TIERS Information Technology Journal
Vol.6, No.1, June 2025, pp. 33~45
P-ISSN: 2723-4533 / E-ISSN: 2723-4541
DOI: https://doi.org/10.38043/tiers.v6i1.6610

Ambidextrous AI Governance Design Based on COBIT 2019 Traditional and DevOps for TelCo's Digital Transformation

Nasywah Nabilah Putri[1], Rahmat Mulyana[2], Taufik Nur Adi[3]
nasywahnp@student.telkomuniversity.ac.id[1], rahmat@dsv.su.se[2], taufikna@telkomuniversity.ac.id[3]
[1,3] Information Systems, Faculty of Industrial Engineering, Telkom University, Jawa Barat, Indonesia
[2] Department of Computer and Systems Sciences, Stockholm University, Stockholm, Sweden

ABSTRACT

Artificial intelligence (AI) is a key enabler of digital transformation in telecommunications, improving operational efficiency and customer experience. However, telecom companies face governance challenges such as regulatory compliance risks, security vulnerabilities, and limited risk management capabilities, hindering effective AI adoption. This case study aims to address AI adoption challenges by developing an ambidextrous AI governance framework based on COBIT 2019 and DevOps. Using design science research methodology, the framework was designed and evaluated through semi-structured interviews with key TelCo stakeholders and validated with internal documents until data saturation was reached. The analysis applied the ambidextrous COBIT 2019 framework across seven governance components. Governance and Management Objectives (GMOs) were prioritized based on design factors, devops, national regulations (SOE Minister No.PER-2/MBU/03/2023 and ICT Minister No.5/2021), and literature. As a result, APO12 (Managed Risk) was selected as the key objective. Recommendations include formalizing AI governance roles, enhancing AI-related risk training, and implementing advanced GRC and automation tools. This improvement will increase the APO12 maturity level from 3.83 to 4.66. This improvement will enhance TelCo's capabilities in risk management, compliance, and innovation, offering practical insights for practitioners and contributing to the academic discourse on ambidextrous AI governance for sustainable digital transformation.

Keywords: Ambidextrous AI Governance; Digital Transformation; COBIT 2019; DevOps; APO12

Article Info

Received	:	15-01-2025
Revised	:	11-03-2025
Accepted	:	30-06-2025

Correspondence Author:

Rahmat Mulyana
Department of Computer and Systems Sciences,
Stockholm University,
NOD-huset, Borgarfjordsgatan 12, 164 55 Kista, Sweden
Email: rahmat@dsv.su.se

1. INTRODUCTION

In this era of rapid technological advancement and the emergence of Industry 4.0, organizations are increasingly embracing digital transformation (DT) to boost value creation and address evolving operational demands [1]. Digital transformation is a comprehensive process of change in which organizations integrate digital technologies [2]. It reshapes business models, processes, and customer interactions, driving innovation and competitiveness [3],[4]. While DT brings significant benefits, challenges like high costs and data security concerns persist. However, successful DT enables organizations to optimize resources and improve service delivery [5],[6],[7]. Effective IT governance mechanisms have been identified as critical enablers that influence the success of DT initiatives, ensuring alignment between business strategies and IT capabilities [8]. The telecommunications sector, in particular, faces significant challenges and new opportunities as connectivity and digital integration reach unprecedented levels [9],[10]. Regulatory initiatives aimed at modernizing the telecommunication industry, coupled with global events like the pandemic, have accelerated the adoption of DT. Consequently, DT has shifted from a strategic option to a necessary condition for business resilience and competitiveness amid constant change [11]. DT's primary goal is to boost organizational effectiveness and efficiency by transforming business processes, communication infrastructures, and operational frameworks [12].

Artificial Intelligence (AI) plays a vital role in driving DT by improving operational efficiency and customer service in telecommunications [13]. AI helps TelCo optimize networks, personalize interactions, and predict maintenance needs, supporting faster innovation and better resource management [2],[14]. However, deploying AI also raises governance challenges such as data privacy and transparency that must be managed carefully to ensure successful implementation [15]. As a state owned enterprise (SOE) in the telecommunications sector, TelCo operates under regulatory frameworks such as Ministerial Regulation No. PER-2/MBU/03/2023 [16], this regulation establishes standards for IT governance in SOEs. In this context, robust AI governance is essential to address these challenges and ensure that AI transformation initiatives are executed securely, efficiently, and in full compliance with regulations [17]. AI governance involves the creation and implementation of frameworks, policies, and processes that ensure AI systems operate ethically, legally, and in alignment with societal values [18],[19]. Effective AI governance requires a multidisciplinary and collaborative approach that integrates technological, legal, and social dimensions, with continuous monitoring and adaptation to keep pace with rapid AI advancements [20].

To effectively address these challenges, it is essential to implement ambidextrous IT governance. Ambidextrous IT governance is the ability to simultaneously pursue exploration, which focuses on innovation and new IT capabilities, and exploitation, which optimizes existing IT resources for efficiency [12].This dual approach enhances organizational agility to effectively respond to changing environments [8]. Ambidextrous IT governance is defined as “a synergistic combination of agile-adaptive and traditional mechanisms that balance exploration, emphasizing flexibility, innovation, and adaptability, also exploitation, which prioritizes stability, control, and efficiency, allowing organizations to optimize their digital and IT risks and resources toward value realization” [11]. Managing emerging technologies like AI requires this balance to ensure both innovation and strong controls over privacy and ethics [21]. The effectiveness of ambidextrous IT governance has been demonstrated in improving digital transformation success and organizational performance [22],[23].

Previous research emphasizes the importance of IT governance (ITG) in ensuring the success of digital transformation [12]. COBIT 2019 is commonly used to guide ITG implementation due to its comprehensive approach to measuring and monitoring IT performance [24]. Furthermore, DevOps practices support transformation by accelerating development through automation and collaboration, enabling organizations to adopt new technologies, such as AI, more effectively [25],[26]. COBIT 2019 is an IT governance framework that helps organizations align IT with business goals [27]. The framework includes 40 objectives across five domains and allows for customization through design factors and focus areas [28]. DevOps focus area is emphasized as a crucial focus, highlighting the importance of development operations collaboration. According to [25], DevOps refers to a set of principles and practices that facilitate cooperation among software development teams and other stakeholders throughout the agile software development lifecycle [29],[26]. Through empirical studies employing the Delphi method, Mulyana et al.[8] demonstrated the substantial influence of ambidextrous IT governance, which integrates traditional and agile-adaptive methods, on the successful execution of DT initiatives [30]. This model has been validated in the banking sector, demonstrating its effectiveness in improving organizational performance through the implementation of key governance mechanisms [6]. Previous banking research has extensively applied COBIT 2019 frameworks focusing on governance and management objectives, IT services, risk management, information security, and DevOps [21],[29]. This study adopts an ambidextrous approach by combining the traditional principles of COBIT 2019 with the focus area of DevOps to develop a flexible yet structured AI governance framework tailored for telecommunications [22],[23],[31]. Due to the dynamic and complex nature of the telecommunications industry, this integrated governance model balances stability and agility to enhance the success and sustainability of AI digital transformation in the telecommunications sector (TelCo) [32],[33].

