Available online at: http://e-jurnal.lppmunsera.org/index.php/JSMI

Jurnal Sistem dan Manajemen Industri
(Journal System and Management of Industries)

ISSN (Print) 2580-2887 ISSN (Online) 2580-2895

Ambidextrous IoT governance to support EnergyCo's digital transformation based on COBIT 2019 traditional and DevOps

Prima Audina Wibowo[1*], Rahmat Mulyana[2], Hanif Fakhrurroja[1]
[1]Department of Information System, Telkom University, Jl. Telekomunikasi No.232, Bandung, West Java 40288, Indonesia
[2]Department of Computer and System Sciences, DSV Stockholm University, NOD-huset, Borgarfjordsgatan 12, 164 55 Kista, Sweden

ARTICLE INFORMATION

Article history:

Received: June 16, 2025
Revised: December 15, 2025
Accepted: December 27, 2025

Keywords:

Ambidextrous IoT governance
COBIT 2019
DevOps
Digital transformation
EnergyCo

ABSTRACT

The accelerating digital transformation in the energy sector demands robust governance mechanisms for emerging technologies, particularly the Internet of Things (IoT). This study examines the governance challenges faced by an energy company in Indonesia as it strives to manage IoT ecosystems while meeting regulatory requirements and achieving organizational objectives. Despite IoT's critical role in enabling digital transformation, limited Research has explored IoT governance frameworks grounded in COBIT 2019, especially within the energy domain. To bridge this gap, this study develops an ambidextrous IoT governance framework by integrating the Traditional and DevOps Focus Area mechanisms from COBIT 2019. The framework is designed to balance stability and adaptability in managing IoT-related risks. A Design Science Research methodology is employed, complemented by a case study approach involving interviews, questionnaires, and internal document analysis to ensure contextual relevance and data saturation. The study identifies and evaluates governance priorities by aligning Governance and Management Objectives (GMOs) with national regulations, design factors, and prior research findings. Based on gap analysis using seven components of the selected GMO, DSS (Managed Security Services), the study proposes targeted improvements to IoT governance. These include strengthening leadership accountability, advancing cybersecurity competencies, and enhancing system monitoring capabilities. The implementation of these improvements is projected to elevate the DSS maturity level from 3.29 to 3.86, supporting its digital transformation agenda in alignment with COBIT 2019. This Research contributes to the literature by offering a structured, context-aware IoT governance framework and providing actionable insights for practitioners seeking to govern IoT initiatives within complex, regulated environments.

*Corresponding Author

Rahmat Mulyana
E-mail: rahmat@dsv.su.se

1. INTRODUCTION

The advancement of Industry 4.0 technologies continues to reshape how organizations operate, compelling enterprises across sectors to pursue digital transformation (DT) to remain adaptive and competitive [1], [2]. Among these technologies, the Internet of Things (IoT) stands out as a key enabler, particularly in sectors involving infrastructure and operations, by supporting real-time data acquisition, automation, and system responsiveness [3]. Its application can drastically improve operational effectiveness and drive efficiency [4]. Nonetheless, implementing IoT in power-related organizations introduces significant technical and managerial challenges, particularly in areas such as system interoperability, seamless integration, efficient data

http://dx.doi.org/10.30656/jsmi.v9i2.10803

handling, and establishing flexible yet reliable application-layer standards [4], [5]. For instance, the IoT promises to enable smarter energy systems, but it also faces significant barriers, such as ensuring secure communication between increasingly connected devices and managing the huge volume of data generated by these devices [6].

EnergyCo, for a government-affiliated ICT provider supporting national energy systems, holds a strategic position in enabling digital infrastructure development across the sector. Guided by regulations such as PER-2/MBU/03/2023 and the Ministry of Communication and Informatics Regulation No. 5/2021, the organization is required to implement IT governance frameworks that ensure reliability, resilience, and accountability. However, IoT initiatives within EnergyCo are constrained by limited flexibility in governance models and the pressing need to align operational agility with regulatory compliance [7].

Traditional governance mechanisms, while well-suited to controlling established systems, often fail to support the dynamic needs of digital transformation [8] and tend to emphasize control and standardization, but frequently fall short in supporting the fast-paced and iterative nature of digital initiatives. Recent literature suggests that ambidextrous IT governance, balancing formal structures with agile principles, can better support innovation and operational consistency in evolving technology landscapes [9], [10]. COBIT 2019 provides a structured framework for such governance, and its DevOps focus area introduces key elements such as automation, cultural alignment, and continuous delivery [11].

