

# Ambidextrous AI Governance for Driving SmartCo's Digital Transformation Using COBIT 2019 Traditional and DevOps

Octamevia Inkaputri Azzahra<sup>1</sup>, Rahmat Mulyana<sup>2</sup>, Taufik Nur Adi<sup>3</sup>

<sup>1,3</sup>Information System, Faculty of Industrial Engineering, Telkom University, Indonesia

<sup>2</sup>Department of Computer and Systems Sciences, Stockholm University, Sweden

## Article Info

### Article history:

Received Jun 23, 2025

Revised Jul 22, 2025

Accepted Oct 29, 2025

### Keywords:

Ambidextrous AI Governance

Digital Transformation

COBIT 2019

Design Science Research

Case Study

## ABSTRACT

Artificial Intelligence (AI) plays a vital role in accelerating digital transformation within the technology sector. This study investigates SmartCo, a technology company seeking to enhance the security and governance of AI implementation using an ambidextrous COBIT 2019 framework that integrates people, processes, and technology. The research adopts a Design Science Research (DSR) methodology, utilizing interviews, questionnaires, and internal document analysis until data saturation was achieved. Governance and Management Objectives (GMOs) were prioritized using design factors, DevOps practices, relevant regulations (ICT Minister Regulation No. 5/2021 and SOE Minister Regulation No. PER-2/MBU/03/2023), and previous studies. DSS05 (Managed Security Services) was selected as the primary focus, reflecting the organization's priority on data protection and secure AI operations. The capability maturity assessment revealed gaps in security leadership, documentation, and process automation, indicating the need for more adaptive and integrated governance. Targeted improvements were implemented, including formalizing governance structures, enhancing security training, and adopting supportive technologies, which increased the DSS05 maturity level from 3.00 to 3.86. A comprehensive roadmap guides further enhancements in security-focused governance. This study provides practical insights for organizations aiming for secure, AI-enabled digital transformation. In addition, it contributes to the theoretical foundation of ambidextrous COBIT 2019 governance frameworks by demonstrating their application in a regulated technology environment.

*This is an open access article under the [CC BY-SA](#) license.*



## Corresponding Author:

Rahmat Mulyana,

Department of Computer and System Sciences,

Stockholm University,

NOD-huset, Borgarfjordsgatan 12, 164 55 Kista, Sweden.

Email: rahmat@dsv.su.se

## 1. INTRODUCTION

Digital transformation has become a fundamental requirement for organizations in every sector to stay competitive in the global market. The rapid development of artificial intelligence (AI) is a key driver of digital transformation, enabling organizations to achieve new levels of operational efficiency and foster innovation [1], [2]. AI-driven solutions allow businesses to automate processes, analyze complex datasets, and quickly adapt to market demands. These advancements have increased pressure on companies to continually innovate and redesign their business models to seize new opportunities and meet evolving customer expectations [2]. As digital disruption accelerates, strategically integrating AI becomes essential for sustainable growth and long-term success [3].

While the benefits of AI adoption are substantial, organizations also face significant challenges, especially in regulated and data-intensive sectors. These challenges include the need for massive data, integration complexity, data dependency, and ensuring algorithm transparency and

workforce readiness to maximize AI's value [4]. In addition, AI deployment raises critical governance issues such as data security, privacy, and compliance with evolving regulations. Organizations must quickly adapt to changing legal and ethical standards while maintaining public trust and operational integrity [5], [6].

Many companies struggle to ensure transparency and accountability in complex AI systems, particularly as risks such as bias and cyber threats increase. In Indonesia, the Financial Services Authority (OJK) underscores the importance of robust AI governance tailored to both local and global requirements in order to manage these risks effectively [5], [7].

In response to such issues, organizations have turned to IT governance mechanisms to navigate digital transformation [8], [9]. These mechanisms involve structural roles, such as IT committees and CIOs, process controls for planning and monitoring, and relational practices for collaboration between IT and business units [9], [10]. By aligning IT strategy with business needs, these governance mechanisms help organizations manage risks and adapt to ongoing change [9].

However, traditional IT governance is often too rigid to address the speed and complexity of AI and digital transformation [11]. Standard frameworks may struggle to keep up with rapid innovation and unique AI risks, such as bias and lack of transparency [12]. This limitation can result in fragmented oversight and slow adaptation to changing technology needs [12], [13]. As a result, organizations need governance models that balance control with agility and support both innovation and compliance [11], [13].

To address these gaps, many studies emphasize the need for ambidextrous IT governance that blends agile and traditional approaches [9], [14]. This hybrid governance model allows organizations to adapt quickly while maintaining necessary controls [9], [15]. Ambidextrous 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” [16]. Recent research shows that balancing formal and relational governance enables firms to achieve both efficiency and flexibility in dynamic environments [14]. This dual approach is especially important for sustaining innovation and performance in the era of digital transformation and AI adoption [15].

Building on these principles, many organizations turn to established frameworks such as COBIT 2019 to implement effective hybrid governance. The COBIT 2019 framework is widely adopted to guide IT governance, risk management, and value delivery in digital transformation initiatives [17]. This model enables organizations to align IT strategy, monitor performance, and address regulatory requirements, especially in complex environments [18]. Recent advances integrate DevOps into COBIT 2019, promoting agility and collaboration while maintaining control and compliance [19]. Studies show that hybrid governance, combining COBIT and DevOps can improve digital transformation outcomes in technology-driven and regulated sectors [9], [13]. However, challenges remain for organizations like SmartCo, including gaps in governance maturity and the need to tailor frameworks for local regulations and business dynamics [13], [18].

Although IT governance frameworks are widely used, there remains a clear gap in models that support regulated and data-intensive organizations in balancing innovation, agility, and the demands of strict compliance. This issue is especially critical as companies like SmartCo manage large volumes of sensitive customer data while operating under rigorous regulatory oversight. With AI adoption accelerating, organizations face growing pressure to ensure both responsible data management and adherence to legal requirements. This study addresses the gap by evaluating an ambidextrous COBIT 2019 approach, which combines traditional governance with DevOps practices, as a model for effective AI governance. Focusing on SmartCo, a leading national digital solutions provider, this research aims to identify practical governance mechanisms and actionable strategies to support responsible, compliant AI adoption. The main contribution is a governance model that enables organizations to accelerate digital transformation, protect data, manage risks, and stay aligned with regulations. Accordingly, this study seeks to answer: How can ambidextrous

COBIT 2019 governance be applied to support effective, compliant, and innovative AI adoption in a regulated digital organization?

## **2. THEORETICAL FOUNDATION**

### **2.1 Digital Transformation**

Digital transformation is a strategic organizational change driven by the adoption of digital technologies to enhance efficiency, foster innovation, and deliver greater value [20]. This process goes beyond technology adoption, requiring adjustments in business models, organizational structures, and management practices to align with new strategic goals and dynamic market demands. From an industry perspective, digital transformation also involves clearly defining objectives, involving leadership, and addressing practical challenges such as change management and alignment between digital strategies and business priorities, ensuring successful implementation and long-term impact [21].

### **2.2 IT Governance**

IT governance refers to the structures, processes, and relational mechanisms that ensure IT is aligned with business goals, manages risks, and delivers value within organizations [22]. Effective IT governance helps organizations optimize their resources and adapt to changes, especially as digital transformation accelerates and new challenges emerge in the digital era [23].

### **2.3 Artificial Intelligence**

Artificial intelligence refers to the development of systems and technologies that can mimic human intelligence to perform tasks such as decision-making, pattern recognition, and problem-solving [24]. Over time, AI has evolved to include key fields like machine learning, computer vision, robotics, and natural language processing, with its applications now reshaping business operations, driving innovation, and enabling new digital strategies in organizations across industries [1].