However, these studies primarily focus on banking and finance sectors, leaving a gap in understanding how ambidextrous IT governance can be applied to telecommunications. This study definitively fills that gap by applying the ambidextrous COBIT 2019 framework combined with DevOps to create an AI governance model tailored for TelCo. The novelty of this research lies in its focus on the telecommunications industry, balancing stability and agility while addressing AI governance challenges, including data privacy and compliance. Prior research did not fully explore these challenges.

TelCo is a major telecommunications provider in Indonesia, offering mobile and internet services nationwide. The company has advanced its digital infrastructure with 4G/LTE and 5G networks while supporting digital inclusion and sustainability. This case study explores how TelCo manages its digital transformation, focusing on an ambidextrous AI governance framework and providing insights for other telecom companies. This research makes a significant contribution to both academia and practice by addressing the need for AI governance frameworks that balance innovation and control in the dynamic telecommunications industry.

2. RESEARCH METHOD

This study utilized the Design Science Research (DSR) adopted from Hevner [34]. DSR combines theoretical understanding with practical application, making it suitable for designing governance frameworks in information systems [35]. This study also adopts a case study approach, following Yin's [36] recommendation for exploring complex phenomena in real-life settings. The case study method is ideal for investigating how TelCo implements ambidextrous AI governance to support its digital transformation, specifically addressing the "how" and "why" questions related to the integration of COBIT 2019 and DevOps.

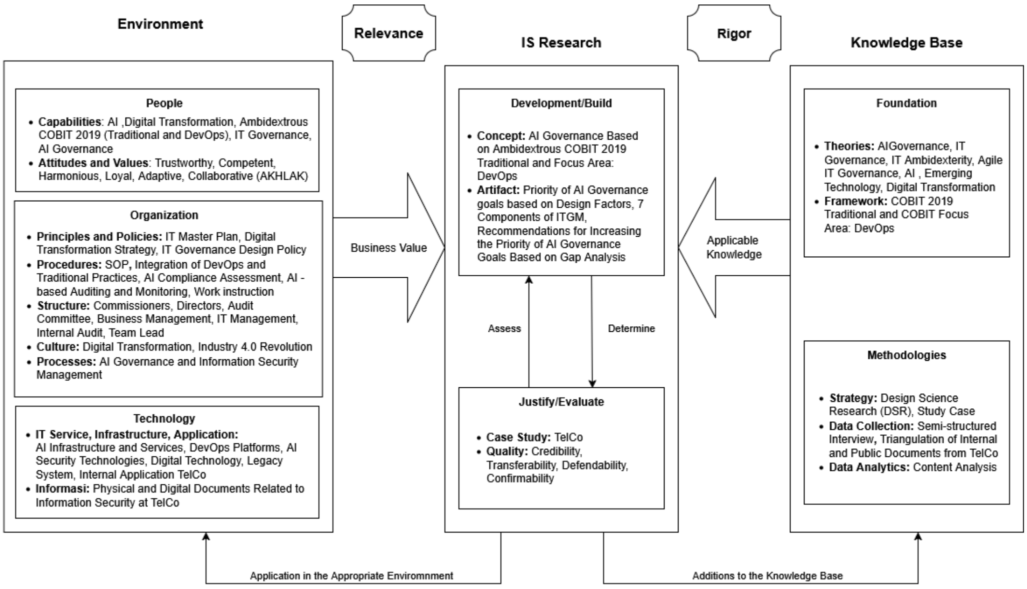
Environment
Relevance
IS Research
Rigor
Knowledge Base
People
• Capabilities: AI ,Digital Transformation, Ambidextrous COBIT 2019 (Traditional and DevOps), IT Governance, AI Governance
• Attitudes and Values: Trustworthy, Competent, Harmonious, Loyal, Adaptive, Collaborative (AKHLAK)
Organization
• Principles and Policies: IT Master Plan, Digital Transformation Strategy, IT Governance Design Policy
• Procedures: SOP, Integration of DevOps and Traditional Practices, AI Compliance Assessment, AI - based Auditing and Monitoring, Work instruction
• Structure: Commissioners, Directors, Audit Committee, Business Management, IT Management, Internal Audit, Team Lead
• Culture: Digital Transformation, Industry 4.0 Revolution
• Processes: AI Governance and Information Security Management
Technology
• IT Service, Infrastructure, Application: AI Infrastructure and Services, DevOps Platforms, AI Security Technologies, Digital Technology, Legacy System, Internal Application TelCo
• Informasi: Physical and Digital Documents Related to Information Security at TelCo
Business Value
Development/Build
• Concept: AI Governance Based on Ambidextrous COBIT 2019 Traditional and Focus Area: DevOps
• Artifact: Priority of AI Governance goals based on Design Factors, 7 Components of ITGM, Recommendations for Increasing the Priority of AI Governance Goals Based on Gap Analysis
Assess
Determine
Justify/Evaluate
• Case Study: TelCo
• Quality: Credibility, Transferability, Defendability, Confirmability
Applicable Knowledge
Foundation
• Theories: AIGovernance, IT Governance, IT Ambidexterity, Agile IT Governance, AI , Emerging Technology, Digital Transformation
• Framework: COBIT 2019 Traditional and COBIT Focus Area: DevOps
Methodologies
• Strategy: Design Science Research (DSR), Study Case
• Data Collection: Semi-structured Interview, Triangulation of Internal and Public Documents from TelCo
• Data Analytics: Content Analysis
Application in the Appropriate Enviromnment
Additions to the Knowledge Base

Figure 1. DSR Research Method adapted from Hevner [34]

Figure 1 presents a modified version of the conceptual framework originally proposed by Hevner [34], which consists of three core components: the environment (people, organizations, technology), the knowledge base (foundational theories and methodologies), and information systems research, which involves creating and evaluating artifacts using inputs from both the environment and the knowledge base.

