. 6, No. 4, August 2025, Page. 1745-1768
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4835

informatics by bridging technical agility with ethical safeguards, enabling organizations to maintain algorithmic transparency, accountability, and responsibility in AI-driven decision-making [31], [36].

2. THEORETICAL FOUNDATION

DT in the banking sector demands more than digitization; it requires a systemic reconfiguration of governance to manage innovation and risk [37], [38]. AI offers significant value through real-time analytics and automation [39]. However, its integration into regulated financial environments introduces critical ethical, technical, and compliance risks that necessitate a governance framework grounded in transparency, fairness, accountability, and alignment with global norms such as OECD AI Principles and EU Trustworthy AI [40], [41], [42]. Despite this, many AI governance principles remain weakly embedded in operational banking practices, particularly under regulatory contexts such as OJK [43], [44]. As a strategic extension of corporate governance, IT governance ensures alignment between digital innovation and risk management objectives [27], [45]. COBIT 2019 offers a structured yet flexible governance architecture combining governance and management objectives with modularity and performance metrics [19], [46], [47]. It further supports DevOps integration to accelerate AI delivery through agile, lean, and collaborative IT practices [20], [48]. However, relying solely on traditional control-based governance or agile frameworks is insufficient in banking, where regulatory strictness coexists with innovation imperatives [30]. This necessitates ambidextrous IT governance, a synergistic combination of agile-adaptive and traditional mechanisms that balance exploration, emphasizing flexibility, innovation, and adaptability, with exploitation, which prioritizes stability, control, and efficiency, allowing organizations to optimize their digital and IT risks and resources toward value realization. [17], [30]. Such duality is essential for AI governance, where ethical accountability must evolve alongside technological advancement [18]. This study addresses the gap in integrative frameworks that unify COBIT 2019 Traditional and DevOps for managing AI in DT [19], [20], [21].

3. RESEARCH METHODOLOGY

3.1. Conceptual Model

This study employs a conceptual model grounded in the Design Science Research (DSR), which emphasizes the structured development and rigorous evaluation of information technology artifacts to address clearly defined organizational problems within a specific domain [49]. As shown in Figure *1*, the DSR framework is composed of three interdependent components: the environment, the information systems research process, and the knowledge base. This study adopts a case study approach aligned with Yin's, suitable for investigating complex organizational phenomena within real-life contexts [50]. Given the focus on understanding dynamic governance mechanisms under conditions of technological transformation, this approach provides the flexibility and contextual richness necessary to examine how BankCo enacts ambidextrous AI governance by blending traditional control frameworks with agile operational practices in pursuit of digital transformation.

This study employs the DSR framework to construct an AI governance model tailored to BankCo's organizational context. The environment component captures contextual relevance by reflecting digital capabilities, transformation strategies, and formalized governance practices, including policies, structural roles, and supporting technologies. The IS research component operationalizes the DSR cycle through iterative build and evaluation processes, producing governance artifacts such as design factors and AI oversight objectives developed with COBIT 2019 Traditional and DevOps, and validated through case-based assessments applying credibility, transferability, dependability, and confirmability. The knowledge base reinforces methodological rigor by grounding the study in established theories of IT governance, DT, AI, and ambidextrous IT, supported by qualitative strategies, including semi-structured interviews, triangulated data sources, and content analysis.

Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 6, No. 4, August 2025, Page. 1745-1768
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4835

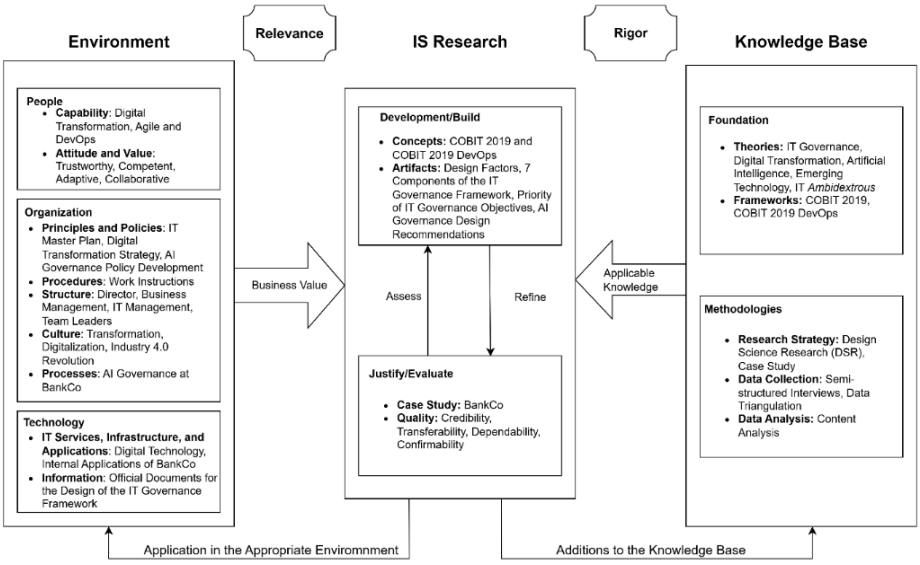

Figure 1. Design Science Research adopted from Hevner [49]

3.2. Research Process

The research process comprises five interconnected phases: Problem Identification, Requirement Determination, Design and Development, Demonstration, and Evaluation, as visualized in Figure 2 [51].

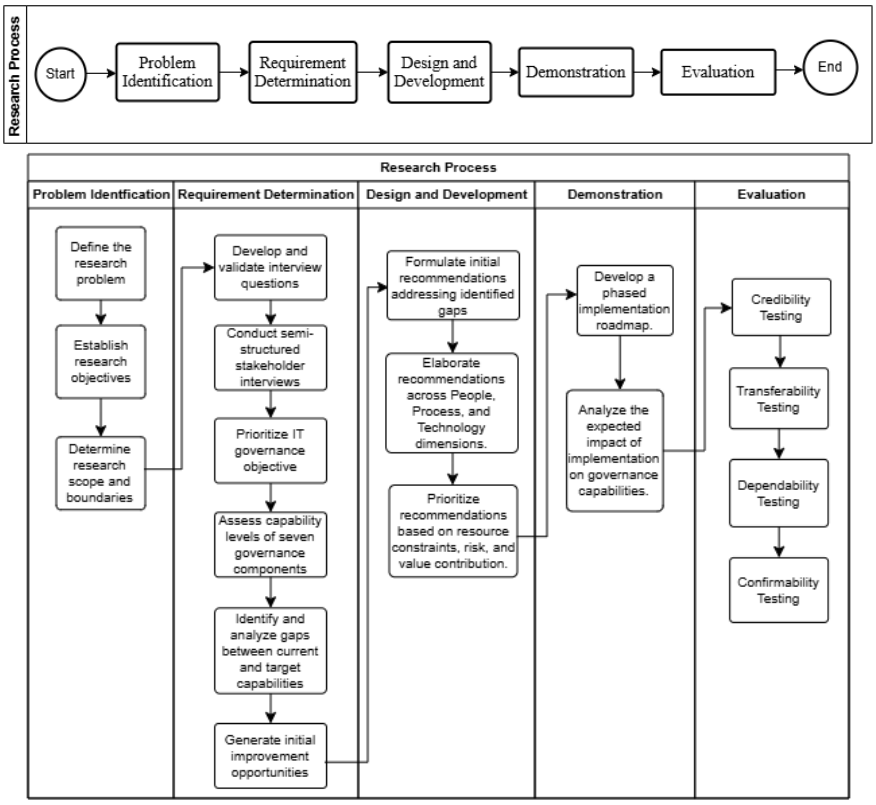

Figure 2. Research Process

In the Problem Identification phase, the research problem was clearly defined and validated through expert consultations to align with unresolved AI governance challenges in the banking sector. During the Requirement Determination phase, semi-structured interviews were conducted to capture contextual requirements, prioritize governance objectives, and assess capability levels across COBIT

Vol. 6, No. 4, August 2025, Page. 1745-1768
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4835