COBIT 2019, with its comprehensive Governance and Management Objectives (GMOs), provides a solid foundation for such governance. In particular, the ambidextrous IT governance model, which integrates traditional control mechanisms with agile, adaptive practices and the DevOps focus area, promotes continuous improvement and rapid delivery essential for IoT governance in dynamic environments.

In highly regulated industries such as banking and telecommunications, where digital services must adhere to stringent availability, security, and compliance standards, DevOps has already been effectively implemented. DevOps-based delivery pipelines are utilized in banking to release digital onboarding, payment services, and mobile banking capabilities multiple times a week, while adhering to internal IT governance controls and PCI-DSS regulations. Similar to this, large telecom companies employ DevOps techniques to manage customer-facing apps and OSS/BSS platforms, resulting in faster release cycles, lower incident rates, and more reliable service-level fulfilment. These examples show that when DevOps is integrated with automated controls, monitoring, and traceability, it can coexist alongside established IT governance frameworks and even enhance them. From a conceptual standpoint, the energy industry faces similar challenges: IoT-based systems for asset management, substation monitoring, and smart meters must balance stringent safety and compliance standards with rapid adaptation to evolving operational and cybersecurity threats. Therefore, a comparable DevOps-enabled IoT governance approach is anticipated to be successful when deployed in energy-sector SOEs, given the demonstrated capacity of DevOps to support both high-frequency change and robust governance in banking and telecoms.

This study aims to address key gaps in IoT governance for state-owned enterprises in the energy sector, with a particular focus on EnergyCo, a government-affiliated ICT provider that supports national energy systems. The main contributions of this Research are described as follows:

1. Designing a tailored IoT governance framework for EnergyCo by integrating the principles of COBIT 2019 governance with agile, adaptive practices from the DevOps focus area. This approach ensures a balance between stability and innovation, optimizing both organizational control and the flexibility required to manage IoT ecosystems.
2. Proposing a hybrid governance model that enables EnergyCo to manage IoT-related risks and resources effectively, ensuring alignment with digital transformation goals and compliance with regulatory requirements such as PER-2/MBU/03/2023 and Ministry of Communication and Informatics Regulation No. 5/2021.
3. Providing actionable insights for improvement by analyzing EnergyCo’s current IoT governance maturity, identifying key gaps, and suggesting improvements in leadership roles, security practices, and automation. These recommendations are aimed at enhancing the overall IoT governance capability, thereby contributing to the company’s successful digital transformation journey.

The main contributions of the Research focus on advancing IoT governance practices in state-owned enterprises to ensure that digital transformation goals are achieved while meeting regulatory and operational requirements. Given these factors, EnergyCo serves as a case study representing state-owned enterprises in the energy sector, which face unique challenges and opportunities in managing IoT governance as part of their digital transformation. The findings from this study will provide valuable insights into how an ambidextrous governance approach can facilitate successful IoT integration [12].

2. RELATED WORK

As organizations pursue digital transformation (DT), they are increasingly integrating emerging technologies, such as the Internet of Things (IoT), into

http://dx.doi.org/10.30656/jsmi.v9i2.10803

their operations. These technologies offer opportunities to improve efficiency, flexibility, and competitiveness [1]. However, IoT implementation brings challenges such as system interoperability, data security, and regulatory compliance, particularly in highly regulated sectors like energy. In this context, governance mechanisms are critical for managing both the risks and the benefits of these technologies [12]. As organizations strive to leverage IoT to transform their operations, they must navigate the tension between exploring innovative solutions and effectively exploiting existing resources [7]. This balancing act requires a governance framework that is both rigorous in maintaining control and flexible enough to allow for continuous innovation.