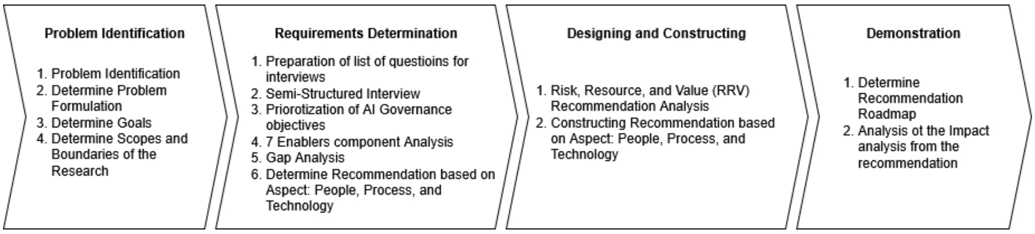
Problem Identification
1. Problem Identification
2. Determine Problem Formulation
3. Determine Goals
4. Determine Scopes and Boundaries of the Research
Requirements Determination
1. Preparation of list of questioins for interviews
2. Semi-Structured Interview
3. Priorotization of AI Governance objectives
4. 7 Enablers component Analysis
5. Gap Analysis
6. Determine Recommendation based on Aspect: People, Process, and Technology
Designing and Constructing
1. Risk, Resource, and Value (RRV) Recommendation Analysis
2. Constructing Recommendation based on Aspect: People, Process, and Technology
Demonstration
1. Determine Recommendation Roadmap
2. Analysis of the Impact analysis from the recommendation

Figure 2. Research Process

Figure 2 the research follows a DSR process with four stages adapted from Johannesson and Perjons [37]: identifying the problem, specifying requirements through semi-structured interviews, designing and constructing governance artifacts based on COBIT 2019 and DevOps, and demonstrating the process with a roadmap focused on resources, risks, and value [38]. Table 1. presents the details of the interviews conducted.

Table 1. Primary Data

Respondent	Position	Justification for Selection
Respondent 1 (R1)	Network Architecture Division	Responsible for emerging technology adoption and AI integration in network infrastructure.
Respondent 2 (R2)	Integration Management Office Performance Monitoring Lead	Strategies for emerging technologies and digital transformation, with a focus on AI
Respondent 3 (R3)	General Manager Charging Platform	Responsible for managing the IT structure, competitive strategy, and employee training for AI-based systems.
Respondent 4 (R4)	General Manager of Service Delivery Management	Leads AI-based optimization of network services and is directly involved in AI risk management.

Respondent	Position	Justification for Selection
Respondent 5 (R5)	Strategic Technology Research and Collaboration Manager	Focus on strategic planning for AI, agile development, and risk evaluation for emerging technology.
Respondent 6 (R6)	General Manager of IT Budgeting & Strategic Alignment	Oversees COBIT process assessments for AI, which crucial for AI governance.

Data was collected through 6 (six) respondent interviews during the period of February-May 2025. The respondents were selected based on their roles in TelCo's digital transformation and AI governance. The selection focused on respondents' experience in adopting emerging technologies, particularly AI, and implementing COBIT 2019. Table 2 presents the secondary data used to support the primary data in analyzing TelCo's condition to identify necessary improvement recommendations.

Table 2. Secondary Data

Secondary Data	Description
TelCo Profile	The overview of the company
TelCo Organizational Structure	The hierarchy and organizational structure of TelCo
TelCo Annual Report 2023	Yearly report detailing the company's financial and operational performance.
TelCo Sustainability Report 2023	TelCo's actions and programs aimed at achieving social, environmental, and economic sustainability objectives.
TelCo Governance Policy Report	A document or report that outlines the TelCo's specific governance policies.
Regulation	It includes policies that relate to TelCo's business operations and processes.

Data from semi-structured interviews were triangulated with internal secondary documents on Table 2 is an iterative process was conducted until data saturation was reached, ensuring that no new themes or information emerged, in accordance with Fusch and Ness [39]. This approach strengthened the validity and reliability of the research findings [40],[41]. The data analysis prioritized design factors and DevOps focus areas, evaluated GMOs with literature and regulatory integration, assessed maturity levels across governance components to identify gaps, and formulated prioritized improvement recommendations based on resource, risk, and value. This led to a structured implementation roadmap and impact evaluation.

3. RESULTS AND DISCUSSION

3.1 GMO Prioritization Result

At this stage, the priority scores shown in Table 3 are derived from four main parameters: regulatory frameworks including ICT Minister No.5/2021[42] and SOE Minister No.PER-2/MBU/03/2023 [16], the Design Factors from COBIT 2019 [28], and the DevOps Focus Area [25] within COBIT 2019. Additionally, findings from three previous AI [13],[19],[18]. The final priority rankings are calculated by averaging these weights, ensuring a comprehensive balance between regulatory requirements, governance models, and academic insights.

Table 3. GMO Prioritization Result

ITGM Objective	**COBIT 2019 Design Factors** [28]	**COBIT 2019 DevOps** [25]	**ICT Minister Regulation** [42]	**SOE Minister Regulation** [16]	**AI Governance Paper 1** [18]	**AI Governance Paper 2** [13]	**AI Governance Paper 3** [19]	Final Score
APO12—Managed Risk	85	33	100	100	100	100	100	88

Based on Table 3 the final score of 88 for ITGM objective APO12—Managed Risk was calculated as the average of several criteria scores: The COBIT 2019 Design Factor scored 85; the COBIT 2019 DevOps Focus Area scored 33; and the ICT MINISTER NO.5/2021 and SOE Ministerial Regulations each scored 100. Three previous studies also scored 100. Based on its alignment with the framework, DevOps practices, national regulations, and relevant literature, this assessment indicates that APO12 is a high-priority objective.

3.2 Gap Analysis Result

1) Process Component

Table 4 shows the evaluation of process component capabilities by measuring how well each activity related to the IT Governance and Management objective is performed.

.

Table 4. Process Component

Management Practice	Achievement	Capability Level
APO12.01 Collect data	100% F (Fully)	2
	100% F (Fully)	3
	100% F (Fully)	4
APO12.02 Analyze risk	92% F (Fully)	3
	50% F (Partially)	4
	100% F (Fully)	5
APO12.03 Maintain a risk profile	100% F (Fully)	2
	100% F (Fully)	3
	100% F (Fully)	4
APO12.04 Articulate risk	75% L (Largely)	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

In Table 4 the results indicate that the capacity levels vary across different areas, some fully meet the targets, while others need additional development to improve their capabilities.

2) Organizational Structure Component

Table 5 below outlines the organizational roles that TelCo needs to establish to fulfill the GMO, especially APO12—Managed Risk.