2019 components. The data collection process in this study adopted a rigorous qualitative approach, combining primary and secondary data sources, as detailed in Table 1. Primary data were obtained through semi-structured interviews conducted between March and May 2025 with three key informants at BankCo: the IT Strategic Planning & Governance Officer, IT Strategic Planning and Development Officer, Digital Risk Assessment Officer, IT Security Officer, and Internal Audit Officer. These individuals were purposefully selected for their strategic roles and direct IT governance, compliance, and risk management involvement. Semi-structured interviews provided a methodological benefit, allowing controlled but flexible exchanges. This approach allowed researchers to maintain thematic consistency while responding to each informant's contextual realities and experiential depth. Studying AI governance systems is appropriate for this method since institutional complexity and changing regulatory environment call for interpretative depth and contextual sensitivity. Complementing the interviews, secondary data were drawn from official documents such as the Annual Report, Sustainability Report, IT Audit Report, Standard Operating Procedure (SOP)s, compliance training records, and the Special Policy on IT, Digital & Cyber Risk. These documents served both as triangulation tools and empirical guides, enriching the interpretive depth and enabling cross-verification of findings [52]. After collecting primary and secondary data, the analysis began by identifying high-priority Governance and Management Objectives (GMOs) using the COBIT 2019 framework and DevOps Focus Area. The current governance state at BankCo was assessed through COBIT's seven enablers, allowing a structured evaluation of capabilities across people, processes, and technology. After that, a gap analysis was done to see how the current situation compared to the target maturity levels. This led to governance recommendations specific to BankCo's AI implementation setting. The study used trustworthiness criteria and a pre-and post-capability maturity assessment to check the model's credibility, relevance, and real-world impact.

Table 1. Primary and Secondary Data

Topic	Date Range	Respondent	Position
Primary Data			
Discussing aspects related to the organizational profile, as well as IT governance strategies and practices implemented at BankCo.	March - May 2025	Interviewee 1	IT Strategic Planning & Governance Officer
Discussing compliance with regulations applied in IT governance at BankCo.		Interviewee 2	IT Strategic Planning & Development Officer
Discussing information risk management in the governance applied at BankCo.		Interviewee 3	Digital Risk Assessment Officer
Discussing cybersecurity, incident response, and security governance at BankCo.		Interviewee 4	IT Security Officer
Discussing audit, control assurance, and IT risk compliance at BankCo.		Interviewee 5	Internal Audit Officer
Secondary Data			
BankCo Annual Report 2024, BankCo Sustainability Report 2024, Organizational Structure Document, IT Audit Report, Compliance Training Documents, SOPs, Special Policy on IT, Digital & Cyber Risk Management Procedures			

The Design and Development phase involved potential improvement initiatives across people, process, and technology dimensions, which were then prioritized based on Resources, Risk, and Value (RRV). This method evaluates each initiative based on three dimensions: Resources, which considers the availability and estimated requirement of time, budget, workforce, and supporting tools (Song et al., 2022); Risk, which assesses the potential impact of not implementing the initiative, including operational disruptions or strategic misalignment [53], [54]; and Value, which measures the expected benefits not only in terms of cost efficiency and quality enhancement, but also long-term sustainability,

stakeholder satisfaction, and alignment with strategic goals [55]. Each component was rated on a one to three scale using expert judgment and then weighted equally to generate a composite RRV score. Initiatives with higher RRV scores were prioritized for implementation due to their strategic importance, risk mitigation potential, and organizational value contribution. The Demonstration phase operationalized these recommendations into a phased implementation roadmap to evaluate their projected impact on governance capability maturity and support value-driven DT.

The evaluation stage in this research was conducted comprehensively to assess the scientific quality, reliability, and effectiveness of the developed governance model, using the qualitative trustworthiness criteria approach as proposed [51], namely credibility, transferability, dependability, and confirmability were implemented systematically and are summarized in Table 2.

Table 2. Model Validation [51]

Criteria	Description	Validation Strategy
Credibility	Ensures that the findings are truthful and accurately represent participants' perspectives.	Triangulation of interview data, document analysis, and expert/supervisor validation.
Transferability	Assesses whether the findings can be applied to similar contexts beyond the immediate research setting.	Generalization of governance principles for financial institutions implementing AI.
Dependability	Demonstrates that the research process is consistent, traceable, and could be repeated in similar contexts.	Complete documentation of methodology, with continuous consultation with practitioners.
Confirmability	Confirms that the findings are shaped by data and not researcher bias.	Compilation of audit trail and validation by external experts and stakeholders.

Table 2 outlines the four trustworthiness criteria used to validate the model. Each was addressed through systematic strategies ensuring credible findings, transferable insights, consistent processes, and objective, evidence-based results. To evaluate the effectiveness of the Ambidextrous COBIT 2019 Traditional and DevOps model, this study applied a pre-implementation and post- implementation of capability maturity across COBIT's seven governance components.

4. ANALYSIS AND RESULT

4.1. GMO Prioritization Result

This section outlines the prioritization of GMO at BankCo, which is constructed through the integration of COBIT 2019 Design Factors [46], COBIT 2019 DevOps Focus Area [20], and regulatory requirements from POJK No.11/2022 and SOE Minister No.PER-2/MBU/03/2023 [29]. To enrich the contextual relevance and governance alignment, insights from three prior studies were considered. These studies address essential dimensions of AI governance, including transparency and risk management frameworks [12], knowledge gaps and future governance agendas [14], and structural clarity with stakeholder engagement for ethical AI management [56]. In Table 3, show the Final score of objectives based on the average value of all factors considered and provide a solid basis for implementing AI governance.

Table 3. GMO Prioritization Result

Factor Considered	GMO Prioritization	
	MEA03: Managed Compliance with External Requirements	APO12: Managed Risk

COBIT 2019 Design Factor [57]	100	70
COBIT 2019 DevOps [20]	33	33
POJK No.11/2022 [28]	100	100
SOE Minister No.PER-2/MBU/03/2023 [29]	100	100
AI Governance Paper 1 [12]	100	100
AI Governance Paper 2 [14]	100	100
AI Governance Paper 3 [56]	100	100
Final Score	**90**	**86**

In Table 3, the highest weighted priority is MEA03, with a score of 90. This underscores the need to ensure compliance with external regulations. Next, APO12 scored 86, affirming the importance of risk management in ensuring the sustainability and operational integrity of the organization.

4.2. Gap Analysis Result

4.2.1. Process Component

Table 4. Process Component

Management Practice	Achievement	Capability Level
MEA03: Managed Compliance with External Requirements		
MEA03.01 Identify external compliance requirements	88% F (Fully)	2
	100% F (Fully)	3
MEA03.02 Optimize response to external requirements	50% P(Partially)	3
MEA03.03 Confirm external compliance	100% F (Fully)	3
	100% F (Fully)	4
	100% F (Fully)	5
MEA03.04 Obtain assurance of external compliance	88% F (Fully)	2
	100% F (Fully)	3
	100% F (Fully)	4
Capability Maturity Level Score		3.5
APO12: Managed Risk		
APO12.01 Collect data	100% F (Fully)	2
	100% F (Fully)	3
	100% F (Fully)	4
APO12.02 Analyze risk	100% F (Fully)	3
	50% P(Partially)	4
	100% F (Fully)	5
APO12.03 Maintain a risk profile	100% F (Fully)	2
	100% F (Fully)	3
	75% L (Largely)	4
APO12.04 Articulate risk	88% F (Fully)	3
	100% F (Fully)	4
APO12.05 Define a risk management action portfolio	100% F (Fully)	2
	100% F (Fully)	3
APO12.06 Respond to risk	100% F (Fully)	3
	100% F (Fully)	4
	100% F (Fully)	5
Capability Maturity Level Score		3.6

Table 4 above evaluates the process component capabilities by analyzing the extent to which key governance activities aligned with GMOs, specifically MEA03 and APO12, have been implemented.

Table *4* presents the capability maturity levels of MEA03 and APO12, with scores of 3.5 and 3.6, respectively, indicating varying degrees of maturity across process activities. While certain areas have

Vol. 6, No. 4, August 2025, Page. 1745-1768
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4835

achieved their targets, others require further capability improvements to strengthen the overall effectiveness of AI governance.

