International Journal of Advances in Data and Information Systems
Vol. 6, No. 2, August 2025, pp. 357~375
ISSN: 2721-3056, DOI: 10.59395/ijadis.v6i2.1398

Ambidextrous Cloud Governance Approach to Enhance TelCo's Digital Transformation Using COBIT 2019 Traditional and DevOps

Novi Andriani[1], Rahmat Mulyana[2], Rd. Rohmat Saedudin[3]
[1,3] Information System, Faculty of Industrial Engineering, Telkom University, Indonesia
[2] Department of Computer and Systems Sciences, Stockholm University, Sweden

Article Info

Article history:

Received May 08, 2025
Revised May 28, 2025
Accepted Jul 12, 2025

Keywords:

Ambidextrous Cloud Governance,
Digital Transformation,
COBIT 2019,
DevOps,
DSS04,
Design Science Research,
Case Study,
Telecommunication.

ABSTRACT

Cloud computing plays a crucial role in accelerating digital transformation within the telecommunications sector by enhancing operational efficiency, scalability, and service innovation. However, TelCo faces difficulties in aligning its cloud adoption with effective governance, particularly in ensuring continuous service delivery and resilience. This study proposes a cloud governance framework based on the ambidextrous integration of COBIT 2019 Traditional components and DevOps Focus Area. Employing a Design Science Research methodology, data were collected through semi-structured interviews guided by a structured questionnaire and triangulated with internal documents until data saturation was achieved. Governance and Management Objectives were prioritized using the ambidextrous COBIT 2019 lens, supported by regulatory guidelines from the SOE Minister No. PER-2/MBU/03/2023 and the ICT Minister No. 5/2021, as well as relevant prior studies. The analysis highlighted DSS04: Managed Continuity as the most critical focus area. A capability gap assessment identified vacant leadership roles, overlapping responsibilities, and the lack of Infrastructure as Code (IaC) implementation in cloud services. Recommended improvements include formal assignment of leadership positions, clarification of IT responsibilities, and the adoption of IaC practices. These enhancements are expected to raise the capability maturity of DSS04 from 3.25 to 3.87, representing a 0.62 increase in business continuity readiness. This study contributes to research by extending ambidextrous governance theory to cloud continuity management and provides practical guidance for telecommunications providers seeking to improve operational resilience and manage risks effectively in their digital transformation efforts.

This is an open access article under the CC BY-SA license.

Corresponding 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

Many organizations have adopted Digital Transformation (DT) by leveraging information technology to create value and achieve operational objectives [1]. In the era of the Fourth Industrial Revolution, marked by increasing digital interconnectivity, enterprises are facing unprecedented challenges and opportunities in attaining operational excellence, particularly within the telecommunications sector. A range of interrelated factors including regulatory directives aimed at modernizing the telecommunications industry and the drastic global shifts brought about by the COVID-19 pandemic have significantly accelerated the pace of DT. DT has now become imperative for most

organizations in a world characterized by sudden and continuous change [2]. The primary objective of DT is to enhance organizational performance and efficiency across business functions, communication networks, and operational domains [3].

Within this context, cloud computing emerges as a key enabling technology that supports the efficiency and scalability of enterprise information systems, allowing organizations to quickly adapt to evolving demands during the DT process [4]. Specifically, in the telecommunications sector, DT plays a critical role in boosting operational efficiency, accelerating service innovation, and meeting increasingly dynamic customer demands. The adoption of cloud computing technology contributes significantly by improving infrastructure flexibility, optimizing operational costs, and enabling the provision of scalable cloud-based services that respond effectively to growing data and bandwidth needs [5].

However, the adoption of cloud computing also introduces significant challenges, especially concerning data security, privacy protection, and compliance with applicable regulations [6]. These security concerns are closely linked to cloud governance, which involves management practices and policy enforcement aimed at maintaining the security and integrity of the cloud environment [7]. Therefore, effective implementation of Information Technology Governance (ITG) becomes essential in managing digital strategies comprehensively and ensuring the successful realization of DT initiative [8].

TelCo is a State-Owned Enterprise (SOE) providing services in the telecommunications sector. The Ministry of State-Owned Enterprises has issued guidelines through Ministerial Regulation No. PER-2/MBU/03/2023, which establishes standards for good Information Technology Governance (ITG) in SOE operations, including principles of information security. Furthermore, the regulation outlines the implementation of Good Corporate Governance (GCG) within SOEs, encompassing aspects such as transparency, accountability, social responsibility, and business ethics. The objective of this regulation is to enhance the performance and transparency of SOEs while promoting efficient and effective management to deliver optimal benefits to society and the state [9]. Therefore, the effective implementation of cloud governance is a critical factor to ensure that DT initiatives are executed securely, efficiently, and in compliance with applicable regulations.

Previous research has identified the significant role of ITG in supporting the success of DT [8]. To effectively assess and evaluate ITG, a framework that serves as a guideline is essential to ensure compliance with established standards. Therefore, COBIT 2019 is selected as the primary framework due to its comprehensive focus on measuring and monitoring IT performance [10]. In addition, DevOps practices play a crucial role in supporting DT by accelerating the software development lifecycle through automation and enhanced team collaboration, thereby improving innovation speed and operational efficiency. Furthermore, DevOps enables organizations to adopt disruptive technologies more adaptively and strengthens their ability to respond to the rapidly evolving dynamics of the digital market [11].

Through a Delphi study approach, Mulyana et al. [1], identified the influence of ITG on the implementation of DT and introduced a governance model that integrates both traditional and agile-adaptive approaches, referred to as Ambidextrous IT Governance [12]. This governance model is designed to balance the objectives of operational efficiency and innovation, and is informed by the resource orchestration logic framework [13]. The model has been empirically validated through a case study at Bank BRI, demonstrating its effectiveness in supporting successful DT initiatives through the implementation of seven key governance mechanisms [14]. Previous research in the banking context has employed various approaches based on COBIT 2019, including the governance and management objective (GMO) approach, which has been extensively studied [15], [16]. Additionally, other approaches have focused on four key areas: IT services, IT risks, information security, and DevOps [17], [18], [19].

In this research, an ambidextrous approach is applied by integrating the traditional principles of COBIT 2019 with the DevOps focus area. The COBIT 2019 framework is selected as the foundational model due to its emphasis on comprehensive measurement and monitoring of IT performance [10]. Moreover, the COBIT 2019 DevOps focus area specifically supports the development of software, services, and solutions throughout the DT journey [20]. This combined approach enables a form of cloud governance that is simultaneously structured and flexible, allowing TelCo to meet evolving service demands without compromising stability. Unlike prior studies that primarily focus on the financial sector,

this research applies the IT ambidexterity concept in the telecommunications industry, where complex and dynamic conditions necessitate a balanced governance strategy to ensure successful transformation.

TelCo, one of Indonesia's leading telecommunications operators, delivers nationwide mobile and internet services while actively advancing its digital infrastructure through the deployment of 4G/LTE and 5G technologies. It also promotes digital inclusion and sustainability initiatives in alignment with national goals. While the study focuses on TelCo, an Indonesian state-owned telecommunications provider, the findings offer valuable insights into the digital transformation and governance challenges faced by similar state-owned enterprises in emerging markets. However, the applicability of these findings to private-sector telecoms or organizations outside Indonesia may require careful adaptation, considering regional, regulatory, and operational differences. The findings are highly relevant within the specific context of Indonesia's telecommunications sector, where unique regulatory frameworks and market dynamics shape the adoption and execution of digital transformation strategies. This case study explores TelCo's approach to digital transformation using an ambidextrous cloud governance model that integrates COBIT 2019 traditional mechanisms with DevOps principles. The study aims to offer actionable insights for other telecom firms undertaking similar transformation journeys and seeks to answer the research question: "*How can an ambidextrous cloud governance approach based on COBIT 2019 Traditional and DevOps support digital transformation in a telecommunication company*?"

2. THEORETICAL FOUNDATIONS

2.1. Digital Transformation

Digital Transformation (DT) is a type of Business Transformation driven by emerging technologies and the adoption of corporate culture [21]. It fundamentally reshapes business processes and models to enhance customer value and competitive advantage. Successful DT enables companies to become more productive, efficient, customer-oriented, and technologically advanced, thereby enhancing their competitiveness in the market [22]. In the telecommunications sector specifically, DT plays a pivotal role in improving operational efficiency, accelerating service innovation, and addressing increasingly dynamic customer demands.