Table 5. Organizational Structure Component

Organization Structure	Source	Current State
Chief Information Officer	COBIT 2019	The CIO role is carried out by the Director of Information Technology, who is responsible for overall IT strategy and management.
Chief Information Security Officer	COBIT 2019	Chief Information Security Officer (CISO) role is carried out by the Director of Information Technology.
Business Process Owners	COBIT 2019	They are identified within the respective business units. accountability for process management and performance related to IT risk.
Head Development	COBIT 2019	This function are handled by the IT Customer Touchpoint and Digital Product Solutions Group .
Head IT Operations	COBIT 2019	The Head IT Operations role is represented by Vice President of IT Operation & Infrastructure.
Information Security Manager	COBIT 2019	Handled by the ICT Security Management Group under the Directorate of Information Technology.
Privacy Officer	COBIT 2019	Privacy Officer role is held by the compliance and legal units under the Finance and Risk Management Directorate.
Project Management Office	COBIT 2019	PMO function is managed by the Planning & Transformation Directorate, overseeing coordination and supervision of strategic projects.
Head IT Administration	COBIT 2019	Head of IT Administration are integrated within units under the IT Directorate, primarily under the IT Operation and Infrastructure Group.
Service Manager	COBIT 2019	The Service Manager function is carried out by the Manager IT Service Quality & Performance Management.
Business Continuity Manager	COBIT 2019	BCM role at TelCo is managed by the Business Continuity Manager and Infrastructure Risk Manager.
Chief Risk Officer	COBIT 2019	Run by the Director of Finance and Risk Management who leads the company's risk.
Chief Technology Officer	COBIT 2019	The CTO function is carried out by the Director of Information Technology
Chief Digital Officer	COBIT 2019	The CDO is carried out by the Director of Planning & Transformation.
Enterprise Risk Committee	COBIT 2019	There is a Risk Management Committee that oversees the company's risks.
Data Management Function	COBIT 2019	The Data Management team at TelCo drives business improvements by collecting, processing, and visualizing data.
Head Architect	COBIT 2019	Architect role at TelCo is managed by the IT Enterprise Architecture and Strategy Group

Table 5 shows that TelCo has a complete organizational structure, but the Development, Operations, Risk, and Compliance teams still work separately. To succeed with DevOps, there needs to be more collaboration between IT and business teams so processes can be faster and results better.

3) Information Component

The following Table 6 Shows information outputs for each management practice that must be fulfilled to achieve the APO12—Managed Risk GMO.

Table 6. Information Component

Management Practice	Information Output	Current State
APO12.01 Collect data	Emerging risk issues and factors	TelCo captures digital and operational risks, as well as integration risks.
	Data on risk events and contributing factors	Operational cyber threat and incident monitoring systems are used to routinely collect risk event data.
	Data on the operating environment relating to risk	Monitoring of regulatory risks, market competition and macroeconomic conditions is carried out periodically.
APO12.02 Analyze risk	Risk analysis results	TelCo conducts risk analysis according to ISO 31000:2018 standards, covering cybersecurity, and digital transformation.
	I&T risk scenarios	Various IT risk and digital transformation scenarios are analyzed for mitigation and planning.
	Scope of risk analysis efforts	Risk analysis covers all business lines and key functions related to digital transformation and services.
APO12.03 Maintain a risk profile	Aggregated risk profile, including status of risk management actions	Aggregated risk profiles with monitoring of mitigation status are conducted by the Risk Management Committee and reported to the Board of Directors.
	Documented risk scenarios by line of business and function	Risk scenarios are documented in detail by business line and related functions
APO12.04 Articulate risk	Risk analysis and risk profile reports for stakeholders	Risk reports are periodically submitted to internal stakeholders, including the Board of Commissioners and Board of Directors.
	Results of third-party risk assessments	External risk assessments are conducted by third parties, particularly for cybersecurity and compliance.
	Opportunities for acceptance of greater risk	TelCo identifies and evaluates opportunities to accept higher risks in the context of digital innovation.
APO12.05 Define a risk management action portfolio	Project proposals for reducing risk	Various strategic projects and programs are implemented to mitigate risks, including strengthening cybersecurity and IT transformation.
APO12.06 Respond to risk	Risk impact communication	Risk impact communication is carried out through internal reports and structured risk management forums.
	Risk-related root causes	Root cause analysis of risks is performed to ensure continuous improvement actions.
	Risk-related incident response plans	Risk incident response plans including disaster recovery and cyber security response have been prepared and tested regularly.

In Table 6 TelCo has a strong foundation in managing traditional risk information, it faces challenges with AI digital transformation risks. There are gaps in the timely detection, automated monitoring, and integration of real-time AI risk data.

4) People, Skills, and Competencies Component

Table 7 presents the set of skills required to effectively achieve the GMO APO12—Managed Risk.

Table 7. People, Skills, and Competencies Component

Skills	Current State
Business risk management	TelCo has a robust risk management function. Skilled staff handle business and digital transformation risks and receive periodic training and certifications.
Information assurance	Information security management is a key focus, supported by cybersecurity training and ISO/IEC 27001 certification. However, AI risk and digital technology skills require improvement.
Risk management	TelCo has a structured risk management system. Its dedicated team is skilled in identifying, analyzing, and mitigating risks. The team receives continuous training and adheres to international best practices.

.

In Table 7 TelCo has strong competencies in business risk and information assurance supported by Finance & Risk and IT teams but needs to improve AI risk training and cross-functional coordination for effective governance.

5) Principles, Policies, and Procedures Component

The following Table 8 shows the relevant policies of each management practice that must be achieve the ITGM Objective APO12—Managed Risk.

Table 8. Principles, Policies, and Procedures Component

Policy	Current State
Enterprise risk policy	TelCo has implemented a comprehensive enterprise risk management policy aligned with ISO 31000. The policy is supported by an active Risk Management Committee and regular documentation and socialization to ensure compliance.
Fraud risk policy	TelCo has a fraud risk management policy that covers prevention, detection, and handling. This policy is supported by a whistleblowing program, internal audits, and anti-fraud training.

In Table 8 shows TelCo has strong traditional risk policies but lacks agility in AI and digital risks, with limited DevOps integration and room for improvement in detection, monitoring, and response.

6) Culture, Ethnics, and Behavior Component

The following Table 9 shows the key culture elements of each management practice that must be met to achieve the ITGM objective APO12: Managed Risk.

Table 9. Culture, Ethnics, and Behavior Component

Key Culture Elements	Current State
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.	TelCo's senior management has a strong commitment to a transparent risk culture, supporting risk practices and open communication. They ensure accountability through business ownership and incentivize effective risk management with reward programs, while continuously monitoring risk and progress.

In Table 9 TelCo has established a solid foundation for risk culture, yet gaps remain in the formalization of reward systems, proactive risk monitoring, and the integration of risk culture within DevOps practices.

7) Service, Application, and Infrastructure Component

The following Table 10 shows the service, application, and infrastructure of each management practice that must be met to achieve the ITGM objective APO12—Managed Risk.