4.2.2. Organizational Structures Component

In Table 5, it presents the assessment of the organizational structure component, focusing on how defined roles, responsibilities, and reporting lines support the achievement of MEA03 and APO12.

Table 5. Organizational Structure Component

COBIT Organization Structure	Management Objective	Current State
Chief Executive Officer	MEA03	Held by the President Director. Oversees strategy and operations, including digital and IT transformation.
Chief Financial Officer	MEA03	Held by the Finance Director. Manages budgeting, finance, and IT project expenditures.
Chief Operating Officer	MEA03	Held by the Operations Director. Responsible for daily operations and digital banking services.
Chief Risk Officer	APO12	Held by the Risk Director. Manages all risks, including digital and operational.
Chief Information Officer	MEA03, APO12	Held by the IT Director. Manages IT strategy, operations, development, and security.
Chief Technology Officer	APO12	Held by IT Operations Manager. Oversees infrastructure, system reliability, and technology operations across the enterprise.
Chief Digital Officer	APO12	Held by SEVP Digital Business. Focuses on digital service and channel development.
Chief Information Security Officer	APO12	Represented by Head of IT Security. Handles information security and ISO 27001 compliance.
Enterprise Risk Committee	APO12	Acts as Risk Committee. Guides IT and digital risk policies.
I&T Governance Board	MEA03	Executed by the IT Steering Committee. Oversees IT governance and priorities.
Business Process Owners	MEA03, APO12	Represented by business and IT directors. Own key business processes.
Project Management Office	MEA03, APO12	Managed by IT Project Management. Oversees time, cost, and risk of IT projects.
Data Management Function	APO12	Managed by Data Management & Analytics Unit. Ensures data quality and analytics.
Head Architect	APO12	Managed by IT Architect Head.
Head Development	MEA03, APO12	Managed by Data Management & Analytics Unit. Ensures data quality and analytics.
Head IT Operations	MEA03, APO12	Managed by Data Management & Analytics Unit. Ensures data quality and analytics.
Head IT Administration	MEA03, APO12	Held by IT Portfolio & Project Admin. Manages vendors, assets, and projects.
Service Manager	MEA03, APO12	Held by IT Service Management. Manages Service Level Agreement (SLA) monitoring, service quality, and end-user support across IT services.
Information Security Manager	MEA03, APO12	Held by Banking Delivery System unit. Ensures optimal IT service delivery.
Business Continuity Manager	MEA03, APO12	Held by Operational Risk Team (DORD). Manages business continuity policies, BCP planning, and disaster recovery readiness.

Vol. 6, No. 4, August 2025, Page. 1745-1768
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4835

COBIT Organization Structure	Management Objective	Current State
Privacy Officer	MEA03, APO12	Held by Data Management & Compliance Units. Manages personal data protection, privacy governance, and regulatory compliance.
Legal Counsel	MEA03	Held by Legal Directorate. Manages IT contracts and digital legal matters.
Compliance	MEA03	Held by Compliance Unit. Oversees compliance with OJK, BI, and internal policies.
Audit	MEA03	Conducted by Internal Audit. Assesses internal controls and IT risks.

Table 5 presents the organizational structure of BankCo, showing that most key governance roles are already established and operational, with no major gaps identified in IT and risk management functions. However, the analysis also reveals the absence of a dedicated role or unit for governing emerging technologies, particularly AI. This strategic gap should be addressed to ensure responsible innovation and effective oversight of AI-related risks within digital transformation initiatives.

4.2.3. Information Component

Table 6 summarizes the assessment of the information component, which examines the quality, relevance, and availability of information outputs that support MEA03 and APO12. These outputs are essential for ensuring data-driven decision-making, transparency, and effective alignment between AI governance and enterprise risk and compliance objectives.

Table 6. Information Component

Management Practice	Information Output	Current State
MEA03: Managed Compliance with External Requirements		
MEA03.01 Identify external compliance requirements	Log of required compliance actions	Compliance obligations have been centrally documented within a compliance management system based on GRC.
	Compliance requirements register	Compliance register maintained by Legal and Compliance Unit, but not fully integrated across operations.
MEA03.02 Optimize response to external requirements	Regulatory changes are communicated internally, but no centralized documentation system is in place.	Compliance updates are communicated, though not fully archived in a unified system.
	Updated policies, principles procedures and standards	Policies are updated periodically, yet procedures are not consistently aligned across units.
MEA03.03 Confirm external compliance	Compliance confirmations	Compliance validated through internal audit and governance reporting.
	Identified compliance gaps	Audits reveal gaps in third-party oversight, with inconsistent documentation of follow-ups.
MEA03.04 Obtain assurance of external compliance	Compliance assurance reports	Assurance reported via annual and sustainability disclosures.
	Reports of noncompliance issues and root causes	Reported via whistleblowing and audit; root cause focus remains on internal issues.

Vol. 6, No. 4, August 2025, Page. 1745-1768
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4835

Management Practice	Information Output	Current State
APO12: Managed Risk		
APO12.01 Collect data	Emerging risk issues and factors	Risks identified in risk register, real-time monitoring under development.
	Data on risk events and contributing factors	BankCo-LED system collects incident data for Risk and Control Self-Assessment (RCSA) and control improvements.
	Data on the operating environment relating to risk	Environmental risks integrated quarterly from internal and external sources.
APO12.02 Analyze risk	Risk analysis results	Risk assessments follow ISO 31000 covering strategic and operational risks.
	I&T risk scenarios	Stress-testing scenarios exist for finance; IT-specific scenarios underdeveloped.
	Scope of risk analysis efforts	Includes strategic units; consistency across divisions still limited.
APO12.03 Maintain a risk profile	Aggregated risk profile, including status of risk management actions	Profiles are consolidated in GRC Roadmap 2025–2029, updated quarterly.
	Documented risk scenarios by line of business and function	Partially documented via Business Impact Analysis (BIA) and Business Continuity Management (BCM); format varies by unit.
APO12.04 Articulate risk	Risk analysis and risk profile reports for stakeholders	Shared via OJK, internal dashboards, and sustainability reports.
	Results of third-party risk assessments	Conducted via due diligence; systematization limited.
	Opportunities for acceptance of greater risk	Risk appetite and tolerance formalized; implementation remains conservative.
APO12.05 Define a risk management action portfolio	Project proposals for reducing risk	Proposed in sustainable finance and recovery plans.
APO12.06 Respond to risk.	Risk impact communication	Risk impacts are discussed in forums, yet digital tools for cross-unit response are lacking.
	Risk-related root causes	RCSA conducted; implementation varies by unit.
	Risk-related incident response plans	Established in Business Continuity Plan (BCP) & Disaster Recovery Plan (DRP); tested via simulation.

In Table 6, the assessment of the information component showed that the MEA03 component did not have a centralized integration, especially when it came to keeping track of compliance and regulatory updates. APO12 found problems with documenting risk scenarios, and coordinating incident response, which shows that there must be better cross-functional alignment and digital assistance.

4.2.4. People, Skills and Competencies Component

Table 7 presents the assessment of the people, skills, and competencies component, focusing on the adequacy of human resources, technical expertise, and role-specific capabilities in supporting the implementation of MEA03 and APO12 within the organization.

Table 7. People, Skills and Competencies Component

Skills	Current State
MEA03: Managed Compliance with External Requirements	
Information security	BankCo has a dedicated IT Security Unit operating 24/7, with ISO 27001:2022 certification and structured training programs. Regular awareness campaigns reinforce compliance culture.
APO12: Managed Risk	
Business risk management	The Digital & Operational Risk Division manages enterprise-level risk dashboards, performs self-assessments, and conducts regular scenario analyses aligned with the Special Policy on IT, Digital & Cyber Risk Management Procedures.
Information assurance	Assurance is ensured through multi-layered control involving IT Security, Compliance, and Internal Audit. Structured risk ownership and reporting are embedded in the Three Lines Model.
Risk management	BankCo applies proactive risk governance using RCSA, Key Risk Indicator (KRI) monitoring, and digital risk profiling. These are institutionalized within the Special Policy on IT, Digital & Cyber Risk Management Procedures and guided by continuous internal audit cycles.