### **2.4 AI Governance**

AI governance refers to the frameworks, rules, and processes that ensure the development and use of artificial intelligence are aligned with ethical principles, legal requirements, and organizational goals [5]. Effective AI governance addresses key issues such as accountability, transparency, bias, and risk management, positioning AI as part of an organization's overall governance structure while supporting responsible and trustworthy implementation [25].

### **2.5 Ambidextrous IT Governance**

Ambidextrous IT governance refers to the use of both agile-adaptive and traditional mechanisms to manage technology and digital transformation within organizations. This approach balances the need for flexibility and innovation with the importance of stability and control, allowing organizations to explore new digital opportunities while maintaining operational reliability [11]. By combining these two perspectives, companies can respond quickly to digital disruption, foster sustainable product innovation, and achieve better organizational performance in a changing business environment [15].

## **2.6 Framework Comparison**

### **2.6.1 COBIT 2019**

COBIT 2019 is a framework that guides organizations in managing and governing their information and technology. It makes a clear distinction between governance, which sets direction and ensures objectives are met, and management, which handles daily IT activities. The framework includes domains, objectives, and key components such as processes, organizational structures, and policies to help organizations align IT with business goals and respond to changing needs [17], [26].

### **2.6.2 COBIT 2019 Focus Area DevOps**

COBIT 2019 includes Focus Areas to provide more detailed guidance on specific governance themes, such as DevOps, information security, and digital transformation. The DevOps

Focus Area, for example, adapts COBIT's core principles to support rapid software development, automation, and continuous delivery while maintaining alignment with enterprise goals and effective risk management. By using Focus Areas, organizations can tailor the COBIT framework to address unique needs and challenges within specialized domains, enabling better integration of new practices and technologies into existing governance structures [19].

### **2.6.3 Assessment List for Trustworthy AI (ALTAI)**

The Assessment List for Trustworthy Artificial Intelligence (ALTAI) is a self-assessment tool developed by the European Commission's High-Level Expert Group on AI. ALTAI helps organizations evaluate whether their AI systems meet seven key requirements for trustworthy AI: human agency and oversight, technical robustness and safety, privacy and data governance, transparency, diversity and fairness, societal and environmental well-being, and accountability. This framework guides organizations in identifying risks, improving processes, and fostering the responsible development and use of AI in line with European values and fundamental rights [27].

### **2.6.4 Ethically Aligned Design Framework (EAD)**

The Ethically Aligned Design Framework (EAD), developed by the IEEE Global Initiative, provides high-level ethical principles and practical recommendations for the design, development, and deployment of autonomous and intelligent systems. The framework emphasizes respect for human rights, well-being, data agency, transparency, accountability, and the prevention of misuse, aiming to ensure that technology advances human values and societal benefit. It guides organizations and technologists to embed these values in both technical and policy processes, promoting trust and responsible innovation in autonomous and intelligent systems [28].

### **2.6.5 Explainable Artificial Intelligence (XAI)**

The XAI (Explainable Artificial Intelligence) Framework, introduced by DARPA, is designed to make AI systems more transparent by enabling them to provide clear, understandable explanations for their decisions and actions. This framework promotes the development of machine learning techniques that balance high performance with interpretability, including methods for learning more explainable models and building effective explanation interfaces. The goal is to help users understand, appropriately trust, and effectively manage AI systems, supporting better decision-making and user confidence in real-world applications [29].

### **2.6.6 ISO/IEC 38507:2022**

ISO/IEC 38507:2022 provides governance guidance for organizations adopting and managing intelligent technologies. The standard emphasizes the critical role of governing bodies in ensuring that the use of such technologies aligns with organizational objectives, accountability, oversight, risk management, and compliance. ISO/IEC 38507:2022 also underscores that ultimate responsibility for technology use remains with humans, not with the systems themselves, and that clear policies and controls must be established for integrating intelligent systems into organizational processes [30].

### **2.6.7 NIST AI RMF**

The NIST AI RMF is a flexible, voluntary framework designed to help organizations identify, assess, and manage risks related to intelligent systems throughout their lifecycle. The framework structures risk management into four core functions: Govern, Map, Measure, and Manage. It emphasizes a risk-based approach and highlights values such as reliability, safety, transparency, explainability, privacy, and fairness to ensure trustworthy and responsible implementation of intelligent technologies [30].

## **2.7 Framework Selection**

Various frameworks provide guidance for managing technology and digital transformation, each with distinct strengths and gaps. COBIT 2019 is recognized for its structured processes that support alignment with business goals and effective risk management, while its COBIT 2019 Focus Area DevOps adds flexibility for organizations to innovate and respond quickly [31]. On the other hand, ALTAI and EAD contribute important ethical and transparency principles but do not address operational integration with business and IT processes [27], [28]. XAI advances model

interpretability, but its focus remains technical and does not extend to broader organizational oversight [29].

ISO/IEC 38507 offers high-level guidance on organizational governance and board accountability for technology use, particularly in regulated sectors, yet lacks detailed operational direction [30]. NIST AI RMF provides practical steps for risk management across the technology lifecycle but is centered on risk rather than strategic or operational alignment [32]. Considering these differences, this study uses an ambidextrous governance model by combining the structured controls of *COBIT 2019* and its Focus Area DevOps with ethical and risk management insights from the other frameworks. This hybrid approach enables effective governance, transparency, and flexibility for organizations operating in complex and regulated environments. While ethical and risk management principles from ALTAI, EAD Framework, ISO/IEC 38507:2022, and NIST AI RMF inform the overall governance design, their integration remains largely conceptual in this study. Future research should further operationalize these frameworks within governance models to address the increasing complexity of AI adoption.

## 2.8 Previous Study on AI Governance

Recent research has examined the evolution of AI governance frameworks, highlighting the growing need for ethical standards, adaptable regulations, and practical mechanisms to manage transparency, privacy, and accountability risks in AI systems [33], [34]. Scholars have also observed that the global landscape of AI governance remains fragmented, with many initiatives still developing and lacking unified integration across sectors and countries [34], [35]. At the organizational level, AI governance has been defined as a system of rules, practices, and technological tools that support responsible and effective use of AI within broader corporate governance structures [25]. Studies have further emphasized the challenges faced by regulated industries and public sector organizations, especially in balancing technical, ethical, and legal considerations [5].

While current frameworks and regulations provide general guidance and high-level principles for responsible AI, there are still few models that address the integration of AI governance within established IT governance systems, particularly for organizations in highly regulated and data-intensive environments [6], [35]. In response to these gaps, local regulators such as Indonesia's Financial Services Authority (OJK) have begun to issue guidelines focusing on risk management, compliance, and alignment with international best practices [7]. These developments highlight the ongoing need for adaptive and integrated governance approaches to support responsible and innovative AI adoption.

## 3. RESEARCH METHOD

This research uses the Design Science Research (DSR) approach as proposed by Hevner [36], which emphasizes the process of developing and evaluating artifacts as solutions to real problems in the context of the organization. This approach was chosen because it can produce solutions that are not only theoretically relevant, but also applicable and in accordance with the characteristics of the organization [36]. In this research, the artifact developed is a design of an AI governance that integrates COBIT 2019 principles into one ambidextrous COBIT 2019 framework, which combines aspects of exploitation and exploration to answer the challenges of AI governance in digital transformation.