Table 10. Service, Application, and Infrastructure Component

Service, Infrastructure, and Application	Current State
Crisis management services	TelCo has established crisis management services with response plans, continuity frameworks, and communication channels. These are supported by regular drills.
Governance, risk and compliance (GRC) tools	TelCo uses GRC platforms for risk, compliance, and governance, supporting automated workflows and reporting, though AI risk governance integration is still developing.
Risk analysis tools	TelCo employs risk analysis tools for modeling, scoring, and impact assessment; however, these tools require enhancement for real-time AI risk analytics.
Risk intelligence services	TelCo uses internal and external intelligence services to identify and mitigate risks, with ongoing improvements needed in AI risk intelligence.

In Table 10 shows TelCo has foundational risk management services, but improvements in automation, system integration, and advanced analytics are needed to address AI-driven and digital risks effectively.

3.3 Potential Improvement

Following a gap analysis of seven capability components against the priority IT Governance and Management objective APO12—Managed Risk, the next phase involves identifying the necessary improvements for the TelCo. Tables 11 outlines key improvements in people, processes, and technology based on identified gaps.

Table 11. Potential Improvement

Component	Type	Gap	Potential Improvement
People Aspect			
Organizational Structure	Responsibility & Communication	TelCo lacks strong collaboration between IT and business teams, causing silos that limit effective DevOps and AI governance integration.	Key improvement is building cross-functional DevOps teams that combine IT, business, and AI governance to improve communication, speed delivery, and support responsible AI transformation.
People, Skills, and Competencies Component	Skill & Awareness	TelCo has limited skills in managing AI risks and uneven coverage of risk training.	Implement specialized AI risk management training and certification programs to promote consistent risk awareness across the organization.
Culture, Ethics, and Behavior Component	Communication	TelCo lacks formal reward systems and has not sufficiently integrated risk culture into DevOps practices.	Add and implement reward and recognition programs that encourage proactive risk management and integrate risk culture with DevOps.
Process Aspect			
Process	Procedure	TelCo's AI and digital risk considerations have not been fully integrated into its existing risk management procedures.	Update risk management procedures by explicitly incorporating steps to mitigate AI and emerging digital risks.
Principles, Policies, and Procedures Component	Policy	TelCo's enterprise and fraud risk policies do not adequately address the risks associated with AI and digital transformation.	Revise risk and fraud policies by adding AI risk frameworks and strengthening oversight mechanisms.
Information	Record	TelCo's risk reporting systems lack integration of real-time AI risk data and automation.	Improve information systems by integrating real-time AI risk intelligence into risk reporting and dashboards.
Technology Aspect			
Service, Infrastructure, and Application Component	Tools	TelCo has GRC and risk analysis tools with limited automation and AI-based risk analytics capabilities.	Implement advanced governance, risk, and compliance (GRC) platforms and risk analytics tools that support AI risk analysis and automated monitoring.
	Feature	TelCo's crisis management services lack real-time, AI-powered incident detection and automated response features.	Develop and add AI-enabled real-time incident detection and automated response features within crisis management and disaster recovery services.

In Table 11 highlights TelCo’s key gaps in managing AI and digital risks across people, processes, and technology. Improvements are needed in AI risk training, embedding AI risk in processes, updating policies, and enhancing automation and AI-driven analytics in tools and crisis management services. Addressing these will strengthen TelCo’s governance and risk management in line with its digital transformation goals [43].

3.4 Resource, Risk, and Value (RRV) Analysis

Priorities were established by aggregating the total scores of all proposed improvements. The recommendations with the highest scores were classified as top priorities and organized according to the three categories: people, process, and technology [44]. In the RRV analysis, each criterion (Resource, Risk, and Value) was assigned a qualitative rating of Low, Medium, or High. These ratings were then converted into numerical values. Low is 1, Medium is 2, and High is 3. The Resource criterion evaluated whether internal resources, a mix of internal and external resources, or only external resources were needed for implementation. The Risk criterion assessed the potential negative impact of failure on the organization, while the Value criterion focused on the expected performance improvement. These ratings were multiplied to calculate a final score for each recommendation using the formula Score = Resource × Risk × Value. Based on the score, the recommendations were classified into three categories: Low (1–9) represents low-priority improvements with fewer resources and lower risks, Medium (10–18) indicates medium-priority improvements balancing resources, risk, and value, and High (19–27) are high-priority improvements with more resources, higher risks, and significant value.

.

Table 12. RRV Analysis

No	Potential Improvement	Final Score	Category
1	Key improvement is building cross-functional DevOps teams that combine IT, business, and AI governance to improve communication, speed delivery, and support responsible AI transformation.	18	Medium
2	Implement specialized AI risk management training and certification programs.	12	Medium
3	Add and implement reward and recognition programs to encourage proactive risk management and integrate risk culture with DevOps.	12	Medium
4	Update risk management procedures by incorporating AI and emerging digital risk mitigation steps explicitly.	12	Medium
5	Revise risk and fraud policies by adding AI risk frameworks and strengthening oversight mechanisms.	12	Medium
6	Improve information systems by integrating real-time AI risk intelligence into risk reporting and dashboards.	8	Low
7	Implement advanced GRC platforms and risk analytics tools supporting AI risk analysis and automated monitoring.	8	Low
8	Develop and add AI-enabled real-time incident detection and automated response features within crisis management and disaster recovery services.	8	Low

Table 12 shows that most improvements are categorized as "Medium" priority, with a few falling under "Low" priority. These improvements are manageable within TelCo's existing resources, focusing on enhancing AI integration, risk management, and communication. No recommendations reached "High" priority due to the relatively manageable scale of the improvements, which do not involve significant resource demands or pose high risks, but rather focus on more gradual, incremental changes.

3.5 Implementation Roadmap

This study has completed data collection and analysis as of May 2025. Based on the RRV analysis. Table 13 presents a proposed implementation roadmap intended to guide TelCo in applying the recommended improvements from 2026 to 2027. The roadmap reflects prioritized initiatives and is designed as a strategic recommendation rather than an executed or ongoing implementation plan.

Table 13. Implementation Roadmap

No	Potential Improvement	2026				2027			
		Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
People Aspect									
1	Key improvement is building cross-functional DevOps teams that combine IT, business, and AI governance to improve communication, speed delivery, and support responsible AI transformation.	📋	🛠	🛠	🛠	📊			
2	Implement specialized AI risk management training and certification programs.		📋	🛠	🛠	🛠	📊		
3	Add and implement reward and recognition programs to encourage proactive risk management and integrate risk culture with DevOps.			📋	🛠	🛠	🛠	📊	
Process Aspect									
4	Update risk management procedures by incorporating AI and emerging digital risk mitigation steps explicitly.	📋	🛠	🛠	🛠	📊			
5	Revise risk and fraud policies by adding AI risk frameworks and strengthening oversight mechanisms.		📋	🛠	🛠	🛠	📊		
6	Improve information systems by integrating real-time AI risk intelligence into risk reporting and dashboards.			📋	🛠	🛠	🛠	📊	
Technology Aspect									
7	Implement advanced GRC platforms and risk analytics tools supporting AI risk analysis and automated monitoring.	📋	🛠	🛠	🛠	📊			
8	Develop and add AI-enabled real-time incident detection and automated response features within crisis management and disaster recovery services.		📋	🛠	🛠	🛠	📊		

📋= Planning/Preparation 🛠= Implementation/Development 📊= Monitoring & Evaluation

Table 13 shows outlines TelCo's proposed plan to strengthen its people, processes, and technology from 2026 to 2027. It depicts the roadmap for further development.