Table 7 highlights BankCo's human resource competencies in the MEA03 and APO12 domains. A 24/7 IT Security Unit and ISO 27001:2022 certification reflect strong compliance practices. To support adaptive AI governance, targeted training in AI compliance, ethics, and risk.

4.2.5. Policies and Procedures Component

Table 8 outlines the assessment of the policies and procedures component, which evaluates the existence, relevance, and implementation of compliance and risk-related policies supporting MEA03 and APO12 objectives.

Table 8. Policies and Procedures Component

Policy	Current State
MEA03: Managed Compliance with External Requirements	
Compliance policy	BankCo enforces a structured compliance framework integrating regulatory, contractual, and internal obligations through cross-functional coordination and executive oversight.
APO12: Managed Risk	
Enterprise risk policy	BankCo's enterprise risk governance is codified through a strategic framework outlined in its risk management policy, emphasizing proactive identification, evaluation, and mitigation of digital, cyber, and operational risks. Risk appetite is embedded within top-down governance structures and supported by integrated risk dashboards.
Fraud risk policy	BankCo's anti-fraud roadmap combines structured assessments and whistleblowing systems to institutionalize early detection and mitigation.

Table 8 shows that BankCo has established robust compliance and risk policies aligned with regulatory and operational standards. However, there are gaps in addressing AI-specific challenges, such as algorithmic accountability, ethical risk management, and adaptive regulatory response.

4.2.6. Culture, Ethics and Behavior Component

Vol. 6, No. 4, August 2025, Page. 1745-1768
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4835

Table 9 presents the assessment of the culture, ethics, and behavior component, focusing on how organizational values, ethical standards, and behavioral norms contribute to the effective implementation of MEA03 and APO12, particularly in supporting responsible and accountable AI governance.

Table 9. Culture, Ethics and Behavior Component

Key Culture Elements	Current State
MEA03: Managed Compliance with External Requirements	
Promote a compliance-aware culture, including zero tolerance of noncompliance with legal and regulatory requirements	BankCo has established a strong compliance culture through a Compliance Unit reporting directly to the Board of Directors, with a mandate to formulate a compliance culture strategy. The Board explicitly oversees the compliance function, including in the Syariah Business Unit, which ensures compliance with positive laws and sharia principles. This culture is enforced through training, internal policies, anti-fraud programs, a whistleblowing system, and the Anti-Fraud Strategy 2024-2026 roadmap.
APO12: Managed Risk	
To support a transparent and participatory risk culture, senior management should set direction and demonstrate visible and genuine support for incorporation of risk practices throughout the enterprise. Management should encourage open communication and business ownership for I&T-related business risk. Desirable behaviors include aligning policies to the defined risk appetite, reporting risk trends to senior management and risk governing bodies, rewarding effective risk management, and proactively monitoring risk and progress on the risk action plan.	The risk management culture in BankCo is strengthened through top management's commitment to directing and overseeing the risk function. BankCo implements the Three Lines Model, reporting risk trends to the Risk Management Committee and integrating risk appetite in policies. The Digital & Operational Risk Management Unit systematically implements practices such as RCSA, digital risk profile dashboard, and monitoring of key risk indicators.

Table 9 reveals that while BankCo demonstrates a mature compliance culture aligned with MEA03, a minor cultural gap remains within APO12 regarding broad-based risk ownership at the operational level. Bridging this gap is vital for AI governance, where collective accountability and risk awareness are key to managing ethical and algorithmic challenges.

4.2.7. Services, Infrastructure and Applications Component

The Services, Infrastructure, and Applications Component analysis in Table 10 is based on MEA03 and APO12, focusing on how BankCo's technological capabilities and support systems align with the objectives of MEA03 and APO12 to strengthen compliance and IT risk management readiness.

Table 10. Services, Infrastructure and Applications Component

Service, Infrastructure, and Application	Current State
MEA03: Managed Compliance with External Requirements	
Regulatory Watch services	BankCo implements an integrated compliance and fraud detection system that enables real-time regulatory monitoring.

Vol. 6, No. 4, August 2025, Page. 1745-1768
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4835

Service, Infrastructure, and Application	Current State
Third-party compliance assessment services	Regular ISO-based vendor audits, embedded in SLA/MSA clauses, are digitally tracked via vendor management systems.
APO12: Managed Risk	
Crisis management services	BankCo established an emergency response unit within the CSIRT (Computer Security Incident Response Team) structure that follows the cycle of preparation, detection and analysis, containment, recovery, and post-incident.
Governance, risk and compliance (GRC) tools	BankCo implemented an integrated risk dashboard that combines data from ERM, Fraud System, Advisory, Governance, and Assurance units. GRC tools support digitalized reporting, supervisory functions, and strategic decision-making.
Risk analysis tools	BankCo applies an integrated risk assessment approach to IT, digital, and cyber domains by analyzing root causes, evaluating likelihood and impact, and calculating residual risk. Regular monitoring through KRIs, RCSA, and major incident reviews ensures risk visibility.
Risk intelligence services	The Digital and Operational Risk Unit manages risk intelligence services, including Top Risk Analysis, digital risk dashboards, and Key Risk Indicator (KRI) monitoring.

Table 10 indicates that BankCo has established a robust risk and compliance services infrastructure. However, minor gaps remain in integrating third-party audit outcomes and leveraging AI-driven analytics for emerging risks.

4.3. Potential Improvements

Based on the previous gap analysis results, Table 11 outlines targeted potential improvements to address deficiencies identified in the MEA03 and APO12 domains. These improvements are systematically categorized into three core dimensions: people, process, and technology. This structured approach ensures holistic enhancement of AI governance capabilities, aligning organizational practices with compliance and risk management standards while offering actionable and measurable steps to strengthen ethical, transparent, and resilient AI implementation.

Table 11. Potential Improvements

Component	Gap	Type	Potential Improvements
MEA03: Managed Compliance with External Requirements			
Process	No formal AI compliance procedure	Procedures	Develop AI procedure for fairness, transparency, and regulatory alignment
Organizational Structure	Undefined responsibilities in managing AI-related compliance risks	Responsibility	Define AI compliance roles across governance lines.
People, Skills, and Competencies	Lack of targeted training programs on AI compliance and governance	Skills & Awareness	Provide AI compliance and ethics training.
Culture, Ethics, and Behavior	Limited cross-unit awareness of algorithmic regulations and obligations	Communication	Conduct AI ethics awareness and knowledge sharing.
Policy and Procedures	Compliance policy does not include AI-specific principles	Policy	Create an AI Compliance Policy with explainability, fairness, and traceability.

Vol. 6, No. 4, August 2025, Page. 1745-1768
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4835

Component	Gap	Type	Potential Improvements
	such as explainability and accountability		
Policy and Procedures	Lack of technical work instructions to assess AI systems	Work Instruction	Provide instructions for AI bias testing and documentation.
Information	Fragmented documentation and tracking of AI-related compliance actions	Record	Centralize AI compliance records in GRC system.
Services, Infrastructure, Applications	Absence of automated tools to monitor AI compliance	Tools	Use GRC tools with AI compliance automation.
Services, Infrastructure, Applications	Lack of AI-specific logging and control features	Features	Add AI logging and monitoring in compliance dashboards.
APO12: Managed Risk			
Process	No SOPs for AI risk validation during business impact assessments (BIA)	Procedures	Include AI risks in BIA through SOPs.
Organizational Structure	Weak coordination between risk, IT, and digital project teams on AI-related risks	Responsibility	Form cross-unit AI risk review team.
People, Skills, and Competencies	Inadequate expertise in assessing AI risks and ethical AI deployment	Skills & Awareness	Train staff on AI risk modeling and ethics.
Culture, Ethics, and Behavior	Operational risk ownership on AI remains weak at lower levels	Communication	Integrate AI risk into KPIs and bottom-up reporting.
Policy and Procedures	AI-specific risk elements are not explicitly reflected in enterprise risk policy	Policy	Update risk policy with AI-specific threats.
Policy and Procedures	Lack of guidance for reliability and ethical verification of AI systems	Work Instruction	Create AI User Acceptance Testing (UAT) and ethical verification guides.
Information	AI risk scenarios are inconsistently documented across business lines	Record	Standardize and integrate AI risk records and KRIs.
Services, Infrastructure, Applications	Absence of AI-specific tools to measure residual risks and KRI performance	Tools	Implement AI risk modules with residual risk tracking.
Services, Infrastructure, Applications	Risk dashboards do not visualize AI exposure in real time	Features	Enable AI exposure monitoring in dashboards.