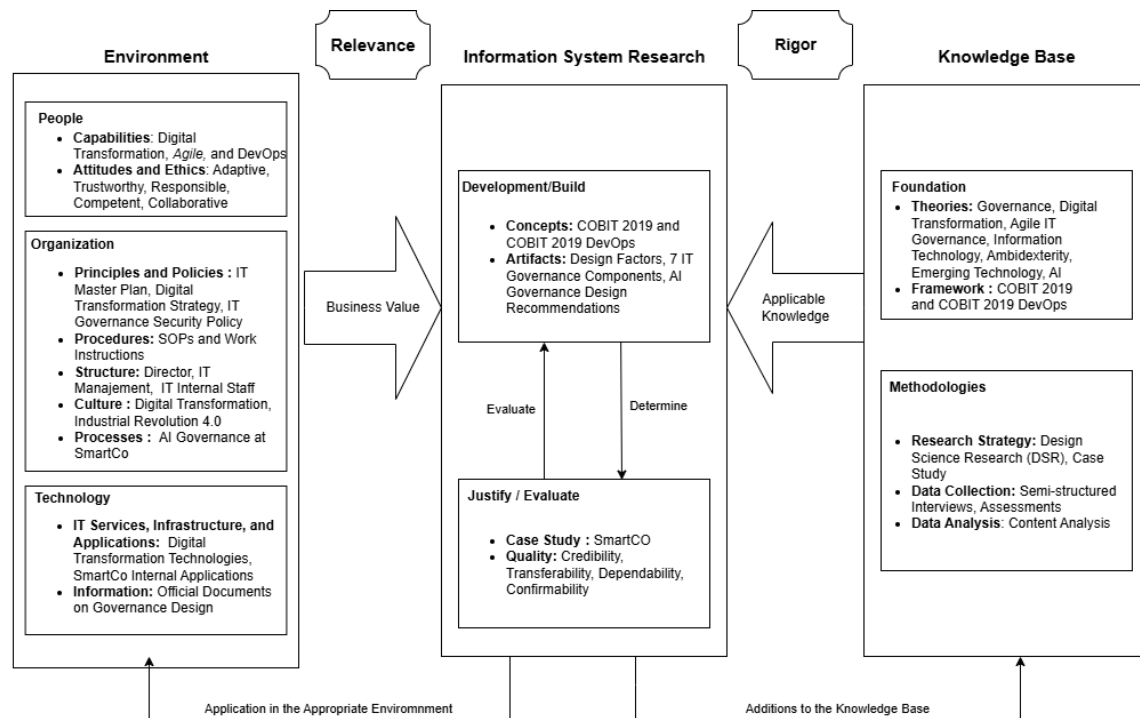


Figure 1. Conceptual Model for DSR Approach Applied to AI Governance Design at SmartCo

Figure 1 presents the conceptual model that underpins this research, adapted from Hevner's DSR framework. This model structures the study into three core components: Environment (organizational and technological context), Knowledge Base (theories and governance frameworks), and Information System Research (iterative development and evaluation of governance artifacts). By applying this model, the research ensures that solutions for AI governance at SmartCo are both contextually relevant and theoretically grounded. The framework also guides the systematic collection and validation of evidence, promoting rigor and ensuring that findings can be practically applied within the organization. The use of DSR provides a clear path for balancing theory and practice, which is essential for effective digital transformation in regulated environments. The evaluation is carried out through triangulation of data sources, analysis of organizational context, and validation of the effectiveness of artifacts based on input from stakeholders. In addition to the DSR framework, this study adopts a case study approach as recommended by Yin, which is particularly suitable for investigating complex, contemporary phenomena within real-life organizational contexts, especially when addressing “how” or “why” questions. The case study method enables an in-depth exploration of how SmartCo implements ambidextrous AI governance to drive its digital transformation, ensuring that both the process and outcomes are deeply contextualized and practically relevant [37].

To ensure that the research process runs in a directed and systematic manner, this study follows the problem-solving stages arranged based on the Design Science Research (DSR) approach. These stages describe how problems are identified, needs are formulated, artifacts are built and implemented and validated through qualitative standardized evaluations [36]. The following figure shows the systematic stages of research used in this study.

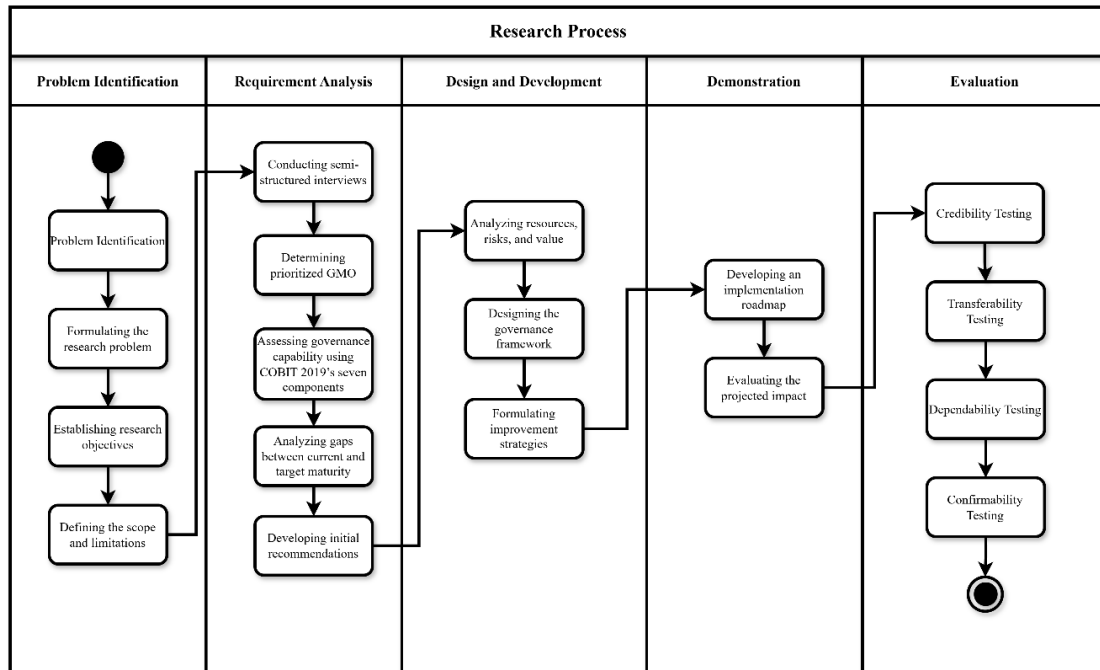


Figure 2 Structure Research Process

Figure 2 presents the research process, which consists of five main stages: problem identification, requirement analysis, design and development, demonstration, and evaluation. The study begins by defining objectives and scope, then proceeds with requirement analysis through interviews and gap assessment of governance priorities. The resulting insights guide the design of improvement strategies across people, process, and technology dimensions. In the demonstration phase, an implementation roadmap is developed, and its potential impact is analyzed. The evaluation phase applies qualitative criteria such as credibility, transferability, dependability, and confirmability to ensure the framework's rigor. Both primary data, collected from interviews, and secondary data, drawn from organizational documents, support a comprehensive analysis. Primary data refers to information obtained directly from the research process, while secondary data is sourced from existing reports and official publications. Further details on data types, sources, and collection techniques are provided in the following section [38].