2.2. Ambidextrous IT Governance

Ambidextrous IT governance reflects a combination of exploratory and exploitative capabilities, offering organizations the opportunity to innovate continuously without compromising operational stability [1], [3]. It is defined as "a synergistic combination of agile-adaptive and traditional mechanisms that balance exploration emphasizing flexibility, innovation, and adaptability and exploitation, which prioritizes stability, control, and efficiency, allowing organizations to optimize their digital and IT risks and resources toward value realization"[14]. Informed by this approach, the governance model fosters accelerated innovation while simultaneously ensuring strong compliance and effective risk management, thereby maintaining overall organizational resilience and stability [23].

2.3. Emerging Technologies and Cloud Computing

Emerging technologies refer to innovations that are continuously evolving and have significant potential to create new industries or transform existing ones [24]. These innovations drive substantial changes in business competition, social development, and daily life. Such technologies create opportunities for technology-driven transformations that have a broad impact across various sectors, while simultaneously changing the way individuals interact with their surrounding environment [25]. One of the most prominent examples of emerging technologies is cloud computing, which provides flexible, scalable, and efficient access to IT resources through the internet. This technology has become a key catalyst in DT for businesses by driving fundamental changes in data management and information system development [4].

By offering scalable resources, cloud computing enables efficiency in data processing, reducing the risk of over- or under-provisioning capacity, and supporting the rapid execution of large-scale tasks. This technology has become a key catalyst in accelerating DT [26]. In the telecommunications sector, the implementation of cloud computing facilitates network function virtualization using low-cost hardware, significantly reducing capital expenditures (CAPEX) and operational expenditures (OPEX). This shift

also enables enhanced resource utilization efficiency, faster service delivery, and the development of intelligent, scalable management platforms to support future service innovations [27].

2.4. IT Governance and Cloud Governance

IT Governance is defined as "the responsibility of executives and the board of directors; it consists of the leadership, organizational structures, and processes that ensure that the enterprise's IT sustains and extends the enterprise's strategies and objectives" [28]. This definition highlights the accountability of executives and the board of directors in ensuring that the organization's IT supports and enhances the company's strategies and goals. Cloud governance, on the other hand, refers to the IT governance perspective focused on accountability, defining decision-making rights, and balancing benefits, risks, and resources in environments adopting cloud computing [7]. According to Fortis & Munteanu [29], effective cloud governance not only ensures the confidentiality and security of data but also guarantees the integrity of the stored information.

2.5. Frameworks Comparison

2.5.1. COBIT 2019 and DevOps Focus Area

Developed by ISACA, COBIT 2019 serves as a comprehensive framework for IT governance and management, enabling organizations to generate business value while effectively handling IT-related risks and resources. Its adaptability facilitated by design factors and focus areas supports the customization of governance systems to meet specific organizational requirements [10], [30]. Through the DevOps Focus Area, COBIT 2019 aligns governance with contemporary DevOps methodologies by incorporating the CALMS model, which emphasizes Culture, Automation, Lean principles, Measurement, and Sharing [20]. The integration of DevOps principles within COBIT 2019 supports faster software development and delivery by promoting a culture of collaboration, automation, and continuous improvement. In the context of TelCo, this enables more agile responses to technological advancements while ensuring governance practices remain robust and aligned with strategic objectives.

2.5.2. NIST 800-145 Cloud Computing Framework

NIST 800-145 Cloud Computing Framework, published by the National Institute of Standards and Technology (NIST), aims to facilitate comprehensive comparisons between cloud services and their implementation strategies. It explains service models like Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), which are critical for understanding service levels and controls provided by service providers. The framework helps users understand their needs and the capabilities of service providers, aiding informed decision-making while allowing for flexibility in interpretation, recognizing that decisions often involve both objective and subjective perspectives [31]. While NIST 800-145 is excellent for comparing cloud service models, its focus on service-level agreements (SLAs) and flexibility makes it particularly useful for understanding cloud services' technical aspects. However, it does not provide as comprehensive a governance framework for overall IT performance as COBIT 2019, which covers strategic alignment, performance measurement, and risk management beyond the technical level.

2.5.3. ISO/IEC 27017 Cloud Security

ISO/IEC 27017 is an information security standard framework that provides additional security controls specifically for cloud computing environments. This framework was developed to address the limitations of existing standards such as ISO 27002. The standard is intended not only for cloud customers but also for cloud service providers. Its purpose is to assist organizations in managing information security risks associated with the use of cloud computing services [32]. The framework offers guidance on implementing effective security measures for cloud services, covering areas such as data classification, encryption, access management, and incident response [33]. While ISO/IEC 27017 focuses specifically on cloud security and offers a detailed framework for managing information security risks, it is narrower in scope compared to COBIT 2019, which provides a more holistic approach to governance, including performance measurement, strategic alignment, and risk management. In this context, COBIT

2019 provides a more comprehensive governance structure that includes security and extends beyond just cloud environments.

2.5.4. ITIL 4

ITIL 4 (Information Technology Infrastructure Library) is a widely recognized framework for IT service management (ITSM), focusing on delivering value to customers through efficient and effective IT services. It integrates agile, DevOps, and lean practices into the service management lifecycle to enhance service delivery and performance [34]. While ITIL 4 is crucial for managing IT services and improving operational efficiency, it is primarily focused on service management and does not encompass the broader governance structures addressed by COBIT 2019. ITIL 4 can be used alongside COBIT 2019 to support IT governance by optimizing service management practices.

2.5.5. TOGAF

TOGAF (The Open Group Architecture Framework) is an enterprise architecture framework that helps organizations align their IT strategies with business goals. It is centered around the Architecture Development Method (ADM), which guides the creation, implementation, and maintenance of enterprise architectures [35]. TOGAF is a robust framework for structuring IT architectures but lacks the comprehensive governance approach that COBIT 2019 provides. While TOGAF can support the design and alignment of enterprise IT structures, COBIT 2019 integrates governance, performance measurement, and risk management, making it more comprehensive for organizational IT governance.

2.6. Frameworks Selection

Based on the analysis performed, this research utilizes COBIT 2019, incorporating its DevOps Focus Area, as the core framework, underpinned by the principles of ambidextrous IT governance. This cohesive model offers a holistic, flexible, and adaptive approach to governance, facilitating cloud-driven DT within the telecommunications industry, while ensuring regulatory compliance, operational continuity, and the capacity to evolve with technological advancements. COBIT 2019 was selected as the core framework because it provides a comprehensive approach to IT governance and offers the necessary flexibility for dynamic environments like TelCo's digital transformation journey. The integration of traditional governance mechanisms and agile DevOps practices allows TelCo to respond effectively to changing market demands and technological innovations while ensuring compliance and operational continuity. While the other frameworks (NIST 800-185, ISO/IEC 27017, ITIL 4, and TOGAF) provide valuable insights into specific aspects like cloud security, service management, and architecture, COBIT 2019 stands out for its broader governance approach that is aligned with business strategy and digital transformation goals.

2.7. Prior Research on Cloud Governance

This research draws upon key insights from three major prior studies to provide a solid foundation for evaluating and prioritizing Governance and Management Objectives (GMOs) in the context of cloud governance. The first study, “Cloud Governance: A Comprehensive Framework” by Thuraisingham [7], highlights the importance of clearly defined responsibilities and the integration of cloud governance with broader enterprise cybersecurity and emerging technology strategies. It also underlines the need for continuous evaluation and certification to maintain compliance with security, privacy, and regulatory standards in evolving cloud environments [7]. The second study, “An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions” by Chauhan et al. [33], reviews several prominent cloud security frameworks, including COBIT 5, NIST, ISO 27017, CSA STAR, and AWS Well-Architected. The authors argue that no single framework sufficiently addresses all cloud security requirements. Instead, they propose a tailored approach that combines encryption, fine-grained access controls, continuous monitoring, and incident response to effectively mitigate risks in diverse organizational contexts [33]. The third study, “Cloud-Based Data Governance: Ensuring Security, Compliance, and Privacy” by Naik [36], explores the challenges of data protection within multi-tenant cloud environments. The paper emphasizes the role of encryption, identity and access management (IAM), and real-time monitoring in ensuring both data security and business continuity [36]. Together, these studies offer both conceptual and practical perspectives that are essential for prioritizing GMOs.