Table 11 outlines key improvement opportunities to strengthen BankCo's AI governance maturity across MEA03 and APO12. The gaps include the absence of formal procedures, unclear responsibilities, limited staff competencies, and lack of AI-specific policies, tools, and records. To address these, the study recommends developing AI compliance procedures, defining roles, providing targeted training, enhancing cross-unit communication, and updating policies to reflect fairness, explainability, and ethical AI use. Technical enhancements include centralized documentation, automated compliance tools, AI-

specific risk tracking features, and integrated dashboards. These improvements aim to operationalize AI governance through structured, auditable, and proactive mechanisms.

4.4. Resource, Risk, Value (RRV) Analysis

The Resource, Risk, and Value (RRV) Analysis is a structured and integrated approach for evaluating and prioritizing potential improvements by assessing three critical dimensions: resource, risks, and value. As shown in Table 12, the final score is calculated by combining these three elements into a single composite indicator that reflects each initiative's overall viability and impact.

Table 12. RRV Analysis

Potential Improvement	Final Score	Priority
People Aspect		
Form cross-unit AI risk review team	18	1
Define AI compliance roles across governance lines	12	2
Integrate AI risk into KPIs and bottom-up reporting	12	3
Provide AI compliance and ethics training	8	4
Train staff on AI risk modelling and ethics	8	5
Conduct AI ethics awareness and knowledge sharing	8	6
Process Aspect		
Create an AI Compliance Policy with explainability, fairness, and traceability	27	1
Update risk policy with AI-specific threats	18	2
Develop AI procedure for fairness, transparency, and regulatory alignment	12	3
Standardize and integrate AI risk records and KRIs	12	4
Centralize AI compliance records in GRC system	9	5
Provide instructions for AI bias testing and documentation	8	6
Include AI risks in BIA through SOPs	8	7
Create AI UAT and ethical verification guides	8	8
Technology Aspect		
Add AI logging and monitoring in compliance dashboards	27	1
Enable AI exposure monitoring in dashboards	27	2
Use GRC tools with AI compliance automation	12	3
Implement AI risk modules with residual risk tracking	8	4

The scoring framework in Table 12 provides a consistent, transparent, and evidence-based method for prioritizing actions within the context of AI governance. this analysis provides a comprehensive basis for strategic decision-making by classifying each initiative according to its final score and corresponding priority category.

4.5. Implementation Roadmap

Table 13 presents a phased implementation roadmap for the period 2025–2026, structured according to the priority ranking of initiatives based on the Resources-Risk-Value (RRV) analysis. This roadmap aims to guide the execution of governance improvements aligned with BankCo’s strategic objectives in compliance and risk management.

As shown in Table 13, each initiative is systematically scheduled to ensure structured implementation and alignment with BankCo's responsible AI governance direction. This roadmap also aims to close essential capability gaps and strengthen BankCo's preparedness to handle the emerging risks associated with AI technologies.

Table 13. Implementation Roadmap

Vol. 6, No. 4, August 2025, Page. 1745-1768
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4835

Potential Improvement	2025				2026			
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
People Aspect								
Form cross-unit AI risk review team								
Define AI compliance roles across governance lines								
Integrate AI risk into KPIs and bottom-up reporting								
Provide AI compliance and ethics training								
Train staff on AI risk modeling and ethics								
Conduct AI ethics awareness and knowledge sharing								
Process Aspect								
Create an AI Compliance Policy with explainability, fairness, and traceability								
Update risk policy with AI-specific threats								
Develop AI procedure for fairness, transparency, and regulatory alignment								
Standardize and integrate AI risk records and KRIs								
Centralize AI compliance records in GRC system								
Provide instructions for AI bias testing and documentation								
Include AI risks in BIA through SOPs								
Create AI UAT and ethical verification guides								
Technology Aspect								
Add AI logging and monitoring in compliance dashboards								
Enable AI exposure monitoring in dashboards								
Use GRC tools with AI compliance automation								
Implement AI risk modules with residual risk tracking								

4.6. Impact of Recommendations on BankCo

Figure 3 shows the measurable improvement in process capability following the implementation of the key recommendations. The average capability level increased from 3.55 to 3.95 in MEA03 and APO12, indicating improved regulation compliance and risk management effectiveness at BankCo.

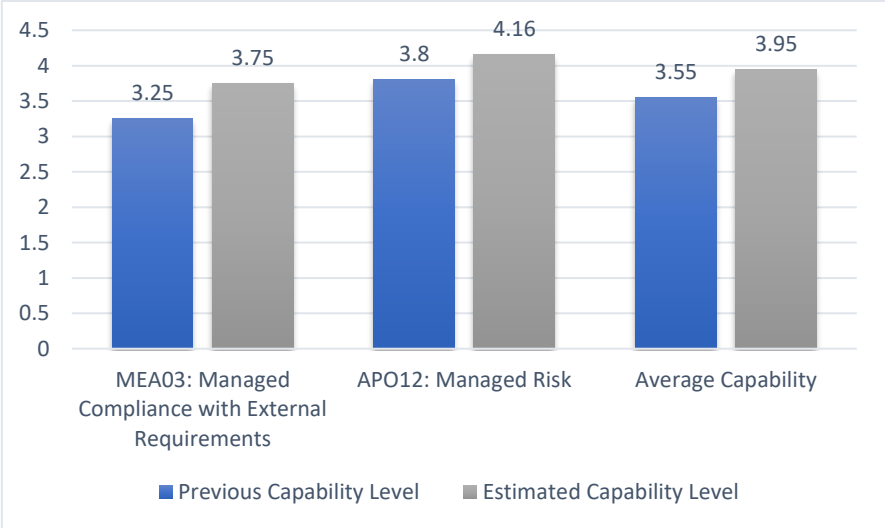

Figure 3. Estimation of Impact on Process Component

Figure 3 presents a comparative evaluation of BankCo's AI governance components, including organizational structure, information, people, skills and competencies, culture and ethics, principles and

Vol. 6, No. 4, August 2025, Page. 1745-1768
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4835

policies, and supporting services and infrastructure, based on their condition in the Pre-implementation State and the Post-implementation State.

Table 14. Estimation of Impact on Governance Component

Pre-implementation State	Post-implementation State
Process Component	
No formal AI compliance/risk procedures	Procedures aligned with AI regulations developed
Organization Structure Component	
No formal AI roles	AI Governance and Risk Officers appointed
Weak team coordination	Cross-unit AI risk team formed
Information Component	
Scattered compliance data	Data standardized and centralized
No AI-specific GRC system	GRC integrated for AI records
People, Skills and Competencies Component	
No AI compliance training	Staff trained in AI ethics and risk
Lack of AI risk skills	AI risk modeling skills improved
Policies and Procedures Component	
No AI principles in policies	AI policy with fairness, explainability developed
No ethical/reliability guidance	UAT and ethics verification guides created
No guidance for ethical checks	Work instructions for AI ethics issued
Culture, Ethics and Behavior Component	
Low awareness of AI obligations	AI ethics programs launched
Weak AI risk ownership	AI risks included in KPIs and reports
Services, Infrastructure and Applications Component	
No AI compliance/risk tools	GRC tools with AI modules used
No AI visibility in dashboards	Real-time AI monitoring added

The implementation made clear improvements across the structure, skills, information, policies, culture, and systems. Key roles were formalized, data centralized, staff trained, policies and SOPs established, risk ownership strengthened, and real-time AI monitoring enabled. These changes support stronger compliance, ethical AI use, and better risk management. Although the analyzed developments demonstrate a degree of maturity in the organization's general governance structures, they reveal that AI-specific oversight remains in its infancy. To support responsible and regulation-aligned AI deployment, further refinement is needed by institutionalizing targeted mechanisms addressing algorithmic accountability, ethical safeguards, and regulatory coherence.

