Scientific Journal of Informatics
Vol. 12, No. 3, August 2025

p-ISSN 2407-7658 https://journal.unnes.ac.id/journals/sji/index e-ISSN 2460-0040

Ambidextrous Blockchain Governance Approach for Advancing SmartCo's Digital Transformation Using COBIT 2019 Traditional and DevOps

Izzah Khairiyah[1], Rahmat Mulyana[2], Tien Fabrianti Kusumasari[3]
[1,3]Information Systems, Faculty of Industrial Engineering, Telkom University, Indonesia
[2]Department of Computer and System Science, Stockholm University, Sweden

Abstract.
Purpose: This study aims to design an ambidextrous governance model based on COBIT 2019 Traditional and DevOps Focus Areas, focusing on DSS05 (Managed Security Services), to enhance SmartCo's security readiness for blockchain adoption.
Methods: Adopting the Design Science Research (DSR) and case study methodology, data were gathered through semi-structured interviews with six key stakeholders at SmartCo and triangulated with internal documents until data saturation was achieved. Governance and Management Objectives (GMOs) were prioritized using organizational design factors, the relevance of COBIT 2019 DevOps guidance, national regulations (ICT Minister No.5/2021 and SOE Ministerial No. PER-2/MBU/03/2023), and insights from prior research.
Results: The study presents an ambidextrous design of the seven governance components for DSS05, addressing people, process, and technology dimensions. Recommendations include formalizing dedicated security roles, standardizing procedures, issuing new policies, and adopting a Security Information and Event Management (SIEM) system. Implementation is projected to improve the DSS05 process capability from 3.29 to 3.86.
Novelty: This research contributes to the IT governance body of knowledge by proposing a practical pre-implementation governance model for blockchain security in technology-focused enterprises. Its originality lies in the application of the ambidextrous COBIT 2019 framework to the DSS05 objective and the use of a comprehensive multi-criteria prioritization method to guide governance of emerging technologies.

Keywords: Ambidextrous Blockchain Governance, Digital Transformation, COBIT 2019, DevOps, DSS05
Received June 2025 / **Revised** July 2025 / **Accepted** August 2025

INTRODUCTION

Digital Transformation (DT) has become a primary focus and a necessity for organizations to address the pressures of technological innovation and changes in consumer behavior to survive and thrive in the current digital era [1], [2], [3]. For digital infrastructure providers like SmartCo, this transformation is driven by the dual pressures of adopting disruptive technologies to maintain a competitive edge while simultaneously adhering to increasingly stringent regulatory standards [4], [5]. Blockchain technology is present as one of the innovations that promises to increase the efficiency, transparency, and security of business processes [6], [7], [8]. IDC estimates global blockchain spending to reach USD 19 billion in 2024, while the digital transformation market is projected to grow from USD 2.2 trillion in 2024 to nearly USD 11 trillion by 2032 [9], [10]. However, its adoption at the organizational level raises new challenges, especially in the aspect of information technology governance [11]. The absence of a centralized control structure in many blockchain implementations necessitates a more adaptive and collaborative governance approach [12]. SmartCo, as a digital infrastructure provider, manages nationwide infrastructure with over 2,500 network points of presence, supporting more than 120 enterprise-scale digital services and significant annual IT investments. While exploring the use of blockchain technology, recent internal assessments have identified the absence of an integrated blockchain governance framework, highlighting the need for a model aligned with the company's strategic direction to ensure effective and secure implementation [5].

[1]*Corresponding author.
Email addresses: izzahkhairiyah@student.telkomuniversity.ac.id (Khairiyah), rahmat@dsv.su.se (Mulyana), tienkusumasari@telkomuniversity.ac.id (Kusumasari)

DOI: 10.15294/sji.v12i3.26974

Previous studies have shown that ambidextrous IT governance, a combination of traditional and agile-adaptive mechanisms, plays a crucial role in supporting digital transformation [13], [14]. For instance, a Delphi study involving the banking and insurance sectors in Indonesia revealed the importance of ambidextrous mechanisms for maintaining stability while encouraging digital innovation [15]. Furthermore, the influence of these mechanisms on organizational performance has been confirmed to be fully mediated by the success of digital transformation [15]. A case study by Mulyana, Rusu, and Perjons [13] found seven key ambidextrous ITG mechanisms that have been shown to improve performance by speeding up digital strategies. Ambidextrous IT governance mechanisms have also been shown to effectively support digital transformation initiatives across various organizational contexts [16]. Conceptually, this ambidextrous approach bridges the need for exploration and exploitation in information technology management to create sustainable business value [17]. These findings reinforce the urgency of implementing balanced IT governance for organizations facing technological disruption.

Blockchain governance refers to how organizations manage decision-making structures, responsibility sharing, and compliance in a decentralized system [18], [19]. To be effective, blockchain governance must balance technical and social aspects, such as code control, community roles, and context mechanisms [7], [20]. The success of governance depends on the extent to which the system can ensure transparency, accountability, and legitimacy of decision-making [21]. Meanwhile, COBIT 2019 has been widely used to align IT management with organizational business goals, and through the DevOps focus area, this framework is extended to support automation and cross-functional collaboration [22], [23]. The challenge often lies in effectively tailoring and integrating these frameworks to suit specific organizational needs and agile development cycles [24]. In this study, the two approaches are combined in an ambidextrous framework, where traditional COBIT 2019 is used to maintain structure, control, and compliance, while the DevOps approach supports implementation and speed adaptation. This combination is specifically designed to build blockchain governance at the pre-implementation stage at SmartCo, so that organizations are ready to face the dynamics of technology and the demands of digital transformation.

Although the topic of blockchain governance is increasingly discussed, most studies still focus on basic definitions and concepts without providing direct application in real organizations [19], [25]. Many focus on technical or social aspects separately, whereas the complexity of blockchain requires a comprehensive understanding of both [18], [26]. The use of COBIT 2019 as a governance framework is actually quite widespread, but not many have explicitly linked it to the blockchain context, let alone combined it with a DevOps approach. Studies such as [19] also show that even in the public sector, the use of blockchain is not fully supported by an adequate governance framework. On the other hand, the ambidextrous approach to IT governance has so far been more widely applied in highly regulated sectors such as banking [27], [28]. Therefore, this study attempts to offer an alternative approach by designing a blockchain governance model that combines the rigor of traditional COBIT and the agility of DevOps for the digital service provider sector, such as SmartCo.