They ensure that the governance model addresses high-level strategic objectives while also responding to real-world challenges in cloud security particularly relevant to TelCo's DT initiatives.

3. RESEARCH METHOD

This research employs a conceptual framework adopted from the Design Science Research (DSR) model developed by Hevner [37]. This model integrates two paradigms in information systems research: behavioral science and design science. The DSR methodology emphasizes the systematic and rigorous process of creating and evaluating artifacts to address specific problems in a structured and comprehensive manner [37]. This research adopts the case study approach recommended by Yin [38], which is particularly suitable for exploring complex contemporary phenomena in real-life contexts, especially when the research aims to answer "how" or "why" questions. This method allows the researcher to delve deeply into how telecommunications companies, such as TelCo, implement ambidextrous cloud governance to support their DT. By integrating traditional COBIT 2019 principles with more flexible methodologies like DevOps, the company can maintain operational stability while adapting to rapid technological changes. The case study approach enables a more comprehensive understanding of the challenges faced and the strategies implemented in managing the transition to a more structured and effective cloud governance framework.

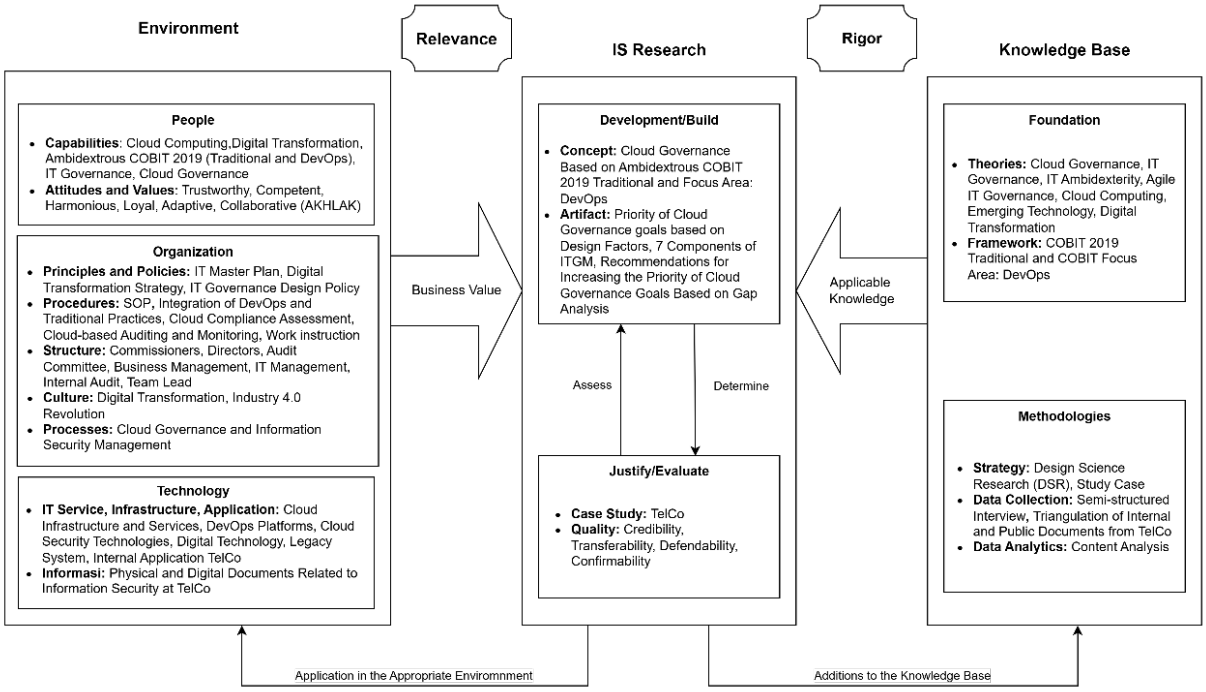


Figure 1. Research Method adapted from Hevner et al. [37]

The conceptual framework developed by Hevner et al. [37] is adapted into a model featuring three primary elements: environment, knowledge base, and information systems research, as illustrated in Figure 1. These components represent the core of the research framework applied in this study. The environment is broken down into subcategories, including people, organizational, and technological aspects, while foundations and methodologies are grouped within the knowledge base. Thus, information systems research primarily focuses on integrating these environmental and knowledge base elements through two related processes: development/building and justification/evaluation [37].

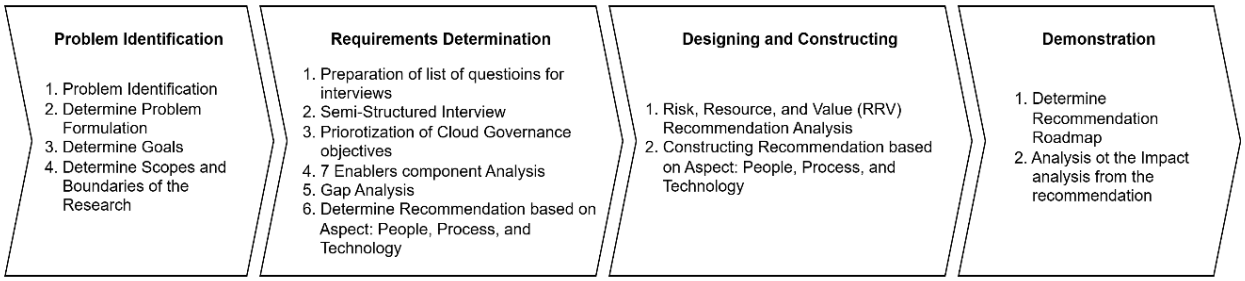


Figure 2. Research Process

Figure 2 illustrates the research process adopted from Johannesson and Perjons [39], comprising four main stages: Problem Identification, which includes problem formulation, research objectives, and scope definition; Requirements Determination, involving the development of interview questions, semi-structured interviews, prioritization of cloud governance objectives, analysis of enablers, gap analysis, and formulation of recommendations based on people, process, and technology aspects; Designing and Constructing, which encompasses the analysis of recommendations using the Risk, Resource, and Value (RRV) approach and the construction of integrated recommendations; and the Demonstration stage, focusing on the preparation of a recommendation roadmap and impact analysis. This approach is conducted sequentially and systematically to produce a comprehensive and practical cloud governance framework.

The research employs a qualitative methodology with two primary data collection instruments. The first instrument is semi-structured interviews serving as primary data, while the second is content analysis of relevant documents sourced both internally and externally, constituting secondary data [40]. To minimize potential biases, the data collection process involved multiple internal stakeholders, ensuring diverse perspectives were captured. Additionally, relevant quantitative metrics, including service delivery performance indicators such as incident resolution times and system uptime, were integrated to provide a more objective and measurable assessment of TelCo's operational efficiency. Data collection continues until data saturation is achieved, defined as the point at which sufficient data has been gathered to replicate the study and no new information emerges [41]. Specific primary data collected from interviews can be seen in Table 1.

Table 1. Primary Data

Respondent	Positon	Discussion
R1	Network Architecture Division	This discussion covers emerging technology adoption in TelCo, focusing on risk management, cloud integration challenges, and ambidextrous product development to improve services.
R2	Integration Management Office Performance Monitoring Lead	This discussion explores strategies for adopting emerging technologies and highlights the importance of DT, including business process simplification and agile methodology implementation.
R3	General Manager Charging Platform	This discussion covers TelCo's IT structure, operational efficiency innovations, competitive strategies, employee training for technology adaptation, and emerging technology adoption.
R4	General Manager of Service Delivery Management	This discussion examines the use of emerging technologies such as AI, IoT, and cloud computing to enhance network services, focusing on 5G development, enterprise solutions, and TelCo's compliance with data security regulations.
R5	Strategic Technology Research and Collaboration Manager	This discussion outlines TelCo's strategic, Agile-driven development of emerging technologies like AI, IoT, and Cloud, emphasizing collaboration and comprehensive risk evaluation to ensure successful business transformation.
R6	General Manager of IT Budgeting & Strategic Alignment	This discussion covers how TelCo manages security, access, and governance of emerging technologies like IoT, Cloud, and AI using DevOps, automation, and centralized policies, along with cloud platforms for internal collaboration, training, and information security standards implementation.