3.6 Impact of Recommendation Implementation

Figure 3 shows the impact of the improvement implementation on TelCo through a comparison of capability levels before and after the improvement was implemented.

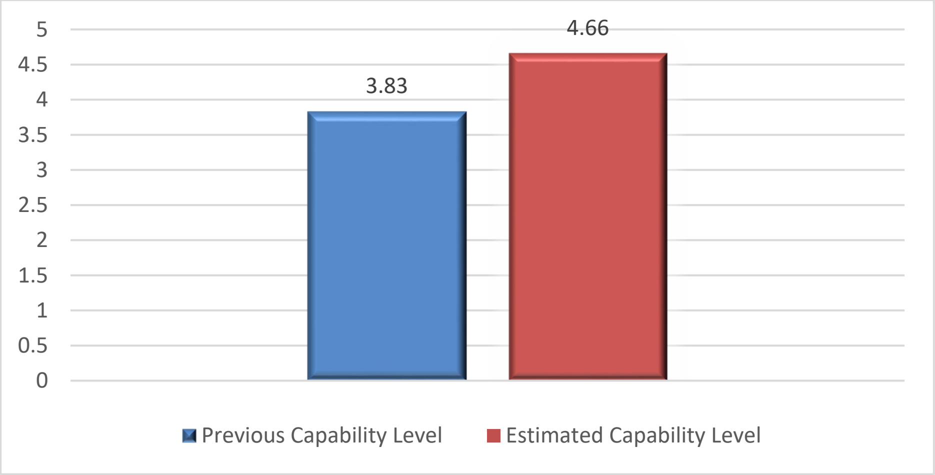

Figure 3. Estimation of Impact Recommendation Implementation

Figure 3 shows the maturity level increase from 3.83 to 4.66, was estimated by conducting a gap analysis between the current condition (3.83) and the target in the assessment process. Then, the total sum of the improvements was divided by the 6 (six) practices under APO12 to calculate the final maturity level. Table 14 presents the status of TelCo's organizational structure, information, people, skills, culture, policies, services, infrastructure, and applications before and after implementing the recommended IT governance improvements.

Table 14. Estimation of Impact on Governance Component

Previous State	State After Recommendation
Organization Structure Component	
TelCo's IT and business teams work separately with limited collaboration, causing slow feedback and reduced agility	Integrated cross-functional DevOps teams that combine IT, business, and AI governance. This improves communication, speeds delivery, and enhances digital transformation outcomes.
Information Component	
Risk reporting systems lack integration of real-time AI risk data and automation; risk intelligence tools not fully utilized.	Enhanced risk reporting systems integrating real-time AI risk intelligence and automation; implementation of advanced risk intelligence tools.
People, Skills and Competencies Component	
Limited AI risk management skills and uneven coverage of risk training; no specialized certification programs.	Implementation of specialized AI risk management training and certification programs such as CRISC, ISO31000:2018 Risk Management, and ERM certifications.
Culture, Ethics, and Behavior	
Risk culture exists but reward systems are informal and risk awareness integration with DevOps practices is insufficient.	Established formal reward and recognition programs; integrated risk culture fully with DevOps practices.
Principles, Policies, and Procedures	
Existing policies do not adequately cover AI and digital risks; privacy aspects are insufficiently addressed in ISMS guidelines.	Revised and expanded policies including AI risk frameworks and strengthened privacy guidelines within ISMS and risk management.
Services, Infrastructure, and Applications	
Limited use of governance, risk, and compliance (GRC) tools; crisis management lacks AI-powered incident detection and automated response features.	Deployment of advanced GRC platforms and AI-enabled crisis management services with real-time incident detection and automated response capabilities.

Table 14 shows key improvements in TelCo's governance, including better AI risk data integration, enhanced skills through training, a stronger risk culture with reward programs, updated AI risk policies, and the deployment of advanced GRC and AI-powered crisis management tools.

3.7 Discussion

TelCo's review confirms that three governance components Oganizational Structure, Information, Principles, Policies, and Procedures already align with key COBIT 2019 and SOE mandates. These components provide clear roles, complete risk data cycles, and ISO 31000-aligned policies. The other four components People, Skills and Competencies, Culture, Ethics, and Behavior, Services, Infrastructure, and Applications still lag. They need AI-risk training, a stronger DevOps-oriented culture, updated procedures for real-time AI

.

controls, and automated GRC/analytics tools. This contrast clearly identifies where TelCo is compliant and where targeted improvements are still required. This finding is consistent with Mulyana et al. [21], who highlight the importance of a strong organizational foundation and clear policies in AI governance but show the need to strengthen technology and culture, particularly in automation, real-time AI risk monitoring, and fostering an adaptive innovation culture. These findings align with those of Birkstedt et al. [13], who observed that telecom firms with mature structures still struggle to embed AI-oriented risk analytics and DevOps culture, and Slimani et al.[2], who reported similar gaps between policy maturity and technological readiness in AI-driven network projects. This study's main contribution is developing an ambidextrous AI governance framework, combining traditional COBIT 2019 principles with agile DevOps practices, highlighting the critical role of technology and culture in effective AI governance. Our framework is different from other studies in banking and finance[8],[15], Those studies offered governance models for specific sectors and did not focus on integrating DevOps or AI-specific risk controls. Our framework extends the lens to telecommunications, explicitly incorporating DevOps practices, AI-risk metrics, and real-time GRC tooling. This fills in the missing information and explains the methods used in earlier work. The framework provides a customized solution for telecommunications, balancing AI risk management, innovation, and compliance, enriching both academic and practical AI governance.