2.1. Digital transformation

Digital transformation is a process of significant change driven by the innovative use of digital technology and the strategic deployment of substantial resources and capabilities. This process aims to enhance entities, including business networks, industries, organizations, and stakeholders, while also redefining the value these entities provide to their stakeholders [13]. DT also significantly impacts the achievement of organizational performance. By implementing digital transformation DT), which accelerates digitalisation within the organization, it is believed that it can bring about changes in the company, including improvements in business processes, operations, and customer experience [4]. Digital transformation is a unique transformation that organizations undergo, as it depends on understanding the role of data and available technologies, which bring about drastic changes to an organization's structure and capabilities [13]. Digital transformation (DT) refers to the integration of digital technologies into all areas of business, fundamentally changing how organizations operate and deliver value to customers [14]. In the energy sector, IoT enables the transformation of traditional grids into intelligent, data-driven networks by facilitating real-time monitoring, smart grid control, and predictive maintenance, thus improving energy efficiency, grid reliability, and demand response capabilities [15].

2.2. Ambidextrous IT governance

Ambidextrous IT governance combines both exploration (the adoption of new technologies and innovations) and exploitation (the optimization of existing resources and systems). This dual approach enhances organizational agility, enabling organizations to innovate and maintain stability simultaneously. An ambidextrous IT governance mechanism 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"*[1]. This dual approach enables organizations to navigate the rapid evolution of IoT technologies while maintaining governance over risk management and compliance.

Studies such as those by Jöhnk *et al.* [9] and Mulyana *et al.* [16] have demonstrated the effectiveness of ambidextrous IT governance in sectors like banking and insurance. Organizations must be able to "explore and exploit" simultaneously, competing in mature markets with existing technologies while also exploring new technologies and markets [17]. However, its application in the energy sector, particularly in the context of SOEs like EnergyCo, remains underexplored. This Research extends the ambidextrous IT governance model to IoT governance within EnergyCo, focusing on the balance between technological exploration and operational exploitation in a highly regulated environment.

2.3. COBIT 2019

COBIT 2019 is a comprehensive IT governance framework developed by ISACA that helps organizations align their IT operations with overarching business objectives. Unlike traditional models, COBIT 2019 differentiates governance, which deals with strategy formulation and accountability, from management, which is concerned with the execution of day-to-day activities [18]. The framework features 40 key objectives across five core domains and offers flexibility through design factors and focus areas such as IT risk, information security, and DevOps [18], [19]. The framework integrates various aspects, including processes, structures, policies, culture, skills, and technology, to establish adaptable and effective IT governance practices. For organizations like EnergyCo, COBIT 2019 offers a structured yet flexible approach that ensures IoT and other technology initiatives are effectively governed, while also ensuring compliance with national regulations.

2.4. COBIT 2019 DevOps focus area

The DevOps focus area within COBIT 2019 emphasizes the importance of seamless collaboration between development and operations teams to streamline the delivery of IT services. DevOps refers to a set of principles and practices that promote collaboration throughout the agile software development lifecycle, thereby enhancing the speed and quality of deployments [11]. The CALMS framework, which stands for Culture, Automation, Lean, Measurement, and Sharing, forms the foundation of DevOps, ensuring that teams are aligned culturally, operational processes are automated, and performance is continuously measured and improved [11]. DevOps is particularly vital for managing IoT systems, where organizations need to rapidly deploy new technologies

http://dx.doi.org/10.30656/jsmi.v9i2.10803

while maintaining tight control over security and compliance. DevOps *"enables enhanced collaboration across development teams and stakeholders throughout the agile development lifecycle."* [20], [21] further confirms that DevOps optimizes process flows and ensures the robustness of IT systems while mitigating risks, especially in a rapidly evolving environment like digital transformation.

2.5. IoT governance

IoT governance refers to the frameworks, processes, and policies used to ensure the secure, compliant, and efficient operation of IoT systems. The challenges of IoT governance, such as ensuring data security, privacy, and system interoperability, are well-documented in existing literature [22], [23]. However, the application of comprehensive IoT governance frameworks in state-owned enterprises (SOEs), particularly in the energy sector, remains under-explored. More recent Research has also highlighted the evolving need for effective governance mechanisms in IoT systems, particularly in the context of sustainability in energy systems [24]. This study contributes to filling this gap by proposing an IoT governance framework that integrates traditional IT governance mechanisms with DevOps principles to address both technological and regulatory challenges [12], [25]. As IoT grows in scope and complexity,