Table 1 displays respondents from various roles within TelCo, providing insights into cloud governance, emerging technology adoption, and DT. Their input covers key areas such as risk management, infrastructure efficiency, and the alignment of technology with organizational strategy, contributing to a comprehensive understanding of TelCo's cloud transformation efforts. Meanwhile, Table 2 presents secondary data utilized to complement the primary data in analyzing the current state of

TelCo. The secondary data was obtained through the triangulation of various relevant corporate documents.

Table 2. Secondary Data

Secondary Data	Description
TelCo Profile	The overview of TelCo
TelCo Annual Report 2023	Includes details about financial results, accomplishments, and approaches executed throughout the fiscal year.
TelCo Sustainability Report 2023	Outlines TelCo's actions and programs aimed at accomplishing social, environmental, and economic sustainability objectives.
TelCo Governance Policy Report	A document or report that outlines governance policies specifically for the TelCo.
Regulation	Encompasses policies pertinent to TelCo's commercial activities and operational processes.

Table 2 presents the secondary data used to complement the primary data in analyzing TelCo's current state. This includes relevant corporate documents such as the annual report, sustainability report, and governance policy report, which provide insights into TelCo's financial performance, sustainability initiatives, and governance practices.

The data analysis process integrates the prioritization of design factors with the classification of DevOps focus areas. Subsequently, the Governance and Management Objectives (GMO) are evaluated by synthesizing insights from relevant literature and regulatory requirements, and expert reviews from external stakeholders. This is followed by a capability level assessment across the seven components to identify existing gaps and formulate actionable improvement recommendations. These recommendations are further prioritized based on considerations of resources, risks, and value, culminating in the development of a structured implementation roadmap and an evaluation of the potential impact of its execution.

4. RESULTS AND DISCUSSION

4.1. GMO Prioritization Result

At this stage, the accumulated prioritization scores summarized in Table 3 are derived from four key parameters: the COBIT 2019 Design Factors [42], COBIT 2019 DevOps Focus Area [20], and two regulatory frameworks, namely the SOE Minister No. PER-2/MBU/03/2023 [9], and the ICT Minister No. 5/2021 [43]. Additionally, insights from three prior studies on cloud computing governance were incorporated. Each source contributes a weighted score reflecting its relevance and influence on cloud governance priorities. The final prioritization score is calculated by averaging the values obtained from these contributing elements.

$$\overline{Final\ Score} = \frac{X_{1+}\ X_{2+}X_{3+}X_{4+}X_{5+}X_{6+}X_{7}}{7}$$

Table 3. GMO Prioritization Result

GMO	COBIT 2019 Design Factor [42]	COBIT 2019 DevOps Focus Area [20]	SOE Minister No. PER-2/MBU/03/2023 [9]	ICT Minister No. 5/2021 [43]	Previous Studies			Final Score
					Cloud Governance Paper 1 [7]	Cloud Governance Paper 2 [36]	Cloud Governance Paper 3 [33]	
DSS04: Managed Continuity	70	67	100	100	100	100	100	91

Table 3 presents the aggregated weighting results from the prioritization assessment of the Governance and Management Objectives (GMO). Among the highest-ranked objectives is DSS04: Managed Continuity, which received a final priority score of 91.

4.2. Gap Analysis Result

4.2.1. Process Component

Process component capabilities are assessed in Table 4 by evaluating the level of achievement for each activity associated with the Governance and Management Objectives (GMOs). The table presents both the percentage of achievement and the corresponding capability level for each evaluated activity.

Table 4. Process Component

Management Practice	Achievement	Capability Level
DSS04.01 Define the business continuity policy, objectives and scope	100% F (Fully)	2
	100% F (Fully)	3
	50% P (Partially)	4
DSS04.02 Maintain business resilience	92% L (Largely)	2
	90% F (Fully)	3
DSS04.03 Develop and implement a business continuity response	100% F (Fully)	2
	100% F (Fully)	3
	100% F (Fully)	4
DSS04.04 Exercise, test and review the business continuity plan (BCP) and disaster response plan (DRP)	90% F (Fully)	2
	50% P (Partially)	3
	100% F (Fully)	4
	50% P (Partially)	5
DSS04.05 Review, maintain and improve the continuity plans	92% F (Fully)	3
DSS04.06 Conduct continuity plan training	100% F (Fully)	2
	100% F (Fully)	3
	100% F (Fully)	4
DSS04.07 Manage backup arrangements	92% F (Fully)	2
	100% F (Fully)	3
DSS04.08 Conduct post-resumption review	100% F (Fully)	3
	100% F (Fully)	4
	100% F (Fully)	5

Table 4 presents the research findings, revealing variations in capability levels across different areas. While several activities have fully met the expected targets, demonstrating optimal capability maturity, others still require further development to achieve higher levels of maturity and align with the desired standards.

4.2.2. Organizational Structure Component

To achieve the cloud governance objectives within the DSS04 domain, TelCo must establish several key organizational roles, as detailed in Table 5.

Table 5. Organizational Structure Component

Organization Structure	Source	Current State
Executive Committee	COBIT 2019 & COBIT 2019 DevOps	The Board of Commissioners at TelCo acts as the main supervisory body, conducting general and special oversight according to the Articles of Association, providing advice to the Board of Directors in carrying out their duties.
Chief Operation Officer	COBIT 2019 & COBIT 2019 DevOps	TelCo currently does not have a Chief Operation Officer position.
Chief Information Officer	COBIT 2019 & COBIT 2019 DevOps	The CIO role is performed by the Director of Information Technology, who is responsible for overall IT strategy and management.
Chief Technology Officer	COBIT 2019 & COBIT 2019 DevOps	The CTO role is performed by the Director of Information Technology.
Chief Information Security Officer	COBIT 2019 & COBIT 2019 DevOps	The CISO role is performed by the Director of Information Technology.
Business Process Owners	COBIT 2019	Each relevant business unit is responsible for managing processes and performance associated with IT continuity.
Data Management Function	COBIT 2019 & COBIT 2019 DevOps	TelCo's Data Management team drives business improvements through data collection, processing, and visualization.
Head Architect	COBIT 2019 & COBIT 2019 DevOps	TelCo's IT Enterprise Architecture and Strategy Group operates under the Director of Information Technology, responsible for enterprise IT architecture development and management.
Head Development	COBIT 2019	TelCo appoints a Head of Development who leads development areas and coordinates with the Director of Information Technology to align projects and functions.
Head IT Operation	COBIT 2019	TelCo has a Vice President of IT Operation and Infrastructure who oversees daily IT operations and infrastructure management.
Service Manager	COBIT 2019 & COBIT 2019 DevOps	TelCo assigns a General Manager for IT Service Quality Management and a Manager for Service Performance Management under the IT Director to

Organization Structure	Source	Current State
		ensure operational service quality.
Information Security Manager	COBIT 2019 & COBIT 2019 DevOps	TelCo's ICT Security Risk Management Manager is responsible for managing information security and communication risks across the organization.
Business Continuity Manager	COBIT 2019 & COBIT 2019 DevOps	TelCo's Business Continuity Management and Infrastructure Risk Management fall under the Director of Finance and Risk, responsible for BCM program development and infrastructure risk mitigation.
Product Owner/Manager	COBIT 2019 DevOps	TelCo employs Product Owners/Managers responsible for product and service domains aligned with organizational roles.
Software Development Manager	COBIT 2019 DevOps	TelCo has a Lead Software Developer who leads software development activities.
Testing Manager	COBIT 2019 DevOps	TelCO has a Manager IT System Integration Testing Management
Systems Operations Manager	COBIT 2019 DevOps	TelCo currently does not have a designated Systems Operations Manager position.
Release Manager	COBIT 2019 DevOps	TelCo assigns a Product & Release Manager responsible for managing product and software release cycles.
Automation Manager	COBIT 2019 DevOps	TelCo's Procurement Analytics, System and Automation Manager handles IT procurement, systems management, and automation.
Systems Architect Manager	COBIT 2019 DevOps	TelCo's Systems Architect Manager leads IT system architecture and security planning under the Enterprise Architecture and Strategy Group.

Table 5 highlights a gap in TelCo's organizational structure. Currently, strategic positions such as the Chief Operating Officer remain unfilled, and key roles such as the Chief Technology Officer (CTO), Chief Information Security Officer (CISO), and Head Architect are consolidated under a single directorate. This situation poses risks, including unclear role definitions, imbalanced workloads, and potential overlaps in responsibilities. Furthermore, the absence of a dedicated Systems Operations Manager indicates the need for a more structured strengthening of IT operational capabilities.