Table 1. Primary Data

| No. | Respondent   | Position                         | Discussion Summary                                  | Motivation for Selection                                                                              |
|-----|--------------|----------------------------------|-----------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| 1   | Respondent 1 | Chief Executive Officer          | Business focus and digital transformation strategy. | Represents top management's strategic perspective on digital transformation and governance priorities |
| 2   | Respondent 2 | IT Architecture Manager          | IT structure and technology readiness.              | Provides insights on enterprise IT architecture and readiness for AI governance                       |
| 3   | Respondent 3 | IT Internal Staff                | COBIT-based IT maturity assessment.                 | Involved in internal IT governance processes and COBIT implementation                                 |
| 4   | Respondent 4 | Application Operations Division  | Application management and DevOps adoption.         | Responsible for DevOps and operationalization of technology practices                                 |
| 5   | Respondent 5 | Research and Technology Division | Technology innovation and governance practices.     | Oversees research, innovation, and alignment of technology with governance                            |
| 6   | Respondent 6 | System and Technology Division   | IT systems strategy and digital infrastructure.     | Ensures technical infrastructure supports AI and digital transformation                               |

Table 1 shows that interviewees covered executive, managerial, and operational IT roles, offering a broad perspective on business strategy, technology readiness, and COBIT 2019 maturity. Respondents were purposefully selected based on their roles and responsibilities to ensure

representation of both strategic and operational aspects of AI governance at SmartCo. This approach supports the triangulation of insights from different organizational levels and increases the validity of the qualitative findings. Interviews continued until data saturation, following the approach of Fusch and Ness [39]. Secondary data from internal documents was also used to support assessment and validation. Table 2 provides further details on these secondary sources.

Table 2. Secondary Data

| No. | Secondary Data                 | Discussion Summary                                  |
|-----|--------------------------------|-----------------------------------------------------|
| 1   | Annual Report 2023             | Summary of SmartCo's annual performance.            |
| 2   | Corporate Governance Guideline | Guidelines and principles for corporate governance. |
| 3   | Code of Ethics                 | Standards of conduct for all SmartCo personnel.     |
| 4   | Sustainability Report 2023     | ESG related performance and initiatives in 2023.    |

Table 2 presents the secondary data supporting this research, which comprises internal documents related to SmartCo's governance and sustainability practices. These sources provide additional evidence to validate the assessment findings and ensure the proposed governance framework is consistent with corporate policies and performance standards.

This study focuses on individuals with strategic roles in IT and AI governance at SmartCo. Participants were selected using purposive sampling to ensure relevant knowledge and experience [40]. Data were collected through semi-structured interviews, which allowed for deeper exploration of organizational experiences in AI implementation. This method was chosen to capture narrative and non-verbal insights not accessible through quantitative tools [41]. Interview data were analyzed thematically and mapped to the seven governance capability components in the COBIT 2019 framework, aiming to identify gaps between current practices and target conditions. This study is limited to a single organizational case and primarily involves IT and executive respondents, with data drawn mostly from internal documents and interviews. These limitations are discussed further in the Discussion section.

## 4. RESULTS AND DISCUSSION

### 4.1 Governance Management Objectives (GMO) Prioritization Results

Table 3 shows the cumulative assessment scores for the prioritized GMO based on four key evaluation criteria.

Table 3. Cumulative Prioritization Scores for DSS05

| GMO                                       | COBIT 2019<br>Design Factor<br>[17] | COBIT 2019<br>Focus Area<br>DevOps [19] | SOE Minister<br>Regulation No.<br>PER-<br>2/MBU/03/2023<br>[42] | ICT Minister<br>Regulation<br>No. 5/2021<br>[43] | Wu et al.<br>(2024) [44] | Birkstedt<br>(2023) [34] | Wirtz et al.<br>(2020) [45] | Final Score |
|-------------------------------------------|-------------------------------------|-----------------------------------------|-----------------------------------------------------------------|--------------------------------------------------|--------------------------|--------------------------|-----------------------------|-------------|
| DSS05:<br>Managed<br>Security<br>Services | 90                                  | 67                                      | 100                                                             | 100                                              | 100                      | 100                      | 100                         | 94          |

Table 3 presents the cumulative prioritization scores for the DSS05 (Managed Security Services) governance objective. The scoring reflects a holistic assessment using COBIT 2019 design factors, DevOps alignment, key regulatory requirements, and benchmarks from recent AI governance studies. The consistently high scores indicate that DSS05 is viewed as a strategic priority for strengthening security management and compliance within the organization. This prioritization provides a strong foundation for focusing governance improvements in subsequent analysis.

## 4.2 Capability Assessment

### 4.2.1 Process Component

Table 4 details the achievement levels and capability ratings for each management practice within the DSS05 (Managed Security Services) process component.

Table 4. DSS05 Capability Assessment Results

| Management Practice                                                                         | Achievement     | Capability Level |
|---------------------------------------------------------------------------------------------|-----------------|------------------|
| DSS05.01 Protect against malicious software.                                                | 100% (Fully)    | 2                |
|                                                                                             | 100% (Fully)    | 3                |
|                                                                                             | 100% (Fully)    | 4                |
|                                                                                             | 100% (Fully)    | 2                |
| DSS05.02 Manage network and connectivity security.                                          | 100% (Fully)    | 3                |
|                                                                                             | 100% (Fully)    | 4                |
|                                                                                             | 94% (Fully)     | 2                |
| DSS05.03 Manage endpoint security.                                                          | 75% (Largely)   | 3                |
|                                                                                             | 50% (Partially) | 4                |
|                                                                                             | 100% (Fully)    | 2                |
| DSS05.04 Manage user identity and logical access.                                           | 83% (Largely)   | 3                |
|                                                                                             | 67% (Largely)   | 4                |
|                                                                                             | 88% (Fully)     | 2                |
| DSS05.05 Manage physical access to I&T assets.                                              | 83% (Largely)   | 3                |
|                                                                                             | 50% (Partially) | 4                |
|                                                                                             | 100% (Fully)    | 2                |
| DSS05.06 Manage sensitive documents and output devices.                                     | 100% (Fully)    | 3                |
|                                                                                             | 100% (Fully)    | 4                |
|                                                                                             | 100% (Fully)    | 2                |
| DSS05.07 Manage vulnerabilities and monitor the infrastructure for security related events. | 100% (Fully)    | 2                |
|                                                                                             | 100% (Fully)    | 3                |

Table 4 shows that most DSS05 security management practices at SmartCo have reached a high level of implementation, especially in areas like protecting against malicious software, managing sensitive documents, and monitoring vulnerabilities. However, some practices, including endpoint security, user access, and physical access management, have not yet achieved the highest capability levels. This indicates that while the core controls are well-established, there are still gaps that need attention, particularly in consistently applying advanced processes and improving documentation or training in certain areas.

### 4.2.2 Organizational Structure Component

Table 5 outlines the key organizational roles relevant to the DSS05 domain, along with their sources and the current state of implementation at SmartCo.

Table 5. Organizational Structure Component

| Organization Structure             | Source     | Current State                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Chief Information Officer          | COBIT 2019 | SmartCo's CIO role is held by the Director of IT Services, who is responsible for policy formulation, implementation, and IT innovation, including information security.                                                                                                                                                                                                                          |
| Chief Information Security Officer | COBIT 2019 | CISO is managed by the VP IT Systems and is responsible for IT and information security. However, oversees information and AI system security. Responsible for identifying and mitigating AI-specific risks, developing AI security policies, and leading incident response for AI systems. Ensures compliance with AI-related security standards and participates in AI system risk assessments. |
| Business Process Owner             | COBIT 2019 | SmartCo's business process ownership is distributed among relevant unit heads and managers.                                                                                                                                                                                                                                                                                                       |
| Head Human Resources               | COBIT 2019 | SmartCo's Head of HR manages all HR functions, including recruitment and development.                                                                                                                                                                                                                                                                                                             |
| Head Development                   | COBIT 2019 | SmartCo's Head of Development oversees IT project planning, development, and maintenance.                                                                                                                                                                                                                                                                                                         |