However, to date, no prior study has explicitly integrated traditional COBIT 2019 and DevOps into an ambidextrous blockchain governance model for the pre-implementation phase in the digital infrastructure sector [23], [29]. Furthermore, there has been no study that combines multi-criteria techniques based on organizational design factors, national regulations, and previous research findings in prioritizing Governance and Management Objectives (GMOs) [30]. This study fills this gap by offering an ambidextrous COBIT 2019-based blockchain governance model designed for the digital infrastructure technology sector, such as SmartCo. This unique approach lies in the selection of GMO DSS05 (Managed Security Services) as the focus, because the security aspect is crucial in the process of blockchain technology adoption [6], [30]. This study aims to design a DSS05-based governance solution, compile seven components of ambidextrous governance capabilities, and build an implementation roadmap that supports SmartCo's readiness to proactively manage blockchain security systems.

THEORETICAL FOUNDATION

Digital Transformation

Digital Transformation (DT) refers to the fundamental integration of digital technology into all aspects of a business, fundamentally changing how organizations operate and deliver value to customers [31]. DT is a process aimed at improving an entity by triggering significant changes in its properties through combinations of information, computing, communication, and connectivity technologies [32]. Successful DT is crucial for responding to changing customer behaviors and dynamic market demands [33]. In the context of SmartCo, DT serves as the strategic foundation for adopting emerging technologies such as blockchain, ensuring that governance innovations are aligned with organizational objectives, regulatory compliance, and the evolving needs of national digital infrastructure.

Blockchain Technology and Governance

Blockchain technology, as a decentralized and immutable ledger, offers the potential for increased efficiency, transparency, and security [34]. However, its adoption presents significant governance challenges related to decision-making structures, accountability, and compliance in decentralized environments [35]. Key blockchain governance challenges include technical aspects like protocol management and security, as well as non-technical aspects such as regulation, standards, and stakeholder engagement [36]. Therefore, designing a robust governance framework becomes very important, especially for organizations preparing to adopt blockchain as part of their digital transformation.

Ambidextrous IT Governance

Ambidextrous IT governance 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”[17]. This approach is crucial for organizations to innovate while optimizing existing operations. For SmartCo, applying an ambidextrous IT governance approach is essential to balance the innovative potential of blockchain technology with the stability, security, and compliance required in managing critical national digital infrastructure.

METHODS

Conceptual Model

This study uses the Design Science Research (DSR) approach, which is considered relevant for designing and evaluating new information technology artifacts to solve real problems in organizations while contributing to the development of knowledge [37]. DSR was chosen because it provides a systematic framework, starting from the problem identification stage and solution design, to initial testing of the developed ambidextrous blockchain governance model. In this study, the DSR process is the main guideline in each stage, and the visualization of the flow is presented in Figure 1 to illustrate the main steps and activities carried out to achieve the research objectives.

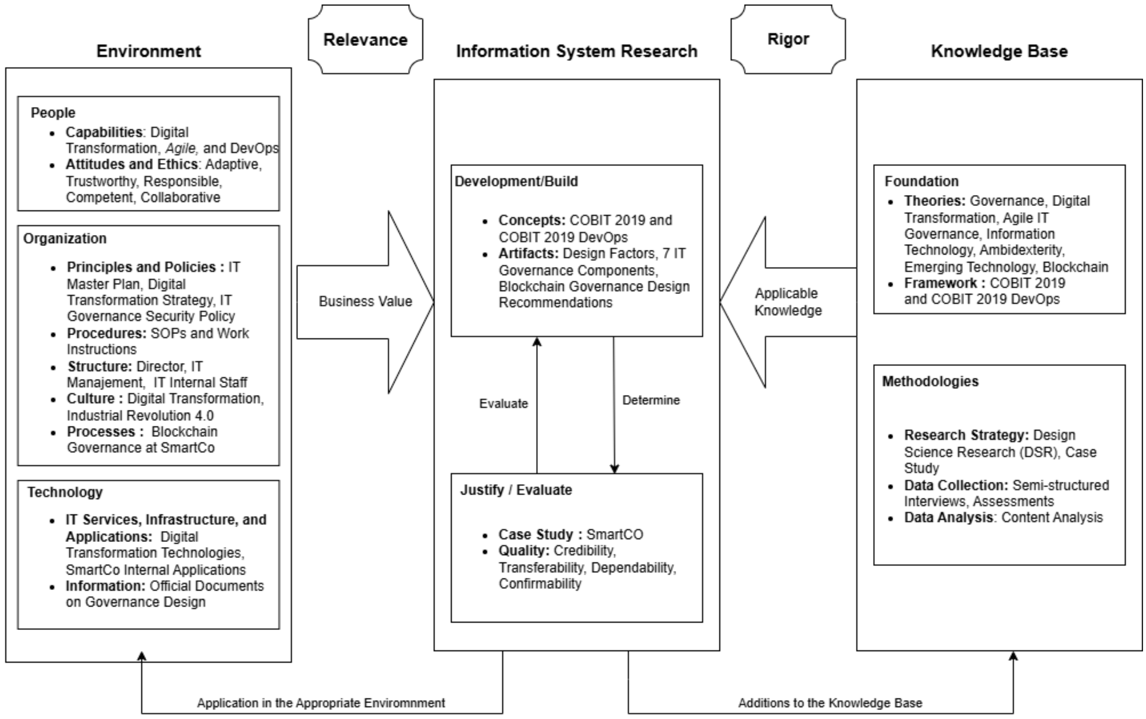
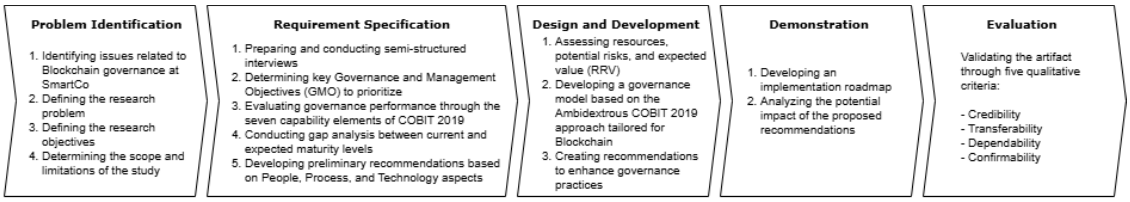