5. DISCUSSION

5.1. Institutional Challenges in Governing AI in State-Owned Banks

This study reveals a significant institutional challenge in deploying ethical and effective AI governance within state-owned financial institutions, particularly in Indonesia and ASEAN. A persistent gap exists between strategic governance levels consisting of directors and executive oversight functions in the operational units responsible for implementing AI systems. Operational personnel often lack the mandate and competency to address critical AI-specific risks such as algorithmic bias, model drift, and opaque decision-making [11], [58]. This disconnect is compounded by bureaucratic inertia common in Indonesian SOEs, hindering agility and rapid iteration during AI system development and deployment. The results from BankCo, a state-owned bank going through a digital transformation, show that institutions have trouble with AI governance when technology moves faster than governance can react. The typical top-down structure, which has executive-level oversight but not enough responsibility at the operational level, generates a vertical asymmetry that makes it harder for the company to respond to AI-

Vol. 6, No. 4, August 2025, Page. 1745-1768
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4835

specific issues. This fragmentation leads to ethical blind spots and delays in fixing new algorithmic problems like bias and model drift. Although COBIT 2019 Traditional provides clear governance roles, its top-down orientation lacks the agility needed for dynamic AI environments. In contrast, DevOps enables horizontal collaboration and continuous integration but, without governance embedding, can result in uncoordinated decision-making and risk blindness [13], [14].

5.2. Comparison with Existing AI Governance Models

The suggested ambidextrous AI governance approach is compared to well-known worldwide frameworks. The OECD AI Principles provide a strong ethical framework, focusing on principles that put people first, openness, and responsibility. However, they are primarily just goals and do not have any specific ways to implement them in institutional IT governance [59]. Similarly, IEEE's Ethically Aligned Design provides a rich set of ethical imperatives for autonomous systems but falls short of offering integration pathways into enterprise governance structures like COBIT [60]. The European Union's AI Act and the European Commission's Ethics Guidelines for Trustworthy AI are strong on compliance. However, they are heavily context-bound to EU institutions and less adaptable to Indonesia's regulatory and institutional landscapes [41]. While ISO/IEC 42001 presents a novel AI management standard, it remains early in its adoption, especially within agile-oriented IT contexts such as DevOps. In contrast, this study's model integrates COBIT 2019 Traditional with the DevOps Focus Area and adapts AI-specific ethical controls directly into enterprise IT processes, making it highly actionable and regulatory-aligned [39].

5.3. Theoretical Contribution and Novelty

This research advances the theoretical conversation by bridging a persistent gap in the literature: the disconnection between high-level ethical guidelines and the operational governance of AI in financial institutions. The ambidextrous model harmonizes structured governance from COBIT 2019 with the flexibility of DevOps to accommodate both control and adaptability. Unlike normative and philosophical frameworks, this study offers a pragmatic, auditable, and empirically grounded governance architecture. The integration of fairness, explainability, and accountability principles is made tangible through institutional mechanisms, including role formalization (Chief AI Risk Officer), AI ethics dashboards, and SOPs for bias detection and impact analysis. Moreover, applying the RRV (Resource-Risk-Value) lens strengthens prioritization and links governance design to strategic business value and compliance exposure. The capability improvement from 3.55 to 3.95 in APO12 and MEA03, respectively, substantiates the model's effectiveness.

5.4. Practical Implications for Digital Governance in SOEs

Practically, the study offers a roadmap for AI governance tailored to the governance dynamics of Indonesian and ASEAN state-owned enterprises. It recommends formalizing AI-specific governance roles such as the Chief AI Risk Officer (CAIRO) and forming AI Risk Boards that span compliance, IT, legal, and operational units. To ensure continuous oversight and accountability, organizations should deploy GRC (Governance, Risk, and Compliance) platforms with embedded AI monitoring capabilities as traceability engines, real-time audit logs, and alert systems aligned with regulatory thresholds. In addition, adding things like algorithmic fairness audits and ethical override methods to standard operating procedures is a good way to ensure that institutions can put ethics into practice instead of just following the regulations. This approach aligns closely with regulatory requirements such as POJK No.11/2022 and SOE Minister Regulation No. PER-2/MBU/03/2023, supporting agile governance without sacrificing control of AI in the Financial Sector.

5.5. Strategic and Long-Term Impacts

In terms of strategic relevance, this governance model contributes directly to national and regional efforts in innovative governance and digital public sector transformation. The model can serve as a referential architecture for inclusion in Indonesia's AI-related policies, including the UU PDP (Personal Data Protection Law), OJK's AI regulatory frameworks, and future SOE digital transformation blueprints. From a long-term perspective, embedding AI governance into enterprise architecture fosters algorithmic accountability, strengthens public trust, and contributes to financial stability. It positions AI governance as a pillar of national cyber-resilience and corporate responsibility in the face of rising algorithmic influence on financial inclusion and customer profiling. Moreover, this study contributes to the field of information systems by offering a replicable and auditable model that transforms AI ethics from abstract principles into institutional practice.

6. CONCLUSION

This study proposes and validates an ambidextrous AI governance model tailored for state-owned banks undergoing digital transformation in highly regulated environments. The approach fills a big vacuum in governance by integrating the structured oversight of COBIT 2019 Traditional with the agile flexibility of the DevOps Focus Area. This helps manage AI-specific risks, ethical issues, and legal obligations. This research contributes by turning vague ethical ideas like fairness, accountability, and transparency into real-world systems and processes. This moves the conversation forward in the field of information systems governance, especially in the fields of computer science and informatics.

1. The model operationalizes ethical AI governance through formal roles, processes, and real-time monitoring tools, enhancing accountability in digital banking.
2. It demonstrates capability improvement from 3.55 to 3.95, indicating a measurable enhancement in AI risk and compliance readiness across MEA03 and APO12.
3. It provides a replicable and auditable reference architecture for aligning AI innovation with national regulations (POJK No.11/2022, PER-2/MBU/03/2023).
4. The integration of Resource-Risk-Value (RRV) analysis ensures that improvements are prioritized based on feasibility, strategic impact, and risk mitigation.
5. The model contributes to theoretical advancement in ambidextrous IT governance by embedding ethical AI oversight within institutional frameworks, not merely as aspirational guidelines.

Despite its contributions, the study acknowledges limitations in its single-case qualitative design, which may affect generalizability across diverse institutional and cultural contexts. Future research should conduct comparative studies across industries and geographies, develop quantitative maturity indices, and incorporate co-governance mechanisms such as human-in-the-loop frameworks to strengthen participatory ethics in AI oversight. These extensions will ensure that AI governance models remain adaptive, inclusive, and context-sensitive while contributing to resilient and trustworthy digital transformation across sectors.

CONFLICT OF INTEREST

The authors declares that there is no conflict of interest between the authors or with research object in this paper.

REFERENCES

[1] R. Kumar Batchu, “Digital Transformation in Banking: Navigating the Technological Frontier,” *International Machine learning journal and Computer Engineering*, vol. 7, no. 7, pp. 1–13, Feb. 2024, [Online]. Available: https://mljce.in/index.php/Imljce/article/view/21

[2] É. Marcon, M. A. Le Dain, and A. G. Frank, “Designing business models for Industry 4.0 technologies provision: Changes in business dimensions through digital transformation,” *Technol Forecast Soc Change*, vol. 185, Dec. 2022, doi: 10.1016/j.techfore.2022.122078.