4. CONCLUSION

This study developed an ambidextrous AI-governance framework that fuses COBIT 2019 with DevOps, tailored for TelCo. The framework effectively addressed gaps in leadership roles, risk training, automation, and risk management practices. This led to an estimated increase in the APO12 Managed Risk maturity level, from 3.83 to 4.66. Although the case study approach provides deep insights into TelCo's specific context, the findings may be applicable only to a limited extent to other organizations or industries due to contextual differences. Nevertheless, this research contributes to the academic literature by applying ambidextrous IT governance concepts to AI governance in the relatively unexplored field of telecommunications. In practice, it offers TelCo and similar organizations a structured, adaptive model that balances innovation and control to ensure secure, compliant, and sustainable AI adoption. This study is limited to the telecommunications sector, so its findings may not be directly applicable to other industries. Future research must test the framework across diverse contexts and use quantitative methods. The study is complete. TelCo will roll out the recommended actions during 2026–2027.

CONFLICT OF INTEREST STATEMENT

The Authors state no conflict of interest.

REFERENCE

[1] M. Malik, A. Andargoli, K. Pala, and G. L. Tortorella, 'Towards explaining the effects of the human-technology dynamic on human agency in digital transformations', *Int. J. Inf. Manage.*, vol. 84, no. April, p. 102915, 2025, doi: 10.1016/j.ijinfomgt.2025.102915.

[2] K. Slimani, S. Khoulji, A. Mortreau, and M. L. Kerkeb, 'From tradition to innovation: The telecommunications metamorphosis with AI and advanced technologies', *J. Auton. Intell.*, vol. 7, no. 1, pp. 1–11, 2024, doi: 10.32629/jai.v7i1.1099.

[3] O. Pricopoaia, N. Cristache, A. Lupașc, and D. Iancu, 'The implications of digital transformation and environmental innovation for sustainability', *J. Innov. Knowl.*, vol. 10, no. 3, 2025, doi: 10.1016/j.jik.2025.100713.

[4] D. Plekhanov, H. Franke, and T. H. Netland, 'Digital transformation: A review and research agenda', *Eur. Manag. J.*, vol. 41, no. 6, pp. 821–844, 2023, doi: 10.1016/j.emj.2022.09.007.

[5] B. Al-haimi, H. Khalid, N. H. Zakaria, and T. H. Jasimin, 'Digital transformation in the real estate industry: A systematic literature review of current technologies, benefits, and challenges', *Int. J. Inf. Manag. Data Insights*, vol. 5, no. 1, p. 100340, 2025, doi: 10.1016/j.jjimei.2025.100340.

[6] J. Fernandez-Vidal, F. Antonio Perotti, R. Gonzalez, and J. Gasco, 'Managing digital transformation: The view from the top', *J. Bus. Res.*, vol. 152, no. January, pp. 29–41, 2022, doi: 10.1016/j.jbusres.2022.07.020.

[7] M. Baslyman, 'Digital Transformation from the Industry Perspective: Definitions, Goals, Conceptual Model, and Processes', *IEEE Access*, vol. 10, pp. 42961–42970, 2022, doi: 10.1109/ACCESS.2022.3166937.

[8] R. Mulyana, L. Rusu, and E. Perjons, 'IT Governance Mechanisms that Influence Digital Transformation: A Delphi Study in Indonesian Banking and Insurance Industry', *Pacific Asia Conf. Inf. Syst. (PACIS), AI-IS-ASIA*, pp. 1–16, 2022, [Online]. Available: https://aisel.aisnet.org/pacis2022/267/

[9] C. Gong and V. Ribiere, 'Developing a unified definition of digital transformation', *Technovation*, vol. 102, no. December 2020, p. 102217, 2021, doi: 10.1016/j.technovation.2020.102217.

[10] P. S. Arce-López, D. Cabeza-Pullés, A. Ruiz-Moreno, and T. Ortega-Egea, 'Ever-present cognitive diversity: The mediating role of sentimentality and creative self-efficacy in achieving ambidextrous behavior', *Think. Ski. Creat.*, vol. 57, no. August 2023, 2025, doi: 10.1016/j.tsc.2025.101856.

[11] 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', *Proc. 31st Int. Conf. Inf. Syst. Dev.*, 2023, doi: 10.62036/isd.2023.33.

[12] R. Mulyana, L. Rusu, and E. Perjons, 'IT governance mechanisms influence on digital transformation: A systematic literature review', *27th Annu. Am. Conf. Inf. Syst. AMCIS 2021*, pp. 0–10, 2021, [Online]. Available:

https://aisel.aisnet.org/amcis2021/adv_info_systems_general_track/adv_info_systems_general_track/19/

[13] T. Birkstedt, M. Minkkinen, A. Tandon, and M. Mäntymäki, 'AI governance: themes, knowledge gaps and future agendas', *Internet Res.*, vol. 33, no. 7, pp. 133–167, 2023, doi: 10.1108/INTR-01-2022-0042.

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

[15] 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, p. 101929, 2024, doi: 10.1016/j.giq.2024.101929.

[16] BUMN, 'Peraturan Menteri Badan Usaha Milik Negara Pedoman Tata kelola dan Kegiatan Korporasi Signifikan Badan Usaha Milik Negara', 2023. [Online]. Available: https://bumn.go.id/

[17] Y. Gong, J. Yang, and X. Shi, 'Towards a comprehensive understanding of digital transformation in government: Analysis of flexibility and enterprise architecture', *Gov. Inf. Q.*, vol. 37, no. 3, p. 101487, 2020, doi: 10.1016/j.giq.2020.101487.

[18] C. Wu, H. Zhang, and J. M. Carroll, 'AI Governance in Higher Education: Case Studies of Guidance at Big Ten Universities', *Futur. Internet*, vol. 16, no. 10, 2024, doi: 10.3390/fi16100354.

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

[20] G. Gordon, B. Rieder, and G. Sileno, 'On mapping values in AI Governance', *Comput. Law Secur. Rev.*, vol. 46, p. 105712, 2022, doi: 10.1016/j.clsr.2022.105712.

[21] R. Mulyana, L. Rusu, and E. Perjons, 'Key ambidextrous IT governance mechanisms for successful digital transformation: A case study of Bank Rakyat Indonesia (BRI)', *Digit. Bus.*, vol. 4, no. 2, p. 100083, 2024, doi: 10.1016/j.digbus.2024.100083.

[22] R. Mulyana, L. Rusu, and E. Perjons, 'Key Ambidextrous IT Governance Mechanisms Influence on Digital Transformation and Organizational Performance inDigital Transformation and Organizational Performance in Indonesian Banking and InsuranceIndonesian Banking and Insurance', 2024, pp. 173–197. doi: 10.1007/978-3-031-57189-3_9.

[23] J. Zhen, Z. Xie, and K. Dong, 'Impact of IT governance mechanisms on organizational agility and the role of top management support and IT ambidexterity', *Int. J. Account. Inf. Syst.*, vol. 40 (C), 2021, doi: 10.1016/j.accinf.2021.100501.