Relevance
Rigor
Environment
Information System Research
Knowledge Base
People
Capabilities: Digital Transformation, Agile, and DevOps
Attitudes and Ethics: Adaptive, Trustworthy, Responsible, Competent, Collaborative
Organization
Principles and Policies : IT Master Plan, Digital Transformation Strategy, IT Governance Security Policy
Procedures: SOPs and Work Instructions
Structure: Director, IT Manajement, IT Internal Staff
Culture : Digital Transformation, Industrial Revolution 4.0
Processes : Blockchain Governance at SmartCo
Technology
IT Services, Infrastructure, and Applications: Digital Transformation Technologies, SmartCo Internal Applications
Information: Official Documents on Governance Design
Business Value
Development/Build
Concepts: COBIT 2019 and COBIT 2019 DevOps
Artifacts: Design Factors, 7 IT Governance Components, Blockchain Governance Design Recommendations
Evaluate
Determine
Justify / Evaluate
Case Study : SmartCO
Quality: Credibility, Transferability, Dependability, Confirmability
Applicable Knowledge
Foundation
Theories: Governance, Digital Transformation, Agile IT Governance, Information Technology, Ambidexterity, Emerging Technology, Blockchain
Framework : COBIT 2019 and COBIT 2019 DevOps
Methodologies
Research Strategy: Design Science Research (DSR), Case Study
Data Collection: Semi-structured Interviews, Assessments
Data Analysis: Content Analysis
Application in the Appropriate Environmnent
Additions to the Knowledge Base

Figure 1. Conceptual Model
Source: adapted from [37]

As seen in Figure 1, this study began with the problem identification stage, which aimed to understand SmartCo's needs in building blockchain governance as it seeks to carry out its digital transformation. This initial understanding was obtained through a literature review to map relevant challenges. Next, in the design and development stage, data was collected from various sources, including interviews, company documents, national regulations, scientific literature, and references from the framework COBIT 2019, traditional, and DevOps. The data was used to determine relevant design factors and run a multi-criteria prioritization process to select the main governance objectives to focus on. Thereafter, an assessment of the existing conditions and targets of these objectives was carried out, followed by a gap analysis and the design of an ambidextrous governance model that included aspects of people, process, and technology. As part of the DSR cycle, the demonstration and evaluation phase was also carried out by preparing an implementation roadmap and estimating the impact of the resulting design on blockchain governance readiness at SmartCo. This entire research process is embedded within a case study framework. The case study methodology was selected based on the principles outlined by Yin (2009) [38], which offers a robust framework for an in-depth investigation of a contemporary issue, such as governance design, within its real-life operational context. This approach is particularly effective for addressing explanatory "how" and "why" research inquiries, thus making it ideal for a detailed exploration of the specific context and mechanisms through which SmartCo can develop and apply an ambidextrous blockchain governance model.

Research Process

This research process follows the DSR approach, which consists of five main stages, namely problem identification, requirement specification, design and development, demonstration, and evaluation, as shown in Figure *2*. Each stage is designed to build a structured and applicable governance solution according to the context of a digital organization [37].



Problem Identification

1. Identifying issues related to Blockchain governance at SmartCo
2. Defining the research problem
3. Defining the research objectives
4. Determining the scope and limitations of the study

Requirement Specification

1. Preparing and conducting semi-structured interviews
2. Determining key Governance and Management Objectives (GMO) to prioritize
3. Evaluating governance performance through the seven capability elements of COBIT 2019
4. Conducting gap analysis between current and expected maturity levels
5. Developing preliminary recommendations based on People, Process, and Technology aspects

Design and Development

1. Assessing resources, potential risks, and expected value (RRV)
2. Developing a governance model based on the Ambidextrous COBIT 2019 approach tailored for Blockchain
3. Creating recommendations to enhance governance practices

Demonstration

1. Developing an implementation roadmap
2. Analyzing the potential impact of the proposed recommendations

Evaluation

Validating the artifact through five qualitative criteria:

- Credibility
- Transferability
- Dependability
- Confirmability

Figure 2. Research Process
Source: adapted from [37]

Figure 2 illustrates the research flow that runs systematically, starting from the problem identification stage to the final evaluation of the developed design. The process sequentially carries out the formulation of needs, compilation of a governance model, and demonstration through the preparation of an implementation roadmap. The evaluation stage is carried out by considering a number of important aspects, such as credibility, transferability, consistency, and confirmability, to ensure that the resulting solution can not only be applied practically but also has a strong scientific basis [39]. Data collection was conducted through semi-structured interviews with six internal representatives who have strategic roles in IT management and digital transformation. Details of respondents and discussion topics are summarized in Table 1.

Table 1. Profile of Primary Data Respondents Source

Respondence	Position	Discussion Summary
Responden 1 (R1)	Chief Executive Officer	Discussed the introduction of the research topic, IT governance, and the state of emerging technologies within the company.
Responden 2 (R2)	Manager IT Architecture	Explained IT governance practices and the use of emerging technologies in the company's operations.
Responden 3 (R3)	IT Internal Staff	Further discussing the current state of IT governance from an operational and internal execution perspective.
Responden 4 (R4)	Subdivision of Research and Technology	Discussed company governance for assessment purposes from a research and technology perspective.
Responden 5 (R5)	Application Services Division	Discussed company governance for assessment purposes concerning application services.
Responden 6 (R6)	SmartCo Operations Application Division	Discussed company governance for assessment purposes from an application operations viewpoint.

Based on Table 1, the primary data were obtained from six respondents who were selected as key informants representing strategic areas relevant to blockchain governance, ensuring that the perspectives collected are directly aligned with organizational decision-making and implementation readiness. In addition to primary data, this study also uses secondary data in the form of internal company documents. Table 2 shows a list of documents used as secondary data to support the validation and contextualization of the designed governance model.

Table 2. Secondary Data

Secondary Data	Description
SmartCo Annual Report 2023	A comprehensive overview of SmartCo's achievements and key developments throughout the year.
Corporate Governance Guideline	A document outlining the core governance principles and practices that guide how SmartCo is managed and controlled.
Sustainability Report 2023	An account of SmartCo's efforts and performance in environmental, social, and governance (ESG) areas during the 2023 fiscal year.
SmartCo Code of Ethics	A set of ethical standards and behavioral expectations that every member of the SmartCo organization is required to uphold.

Table *2*. Secondary Data illustrates the secondary data collection method, known as document triangulation, that underpins the interview results. The overall data collection process was iterative, following the principles of achieving data saturation, a point where new data no longer generates new insights [40]. Initial interviews were conducted with a core group of stakeholders to gather foundational knowledge. The data from these sessions were transcribed and thematically analyzed to identify preliminary themes and areas for deeper exploration. Based on this initial analysis, subsequent interviews were scheduled with other stakeholders to either confirm, challenge, or expand upon the emerging themes. This cycle of data collection and concurrent analysis continued until no new significant concepts or categories emerged from the final interviews, indicating that data saturation had been reached. To further enhance credibility, the findings from the saturated interview data were then confirmed and strengthened through document triangulation using the secondary data sources listed in Table *2*. This process ensures a robust and validated dataset for the subsequent analysis.