Table 1. Literature gap

Study	Year	Focus	Methodology	Key Findings	Research Gap
Mulyana *et al.* [7]	2024	Ambidextrous IT governance in banking	Delphi study	Identified ambidextrous mechanisms for digital transformation	Limited application in the energy sector and IoT governance
Sethi & Sarangi [26]	2017	IoT governance	Literature review	Frameworks for IoT security and compliance	Insufficient focus on comprehensive governance models for SOEs
Mulyana *et al.* [1]	2024	DevOps and digital transformation	Case study	Effective use of DevOps in accelerating digital initiatives	Application to IoT governance remains unexplored in energy SOEs
ISACA [18]	2019	COBIT 2019 Framework	Framework overview	Provides structure for managing IT investments	Limited adaptation for IoT governance within the energy sector
Vejseli *et al.* [17]	2022	Agile IT governance and digital transformation	Qualitative analysis	Identified agile governance dimensions	Application to IoT governance in energy SOEs
Morar *et al.* [27]	2021	IoT Governance Framework	Survey	Proposes a framework for IoT governance across data, infrastructure, and architecture	Limited focus on scalability and integration across industries
Sedrati *et al.* [28]	2023	IoT Governance Requirements	Systematic review	Identifies key requirements for IoT governance, focusing on data management, security, and privacy	Lack of practical implementation for IoT governance frameworks in real-world scenarios
Ammar *et al.* [29]	2018	Security in IoT Frameworks	Survey	Surveys security architectures in popular IoT frameworks and compares their strengths	Insufficient analysis of privacy protection and secure communication in IoT frameworks
This Study		Ambidextrous IoT governance for EnergyCo using COBIT 2019 and DevOps	Design Science Research, Case Study	Proposes and evaluates a hybrid IoT governance framework tailored for SOE in the energy sector	Addresses the lack of real-world application of ambidextrous IoT governance in regulated SOE contexts

http://dx.doi.org/10.30656/jsmi.v9i2.10803

traditional IT governance frameworks face challenges in fully addressing the unique needs of IoT systems [28], [30]. Moreover, the National Institute of Standards and Technology (NIST) is actively developing cybersecurity frameworks tailored specifically for IoT deployments, further emphasising the need for robust governance to address security concerns in IoT systems [31].

To identify the research gap, several studies on IT governance, digital transformation, and IoT governance were reviewed. Table 1 summarizes their focus, methodologies, key findings, and the gaps remaining in the literature. This table provides a comparative overview of various studies, highlighting the limited Research on combining COBIT 2019, DevOps, and ambidextrous governance for IoT, particularly in the energy sector. The table further underscores the critical gaps in applying these frameworks to IoT governance within state-owned enterprises (SOEs), particularly in the energy industry. These gaps include the lack of scalable frameworks, insufficient exploration of IoT governance within energy SOEs, and limited practical implementation across different industries.

Table 1 shows that existing Research has not fully addressed how to govern IoT in complex industries, such as energy. While some studies examine agile or DevOps governance, they often overlook the connection to IoT or COBIT 2019. There is also a lack of practical frameworks that energy companies can apply. This study fills that gap by developing and testing an IoT governance framework for an energy company in Indonesia.

This Research extends existing literature by proposing an ambidextrous IoT governance model explicitly tailored for EnergyCo, a state-owned enterprise in the energy sector. By integrating COBIT 2019's governance practices with the DevOps focus area, this study provides a hybrid governance model that supports rapid IoT deployment while maintaining control over security and regulatory compliance. The addition of this study highlights a novel integration of COBIT 2019 with DevOps principles in the context of IoT governance for SOEs, which has not been thoroughly addressed in prior Research. The findings provide actionable insights for enhancing IoT governance maturity and facilitating successful digital transformation at EnergyCo.

3. RESEARCH METHODS

3.1. Conceptual model

The study employs a Design Science Research (DSR) methodology [32], which is suitable for developing and evaluating artefacts to address practical