4.2.3. Information Component

To fulfill the cloud governance objectives within the DSS04 domain, TelCo is required to meet the output information from each associated management practice, as detailed in Table 6.

Table 6. Information Component

Management Practice	Information Output	Current State
DSS04.01 Define the business continuity policy, objectives and scope.	Policy and objectives for business continuity	TelCo, through the Directorate of Planning and Transformation, incorporates cloud-focused sustainability policies into its strategy to support risk management and ensure continuity of cloud-based digital services.
	Assessments of current continuity capabilities and gaps	TelCo systematically conducts automated attacks, penetration tests, and regular vulnerability scans on its IT systems to identify and mitigate security risks, ensuring operational continuity before threats can be exploited.
	Disruptive incident scenarios	TelCo has defined various incident scenarios that could disrupt business operations as the basis for mitigation planning and continuity plan development.
DSS04.02 Maintain business resilience.	Approved strategic options	TelCo applies structured governance and decision-making processes, backed by risk assessments and documented strategic justifications.
	BIAs	TelCo uses BIA to prioritize critical processes and evaluates strategic options with a minimum 14% IRR threshold.
	Continuity requirements	TelCo maintains service availability by deploying backup systems, redundant data centers, and ongoing testing. While partially implementing Infrastructure as Code (IaC) for cloud provisioning and recovery, further automation enhancements are needed to strengthen continuity.
DSS04.03 Develop and implement a business continuity response.	Incident response actions and communications	TelCo operates a 24/7 Security Incident and Cyber Patrol team to promptly monitor and respond to security and network incidents with coordinated communication. Integration of automated incident response through DevOps monitoring is needed.
	BCP	TelCo requires BCP and DRP for critical systems such as core billing, leveraging high availability configurations across data centers and cloud for scalability.
DSS04.04 Exercise, test and review the business continuity plan (BCP) and disaster response plan (DRP).	Test results and recommendations	TelCo regularly tests failover and DRP at its primary data center, recommending integration into DevOps CI/CD pipelines for automated, frequent testing.

Management Practice	Information Output	Current State
	Test exercises	Periodic BCP and DRP exercises assess infrastructure and team readiness for disruptions.
	Test objectives	Testing is conducted to ensure service continuity, recovery efficiency, and operational process readiness during incidents.
DSS04.05 Review, maintain and improve the continuity plans.	Recommended changes to plans	TelCo updates business continuity plans using ISO 22301-certified BCM and recommends enhancing feedback loops via DevOps monitoring.
	Results of reviews of plans	Continuity plan reviews are documented internally for ongoing improvement and are not publicly disclosed.
DSS04.06 Conduct continuity plan training.	Monitoring results of skills and competencies	Cloud-based readiness and security training are conducted regularly with monitored outcomes. DevOps and cloud-native security training can be added to further enhance competencies.
	Training requirements	TelCo offers ongoing training in operational readiness and information security customized by role and risk level; however, the program currently lacks focused training on cloud continuity and DevOps to enhance readiness and risk management.
DSS04.07 Manage backup arrangements.	Security incident tickets	TelCo manages backup and recovery incidents via a documented ticketing system coordinated by security and infrastructure teams.
	Test results of backup data	TelCo conducts periodic testing and updates of data backups.
	Backup data	TelCo secures data backups with encryption and redundancy but has yet to implement source code version control or Infrastructure as Code for cloud provisioning.
DSS04.08 Conduct post-resumption review.	Approved changes to the plans	TelCo improves preparedness through post-recovery reviews and employs SIEM, automation, and CloudWatch for proactive threat monitoring.
	Post-resumption review report	Evaluation reports are maintained as internal references for improvement and are not published externally.

As presented in Table 6, although TelCo has implemented various information management practices that support business continuity and cloud-based operational resilience, several critical gaps remain that require attention. One key area for improvement is the further development of automated incident response integration through DevOps monitoring, which is essential to enhance threat detection and response effectiveness. Additionally, the implementation of source code version control and Infrastructure as Code (IaC) practices within the cloud environment remains incomplete, adversely impacting data protection capabilities and service recovery. Addressing these gaps is crucial to strengthening TelCo's overall information resilience and security posture.

4.2.4. People, Skills, and Competencies Component

The results of the skills assessment are summarized in Table 7.

Table 7. People, Skills, and Competencies Component

Skills	Current State
Continuity Management	TelCo has a continuous training program focused on operational readiness and information security, including continuity management aspects, utilizing cloud-based learning platforms such as LinkedIn Learning. Competency monitoring is conducted regularly to ensure staff comprehension of continuity policies and procedures. However, specialized training on BCP and DRP can be further enhanced, particularly by incorporating content on cloud continuity and DevOps practices.

Table 7 illustrates that TelCo has implemented continuous training programs through cloud-based learning platforms such as LinkedIn Learning to ensure employees understand contingency policies and procedures. However, the current training initiatives lack targeted content specifically addressing cloud continuity and DevOps practices. This shortfall underscores the need for more specialized training modules to enhance operational preparedness and organizational resilience in the DT era.

4.2.5. Principles, Policies, and Procedures Component

Table 8 presents the relevant policies that must be adhered to in the management practice of DSS04.

Table 8. Principles, Policies, and Procedures Component

Policy	Current State
Business continuity policy	TelCo has formed a dedicated team within the Directorate of Planning and Transformation to oversee business sustainability and operational continuity, covering testing and incident response for both on-

	premises and cloud systems. However, integration of cloud continuity planning into the initial cloud deployment phases remains incomplete.
Crisis management policy	TelCo's crisis management policy defines clear roles and escalation paths, enabling coordinated rapid response and undergoing regular simulation testing. Recovery Time Objectives (RTO) have been formally documented.

Table 8 presents that TelCo has established a dedicated team tasked with managing business sustainability and ensuring operational continuity across both on-premises and cloud environments. The organization's crisis management policy outlines clearly defined roles and escalation procedures, supported by regular simulation exercises. However, the integration of cloud continuity planning into the early stages of cloud deployment remains insufficient. This indicates a critical area for improvement to enhance the readiness and resilience of cloud services from the outset.

4.2.6. Culure, Ethics, and Behavior Component

Table 9 presents the cultural elements associated with the management practice of DSS04.

Table 9. Culture, Ethics, and Behavior Component

Key Culture Elements	Current State
Embed the need for business resilience in the enterprise culture. Regularly and frequently update employees about core values, desired behaviors and strategic objectives to maintain the enterprise's composure and image in every situation. Regularly test business continuity procedures and disaster recovery.	TelCo has embedded the importance of business resilience into its corporate culture through internal communication and regular training. Core values and expected behaviors are routinely communicated to maintain organizational readiness and reputation. Additionally, business continuity and disaster recovery procedure simulations and tests are conducted regularly to ensure operational preparedness.

Table 9 indicates that TelCo has successfully embedded the importance of business resilience into its corporate culture through effective internal communication and regular training. Core values and expected behaviors are consistently communicated to maintain organizational readiness and corporate reputation. Furthermore, business continuity and disaster recovery procedures are regularly tested through simulations and exercises, ensuring a high level of operational preparedness and responsiveness to potential disruptions.

4.2.7. Service, Infrastructure, and Application Component

Table 10 presents the services, infrastructure, and applications related to the management practice of DSS04.

Table 10. Service, Infrastructure, and Application Component

Services, Infrastructure, and Application	Current State
External hosting services	TelCo utilizes external hosting services from global providers such as Microsoft Azure, AWS, and Google Cloud to enhance the scalability and availability of its digital services. Hosting management adheres to corporate security and governance standards.
Incident monitoring tools	TelCo operates a 24/7 Security Incident and Cyber Patrol team that proactively monitors and responds to security and network incidents through coordinated communication. Currently, the integration of automated incident response via DevOps monitoring requires further development to enhance the speed and effectiveness of incident handling.
Remote storage facility services	TelCo provides remote data storage services distributed across multiple data centers, featuring end-to-end encryption and redundant data replication to ensure data availability and security. This infrastructure supports backup and disaster recovery strategies optimized with cloud technologies, including the use of object storage and hybrid cloud solutions for flexible and efficient data recovery.