[24] ISACA, *COBIT 2019 Framework - Introduction and Methodology*. 2019. [Online]. Available: https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004Ko9cEAC

[25] ISACA, *COBIT Focus Area: DevOps*. 2021. [Online]. Available: https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004Ko9dEAC

[26] A. Wiedemann, M. Wiesche, H. Gewald, and H. Krcmar, 'Integrating development and operations teams: A control approach for DevOps', *Inf. Organ.*, vol. 33, no. 3, p. 100474, 2023, doi: 10.1016/j.infoandorg.2023.100474.

[27] L. Jaime and J. Barata, 'How can FLOSS Support COBIT 2019' coverage analysis and a conceptual framework', *Procedia Comput. Sci.*, vol. 219, no. 2022, pp. 680–687, 2023, doi: 10.1016/j.procs.2023.01.339.

[28] ISACA, 'COBIT 2019 Framework- Governance and Management Objectives', COBIT® 2019 Framework. [Online]. Available: https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004Ko9ZEAS

[29] O. H. Plant, J. van Hillegersberg, and A. Aldea, 'Rethinking IT governance: Designing a framework for mitigating risk and fostering internal control in a DevOps environment', *Int. J. Account. Inf. Syst.*, vol. 45, no. January 2021, p. 100560, 2022, doi: 10.1016/j.accinf.2022.100560.

[30] R.Mulyana, 'IT Governance Influence on Digital Transformation', Stockholm University, Stockholm, Sweden, 2025. [Online]. Available: https://urn.kb.se/resolve?urn=urn:nbn:se:su:diva-242507

[31] R. Mulyana, L. Rusu, and E. Perjons, 'Association for Information Systems Association for Information Systems Key Ambidextrous IT Governance Mechanisms In>uence on Key Ambidextrous IT Governance Mechanisms In>uence on Digital Transformation and Organizational Performance in Digital Transforma', no. July, pp. 1–16, 2024, [Online]. Available: https://aisel.aisnet.org/pacis2024

[32] N. Iqza, W. Ode Rayyani, and F. Syah, 'Analysis of Financial Performance in Telecommunication Companies listed on the BEI', *Int. Econ. Bus. Conf.*, vol. 1, no. 1, pp. 356–364, 2023, doi: https://doi.org/10.35912/iecon.v1i1.154.

[33] N. Vemuri, N. Thaneeru, and V. Manoj Tatikonda, 'AI-Driven Predictive Maintenance in the Telecommunications Industry', *J. Sci. Technol.*, vol. 3, no. 2, pp. 21–45, 2022, doi: 10.55662/jst.2022.3201.

[34] Hevner, 'Design Science in Information Systems Research', 2004, doi: https://doi.org/10.2307/25148625.

[35] Y. Bozkurt, A. Rossmann, Z. Pervez, and N. Ramzan, 'Development and evaluation of an urban data governance reference model based on design science research', *Gov. Inf. Q.*, vol. 42, no. 2, p. 102025, 2025, doi: 10.1016/j.giq.2025.102025.

[36] R. Yin, 'How to do Better Case Studies: (With Illustrations from 20 Exemplary Case Studies)', in *The SAGE Handbook of Applied Social Research Methods*, 2455 Teller Road, Thousand Oaks California 91320 United States: SAGE Publications, Inc., 2009, pp. 254–282. doi: 10.4135/9781483348858.n8.

[37] P. Johannesson and E. Perjons, *An introduction to design science*, vol. 9783319106. 2014. doi: 10.1007/978-3-319-10632-8.

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

[39] P. I. Fusch and L. R. Ness, 'Are we there yet? Data saturation in qualitative research', *Qual. Rep.*, vol. 20, no. 9, pp. 1408–1416, 2015, doi: 10.46743/2160-3715/2015.2281.

[40] B. M. Jennings and K. A. Yeager, 'Re-viewing the concept of saturation in qualitative research', *Int. J. Nurs. Stud. Adv.*, vol. 8, no. August 2024, p. 100298, 2025, doi: 10.1016/j.ijnsa.2025.100298.

[41] O. C. Enworo, 'Application of Guba and Lincoln's parallel criteria to assess trustworthiness of qualitative research on indigenous social protection systems', *Qual. Res. J.*, vol. 23, no. 4, pp. 372–384, 2023, doi: 10.1108/QRJ-08-2022-0116.

[42] KOMINFO, 'Peraturan Menteri Komunikasi dan Informatika Republik Indonesia No 5 Tahun 2021 Tentang Penyelenggaraan Telekomunikasi', *Pap. Knowl . Towar. a Media Hist. Doc.*, pp. 12–26, 2021, [Online]. Available: https://jdih.komdigi.go.id/produk_hukum/view/id/768/t/peraturan+menteri+komunikasi+dan+informatika+n

[43] J. Brown, 'An examination of the Skills Framework for the Information Age (SFIA) version 7', *Int. J. Inf. Manage.*, vol. 51, no. April 2019, p. 102058, 2020, doi: 10.1016/j.ijinfomgt.2019.102058.

[44] N. Rashikha, R. Mulyana, and R. Hanafi, 'Using COBIT 2019 SME for Digital Transformation Governance of BPRDCo', pp. 1678–1691, 2019, doi: 10.35889/jutisi.v13i3.2250.

.

BIOGRAPHY OF AUTHORS

Nasywah Nabilah Putri is an undergraduate student in the Information Systems program at Telkom University in Indonesia. She is interested in IT governance, digital transformation, and artificial intelligence (AI). She focuses her academic studies on integrating AI into organizational frameworks, particularly developing AI governance models for the telecommunications industry. She is currently working on a project that explores applying COBIT 2019 Traditional and DevOps methodologies to improve AI governance practices in the sector. She can be contacted at email: nasywahnp@student.telkomuniversity.ac.id

Rahmat Mulyana, S.T., M.T., MBA., Ph.D is a doctoral researcher and lecturer at the Department of Computer and Systems Sciences, Stockholm University, Sweden. He holds a master's degree in information systems from Institut Teknologi Bandung. His research interests include digital transformation, IT governance, ambidextrous organizations, and the strategic adoption of emerging technologies such as AI and cloud computing in regulated industries. He has published extensively in international journals and conferences. He can be contacted at email: rahmat@dsv.su.se

Taufik Nur Adi, S.Kom., M.T., Ph.D is a lecturer and researcher in the Information Systems program at Telkom University, Indonesia. He obtained his master's degree in information systems from Institut Teknologi Sepuluh Nopember (ITS), Surabaya and is currently pursuing his Ph.D. in Industrial Engineering at Pusan National University in South Korea. His research interests include software engineering, machine learning, artificial intelligence, reinforcement learning, and logistics. He is actively involved in academic research and teaching, focusing on applying intelligent systems to improve operational and decision-making processes in various fields. He can be contacted at email: taufikna@telkomuniversity.ac.id