Criteria for GMO Prioritization

In this study, to identify the most critical governance areas for SmartCo in preparing for blockchain adoption, a structured prioritization of COBIT 2019 Governance and GMOs was carried out. This prioritization was based on four key assessment dimensions, each offering a distinct but complementary perspective. These include alignment with the organization's internal context and design factors, relevance to modern DevOps practices, conformity with national regulatory frameworks, and support from previous academic studies. The qualitative assessment was conducted using the COBIT 2019 Design Toolkit, and the scoring process was tabulated and analyzed with Microsoft Excel. This multi-perspective approach was selected to ensure that the chosen GMOs are not only strategically aligned but also contextually grounded, compliant with policy, and supported by credible research. Table 3 below outlines these four assessment aspects and provides a concise description of the evaluation scope for each.

Table 3. Priority Aspect

Priority Aspect	Description
COBIT 2019 Design Factor	This process involves evaluating how well each GMO aligns with the organization's internal characteristics, its digital transformation goals, and the expectations of key stakeholders.
COBIT 2019 DevOps Focus Area	This aspect evaluates the extent to which each GMO supports DevOps principles based on the relevance categorization of primary, secondary, and general.
Regulations	The assessment is carried out on the relevance of each GMO to the provisions in the Regulation of the Minister of ICT Minister No.5/2021 and the SOE Ministerial No. PER-2/MBU/03/2023 [41], [42].
Previous Research	Previous research was used as a reference to identify GMOs that have proven relevant in the context of blockchain governance [7],[18], [19]

Table 3 outlines the core aspects used in the prioritization process, namely organizational design factors, COBIT 2019 DevOps relevance, national regulatory alignment, and support from previous academic research. These criteria were selected to ensure a comprehensive assessment that aligns with the organization's internal context, reflects current technology trends and implementation agility, complies with applicable national and sectoral requirements, and incorporates validated insights from existing scholarly works.

Capability Assessment Method

This study applies the COBIT 2019 capability rating method, which expresses achievement in varying degrees of ratings [22]. The following Table 4 presents the rating system adopted from COBIT to assess capability levels.

Table 4. Capability level value

Achievement	Level
0% - 14%	Not Achieved (N)
15% - 50%	Partially (P)
51% - 85%	Largely (L)
86% - 100%	Fully (F)

Source: adapted from [22]

The capability levels defined in Table 4 above namely Not Achieved (N) for 0% - 14% achievement, Partially (P) for 15% - 50%, Largely (L) for 51% - 85%, and Fully (F) for 86% - 100% are then used to map the actual condition of each management practice within the assessed Governance and Management Objective (GMO) [22]. The results of this capability level mapping become a fundamental basis for conducting a gap analysis between the current state and the target capability levels expected by SmartCo, as well as for formulating relevant improvement recommendations.

RESULTS AND DISCUSSIONS

Priority Objective Analysis Results

A prioritization analysis of Governance and Management Objectives (GMOs) was conducted to identify the most relevant governance focus for SmartCo. This process evaluated various GMOs based on several crucial aspects previously identified, including organizational design factors, relevance to COBIT 2019 DevOps, alignment with national regulations (ICT Minister No.5/2021 and SOE Ministerial No. PER-2/MBU/03/2023), and support from previous research. The final score for each GMO was determined by calculating the average of its scores across all priority components, where each component was assessed for its relevance and impact. The following Table 5 displays the final scored results of this prioritization analysis.

Table 5. GMO Prioritization Result

GMO	ICT Minister No.5/2021	SOE Minister PER-2/MBU/03/2023	Design Factor	COBIT 2019 DevOps	Block-chain Paper 1	Block-chain Paper 2	Block-chain Paper 3	Final Score
DSS05 - Managed Security Services	100	100	90	67	100	100	100	94

Based on the prioritization analysis results presented in Table 5, it is evident that DSS05 (Managed Security Services) achieved the highest final score of 94. This top score indicates that DSS05 is the most crucial and relevant governance area for enhancement at SmartCo in the context of preparing for blockchain technology adoption. Therefore, DSS05 was selected as the primary GMO to be the focus for in-depth analysis and the design of the ambidextrous governance model in this study.

Gap Analysis Result

The Gap Analysis Result section is derived by analyzing the selected GMO, against the seven COBIT 2019 governance components. The following Table 6 presents the current capability level assessment results for each management practice within the Process component of DSS05 at SmartCo.

Table 6. Process Component

Management Practice	Achievement	Capability Level
DSS05 - Managed Security Services		
DSS05.01 Protect against malicious software.	100% (Fully)	2
	92% (Fully)	3
	100% (fully)	4
DSS05.02 Manage network and connectivity security.	88% (Fully)	2
	71% (Largely)	3
	50% (Partially)	4
DSS05.03 Manage endpoint security.	94% (Fully)	2
	100% (Fully)	3
	100% (Fully)	4
DSS05.04 Manage user identity and logical access.	100% (Fully)	2
	94% (Fully)	3
	100% (Fully)	4
DSS05.05 Manage physical access to I&T assets.	100% (Fully)	2
	100% (Fully)	3
	100% (Fully)	4
DSS05.06 Manage sensitive documents and output devices.	100% (Fully)	2
	88% (Fully)	3
	50% (Partially)	4
DSS05.07 Manage vulnerabilities and monitor the infrastructure for security-related events.	100% (Fully)	2
	100% (Fully)	3

The analysis results in Table 6 indicate gaps in several DSS05 Process component practices, for instance, DSS05.02 and DSS05.06. The analysis continues by examining the Organization Structure component. Table 7 presents the detailed assessment of the current state of the Organization Structure component at SmartCo.