Table 10 describes TelCo's utilization of external hosting services and supporting infrastructure to ensure scalability, availability, and security of its digital services. TelCo operates a proactive Security Incident and Cyber Patrol team that monitors and responds to incidents through coordinated communication. However, the integration of automated incident response via DevOps monitoring requires further development to improve the speed and effectiveness of incident handling. The distributed

remote storage infrastructure supports backup and disaster recovery strategies with flexible and efficient hybrid cloud technologies.

4.3. Potential Improvement

To address the identified gaps, potential improvements are directed toward determining the most appropriate changes. The proposed enhancements focus on three main aspects: People, Process, and Technology. These potential improvements are summarized in Table 11.

Table 11. Potential Improvement

Component	Gap	Type	Potential Improvement
People Aspect			
Organizational Structure Component	Currently, several key strategic roles such as Chief Operation Officer are vacant, and critical IT roles (CTO, CISO, Head Architect) are consolidated under a single director, resulting in unclear role definitions and potential workload imbalance. Additionally, there is no dedicated Systems Operations Manager position.	Roles	Fill the vacant Chief Operation Officer and Systems Operations Manager positions, and separate key IT strategic roles to clarify responsibilities and reduce workload.
People, Skills, and Competencies Component	While TelCo has continuous training on operational readiness and information security, the current program lacks specialized content on cloud continuity and DevOps practices.	Skills & Awareness	Enhance the training program by incorporating specialized modules on cloud continuity management, Business Continuity Planning (BCP), Disaster Recovery Planning (DRP), and DevOps practices tailored to different roles.
Process Aspect			
Process Component	Resiliency testing methods such as Chaos Engineering are not yet fully implemented and routinely conducted.	Procedures	Implement comprehensive resiliency testing by adopting Chaos Engineering practices. Schedule and conduct regular resiliency tests across all products and teams to proactively identify system weaknesses and improve recovery capabilities. Provide training and tools to teams to enable effective execution of these tests.
	Distribution, testing, and automation of backups and BCP/DRP lack consistency and control, especially regarding testing frequency and document access.	Procedures	Improve document distribution controls, increase consistency of backup testing, and expand automation of recovery scenarios.
Principles, Policies, and Procedures Component	Integration of cloud continuity planning into the initial cloud deployment phases remains incomplete.	Policy	Complete the integration of cloud continuity planning into the early phases of cloud deployment to ensure risk mitigation and readiness. Strengthening coordination between planning and cloud operations teams.
Information	Integration of automated incident response through DevOps monitoring requires further development to enhance detection and response effectiveness	Procedures	Further develop and implement automated incident response integration via DevOps monitoring to improve effectiveness.
	Source code version control and Infrastructure as Code (IaC) practices on Cloud have not yet been implemented for data protection and service recovery.	Procedures	Implement source code versioning and Infrastructure as Code (IaC) practices on Cloud to enhance data security and recovery processes.
Technology Aspect			
Service, Infrastructure, and Appllication Component	Integration of automated incident response via DevOps monitoring requires further development to improve incident handling speed and effectiveness	Features	Develop and implement DevOps-based automated incident response aligned with cloud governance best practices to enhance service security and resilience.

Table 11 outlines the key improvement opportunities to enhance TelCo's cloud governance maturity in DSS04. Identified gaps include vacant strategic roles, lack of specialized training in cloud continuity and DevOps, and limited automation in incident response and backup management. To address these, the study recommends filling key roles, enhancing training programs, adopting Infrastructure as Code (IaC) practices, and integrating DevOps monitoring automation to improve the resilience and agility of TelCo's cloud services.

4.4. Resource, Risk, Value (RRV) Analysis

By integrating the aspects of resources, risks, and value, this analysis serves to determine risk priorities and support strategic decision-making related to resource allocation for risk mitigation efforts.

The RRV approach has proven effective in providing reliable information on the sensitivity of activities to improvement interventions during project execution [44]. In the application of the RRV analysis, a score of three (3) is assigned when all resources originate internally, the risk impact is confined to a single unit, and the implementation value extends across all units within the company. Conversely, a score of two (2) is given if resource requirements involve both internal and external parties, risks affect multiple units, and the implementation benefits are experienced by several units in the organization. Meanwhile, when resources are entirely external, risks have a broad impact across all units, but the implementation benefits are limited to only one unit, a score of one (1) is assigned. The scores from each aspect are multiplied to produce a final score, which is then classified into three priority levels: Low (1–9), Medium (10–18), and High (19–27). Table 12 presents the results of the priority analysis for potential improvements identified in TelCo based on the RRV analysis.

Final Score = Resource Score x Risk Score x Value Score

Table 12. RRV Analysis

No	Potential Improvement	Final Score	Category
1	Implement comprehensive resiliency testing by adopting Chaos Engineering practices. Schedule and conduct regular resiliency tests across all products and teams to proactively identify system weaknesses and improve recovery capabilities. Provide training and tools to teams to enable effective execution of these tests.	27	High
2	Complete the integration of cloud continuity planning into the early phases of cloud deployment to ensure risk mitigation and readiness. Strengthening coordination between planning and cloud operations teams.	18	Medium
3	Further develop and implement automated incident response integration via DevOps monitoring to improve effectiveness.	18	Medium
4	Implement source code versioning and Infrastructure as Code (IaC) practices on Cloud to enhance data security and recovery processes.	18	Medium
5	Develop and implement DevOps-based automated incident response aligned with cloud governance best practices to enhance service security and resilience.	18	Medium
6	Enhance the training program by incorporating specialized modules on cloud continuity management, Business Continuity Planning (BCP), Disaster Recovery Planning (DRP), and DevOps practices tailored to different roles.	12	Medium
7	Fill the vacant Chief Operation Officer and Systems Operations Manager positions, and separate key IT strategic roles to clarify responsibilities and reduce workload.	12	Medium
8	Improve document distribution controls, increase consistency of backup testing, and expand automation of recovery scenarios.	12	Medium

Table 12 presents the RRV Analysis of proposed improvements for TelCo's cloud governance and managed continuity. The highest priority focuses on implementing Chaos Engineering for resiliency testing. Other key improvements include integrating cloud continuity planning early in deployment, enhancing incident response through DevOps monitoring, and adopting Infrastructure as Code (IaC) for better security and recovery. Additional improvements address organizational roles, training enhancements, and backup processes. This prioritization provides clear guidance for telecommunications companies on how to strategically allocate resources and efforts to enhance cloud-managed continuity capabilities and overall governance maturity. The improvements are categorized into High, Medium, and Low priority levels.

4.5. Implementation Roadmap

An overview of the implementation roadmap, designed based on the RRV analysis results, is presented in Table 13.

Table 13. Implementation Roadmap

No	Initiatives	2026				2027			
		Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1	Implement resiliency testing using Chaos Engineering practices; conduct regular tests across products and teams to identify weaknesses and improve recovery.								
2	Integrate cloud continuity planning early in deployment for risk mitigation and readiness; improve coordination between planning and cloud teams.								
3	Further develop and implement automated incident response integration via DevOps monitoring to enhance detection and response effectiveness.								
4	Implement source code versioning and Infrastructure as Code (IaC) practices on cloud platforms to enhance data security and recovery processes.								

No	Initiatives	2026				2027			
		Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
5	Develop and implement DevOps-based automated incident response aligned with cloud governance best practices to improve service security and resilience.								
6	Enhance the training program with specialized modules on cloud continuity, BCP, DRP, and DevOps practices for specific roles.								
7	Fill the vacant COO and Systems Operations Manager positions, and separate key roles to clarify responsibilities and balance workload.								
8	Improve document distribution controls, increase consistency of backup testing, and expand automation of recovery scenarios.								

The plan for strengthening TelCo's human resources, processes, and technology from 2026 to 2027 is detailed in Table *13*. It includes filling key positions, enhancing training programs, conducting resiliency testing, and automation to boost system recovery and security.

4.6. Impact of Recommendations Implementation

The comparison of capability levels before and after the implementation of improvements, as presented in Table 14, represents the impact of the enhancement efforts at TelCo.