| Organization Structure       | Source            | Current State                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Head IT Operations           | COBIT 2019        | SmartCo's Head of IT Operations ensures IT infrastructure reliability and network security.                                                                                                                                                                                                                                                                                                                           |
| Information Security Manager | COBIT 2019        | SmartCo's Information Security Manager handles policy, monitoring, and incident response.                                                                                                                                                                                                                                                                                                                             |
| Privacy Officer              | COBIT 2019        | The Privacy Officer, under Risk and Compliance, is responsible for regulatory compliance. At present, the role does not formally include responsible for data protection and privacy compliance in AI initiatives. Conducts privacy impact assessments for AI systems, manages AI data governance, ensures user consent for AI data processing, and monitors compliance with data protection laws in AI applications. |
| Product owner/ manager       | COBIT 2019 DevOps | SmartCo's Product Owner formally manages and develops digital and AI-related products.                                                                                                                                                                                                                                                                                                                                |
| Software development manager | COBIT 2019 DevOps | SmartCo's software development is managed by IT Systems, leading software engineering and DevOps teams.                                                                                                                                                                                                                                                                                                               |
| Systems operations manager   | COBIT 2019 DevOps | SmartCo's systems operations manager ensures stable and reliable IT services.                                                                                                                                                                                                                                                                                                                                         |
| Testing manager              | COBIT 2019 DevOps | SmartCo's QA Engineer is responsible for testing and evaluating IT product quality.                                                                                                                                                                                                                                                                                                                                   |
| Release manager              | COBIT 2019 DevOps | SmartCo's Release Manager manages application and service deployment.                                                                                                                                                                                                                                                                                                                                                 |
| Automation manager           | COBIT 2019 DevOps | SmartCo's Automation Manager leads process automation and DevOps monitoring.                                                                                                                                                                                                                                                                                                                                          |
| System architect manager     | COBIT 2019 DevOps | SmartCo's System Architect Manager ensures IT architecture standards and security across developments.                                                                                                                                                                                                                                                                                                                |

Table 5 shows that SmartCo has assigned main roles for information security and privacy based on COBIT 2019 and DevOps principles. However, the company has not yet established a specific assignment of responsibility for AI system security under the CISO, nor a clear role for AI data oversight under the Privacy Officer. This gap indicates the need for more defined responsibilities to address emerging security and privacy risks related to the use of advanced systems.

Ideally, the CISO should be explicitly tasked with overseeing all AI-related security risks, including policy development, risk assessment, and incident response for AI systems. Similarly, the Privacy Officer should supervise AI data governance, conduct privacy impact assessments for AI initiatives, and ensure compliance with data protection regulations specifically in the context of AI deployments. By clearly defining these responsibilities, SmartCo can better manage the unique risks presented by artificial intelligence.

#### 4.2.3 Information Component

Table 6 describes how each DSS05 management practice at SmartCo is supported by specific information outputs and the current state of their implementation.

Table 6. Information Outputs for DSS05

| Management Practice                                | Information Outputs                                                                 | Current State                                                                                                                                                                                       |
|----------------------------------------------------|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DSS05.01 Protect against malicious software.       | Malicious software prevention policy.<br>Evaluations of potential threats.          | SmartCo's policy includes antivirus use, system hardening, and international security certification. SmartCo's threat evaluations are done through regular reporting and incident analysis.         |
| DSS05.02 Manage network and connectivity security. | Connectivity security policy.<br>Results of penetration tests.                      | SmartCo's SOP covers layered network security, 24/7 monitoring, and access control. SmartCo's penetration test reports are maintained by the architecture and security team for regular evaluation. |
| DSS05.03 Manage endpoint security.                 | Security policies for endpoint devices.                                             | SmartCo's SOP requires all endpoints to use security software and antivirus.                                                                                                                        |
| DSS05.04 Manage user identity and logical access.  | Results of reviews of user accounts and privileges.<br>Approved user access rights. | SmartCo's user accounts and privileges are reviewed routinely to enforce least privilege. SmartCo's access rights are set with formal approval and clear responsibility.                            |
| DSS05.05 Manage physical access to I&T assets.     | Access logs.<br>Approved access requests.                                           | SmartCo's facility access is monitored and logged to ensure security. SmartCo's access to IT facilities is given only with                                                                          |

| Management Practice                                                                         | Information Outputs                           | Current State                                                                          |
|---------------------------------------------------------------------------------------------|-----------------------------------------------|----------------------------------------------------------------------------------------|
| DSS05.06 Manage sensitive documents and output devices.                                     | Access privileges.                            | proper approval.                                                                       |
|                                                                                             | Inventory of sensitive documents and devices. | SmartCo's access to sensitive documents/devices is restricted to authorized personnel. |
| DSS05.07 Manage vulnerabilities and monitor the infrastructure for security related events. | Security incident tickets                     | SmartCo's inventory ensures optimal monitoring and control of sensitive assets.        |
|                                                                                             | Security incident characteristics             | SmartCo's security incidents are recorded by the cyber security team for follow-up.    |
|                                                                                             | Security event logs                           | SmartCo's incidents are analyzed to determine causes and recovery steps.               |
|                                                                                             |                                               | SmartCo's event logs are used to detect and respond proactively to threats.            |

From Table 6, SmartCo has clear policies, supporting documents, and regular reviews for each area of information security. These steps help keep controls in place and make sure security remains strong. Even so, it is important for the company to keep checking and updating these measures as new risks appear.

#### 4.2.4 People, Skills, and Competencies Component

Table 7 outlines the key people, skills, and competencies required for effective implementation of DSS05 at SmartCo, along with their current development status.

Table 7. Key Skills and Competencies for DSS05

| Skills                          | Current State                                                                                                                                           |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| Information Security            | SmartCo's cyber security team conducts regular training and has established incident reporting and response processes.                                  |
| Information Security Management | SmartCo manages information security through ISO 27001 certification, regular evaluations, and ongoing procedures and training.                         |
| Penetration Testing             | LANAP team members are trained in penetration testing, SAST/DAST methods, and security checklists, enabling independent testing.                        |
| Security Administration         | Security administrators receive training in access management, system updates, and incident response, supported by ISO 27001 and regular certification. |

As shown in Table 7, SmartCo provides regular training and certification for its security team. These efforts cover information security, management, testing, and administration. Continued skill development is needed so the team stays ready for future challenges.

#### 4.2.5 Principle, Policy, and Procedures Component

Table 8 summarizes the main information security policy implemented at SmartCo and its alignment with international standards.

Table 8. Information Security Policy Alignment

| Policy                      | Current State                                                                                                                                                                                                                                                                                      |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Information security policy | SmartCo has adopted an information security policy based on ISO 27001:2013, defense-in-depth, and corporate governance principles requiring data and system protection. The policy is also guided by the 2024–2028 IT Master Plan as the strategic foundation for information security management. |

Table 8 shows that SmartCo's information security policy is built on ISO 27001:2013 standards, defense-in-depth principles, and corporate governance requirements. By also aligning with the IT Master Plan 2024–2028, SmartCo ensures that data protection and system security are supported by both international best practices and internal strategic planning.

#### 4.2.6 Culture, Ethics, and Behavior Component

Table 9 describes the core cultural element of security awareness at SmartCo and how it is fostered across the organization.

Table 9. Security Awareness Culture

| Key Culture Element                                                                                     | Current State                                                                                                                         |
|---------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| Create a culture of awareness regarding user responsibility to maintain security and privacy practices. | SmartCo's security awareness culture is strengthened through training, SOP enforcement, and a dedicated cyber security response team. |

Table 9 shows that SmartCo builds security awareness through regular training, clear procedures, and a cyber security team. These steps help users take responsibility for keeping systems secure.

#### 4.2.7 Service, Structure, and Application Component

Table 10 presents the main IT services, structures, and security applications implemented at SmartCo, along with their current operational status.