Table 7. Organization Structure Component

Organization Structure	GMO	Current State
Chief Information Officer	DSS05	Director of IT Services - lead and manage company-wide IT strategy, information systems development, and service innovation.
Chief Information Security Officer	DSS05	IT Security and Architecture unit under the Directorate of IT Services - security responsibilities including cybersecurity strategy, ISO 27001 implementation, vulnerability scanning, and incident response
Business Process Owners	DSS05	In SmartCo's organizational structure, each division and directorate has its own Head of Department or Division responsible for its respective business operations. These roles are accountable for the performance of business processes, including aligning service reliability and security with company goals.
Head Human Resources	DSS05	Director of Human Capital Management and Administration - oversees all HR-related functions at SmartCo, including employee development, training, and organizational support.
Head Development	DSS05	Research and Technology Division - responsible for driving system and application development. Within the Directorate of IT Services, internal development teams manage end-to-end software projects, from design to implementation.
Head IT Operations	DSS05	The head of IT operations is functionally handled by the Information Systems Division and the Infrastructure Operations unit under the Directorate of IT Services. These units are responsible for ensuring the availability, stability, and secure operation of IT services.
Information Security Manager	DSS05	Information Technology & Security Architecture - his unit oversees ISO 27001 implementation, cybersecurity maturity, threat detection, and system protection.
Privacy Officer	DSS05	Legal, Risk Management, and Compliance - The responsibility for data privacy and compliance with the Personal Data Protection Law (Law No. 27/2022).
Product Owner/Manager	DSS05	Product Development for Connectivity and Infrastructure Division - This division is responsible for designing and delivering product-based digital services.
Software Development Manager	DSS05	Information Technology Systems Division - This unit handles application development and technology research. It fully covers the scope of software lifecycle management, including tool standardization and development oversight.
Testing Manager	DSS05	SmartCo has not yet established a formal role or division dedicated to system or application testing.
Systems Operations Manager	DSS05	Information Technology Systems Division - this division oversees internal IT operations and system support.
Release Manager	DSS05	Information Technology Systems Division - this division at SmartCo plays a crucial role in handling the internal release of IT services and systems.
Automation Manager	DSS05	Automation functions exist, but no formal or structural position specifically handles automation.
Systems Architecture Manager	DSS05	IT Architecture and Security Subdivision - manages architectural design, system structure, and security alignment.

The assessment in Table 7 indicates that while SmartCo has various key roles to support DSS05, structural gaps were identified, such as the absence of formal roles for a Testing Manager and an Automation Manager. Gap analysis continues by examining the Information component. The following Table 8 presents the details of relevant information outputs from DSS05 management practices, along with their current availability and status at SmartCo.

Table 8. Information Component

Management Practice	Information Output	Current State
DSS05: Managed Security Services		
DSS05.01 Protect against malicious software.	Malicious software prevention policy	Network and endpoint security SOPs are in place.
	Evaluations of potential threats	Threat monitoring is performed by the SOC.
DSS05.02 Manage network and connectivity security.	Connectivity security policy	Interconnection security standards for the Internet and internal network are available.
	Results of penetration tests	Penetration testing has been conducted by SmartCo's IT security team, although report access is limited to specific units.
DSS05.03 Manage endpoint security.	Security policies for endpoint devices	Endpoint protection procedures are documented in internal SOPs, and all laptops connected to the corporate network must have Sophos antivirus installed.
DSS05.04 Manage user identity and logical access.	Results of reviews of user accounts and privileges	Access management is supported by documentation for user provisioning and deprovisioning.
	Approved user access rights	Access rights are controlled through policies governing system and information access.
DSS05.05 Manage physical access to I&T assets.	Description	Physical security procedures are defined for key hardware and facilities.
	Access logs	Access to IT facilities is documented through manual or electronic logs.
	Approved access requests	Physical access approvals are handled through internal authorization workflows.
DSS05.06 Manage sensitive documents and output devices.	Access privileges	Access control to sensitive documents is managed through internal security procedures and privileged access policies.
	Inventory of sensitive documents and devices	Sensitive documents and devices are recorded in an internal inventory maintained by relevant divisions.
DSS05.07 Manage vulnerabilities and monitor the infrastructure for security-related events.	Security incident tickets	Security incidents are recorded and handled through the internal incident response mechanism.
	Security incident characteristics	Characteristics of incidents are identified during analysis and documented in internal follow-up reports.
	Security event logs	Security event logging is supported by SOC operations and infrastructure monitoring systems.

Table 8 indicates that DSS05 information outputs are generally available, though access limitations exist for some reports. Next, an analysis will be conducted on the People, Skills, and Competencies component. The following Table 9 presents an assessment of the state of this component at SmartCo in the context of supporting DSS05.

Table 9. People, Skills, and Competencies Component

Skills	Current State
Information security	SmartCo has conducted internal training and ISO/IEC 27001 certification related to information security.
Information security management	The Information Security Architecture team is responsible for implementing ISMS guidelines and overseeing information security compliance based on internal procedures.
Penetration testing	SmartCo has demonstrated competence in information security management through ISO 27001 Lead Auditor and CISM preparation.
Security administration	SmartCo's SOC team and the IT Operations Division manage infrastructure access, endpoint protection, and internal threat response.

Table 9 shows that SmartCo has a good foundation of skills and competencies in information security, evidenced by internal training and ISO/IEC 27001 certification. The effectiveness of these competent human resources is greatly supported by clear and documented principles, policies, and procedures. Next, an analysis will be conducted on the Principles, Policies, and Procedures component. Table 10 outlines the state of relevant policies that have been established and implemented at SmartCo.

Table 10. Principles, Policies, and Procedures Component

Relevant Policy	Current State
Information security policy	SmartCo has established an information security policy that covers IT governance, access restrictions, user authentication, password protection, and ISO 27001 standardization. This policy is supported by endpoint security procedures, user training, incident handling, and internal SOPs.

Table 10 shows that SmartCo has an information security policy that supports various aspects of DSS05. However, the success of implementing these policies and procedures also depends heavily on how culture, ethics, and behavior are enforced within the organization. Next, the analysis will be conducted on the Culture, Ethics, and Behavior components. Table 11 describes key cultural elements related to security and the efforts of SmartCo.

Table 11. Culture, Ethics, and Behavior Component

Key Culture Elements	Current State
Create a culture of awareness regarding user responsibility to maintain security and privacy practices.	SmartCo has conducted regular training sessions on information security awareness and campaigns as part of ISO 27001 implementation. These include internal communications about secure behavior, protection of personal data, and user responsibility in accessing company systems and information.

From Table 11, it is evident that SmartCo actively endeavors to foster a security-aware culture through regular training and campaigns as part of its ISO 27001 implementation. Next, in Table 12, an analysis will be conducted on the Service, Infrastructure, and Application components.

Table 12. Service, Infrastructure, and Application Component

Service, Infrastructure, and Application	Current State
Directory services	Implemented through biometric access systems integrated in data center operations.
Email filtering systems	Has deployed an effective email filtering solution designed to protect the network from various cyber threats.
Identity and access management system	Identity and access are secured using biometric, SSO, and password controls, aligned with ISO 27001.
Security awareness services	Continuous awareness programs are conducted for employees and customers regarding cybersecurity and data protection.
Security information and event management (SIEM) tools	SmartCo does not have SIEM tools yet.
Security operations center (SOC) services	SOC in operation, actively monitoring and managing cyber threats as part of CSM implementation.
Third-party security assessment services	Third-party audits performed, including ISO 27001, 27017, and 27018 certifications.
URL filtering systems	Internet and network interconnection security standards.