Table 14. Impact Estimation on Process Component

GMO	Previous Capability Level	Estimated Capability Level
DSS04: Managed Continuity		
Total Amount	26	31
Total Score	3.25	3.87

A detailed comparison of the capability scores for the process components of DSS04: Managed Continuity before and after the improvements is presented in Table 14. The capability score is calculated by dividing the capability level by the number of practices in DSS04: Managed Continuity, which consists of 8 practices. This calculation provides a normalized measure of the overall improvement in the process components of DSS04. The capability score increased from 3.25 prior to the improvements to 3.87 afterward, resulting in a significant 0.62 improvement. This improvement reflects a higher capability level achieved after the enhancements were implemented across the 8 practices under DSS04, demonstrating how the improvements impacted the overall capability. Table 15 presents the estimated impact of implementation at TelCo based on recommendations for several other components, including Organizational Structure, Information, People, Skills, and Competencies, Principles, Policies, and Procedures, as well as Service, Infrastructure, and Application.

Table 15. Impact estimation of Other Component

Pre-implementation State	Post-implementation State
Organizational Structure Componenet	
Key strategic roles such as Chief Operation Officer are vacant; critical IT roles are consolidated under a single director causing unclear role definitions and workload imbalance; no dedicated Systems Operations Manager position.	Vacant key positions such as Chief Operation Officer and Systems Operations Manager are filled; key IT strategic roles are separated to clarify responsibilities and balance workload.
Information Component	
Integration of automated incident response via DevOps monitoring is underdeveloped; source code version control and Infrastructure as Code (IaC) practices for data protection and recovery not implemented.	Automated incident response via DevOps monitoring is fully developed and integrated to improve detection and response effectiveness; source code version control and IaC practices implemented to enhance data security and recovery processes.
People, Skills, and Competencies Component	
Continuous training program exists but lacks specialized content on cloud continuity management, BCP, DRP, and DevOps practices tailored to different roles.	Training program enhanced with specialized modules on cloud continuity management, Business Continuity Planning (BCP), Disaster Recovery Planning (DRP), and DevOps practices tailored to roles.
Principles, Policies, and Procedures Component	
Integration of cloud continuity planning into early cloud deployment phases is incomplete.	Cloud continuity planning fully integrated into early cloud deployment phases
Service, Infrastructure, and Application Component	
Automated incident response via DevOps monitoring is underdeveloped, affecting incident handling speed and effectiveness.	DevOps-based automated incident response developed and implemented, aligned with cloud governance best practices to enhance service security and resilience.

Table 15 illustrates the significant improvements in TelCo's governance following the implementation of recommendations, such as filling vacant strategic positions and clarifying

responsibilities by separating roles to reduce workload. The development of automated incident response through DevOps has enhanced the effectiveness of incident detection and response, while the enhancement of training programs covering cloud continuity, BCP, and DRP has strengthened team readiness. Additionally, the full integration of cloud continuity planning during the early stages of deployment, along with the implementation of Infrastructure as Code (IaC) practices, has contributed to an overall improvement in operational resilience and readiness.

4.7. Discussion

TelCo has made significant strides in enhancing Managed Continuity within the context of cloud governance and DevOps practices. The prioritization of DSS04: Managed Continuity with a score of 91 underscores the critical importance of business continuity in TelCo's DT efforts. The company's proactive approach to operational continuity, through the integration of cloud sustainability policies and a continuous training program focused on operational readiness and information security, aligns well with best practices in the industry. Previous studies, such as those by Thuraisingham [7], have highlighted the need for clear roles and integration of cloud governance frameworks to ensure operational resilience. TelCo's practice of integrating automated penetration testing and vulnerability scans supports this integration, showcasing alignment with global cloud governance standards, as emphasized in the work of Chauhan et al. [33]. These initiatives have been critical in contributing to the success of TelCo's DT, ensuring that continuity and resilience are integral to its transformation strategy.

However, despite these advancements, there are still areas requiring further development, particularly in automating incident response through DevOps monitoring. As identified in the gap analysis, TelCo has yet to fully integrate automated incident response mechanisms into its operational processes, which is a critical area for improvement to enhance security incident management. The research by Naik [36], emphasizes the need for comprehensive monitoring and automated recovery mechanisms in multi-tenant cloud environments to ensure business continuity. While TelCo has made progress with the implementation of hybrid cloud solutions and backup strategies, further improvements are needed, particularly through the application of Infrastructure as Code (IaC) for consistent deployment and configuration, as well as the implementation of Chaos Engineering to validate system resilience under failure scenarios. Addressing these gaps will significantly improve TelCo's ability to respond to incidents swiftly and maintain service availability in cloud-based environments, further driving the success of its DT. This aligns with Mulyana et al. [1]'s findings on the integration of traditional and agile-adaptive IT governance models, underscoring the necessity of continuous improvement in governance processes to ensure the success of DT in the telecommunications sector.

5. CONCLUSION

This study recognizes several limitations, including potential biases inherent in the research design and its specific focus on TelCo, which may limit the generalizability of the findings to other contexts or industries. Despite these constraints, the application of the ambidextrous COBIT 2019 framework demonstrates a structured and robust approach for enhancing IT governance, particularly in the context of cloud-based DT. By prioritizing the DSS04 Managed Continuity component and systematically addressing the identified gaps across the dimensions of people, processes, and technology, TelCo was able to achieve a significant 0.62 improvement in capability maturity, from 3.25 to 3.87. This advancement signifies not only an enhanced alignment between IT operations and broader business objectives but also strengthens continuity management practices and regulatory compliance within the organization. The study's outcomes contribute valuable insights for both academic research and practical implementation, offering a replicable model for other telecommunications providers aiming to optimize their governance frameworks in support of evolving cloud technologies and DT initiatives. Future research could expand on this work by exploring additional governance components or applying the framework across diverse organizational settings to validate and extend the findings.

REFERENCES

[1] R. Mulyana, L. Rusu, dan 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*, hal. 1–16, 2022, [Daring]. Tersedia pada: https://aisel.aisnet.org/pacis2022/267/

[2] C. Gong dan V. Ribiere, "Developing a unified definition of digital transformation," *Technovation*, vol. 102, no. July 2020, hal. 102217, Apr 2021, doi: 10.1016/j.technovation.2020.102217.

[3] R. Mulyana, L. Rusu, dan E. Perjons, "How Hybrid IT Governance Mechanisms Influence Digital Transformation and Organizational Performance in the Banking and Insurance Industry of Indonesia," in *Proceedings of the 31st International Conference on Information Systems Development*, Okt 2023. doi: 10.62036/ISD.2023.33.

[4] Hamed Taherdoost, "An Overview of Trends in Information Systems: Emerging Technologies that Transform the Information Technology Industry," *Cloud Comput. Data Sci.*, vol. 4, no. 1, hal. 1–16, Agu 2022, doi: 10.37256/ccds.4120231653.

[5] A. H. M. Jafor, K. S. Azim, M. A. Hossain, A. U. Shayed, N. A. Nikita, dan O. U. Khan, "The Evolution of Cloud Computing & 5G Infrastructure and its Economical Impact in the Global Telecommunication Industry," *Adv. Int. J. Multidiscip. Res.*, vol. 2, no. 5, hal. 1–19, Sep 2024, doi: 10.62127/aijmr.2024.v02i05.1100.

[6] Perdly Setiawan, Raihan Shidqi Putrandi, dan Imelda Imelda, "Systematic Literature Review of Cloud Computing Adoption," *INOVTEK Polbeng - Seri Inform.*, vol. 9, no. 2, hal. 578–586, Okt 2024, doi: 10.35314/74fzvf09.

[7] B. Thuraisingham, "Cloud governance," *IEEE Int. Conf. Cloud Comput. CLOUD*, vol. 2020-Octob, hal. 86–90, 2020, doi: 10.1109/CLOUD49709.2020.00025.

[8] R. Mulyana, L. Rusu, dan E. Perjons, "IT governance mechanisms influence on digital transformation: A systematic literature review," *27th Annu. Am. Conf. Inf. Syst. AMCIS 2021*, hal. 0–10, 2021.

[9] 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," 2023. [Daring]. Tersedia pada: https://www.peraturan.go.id/id/permen-bumn-no-per-2-mbu-03-2023-tahun-2023

[10] ISACA, *COBIT 2019 Framework - Introduction and Methodology*. 2019. [Daring]. Tersedia pada: https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004Ko9cEAC

[11] Sekhar Chittala, "AIOps and DevOps : Catalysts of Digital Transformation in the Age of Automated Operations," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 10, no. 6, hal. 155–166, Nov 2024, doi: 10.32628/CSEIT24106163.