Table 10. Security Services and Tools

| Service, Structure, and Application                    | Current State                                                                                                                             |
|--------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| Directory Service                                      | SmartCo manages user identities and access centrally using LDAP, keeping authentication and authorization updated with employment status. |
| Email Filtering Systems                                | SmartCo provides email filtering with sandbox protection, anti-spam/virus, dual-brand filtering, and email validation features.           |
| Identify and Access Management System                  | LDAP is used for centralized identity and access management, ensuring user authentication and authorization are always current.           |
| Security Awareness Services                            | SmartCo regularly conducts security training and awareness programs for employees, including ISO and SOP workshops.                       |
| Security information and event management (SIEM) tools | SmartCo has implemented SIEM tools to monitor and manage daily security operations.                                                       |
| Security operations center (SOC) services              | The company operates a 24/7 SOC to monitor incidents, detect cyberattacks, and isolate or remediate infected devices.                     |
| Third-party security assessment services               | External audits and ISO certifications exist, but no explicit third-party cyber security assessments have been conducted.                 |
| URL filtering systems                                  | SmartCo's Data Center offers Firewall as a Service with URL filtering to block access to harmful or non-compliant websites.               |

Table 10 shows that SmartCo uses a range of security tools and services, from central directory management to SIEM and a 24/7 security operations center. Security training is also done regularly. Even with these measures and ISO certifications in place, there has not been a dedicated third-party security assessment. This represents a gap in objective external validation and addressing it through regular independent audits would strengthen the organization's technology trust and accountability.

#### 4.3 Potential Improvement

Table 11 summarizes the main gaps identified in SmartCo's current AI governance, along with the recommended types and directions for potential improvement across people, process, and technology aspects.

Table 11. Key Gaps and Potential Improvements for DSS05

| Component                          | Gap                                                                                                                                          | Improvement Category | Potential Improvement                                                                                                                                               |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>People Aspect</b>               |                                                                                                                                              |                      |                                                                                                                                                                     |
| Organizational Structure Component | The CISO does not have a specific responsibility for AI system security.                                                                     | Responsibility       | Assign the CISO formal responsibility for overseeing and mitigating AI security risks.                                                                              |
|                                    | The Privacy Officer does not have a specific role in AI privacy oversight.                                                                   | Responsibility       | Mandate the Privacy Officer to conduct privacy audits and ensure compliance for AI data management.                                                                 |
| <b>Process Aspect</b>              |                                                                                                                                              |                      |                                                                                                                                                                     |
| Process Component                  | Full integration of security in data management, AI system development, and unmanaged device detection is lacking.                           | Procedures           | Enhance security controls and device detection across all data and AI development cycles to address privacy and security risks.                                     |
|                                    | No formal documentation or regular review for access changes, audit trails, or privileged accounts, especially in AI data management.        | Record               | Strengthen documentation and monitoring of access changes in AI systems to ensure auditability, transparency, and protection of sensitive data or models.           |
|                                    | No specific training on physical information security and no automated process for physical access rights during onboarding and offboarding. | Procedures           | Increase staff awareness of physical AI infrastructure security and optimize automation for managing physical access, especially during onboarding and offboarding. |
| <b>Technology Aspect</b>           |                                                                                                                                              |                      |                                                                                                                                                                     |
| Service,                           | There is no integrated external cyber security                                                                                               | Tools                | Integrate third-party security assessment                                                                                                                           |

| Component                            | Gap                                                                                                            | Improvement Category | Potential Improvement                                                                                        |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------|----------------------|--------------------------------------------------------------------------------------------------------------|
| Structure, and Application Component | audit or assessment tool, so the reliability and security of AI systems have not been independently validated. |                      | tools or independent audit services for regular external validation and digital documentation of AI systems. |

Table 11 points out the main gaps found in SmartCo's security and governance. Some roles and procedures are still unclear or incomplete, especially for AI system security and privacy. The table also shows practical steps that can be taken, such as giving the CISO and Privacy Officer more defined responsibilities, improving documentation and physical access controls, and involving third-party experts for regular security checks.

#### 4.4 Resource, Risk, and Value (RRV) Analysis

The final score in Table 12 is determined using a Resource-Risk-Value (RRV) approach. Each proposed improvement is evaluated based on three aspects: resource availability, risk, and value. The scoring criteria are summarized as follows:

- **Resource:** The extent to which the solution relies on internal or external resources (score 3 = only internal resources, 2 = internal + external, 1 = only external).
- **Risk:** The potential negative impact if the solution fails (score 3 = limited to one unit, 2 = affects several units, 1 = affects the entire company).
- **Value:** The contribution of the solution to company performance (score 3 = only for one unit, 2 = several units, 1 = company-wide benefit)

Each criterion is scored based on the predefined scale. The final RRV score is calculated using the formula:

$$RRV \text{ Score} = \text{Resource} \times \text{Risk} \times \text{Value}$$

The resulting RRV scores are classified into three priority levels to facilitate decision-making. Improvements with an RRV score greater than 18 are categorized as High Priority, indicating that these actions have the greatest potential impact and should be addressed first. Scores ranging from 7 to 18 are classified as Medium Priority, representing improvements that are important but not as urgent as those in the high category. Finally, scores of 6 or lower fall into the Low Priority group, signifying actions that may be less critical or can be implemented at a later stage. This categorization allows for an objective and transparent prioritization process, ensuring that improvements with the highest impact and feasibility receive attention and resources first.

Table 12. Priority and Scoring of Proposed Improvements (RRV Analysis)

| No. | Potential Improvement                                                                                                                                               | Final Score | Category |
|-----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|----------|
| 1   | Enhance security controls and device detection across all data and AI development cycles to address privacy and security risks.                                     | 18          | Medium   |
| 2   | Strengthen documentation and monitoring of access changes in AI systems to ensure auditability, transparency, and protection of sensitive data or models.           | 12          | Medium   |
| 3   | Integrate third-party security assessment tools or independent audit services for regular external validation and digital documentation of AI systems.              | 12          | Medium   |
| 4   | Assign the CISO formal responsibility for overseeing and mitigating AI security risks.                                                                              | 8           | Medium   |
| 5   | Mandate the Privacy Officer to conduct privacy audits and ensure compliance for AI data management.                                                                 | 8           | Medium   |
| 6   | Increase staff awareness of physical AI infrastructure security and optimize automation for managing physical access, especially during onboarding and offboarding. | 8           | Medium   |

Based on the Table 12, all proposed improvements are rated as medium priority. This indicates that while each action is important, none require urgent or immediate implementation over the others. The recommendations primarily address key gaps in security, documentation, and role clarity, and are expected to help SmartCo progress toward more effective AI governance if implemented as planned.

#### 4.5 Implementation Roadmap

Table 13 presents the implementation roadmap, mapping the timeline for key recommendations across people, process, and technology aspects. Each initiative is scheduled by quarter to ensure a structured and phased execution, enabling smoother integration and sustainable organizational impact.

Table 13. Implementation Roadmap

| Initiative                                                                                                                                                          | 2026 |    |    |    | 2027 |    |    |    |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|----|----|----|------|----|----|----|
|                                                                                                                                                                     | Q1   | Q2 | Q3 | Q4 | Q1   | Q2 | Q3 | Q4 |
| <b>People Aspect</b>                                                                                                                                                |      |    |    |    |      |    |    |    |
| Assign the CISO formal responsibility for overseeing and mitigating AI security risks.                                                                              |      |    |    |    |      |    |    |    |
| Mandate the Privacy Officer to conduct privacy audits and ensure compliance for AI data management.                                                                 |      |    |    |    |      |    |    |    |
| <b>Process Aspect</b>                                                                                                                                               |      |    |    |    |      |    |    |    |
| Enhance security controls and device detection across all data and AI development cycles to address privacy and security risks.                                     |      |    |    |    |      |    |    |    |
| Strengthen documentation and monitoring of access changes in AI systems to ensure auditability, transparency, and protection of sensitive data or models.           |      |    |    |    |      |    |    |    |
| Increase staff awareness of physical AI infrastructure security and optimize automation for managing physical access, especially during onboarding and offboarding. |      |    |    |    |      |    |    |    |
| <b>Technology Aspect</b>                                                                                                                                            |      |    |    |    |      |    |    |    |
| Integrate third-party security assessment tools or independent audit services for regular external validation and digital documentation of AI systems.              |      |    |    |    |      |    |    |    |

The Table 13 shows the roadmap starts by establishing essential roles and responsibilities, particularly for security and privacy, followed by strengthening process controls and documentation, and finally by implementing technology solutions. This phased approach is intended to ensure that foundational changes are in place before process and technical improvements, thereby supporting effective adoption and minimizing disruption. Progress should be monitored regularly so that adjustments can be made if organizational priorities or resources change.