Potential Improvement

Based on the gap analysis results for the seven DSS05 governance components previously presented, several areas requiring improvement have been identified. These improvements are considered critical to closing the existing capability gaps, strengthening network and endpoint security controls, and ensuring that SmartCo's blockchain adoption is supported by robust governance mechanisms aligned with regulatory and operational requirements. The following Table 13 summarizes these identified gaps along with potential improvements that can be made, categorized by people, process, and technology aspects.

Table 13. Potential Improvement

Component	Gap	Type	Potential Improvement
People Aspect			
Organization Structure	SmartCo has not yet defined formal roles for system testing and automation functions within its organizational structure.	Roles, Responsibilities	Establish dedicated roles for Testing Manager and Automation Manager to ensure the governance of secure and automated deployment processes, which are critical in the implementation of blockchain-based systems.
Process Aspect			
Process	Security testing is only partially integrated into the development pipeline; some secure configurations remain manual.	Procedure	Integrate automated security testing tools into the CI/CD pipeline and standardize secure configuration procedures.
Process	Sensitive document control lacks automated access management and audit trail mechanisms.	Policy	Develop document security policies with role-based access control and automated logging systems for sensitive outputs.
Technology Aspect			
Service, Infrastructure, and Application	SmartCo does not have SIEM tools yet.	Tools	Adding Security Information and Event Management (SIEM) tools that function to manage security information and events (security incidents) that occur in an organization's IT environment.

The potential improvements identified in Table 13, such as establishing new roles, standardizing procedures, developing policies, and adopting new tools, serve as crucial input for designing more detailed governance solutions.

Resource, Risk, and Value Analysis

After various potential improvements were identified, the next step is to determine the implementation priority for each of these proposals. For this purpose, a Resource, Risk, and Value (RRV) analysis was conducted to evaluate the feasibility and impact of each improvement. Each potential improvement was assessed against RRV criteria, and each was scored on a 1-5 scale. The final priority score was calculated as (Value Score) / (Resource Score + Risk Score), with higher scores indicating higher priority. The following Table 14 presents the results of this RRV analysis.

Table 14. RRV Analysis

Potential Improvement	Final Score	Category
Establish dedicated roles for Testing Manager and Automation Manager to ensure the governance of secure and automated deployment processes, which are critical in the implementation of blockchain-based systems.	18	Medium
Develop document security policies with role-based access control and automated logging systems for sensitive outputs.	18	Medium
Integrate automated security testing tools into the CI/CD pipeline and standardize secure configuration procedures.	12	Medium
Adding Security Information and Event Management (SIEM) tools that function to manage security information and events (security incidents) that occur in an organization's IT environment.	8	Low

The RRV analysis results presented in Table 14 show the final scores and priority categories for each potential improvement. For instance, establishing new roles for Testing and Automation Managers and developing document security policies are categorized as Medium with a score of 18, while adding SIEM tools is categorized as Low with a score of 8. The low score for SIEM tools reflects their high resource and cost requirements relative to the immediate benefits, as well as the fact that SmartCo's existing security monitoring already covers basic detection functions, making SIEM implementation less urgent compared to other improvements.

Implementation Roadmap

The following Table 15 presents this recommended implementation roadmap, covering people, process, and technology aspects.

Table 15. Implementation Roadmap

Initiative	2025				2026			
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
People Aspect								
Establish dedicated roles for Testing Manager and Automation Manager to ensure the governance of secure and automated deployment processes, which are critical in the implementation of blockchain-based systems.				▨				
Process Aspect								
Develop document security policies with role-based access control and automated logging systems for sensitive outputs.					▨			
Integrate automated security testing tools into the CI/CD pipeline and standardize secure configuration procedures.						▨		
Technology Aspect								
Adding Security Information and Event Management (SIEM) tools that function to manage security information and events (security incidents) that occur in an organization's IT environment.						▨		

The implementation roadmap presented in Table 15 outlines the planned execution phases for each improvement initiative, such as establishing new roles, developing policies, integrating testing tools, and adding SIEM tools over two years (2025-2026). The systematic execution of this roadmap is expected to gradually and measurably enhance SmartCo's security governance capabilities in preparation for blockchain technology adoption. However, the success of the roadmap is contingent on sustained executive support, adequate budget allocation, and continuous alignment with evolving regulatory requirements.

Recommendations Impact

Table 16 specifically shows the estimated quantitative impact of these design recommendations on the capability levels of each management practice within the DSS05 Process component.

Table 16. Estimation Impact of Design Recommendations on Process Components

Management Practice	Previous Capability Level	Estimated Capability Level
DSS05 - Managed Security Services		
DSS05.01 Protect against malicious software.	4	4
DSS05.02 Manage network and connectivity security.	2	4
DSS05.03 Manage endpoint security.	4	4
DSS05.04 Manage user identity and logical access.	4	4
DSS05.05 Manage physical access to I&T assets.	4	4
DSS05.06 Manage sensitive documents and output devices.	2	4
DSS05.07 Manage vulnerabilities and monitor the infrastructure for security-related events.	3	3
Average Capability	**3.29**	**3.86**

Table 16 indicates that the implementation of the proposed recommendations is projected to significantly increase the average capability of the DSS05 Process component, from 3.29 to 3.86. The positive impact of these improvement recommendations is not limited to the Process component alone. Table 17 presents a comparison of the before and after implementation states for the People, Process, and Technology aspects.

Table 17. Estimation Impact of Other Governance Components

Before Implementation State	After Implementation State
People Aspect	
No formal roles for Testing Manager and Automation Manager	Roles for Testing and Automation are established within the IT division.
Process Aspect	
No policies to secure sensitive documents	Document policies with access control and an audit trail implemented
No standard testing procedures in CI/CD	
	Security testing is integrated into DevOps using automated tools.
Technology Aspect	
Do not have tools related to Security Information and Event Management (SIEM)	SIEM tool deployed to monitor blockchain-related infrastructure

Table 17 illustrates how the proposed recommendations are expected to more broadly transform the state of DSS05 governance at SmartCo. Estimated significant changes include the establishment of new roles such as Testing and Automation Managers in the people aspect, the implementation of document security policies and integrated security testing in the process aspect, and the adoption of new technology tools like SIEM in the technology aspect. Overall, this indicates a potential for a holistic improvement in the readiness and maturity of DSS05 governance.

Discussion

The findings of this study reveal a critical institutional challenge confronting a technology-intensive enterprise like SmartCo. The evidence gathered from SmartCo affirms that conventional, control-centric security frameworks are often too rigid to accommodate the iterative nature of technologies like blockchain. Conversely, unstructured agile practices frequently neglect the robust security assurances required in a high-stakes operational environment. This research addresses such issues by designing an ambidextrous governance model that synthesizes the structural discipline of COBIT 2019 Traditional with the adaptive capabilities of its DevOps Focus Area, tailored specifically for the pre-implementation security of blockchain.