[3] M. Doumpos, C. Zopounidis, D. Gounopoulos, E. Platanakis, and W. Zhang, "Operational research and artificial intelligence methods in banking," Apr. 01, 2023, *Elsevier B.V.* doi: 10.1016/j.ejor.2022.04.027.

[4] OJK, "Blueprint for Digital Transformation in Banking." [Online]. Available: https://www.ojk.go.id/id/berita-dan-kegiatan/info-terkini/Documents/Pages/Cetak-Biru-Transformasi-Digital-Perbankan/BLUEPRINT%20FOR%20DIGITAL%20TRANSFORMATION%20IN%20BANKING.pdf

[5] C. Gong and V. Ribiere, "Developing a unified definition of digital transformation," *Technovation*, vol. 102, pp. 1–17, Apr. 2021, doi: 10.1016/j.technovation.2020.102217.

[6] L. Lachvajderová and J. Kádárová, "Industry 4.0 Implementation and Industry 5.0 Readiness in Industrial Enterprises," *Management and Production Engineering Review*, vol. 13, no. 3, pp. 102–109, 2022, doi: 10.24425/mper.2022.142387.

[7] M. Zahid, I. Inayat, M. Daneva, and Z. Mehmood, "A security risk mitigation framework for cyber physical systems," in *Journal of Software: Evolution and Process*, John Wiley and Sons Ltd, Feb. 2020. doi: 10.1002/smr.2219.

[8] BankCo, "Sustainability Report," 2024. [Online]. Available: https://www.bankco.co.id/

[9] M. A. Camilleri, "Artificial intelligence governance: Ethical considerations and implications for social responsibility," *Expert Syst*, vol. 41, no. 7, pp. 1–15, Jul. 2024, doi: 10.1111/exsy.13406.

[10] S. Mithas, Z. L. Chen, T. J. V. Saldanha, and A. De Oliveira Silveira, "How will artificial intelligence and Industry 4.0 emerging technologies transform operations management?," *Prod Oper Manag*, vol. 31, no. 12, pp. 4475–4487, Dec. 2022, doi: 10.1111/poms.13864.

[11] A. Taeihagh, "Governance of artificial intelligence," *Policy Soc*, vol. 40, no. 2, pp. 137–157, 2021, doi: 10.1080/14494035.2021.1928377.

[12] B. W. Wirtz, J. C. Weyerer, and B. J. Sturm, "The Dark Sides of Artificial Intelligence: An Integrated AI Governance Framework for Public Administration," *International Journal of Public Administration*, vol. 43, no. 9, pp. 818–829, Jul. 2020, doi: 10.1080/01900692.2020.1749851.

[13] B. W. Wirtz, J. C. Weyerer, and I. Kehl, "Governance of artificial intelligence: A risk and guideline-based integrative framework," *Gov Inf Q*, vol. 39, no. 4, pp. 1–17, Oct. 2022, doi: 10.1016/j.giq.2022.101685.

[14] T. Birkstedt, M. Minkkinen, A. Tandon, and M. Mäntymäki, "AI governance: themes, knowledge gaps and future agendas," 2023, *Emerald Publishing*. doi: 10.1108/INTR-01-2022-0042.

[15] R. S. Peres, X. Jia, J. Lee, K. Sun, A. W. Colombo, and J. Barata, "Industrial Artificial Intelligence in Industry 4.0 -Systematic Review, Challenges and Outlook," *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.3042874.

[16] B. Attard-Frost, A. Brandusescu, and K. Lyons, "The governance of artificial intelligence in Canada: Findings and opportunities from a review of 84 AI governance initiatives," *Gov Inf Q*, vol. 41, no. 2, pp. 1–24, Jun. 2024, doi: 10.1016/j.giq.2024.101929.

[17] R. Mulyana, L. Rusu, and E. Perjons, "IT Governance Mechanisms that Influence Digital Transformation: A Delphi Study in Indonesian Banking and Insurance Industry," Montreal: AIS Electronic Library (AISeL), Jul. 2022, pp. 1–10. doi: diva2:1683489.

[18] R. Mulyana, L. Rusu, and E. Perjons, "Key ambidextrous IT governance mechanisms for successful digital transformation: A case study of Bank Rakyat Indonesia (BRI)," *Digital Business*, vol. 4, no. 2, pp. 1–19, Dec. 2024, doi: 10.1016/j.digbus.2024.100083.

[19] ISACA, *COBIT 2019 Framework Governance and Management Objectives*. 2019. [Online]. Available: www.isaca.org

[20] ISACA, *COBIT Focus Area: DevOps Using COBIT 2019*. ISACA, 2021. [Online]. Available: www.isaca.org

[21] R. Mulyana, *IT Governance Influence on Digital Transformation*. Doctoral dissertation, Department of Computer and Systems Sciences, Stockholm University, 2025. [Online]. Available: http://urn.kb.se/resolve?urn=urn:nbn:se:su:diva-242507

Vol. 6, No. 4, August 2025, Page. 1745-1768
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4835

[22] M. Sprajcer *et al.*, "How effective are Fatigue Risk Management Systems (FRMS)? A review," *Accid Anal Prev*, vol. 165, Feb. 2022, doi: 10.1016/j.aap.2021.106398.
[23] S. Umamaheswari, A. Valarmathi, and M. Phil, "Role Of Artificial Intelligence in The Banking Sector Associate professor, Vivekananda institute of management studies Coimbatore M. Raja lakshmi," Chennai, 2023. doi: 10.17762/sfs.v10i4S.1722.
[24] R. Mulyana, L. Rusu, and E. Perjons, "IT Governance Mechanisms Influence on Digital Transformation: A Systematic Literature Review," Association for Information Systems (AIS), Aug. 2021, pp. 1–10. doi: diva2:1612879.
[25] BankCo, "Annual Report," 2024. [Online]. Available: https://www.bankco.co.id/
[26] D. A. S. Bhegawati and M. S. Utama, "The Role of Banking in Indonesia in Increasing Economic Growth and Community Welfare," *South East Asia Journal of Contemporary Business, Economics and Law*, vol. 22, no. 1, pp. 83–91, 2020, [Online]. Available: https://seajbel.com/wp-content/uploads/2020/10/SEAJBEL22_227.pdf
[27] P. G. R. de Almeida, C. D. dos Santos, and J. S. Farias, "Artificial Intelligence Regulation: a framework for governance," *Ethics Inf Technol*, vol. 23, no. 3, pp. 505–525, Sep. 2021, doi: 10.1007/s10676-021-09593-z.
[28] OJK, "Peraturan Otoritas Jasa Keuangan Republik Indonesia Nomor 11/POJK.03/2022 Tentang Penyelenggaraan Teknologi Informasi Oleh Bank Umum." [Online]. Available: https://ojk.go.id/id/regulasi/Documents/Pages/Penyelenggaraan-Teknologi-Informasi-Oleh-Bank-Umum/POJK%2011%20-%2003%20-%202022.pdf
[29] BUMN, "Peraturan Menteri Badan Usaha Milik Negara Nomor PER-2/MBU/03/2023 Tahun 2023 tentang Pedoman Tata Kelola dan Kegiatan Korporasi Signifikan Badan Usaha Milik Negara." [Online]. Available: https://peraturan.bpk.go.id/Details/264291/permen-bumn-no-per-2mbu032023-tahun-2023
[30] R. Mulyana, L. Rusu, and E. Perjons, "How Hybrid IT Governance Mechanisms Influence Digital Transformation and Organizational Performance in the Banking and Insurance Industry of Indonesia," in *The International Conference on Information Systems Development (ISD)*, Lisbon: Association for Information Systems (AIS), 2023, pp. 1–12. doi: 10.62036/isd.2023.33.
[31] J. Schneider, R. Abraham, C. Meske, and J. Vom Brocke, "Artificial Intelligence Governance For Businesses," *Information Systems Management*, vol. 40, no. 3, pp. 229–249, Jun. 2022, doi: 10.1080/10580530.2022.2085825.
[32] M. S. Djanegara, S. Sutarti, and S. A. Dewo, "The Influence of Corporate Governance for the Indonesian Banking Industry in a Pandemic Period," *International Journal of Finance & Banking Studies (2147-4486)*, vol. 11, no. 3, pp. 62–71, Sep. 2022, doi: 10.20525/ijfbs.v11i3.1988.
[33] I. Permatasari, "Does corporate governance affect bank risk management? Case study of Indonesian banks," *International Trade, Politics and Development*, vol. 4, no. 2, pp. 127–139, Oct. 2020, doi: 10.1108/itpd-05-2020-0063.
[34] S. Napitupulu, I. Primiana, S. R. Nidar, N. Effendy, and D. M. Puspitasari, "The effect of management capabilities in implementing good corporate governance: A study from indonesia banking sector," *Journal of Asian Finance, Economics and Business*, vol. 7, no. 1, pp. 159–165, Jan. 2020, doi: 10.13106/jafeb.2020.vol7.no1.159.
[35] M. Mäntymäki, M. Minkkinen, T. Birkstedt, and M. Viljanen, "Putting AI Ethics into Practice: The Hourglass Model of Organizational AI Governance," *ArXiv*, pp. 1–41, Feb. 2023, doi: 10.48550/arXiv.2206.00335.
[36] C. V. R. Padmaja, S. L. Narayana, G. L. Anga, and P. K. Bhansali, "The rise of artificial intelligence: a concise review," *IAES International Journal of Artificial Intelligence*, vol. 13, no. 2, pp. 2224–2233, Jun. 2024, doi: 10.11591/ijai.v13.i2.pp2226-2235.
[37] P. Soto-Acosta, "COVID-19 Pandemic: Shifting Digital Transformation to a High-Speed Gear," *Information Systems Management*, vol. 37, no. 4, pp. 260–266, Oct. 2020, doi: 10.1080/10580530.2020.1814461.
[38] R. Mulyana, L. Rusu, and E. Perjons, "Key Ambidextrous IT Governance Mechanisms Influence on Digital Transformation and Organizational Performance in Indonesian Banking