#### 4.6 Recommendation Impact on SmartCo

Table 14 summarizes the impact of the proposed recommendations on the capability level of DSS05 in SmartCo. The table compares capability levels before and after the implementation of improvement initiatives.

Table 14. Capability Level Improvement

| GMO                              | Previous Capability Level | Estimated Capability Level |
|----------------------------------|---------------------------|----------------------------|
| DSS05: Managed Security Services |                           |                            |
| Total                            | 21                        | 27                         |
| Total Score                      | 3.00                      | 3.86                       |

The results in Table 14 indicate a significant improvement in SmartCo's security management capabilities after the implementation of the proposed recommendations. The total capability score for DSS05 increases from 21 to 27, while the average score improves from 3.00 to 3.86. This progress demonstrates that targeted improvements, such as enhancing endpoint and identity security, strengthening access management, and formalizing oversight roles, have a measurable impact on SmartCo's ability to protect critical assets and respond to security risks. These enhancements not only address identified gaps but also support stronger alignment with COBIT 2019 standards, paving the way for more robust and sustainable security governance in the future. Table 15 outlines the estimated impact of the recommended improvements on SmartCo's organizational structure, process, and technology components. The table provides a comparison between the state before and after implementation to highlight key changes across each area.

Table 15. Impact Estimation

| Pre-Implementation State                                                                                                                                                                                                                  | Post-Implementation State                                                                                                                                                                                    |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Organization Structure Component</b>                                                                                                                                                                                                   |                                                                                                                                                                                                              |
| Both the CISO and Privacy Officer do not have specific responsibilities or defined roles related to AI system security and privacy oversight.                                                                                             | The CISO is formally assigned to oversee AI system security, while the Privacy Officer is given a clear role in AI privacy management and compliance.                                                        |
| <b>Process Component</b>                                                                                                                                                                                                                  |                                                                                                                                                                                                              |
| Security is not fully integrated into data management and AI development, with unmanaged device detection, lack of formal documentation and review for access changes, and no specific training or automation for physical access rights. | Security is fully integrated in data and AI processes, with device detection, formal documentation and review for access, and staff trained and supported by automated management of physical access rights. |
| <b>Service, Application, and Infrastructure Component</b>                                                                                                                                                                                 |                                                                                                                                                                                                              |
| No integrated external cyber security audit or assessment tool, so the reliability and security of AI systems are not independently validated.                                                                                            | Third-party security assessment tools and independent audit services are integrated to provide regular external validation and digital documentation of AI systems.                                          |

As shown in the Table 15, each component has progressed after the implementation of improvements. Responsibilities are now clearly defined, security practices are better integrated, and external validation for AI systems has been strengthened. These changes are expected to make SmartCo’s security governance and operational reliability more robust.

4.7 Discussion

The capability improvement seen at SmartCo, directly results from combining DevOps exploration with COBIT 2019 exploitation. On the exploration side, SmartCo’s teams use weekly sprints and agile tools to quickly experiment and launch AI features, as described in their interviews. Yet, every deployment is still reviewed and approved through COBIT-based processes, ensuring risk assessment, documentation, and compliance. This dual-track is not just theoretical; it is visible in day-to-day work: “We use agile sprints to try new ideas, but COBIT ensures everything is safe and compliant before we go live,” said one team member. This balance aligns with Birkstedt’s and Mulyana’s research on ambidextrous governance, and supports Aldoseri et al.’s finding that both agility and strong governance are key to digital transformation [23], [34], [46].

Still, the study found gaps: The CISO and Privacy Officer do not yet have formal AI-related responsibilities, and third-party security audits remain limited. Not all documentation or device management processes are fully integrated. These findings point to the need for clearer role assignment and ongoing improvement, as outlined in the proposed roadmap. The research is limited by its single-company focus and mainly IT-based perspectives, so future work should involve a wider range of stakeholders and track more direct outcomes.

5. CONCLUSION

This research examined how an ambidextrous COBIT 2019 governance model, integrating DevOps practices, can support secure and compliant AI adoption within a regulated, data-driven organization. The implementation at SmartCo demonstrated that clear roles, updated policies, and targeted technical improvements raised the DSS05 capability score from 3.00 to 3.86, showing tangible progress in governance maturity. The study contributes both theoretically, by bridging international frameworks with local regulatory needs, and practically, by offering actionable steps for organizations facing similar challenges. These findings are limited by the single-case approach and lack of quantitative validation, so further research is needed to test the model’s applicability in other settings. Future research should test this model across different sectors, involve broader stakeholder perspectives, and include quantitative impact measures to validate and extend its applicability. Despite these limitations, the governance model presented here offers a practical reference for organizations seeking to integrate compliance and innovation in their AI adoption journey.

REFERENCES

[1] V. Ratten, “Artificial Intelligence, Digital Trends and Globalization: Future Research Trends,” *FIIB Business Review*, vol. 13, no. 3, pp. 286–293, 2024, doi: 10.1177/23197145231222774.