Examining SmartCo's institutional context more closely exposes a structural disconnect that explains the limitations of its current security governance. The empirical results confirm established challenges, such as process weaknesses in managing network connectivity (DSS05.02) and the absence of a SIEM system, which align with literature indicating that legacy security struggles to address the novel risks of emerging technologies. However, this study offers a more nuanced insight: the absence of formalized roles for a Testing Manager and an Automation Manager within the security governance framework. It reveals a structural inability to embed security controls into agile development pipelines, creating a tangible barrier between the organization's innovation goals and its security requirements. While traditional COBIT provides top-down control, it can lack real-time responsiveness. DevOps, by contrast, promotes iterative collaboration but risks fragmented security oversight without embedded governance. The proposed ambidextrous paradigm reconciles these opposing forces by formalizing adaptive roles and integrating automated controls, framing governance as a dynamic architecture sensitive to both institutional reality and technological evolution.

Positioned within the broader academic discourse on blockchain governance, this study advances the conversation by transforming abstract principles into a concrete, operational framework. A significant portion of existing literature addresses blockchain governance at a conceptual level, focusing on decentralization theory, public sector applications, or post-implementation challenges. This often leaves a gap for private enterprises seeking actionable guidance, particularly at the critical pre-implementation stage. This research bridges that gap by operationalizing ambidextrous governance for a specific, high-stakes security objective (DSS05). Its practical value resides in its ability to translate the abstract need for balancing control and agility into specific, auditable mechanisms, formalizing new security-oriented roles, standardizing security procedures, and integrating automated security testing into the CI/CD pipeline. This reflects the need to embed security governance within agile pipelines rather than overlaying it afterward, ensuring that security evolves with development processes. By embedding these ambidextrous mechanisms into the seven COBIT governance components, this study offers a replicable model that resolves the persistent tension between regulatory-style stability and technological dynamism.

The main theoretical contribution of this study is showing how to create and test a dual-mode governance framework that aims to secure technology before it is widely used. This approach redefines security governance not as a reactive control function, but as a strategic enabler of responsible innovation. The study's novelty is further enhanced by the multi-criteria prioritization method, which provides a structured, evidence-based approach to identifying critical governance areas, thus reducing the ambiguity often associated with such initiatives. The resulting artifact, a detailed, component-based governance design for DSS05, complete with a roadmap and impact estimation, serves as a tangible contribution to the IT governance body of knowledge. It confirms that an ambidextrous approach is not merely a strategic concept but an implementable solution that can build institutional resilience and enable secure, innovation-oriented digital transformation.

CONCLUSION

This study designed an ambidextrous COBIT 2019 traditional and DevOps-based governance model centered on DSS05 (Managed Security Services) to strengthen SmartCo's security readiness in adopting blockchain technology. Through an innovative multi-criteria prioritization technique that synthesizes organizational design factors, COBIT 2019 DevOps relevance, an analysis of national regulations, and previous academic studies, DSS05 was identified as the most crucial Governance and Management Objective (GMO). The resulting governance design includes the seven COBIT 2019 governance components for DSS05, detailed in people, process, and technology aspects with ambidextrous best practices, and is outlined in a strategic implementation roadmap. A significant impact of this research for SmartCo is the projected increase in the security governance capability for DSS05 from an average of 3.29 to 3.86, which substantially enhances the company's preparedness for future blockchain initiatives. Additionally, this study contributes to the IT governance knowledge base by presenting a practical model for pre-implementation blockchain security governance, specifically through the application of the ambidextrous COBIT 2019 approach to DSS05 and a comprehensive GMO prioritization technique in the context of new technologies. Overall, the proposed ambidextrous COBIT 2019 traditional and DevOps-based blockchain governance strengthens SmartCo's readiness for secure blockchain adoption and provides a structured, replicable framework for other technology-intensive enterprises navigating digital transformation. However, this study focuses on a single organization and a single Governance and Management Objective (DSS05), which may limit the generalizability of its findings. Future research could extend the model's application to multiple organizations, sectors, and governance domains to validate and refine its broader applicability.

REFERENCES

[1] R. Mulyana, L. Rusu, and E. Perjons, “IT governance mechanisms influence on digital transformation: A systematic literature review,” *27th Annual Americas Conference on Information Systems, AMCIS 2021*, pp. 0–10, 2021.

[2] É. Marcon, M. A. Le Dain, and A. G. Frank, “Designing business models for Industry 4.0 technologies provision: Changes in business dimensions through digital transformation,” *Technol Forecast Soc Change*, vol. 185, p. 122078, Dec. 2022, doi: 10.1016/J.TECHFORE.2022.122078.

[3] S. Kraus, P. Jones, N. Kailer, A. Weinmann, N. Chaparro-Banegas, and N. Roig-Tierno, “Digital Transformation: An Overview of the Current State of the Art of Research,” *Sage Open*, vol. 11, no. 3, 2021, doi: 10.1177/21582440211047576.

[4] M. Sprajcer *et al.*, “How effective are Fatigue Risk Management Systems (FRMS)? A review,” *Accid Anal Prev*, vol. 165, no. August 2021, p. 106398, 2022, doi: 10.1016/j.aap.2021.106398.

[5] SmartCo, “Annual Report,” p. 9, 2023.

[6] F. Lumineau, W. Wang, and O. Schilke, “Blockchain governance-A new way of organizing collaborations?,” *Organization Science*, vol. 32, no. 2, pp. 500–521, 2021, doi: 10.1287/orsc.2020.1379.

[7] R. van Pelt, S. Jansen, D. Baars, and S. Overbeek, “Defining Blockchain Governance: A Framework for Analysis and Comparison,” *Information Systems Management*, vol. 38, no. 1, pp. 21–41, 2021, doi: 10.1080/10580530.2020.1720046.

[8] M. Javaid, A. Haleem, R. Pratap Singh, S. Khan, and R. Suman, “Blockchain technology applications for Industry 4.0: A literature-based review,” *Blockchain: Research and Applications*, vol. 2, no. 4, p. 100027, 2021, doi: 10.1016/j.bcra.2021.100027.