[12] R. Mulyana, L. Rusu, dan E. Perjons, "Key Ambidextrous IT Governance Mechanisms Infuence on Digital Transformation and Organizational Performance in Indonesian Banking and Insurance," *Pacific Asia Conf. Inf. Syst.*, no. July, hal. 1–16, 2024, [Daring]. Tersedia pada: https://aisel.aisnet.org/pacis2024

[13] M. Kizito, "Ambidextrous IT Governance Enactment in Healthcare: A Comparison between the Swedish and Ugandan Setting," in *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2020, hal. 5573–5582. doi: 10.24251/HICSS.2020.686.

[14] R. Mulyana, L. Rusu, dan 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, hal. 100083, 2024, doi: 10.1016/j.digbus.2024.100083.

[15] D. A. Permana, R. Fauzi, dan R. Mulyana, "Perancangan Tata Kelola Teknologi Informasi Untuk Transformasi Digital di Industri Perbankan Menggunakan Framework Cobit 2019 Domain Align, Plan, And Organise : Studi Kasus Di Bank XYZ," *e-Proceeding Eng.*, vol. 8, no. 5, hal. 1–8, 2021.

[16] O. T. Poetry, R. Fauzi, dan R. Mulyana, "Perancangan Tata Kelola Teknologi Informasi Untuk Transformasi Digital Di Industri Perbankan Menggunakan Framework Cobit 2019 Dengan Domain Deliver, Service and Support: Studi Kasus Bank Xyz It Governance Design for Digital Transformation in Banking Indus," *e-Proceeding Eng.*, vol. 8, no. 5, hal. 9684–9692, 2021.

[17] D. Andika, R. Mulyana, dan L. Ramadhani, "IT Governance Design Based on COBIT 2019 SME Focus Area for UMKM BPRBCo Digital Transformation," *J. Inf. Syst. Res.*, vol. 6, no. 1, hal. 205–218, Okt 2024, doi: 10.47065/josh.v6i1.5905.

[18] A. Viamianni, R. Mulyana, dan F. Dewi, "COBIT 2019 INFORMATION SECURITY FOCUS AREA IMPLEMENTATION FOR REINSURCO DIGITAL TRANSFORMATION," *JIKO (Jurnal Inform. dan Komputer)*, vol. 6, no. 2, hal. 106–115, Agu 2023, doi: 10.33387/jiko.v6i2.6366.

[19] Achmad Fadhli Satriadi, R. Mulyana, dan R. Fauzi, "AGILE IT SERVICE MANAGEMENT DESIGN OF FINTECHCO DIGITALIZATION BASED ON COBIT 2019 DEVOPS FOCUS AREA," *J. Tek. Inform.*, vol. 4, no. 5, hal. 1165–1177, Okt 2023, doi: 10.52436/1.jutif.2023.4.5.1304.

[20] ISACA, "COBIT Focus Area: DevOps." [Daring]. Tersedia pada: https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004Ko9dEAC

[21] D. Tang, "WHAT IS DIGITAL TRANSFORMATION?," *EDPACS*, vol. 64, no. 1, hal. 9–13, Jul 2021, doi: 10.1080/07366981.2020.1847813.

[22] C. Tanushev, "Digital Transformation: The Impact on Corporate Strategy," *Econ. Altern.*, vol. 28, no. 3, hal. 383–404, Sep 2022, doi: 10.37075/EA.2022.3.01.

[23] R. Mulyana, "IT Governance Influence on Digital Transformation," Stockholm University, 2025. [Daring]. Tersedia pada: http://urn.kb.se/resolve?urn=urn:nbn:se:su:diva-242507

[24] O. Yusuf, "Emerging Technologies To Enhance Optimization In The Process Industries," *J. Artif. Intell. Gen. Sci. ISSN3006-4023*, vol. 1, no. 1, hal. 188–199, Jan 2024, doi: 10.60087/jaigs.v1i1.153.

[25] I. Bojanova, R. Kuhn, dan J. Voas, "Emerging Disruptive Technologies," *Computer (Long. Beach. Calif).*, vol. 56, no. 12, hal. 27–30, Des 2023, doi: 10.1109/MC.2023.3314933.

[26] Ridham Singh Bhatia, Nishant Yadav, dan Saarthak Chawla, "Exploring Cloud Computing," *Int. J. Adv. Res. Sci. Commun. Technol.*, hal. 404–408, Apr 2024, doi: 10.48175/IJARSCT-17564.

[27] X. Zhiqun, C. Duan, H. Zhiyuan, dan S. Qunying, "Emerging of Telco Cloud," *China Commun.*, vol. 10, no. 6, hal. 79–85, Jun 2013, doi: 10.1109/CC.2013.6549261.

[28] ISACA, "ISACA GLOSSARY," in *ISACA*, hal. 1–159. [Daring]. Tersedia pada: https://www.isaca.org/-/media/files/isacadp/project/isaca/resources/glossary/glossary.pdf

[29] T.-F. Fortis dan V. I. Munteanu, "From Cloud Management to Cloud Governance," hal. 265–287, 2014, doi: 10.1007/978-1-4471-6452-4_11.

[30] ISACA, *COBIT 2019 Implementation Guide: Implementing and Optimizing an Information and Technology Governance Solution*. 2018. [Daring]. Tersedia pada: https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004Ko9aEAC

[31] E. Simmon, "Evaluation of cloud computing services based on NIST SP 800-145," NIST, Gaithersburg, MD, Feb 2018. doi: 10.6028/NIST.SP.500-322.

[32] "ISO/IEC 27017." [Daring]. Tersedia pada: https://www.iso27001security.com/html/27017.html

[33] M. Chauhan dan S. Shiaeles, "An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions," *Network*, vol. 3, no. 3, hal. 422–450, Sep 2023, doi: 10.3390/network3030018.

[34] Y. Al-Ashmoery *dkk.*, "Impact of Integrating Lean, Agile, and DevOps with ITIL4 Framework for Modern IT Service Management," in *2024 1st International Conference on Emerging Technologies for Dependable Internet of Things (ICETI)*, IEEE, Nov 2024, hal. 1–8. doi: 10.1109/ICETI63946.2024.10777262.

[35] P. Desfray dan G. Raymond, "Chapter 1 - TOGAF®: General Presentation," in *The MK/OMG Press*, P. Desfray dan G. B. T.-M. E. A. with T. Raymond, Ed., Boston: Morgan Kaufmann, 2014, hal. 1–24. doi: https://doi.org/10.1016/B978-0-12-419984-2.00001-X.

[36] S. Naik, "Cloud-Based Data Governance: Ensuring Security, Compliance, and Privacy," *Eastasouth J. Inf. Syst. Comput. Sci.*, vol. 1, no. 01, hal. 69–87, Agu 2023, doi: 10.58812/esiscs.v1i01.452.

[37] A. R. Hevner, S. T. March, J. Park, dan S. Ram, "Design Science in Information Research," *Des. Sci. IS Res. MIS Q.*, vol. 28, no. 1, hal. 75–105, 2004.

[38] 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, hal. 254–282. doi: 10.4135/9781483348858.n8.

[39] P. Johannesson dan E. Perjons, *An Introduction to Design Science*. Cham: Springer International Publishing, 2014. doi: 10.1007/978-3-319-10632-8.

[40] M. Denscombe, *The Good Research Guide for small-scale social research projects*, 4 ed. New York, USA, 2010.

[41] P. Fusch dan L. Ness, "Are We There Yet? Data Saturation in Qualitative Research," *Qual. Rep.*, vol. 20, no. 9, hal. 1408–1416, Sep 2015, doi: 10.46743/2160-3715/2015.2281.

[42] ISACA, "COBIT 2019 Framework: Governance & Management Objectives." [Daring]. Tersedia pada: https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004Ko9ZEAS

[43] KOMINFO, "Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2021 tentang Penyelenggaraan Telekomunikasi," 2021. [Daring]. Tersedia pada: https://jdih.komdigi.go.id/produk_hukum/view/id/768/t/peraturan+menteri+komunikasi+dan+informatika+nomor+5+tahun+2021

[44] J. Song, A. Martens, dan M. Vanhoucke, "Using Earned Value Management and Schedule Risk Analysis with resource constraints for project control," *Eur. J. Oper. Res.*, vol. 297, no. 2, hal. 451–466, Mar 2022, doi: 10.1016/j.ejor.2021.05.036.