- [2] M. Kavak and L. Rusu, "Challenges and Opportunities of Artificial Intelligence in Digital Transformation: A Systematic Literature Review," *Procedia Comput Sci*, vol. 256, pp. 369–377, 2025, doi: 10.1016/j.procs.2025.02.132.
- [3] E. G. Andrzejak, "Ai-powered digital transformation: Tools, benefits and challenges for marketers-case study of lpp," *Procedia Comput Sci*, vol. 219, pp. 397–404, 2023, doi: 10.1016/j.procs.2023.01.305.
- [4] N. Stogiannos *et al.*, "AI implementation in the UK landscape: Knowledge of AI governance, perceived challenges and opportunities, and ways forward for radiographers," *Radiography*, vol. 30, no. 2, pp. 612–621, 2024, doi: 10.1016/j.radi.2024.01.019.
- [5] A. Ghosh, A. Saini, and H. Barad, "Artificial intelligence in governance: recent trends, risks, challenges, innovative frameworks and future directions," *AI Soc*, no. 0123456789, 2025, doi: 10.1007/s00146-025-02312-y.
- [6] P. G. R. de Almeida, C. D. dos Santos, and J. S. Farias, "Artificial Intelligence Regulation: a framework for governance," *Ethics Inf Technol*, vol. 23, no. 3, pp. 505–525, 2021, doi: 10.1007/s10676-021-09593-z.
- [7] OJK, *Tata Kelola Kecerdasan Artifisial Perbankan Indonesia*. Otoritas Jasa Keuangan, 2025.
- [8] R. Mulyana, L. Rusu, and E. Perjons, "IT Governance Mechanisms that Influence Digital Transformation: A Delphi Study in Indonesian Banking and Insurance Industry," *Pacific Asia Conference on Information Systems (PACIS), AI-IS-ASIA*, pp. 1–16, 2022.
- [9] 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.
- [10] J. Zhen, Z. Xie, and K. Dong, "Impact of IT governance mechanisms on organizational agility and the role of top management support and IT ambidexterity," *International Journal of Accounting Information Systems*, vol. 40, p. 100501, 2021, doi: 10.1016/j.accinf.2021.100501.
- [11] R. Mulyana, L. Rusu, and E. Perjons, "Key Ambidextrous IT Governance Mechanisms Influence on Digital Transformation and Organizational Performance in Indonesian Banking and Insurance," no. July, pp. 173–197, 2024, doi: 10.1007/978-3-031-57189-3\_9.
- [12] 2025 ISACA, "Leveraging COBIT for Effective AI System," 2025.
- [13] F. Febrianti and D. N. Utama, "Enhancing IT maturity in the DevOps focus area: a comprehensive assessment with COBIT 2019," *Edelweiss Applied Science and Technology*, vol. 8, no. 4, pp. 926–934, 2024, doi: 10.55214/25768484.v8i4.1472.
- [14] L. H. Lin and Y. L. Ho, "Ambidextrous governance and alliance performance under dynamic environments: An empirical investigation of Taiwanese technology alliances," *Technovation*, vol. 103, no. February, p. 102240, 2021, doi: 10.1016/j.technovation.2021.102240.
- [15] S. Zhang and S. Suntrayuth, "The Synergy of Ambidextrous Leadership, Agility, and Entrepreneurial Orientation to Achieve Sustainable AI Product Innovation," *Sustainability (Switzerland)*, vol. 16, no. 10, 2024, doi: 10.3390/su16104248.
- [16] 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.
- [17] ISACA, *COBIT 2019 Framework - Introduction and Methodology*. 2019.
- [18] G. Morris, W. Tangka, and E. Lompoliu, "Optimizing IT Governance in BTS . id: A COBIT 2019-Based Analysis of Design Factors," vol. 5, no. April, pp. 699–710, 2025.
- [19] ISACA, *COBIT Focus Area: DevOps*. 2021.
- [20] R. B. Carvalho, A. M. P. Reis, C. L. C. Larieira, and L. H. C. Pinochet, "Digital Transformation: Construct Definition Challenges and Scenarios for a Research Agenda,"

- Revista de Administracao Mackenzie*, vol. 22, no. 6, 2021, doi: 10.1590/1678-6971/eRAMD210400.
- [21] M. Baslyman, "Digital Transformation from the Industry Perspective: Definitions, Goals, Conceptual Model, and Processes," *IEEE Access*, vol. 10, pp. 42961–42970, 2022, doi: 10.1109/ACCESS.2022.3166937.
  - [22] B. A. Khamees, "Information Technology Governance and Bank Performance: A Situational Approach," *International Journal of Financial Studies*, vol. 11, no. 1, 2023, doi: 10.3390/ijfs11010044.
  - [23] R. Mulyana, *IT Governance Influence on Digital Transformation*, no. 25. 2025.
  - [24] A. Sharma, A. Sharma, A. Agarwal, S. Parween, A. Shrivastava, and V. Hajra, "Artificial Intelligence and Business Strategy Towards Digital Transformation: A Research Agenda," *Nanotechnol Percept*, vol. 20, no. S6, pp. 46–58, 2024, doi: 10.62441/nano-ntp.v20iS6.5.
  - [25] M. Mäntymäki, M. Minkkinen, T. Birkstedt, and M. Viljanen, "Defining organizational AI governance," *AI and Ethics*, vol. 2, no. 4, pp. 603–609, 2022, doi: 10.1007/s43681-022-00143-x.
  - [26] INFORMATION SYSTEM AUDIT AND CONTROL ASSOCIATION – ISACA, *Governance and Management Objectives*. 2018.
  - [27] European Commission, *The Assessment list for trustworthy artificial intelligence (ALTAI) for self assessment*. 2020. [Online]. Available: <https://ec.europa.eu/digital-single-market/en/news/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment>
  - [28] IEEE, "A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems, First Edition," *IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems*, p. 292, 2019.
  - [29] R. Kremers, "Artificial Intelligence," *Level Design*, pp. 341–368, 2020, doi: 10.1201/b10933-22.
  - [30] iTeh STANDARD, "Governance Implications of the Use of Artificial Intelligence by Organizations," vol. 2022, 2022, [Online]. Available: [www.iso.org](http://www.iso.org)
  - [31] INFORMATION SYSTEM AUDIT AND CONTROL ASSOCIATION – ISACA, *Governance and Management Objectives*. 2018. [Online]. Available: <https://www.isaca.org/resources/cobit>
  - [32] Nist, "Artificial Intelligence Risk Management NIST AI 100-1 Artificial Intelligence Risk Management," *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, 2023.
  - [33] P. G. R. de Almeida, C. D. dos Santos, and J. S. Farias, "Artificial Intelligence Regulation: a framework for governance," *Ethics Inf Technol*, vol. 23, no. 3, pp. 505–525, 2021, doi: 10.1007/s10676-021-09593-z.
  - [34] T. Birkstedt, M. Minkkinen, A. Tandon, and M. Mäntymäki, "AI governance: themes, knowledge gaps and future agendas," *Internet Research*, vol. 33, no. 7, pp. 133–167, 2023, doi: 10.1108/INTR-01-2022-0042.
  - [35] L. Schmitt, "Mapping global AI governance: a nascent regime in a fragmented landscape," *AI and Ethics*, vol. 2, no. 2, pp. 303–314, 2022, doi: 10.1007/s43681-021-00083-y.
  - [36] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design science in information systems research," *MIS Q*, vol. 28, no. 1, pp. 75–105, 2004, doi: 10.2307/25148625.
  - [37] R. Yin, "How to do Better Case Studies: (With Illustrations from 20 Exemplary Case Studies)," *The SAGE Handbook of Applied Social Research Methods*, pp. 254–282, 2014, doi: 10.4135/9781483348858.n8.
  - [38] V. O. Ajayi, "A Review on Primary Sources of Data and Secondary Sources of Data," *European Journal of Education and Pedagogy*, vol. 2, no. 3, pp. 1–7, 2023.
  - [39] 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.
  - [40] S. Campbell *et al.*, "Purposive sampling: complex or simple? Research case examples," *Journal of Research in Nursing*, vol. 25, no. 8, pp. 652–661, 2020, doi: 10.1177/1744987120927206.

- [41] M. Dolczewski, "Semi-structured interview for self-esteem regulation research," *Acta Psychol (Amst)*, vol. 228, no. June, 2022, doi: 10.1016/j.actpsy.2022.103642.
- [42] Peraturan Menteri BUMN RI, "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.
- [43] Kominfo, "Peraturan Menteri Komunikasi dan Informatika Indonesia Nomor 5 Tahun 2021," *Peraturan Menteri Komunikasi dan Informatika Indonesia Nomor 5 Tahun 2021*, vol. 151, no. 2, p. 133, 2021.
- [44] C. Wu, H. Zhang, and J. M. Carroll, "AI Governance in Higher Education: Case Studies of Guidance at Big Ten Universities," *Future Internet*, vol. 16, no. 10, 2024, doi: 10.3390/fi16100354.
- [45] B. W. Wirtz, J. C. Weyerer, and B. J. Sturm, "The Dark Sides of Artificial Intelligence: An Integrated AI Governance Framework for Public Administration," *International Journal of Public Administration*, vol. 43, no. 9, pp. 818–829, 2020, doi: 10.1080/01900692.2020.1749851.
- [46] A. Aldoseri, K. N. Al-Khalifa, and A. M. Hamouda, "AI-Powered Innovation in Digital Transformation: Key Pillars and Industry Impact," *Sustainability (Switzerland)*, vol. 16, no. 5, 2024, doi: 10.3390/su16051790.