[9] “IDC estimates $19 billion global spending on blockchain solutions in 2024 The Block.” Accessed: Aug. 13, 2025. [Online]. Available: https://blockchaintechnology-news.com/news/idc-estimates-19-billion-global-spending-on-blockchain-solutions-in-2024/

[10] “Digital Transformation Market to Record CAGR of 22% by 2032.” Accessed: Aug. 13, 2025. [Online]. Available: https://www.fortunebusinessinsights.com/press-release/global-digital-transformation-market-10744

[11] D. B. Rawat, V. Chaudhary, and R. Doku, “Blockchain Technology: Emerging Applications and Use Cases for Secure and Trustworthy Smart Systems,” *Journal of Cybersecurity and Privacy*, vol. 1, no. 1, pp. 4–18, 2020, doi: 10.3390/jcp1010002.

[12] A. Razzaq *et al.*, “Use of Blockchain in governance: A systematic literature review,” *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 5, pp. 685–691, 2019, doi: 10.14569/ijacsa.2019.0100585.

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

[14] H. Hietala and T. Päivärinta, “Governing collective ambidexterity: Antecedents, mechanisms, and outcomes in digital service ecosystems,” *Gov Inf Q*, vol. 42, no. 1, 2025, doi: 10.1016/j.giq.2024.102001.

[15] R. Mulyana, L. Rusu, and E. Perjons, “IT Governance Mechanisms that Influence Digital Transformation : A Delphi Study in Indonesian Banking and Insurance Industry,” pp. 1–16, 2022.

[16] J. Magnusson, D. Koutsikouri, and T. Päivärinta, “Efficiency creep and shadow innovation: enacting ambidextrous IT Governance in the public sector,” *European Journal of Information Systems*, vol. 29, no. 4, pp. 329–349, 2020, doi: 10.1080/0960085X.2020.1740617.

[17] R. Mulyana, *IT Governance Influence on Digital Transformation*, no. 25. 2025.

[18] G. Laatikainen, M. Li, and P. Abrahamsson, “A system-based view of blockchain governance,” *Inf Softw Technol*, vol. 157, no. April 2022, p. 107149, 2023, doi: 10.1016/j.infsof.2023.107149.

[19] E. Tan, S. Mahula, and J. Crompvoets, “Blockchain governance in the public sector: A conceptual framework for public management,” *Gov Inf Q*, vol. 39, no. 1, p. 101625, 2022, doi: 10.1016/j.giq.2021.101625.

[20] C. Reyes and J. Cutler, “Ready Layer One: Functional Regulation for Blockchain Infrastructure,” pp. 1–39, 2025.

[21] Y. Liu, Q. Lu, G. Yu, H. Y. Paik, and L. Zhu, “Defining blockchain governance principles: A comprehensive framework,” *Inf Syst*, vol. 109, p. 102090, Nov. 2022, doi: 10.1016/J.IS.2022.102090.

[22] ISACA, *Introduction and methodology*. 2019. doi: 10.4324/9780203937600.

[23] ISACA, *COBIT Focus Area: DevOps*. 2021.

[24] I. Hamzane and B. Abdessamad, “A built-in criteria analysis for best IT governance framework,” *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 10, pp. 185–190, 2019, doi: 10.14569/ijacsa.2019.0101026.

[25] N. Tonpe, J. Bachher, R. Mane, S. Udanshiv, A. H. Patil, and Prof. S. Pawar, “BLOCKCHAIN EMERGING TECHNOLOGY,” International Research Journal of Modernization in Engineering Technology and Science. Accessed: Oct. 19, 2024. [Online]. Available: https://www.researchgate.net/publication/362517787_BLOCKCHAIN_EMERGING_TECHNOLOGY#full-text

[26] K. Werbach, “Blockchain Governance,” *The Blockchain and the New Architecture of Trust*, pp. 133–148, 2019, doi: 10.7551/mitpress/11449.003.0012.

[27] 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,” *Proceedings of the 31st International Conference on Information Systems Development*, 2023, doi: 10.62036/isd.2023.33.

[28] P. K. Senyo, S. Karanasios, E. Komla Agbloyor, and J. Choudrie, “Government-Led digital transformation in FinTech ecosystems,” *Journal of Strategic Information Systems*, vol. 33, no. 3, p. 101849, 2024, doi: 10.1016/j.jsis.2024.101849.

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

[30] ISACA, *Governance and Management Objectives*. 2019.

[31] P. C. Verhoef *et al.*, “Digital transformation: A multidisciplinary reflection and research agenda,” *J Bus Res*, vol. 122, no. September 2019, pp. 889–901, 2021, doi: 10.1016/j.jbusres.2019.09.022.

[32] D. Plekhanov, H. Franke, and T. H. Netland, “Digital transformation: A review and research agenda,” *European Management Journal*, vol. 41, no. 6, pp. 821–844, 2023, doi: 10.1016/j.emj.2022.09.007.

[33] C. Gong and V. Ribiere, “Developing a unified definition of digital transformation,” *Technovation*, vol. 102, Apr. 2021, doi: 10.1016/J.TECHNOVATION.2020.102217.

[34] M. Rossi, C. Mueller-Bloch, J. B. Thatcher, and R. Beck, “Blockchain research in information systems: Current trends and an inclusive future research agenda,” *J Assoc Inf Syst*, vol. 20, no. 9, pp. 1388–1403, 2019, doi: 10.17705/1jais.00571.

[35] H. A. Nahi *et al.*, “Blockchain Network for Regulation Decentralized E-Government Systems,” *Data and Metadata*, vol. 4, no. February, 2025, doi: 10.56294/dm2025201.

[36] F. Casino, T. K. Dasaklis, and C. Patsakis, “A systematic literature review of blockchain-based applications: Current status, classification and open issues,” *Telematics and Informatics*, vol. 36, no. May 2018, pp. 55–81, 2019, doi: 10.1016/j.tele.2018.11.006.

[37] A. R. Hevner, S. T. March, J. Park, and S. Ram, “Design Sceince in Information Systems,” *MIS Quarterly*, vol. 28, no. 1, pp. 75–105, 2004.

[38] R. Yin, “How to do better case studies. The SAGE handbook of applied social research methods,” *The SAGE Handbook of Applied Social Research Methods*, pp. 254–282, 2009, doi: 10.4135/9781483348858.n8.

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

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

[41] Permen BUMN, “Peraturan Menteri Badan Usaha Milik Negara Pedoman Tata kelola dan Kegiatan Korporasi Signifikan Badan Usaha Milik Negara,” *Berita Negara RI*, vol. No. 262, no. 262, p. 144, 2023.

[42] Kominfo, “Peraturan Menteri KomIunikasi dan Informartikan Indonesia Nomor 5 Tahun 2021,” *Peraturan Menteri KomIunikasi dan Informartikan Indonesia Nomor 5 Tahun 2021*, vol. 151, no. 2, p. 133, 2021.