Vol. 6, No. 4, August 2025, Page. 1745-1768
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4835

and Insurance," AIS Electronic Library (AISeL), Jul. 2024, pp. 1–16. [Online]. Available: https://aisel.aisnet.org/pacis2024/track15_govce/track15_govce/7

[39] L. McCormack and M. Bendechache, "Ethical AI Governance: Methods for Evaluating Trustworthy AI," pp. 1–9, Aug. 2024, [Online]. Available: http://arxiv.org/abs/2409.07473

[40] P. Ala-Pietilä *et al.*, "The Assessment List for Trustworthy Artificial Intelligence (ALTAI)," *European Commission*, pp. 1–32, 2020, doi: 10.2759/791819.

[41] European Commission, "Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment," *Publications Office of the European Union*, pp. 1–33, Jul. 2020, doi: 10.2759/791819.

[42] M. Mäntymäki, M. Minkkinen, T. Birkstedt, and M. Viljanen, "Defining organizational AI governance," *AI and Ethics*, vol. 2, no. 4, pp. 603–609, Nov. 2022, doi: 10.1007/s43681-022-00143-x.

[43] OJK, "The Indonesian Financial Services Sector Master Plan 2021–2025." [Online]. Available: https://www.ojk.go.id/id/berita-dan-kegiatan/info-terkini/Documents/Pages/Master-Plan-Sektor-Jasa-Keuangan-Indonesia-2021-2025/The%20Indonesian%20Financial%20Services%20Sector%20Master%20Plan%202021-2025.pdf

[44] S. De Haes, W. Van Grembergen, A. Joshi, and T. Huygh, *Enterprise governance of Information Technology: Achieving alignment and value in digital organizations*. Springer, 2020. doi: 10.1007/978-3-030-25918-1.

[45] Ghazi M Qasaimeh and Hussam Eddin Jaradeh, "The Impact of Artificial Intelligence on the Effective Applying of Cyber Governance in Jordanian Commercial Banks," *International Journal of Technology, Innovation and Management (IJTIM)*, vol. 2, no. 1, pp. 68–86, May 2022, doi: 10.54489/ijtim.v2i1.61.

[46] ISACA, *COBIT 2019 Design guide designing an information and technology governance solution*. 2018. doi: www.isaca.org.

[47] R. W. I. Susatyo, E. Indrajit, and E. Dazki, "IT Governance Analysis in Interior Contracting Industry: A COBIT 2019 Approach," *sinkron*, vol. 8, no. 4, pp. 2142–2154, Oct. 2024, doi: 10.33395/sinkron.v8i4.13978.

[48] Achmad Fadhli Satriadi, R. Mulyana, and R. Fauzi, "AGILE IT SERVICE MANAGEMENT DESIGN OF FINTECHCO DIGITALIZATION BASED ON COBIT 2019 DEVOPS FOCUS AREA," *Jurnal Teknik Informatika (Jutif)*, vol. 4, no. 5, pp. 1165–1177, Oct. 2023, doi: 10.52436/1.jutif.2023.4.5.1304.

[49] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design Science in Information Systems Research," Mar. 2004. doi: https://doi.org/10.2307/25148625.

[50] R. K. Yin, *How to do Better Case Studies. The SAGE Handbook of Applied Social Research Methods*. SAGE Publications, Inc., 2009. doi: 10.4135/9781483348858.

[51] A. K. Shenton, "Strategies for ensuring trustworthiness in qualitative research projects," *Education for Information*, vol. 22, no. 2, pp. 63–75, 2004, doi: 10.3233/EFI-2004-22201.

[52] P. I. Fusch and L. R. Ness, "Are We There Yet? Data Saturation in Qualitative Research," *The Qualitative Report*, vol. 20, no. 9, pp. 1408–1416, 2015, doi: 10.46743/2160-3715/2015.2281.

[53] T. Sato, "Risk-based Project Value – The Definition and Applications to Decision Making," *Procedia Soc Behav Sci*, vol. 119, pp. 152–161, Mar. 2014, doi: 10.1016/j.sbspro.2014.03.019.

[54] S. Tangprasert, "A Study of Information Technology Risk Management of Government and Business Organizations in Thailand using COSO-ERM based on the COBIT 5 Framework," *J Appl Sci (Thailand)*, vol. 19, no. 1, pp. 13–24, Jun. 2020, doi: 10.14416/j.appsci.2020.01.002.

[55] R. Testorelli, A. Tiso, and C. Verbano, "Value Creation with Project Risk Management: A Holistic Framework," Jan. 01, 2024, *Multidisciplinary Digital Publishing Institute (MDPI)*. doi: 10.3390/su16020753.

[56] C. Wu, H. Zhang, and J. M. Carroll, "AI Governance in Higher Education: Case Studies of Guidance at Big Ten Universities," *Future Internet*, vol. 16, no. 10, pp. 1–19, Oct. 2024, doi: 10.3390/fi16100354.

[57] ISACA, *COBIT 2019 Framework: Introduction and Methodology*. ISACA, 2018. [Online]. Available: www.isaca.org

Vol. 6, No. 4, August 2025, Page. 1745-1768
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4835

[58] ASEAN, "ASEAN Guide on AI Governance and Ethics Contents," ASEAN Secretariat, 2024, pp. 1–87. [Online]. Available: https://asean.org/wp-content/uploads/2024/02/ASEAN-Guide-on-AI-Governance-and-Ethics_beautified_201223_v2.pdf

[59] OECD, "Recommendation of the Council on Artificial Intelligence," 2019, pp. 1–12. [Online]. Available: http://legalinstruments.oecd.org

[60] IEEE Global Initiative, "Ethically Aligned Design - A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems," *IEEE*, pp. 1–291, Mar. 2019, [Online]. Available: https://ieeexplore.ieee.org/servlet/opac?punumber=9398611

Jurnal Teknik Informatika (JUTIF)
P-ISSN: 2723-3863
E-ISSN: 2723-3871
Vol. 6, No. 4, August 2025, Page. 1745-1768
https://jutif.if.unsoed.ac.id
DOI: https://doi.org/10.52436/1.jutif.2025.6.4.4835