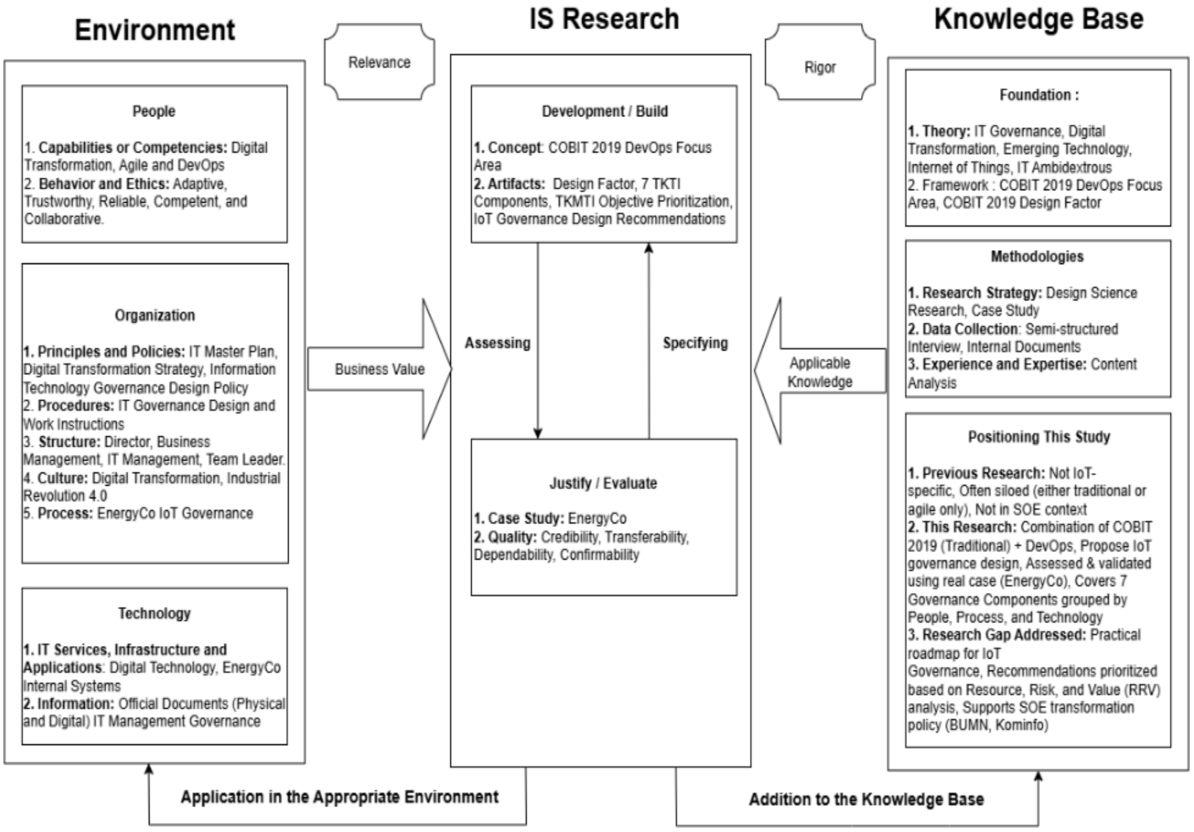
Environment
Relevance
IS Research
Rigor
Knowledge Base
People
1. Capabilities or Competencies: Digital Transformation, Agile and DevOps
2. Behavior and Ethics: Adaptive, Trustworthy, Reliable, Competent, and Collaborative.
Organization
1. Principles and Policies: IT Master Plan, Digital Transformation Strategy, Information Technology Governance Design Policy
2. Procedures: IT Governance Design and Work Instructions
3. Structure: Director, Business Management, IT Management, Team Leader.
4. Culture: Digital Transformation, Industrial Revolution 4.0
5. Process: EnergyCo IoT Governance
Technology
1. IT Services, Infrastructure and Applications: Digital Technology, EnergyCo Internal Systems
2. Information: Official Documents (Physical and Digital) IT Management Governance
Business Value
Development / Build
1. Concept: COBIT 2019 DevOps Focus Area
2. Artifacts: Design Factor, 7 TKTI Components, TKMTI Objective Prioritization, IoT Governance Design Recommendations
Assessing
Specifying
Justify / Evaluate
1. Case Study: EnergyCo
2. Quality: Credibility, Transferability, Dependability, Confirmability
Applicable Knowledge
Foundation :
1. Theory: IT Governance, Digital Transformation, Emerging Technology, Internet of Things, IT Ambidextrous
2. Framework : COBIT 2019 DevOps Focus Area, COBIT 2019 Design Factor
Methodologies
1. Research Strategy: Design Science Research, Case Study
2. Data Collection: Semi-structured Interview, Internal Documents
3. Experience and Expertise: Content Analysis
Positioning This Study
1. Previous Research: Not IoT-specific, Often siloed (either traditional or agile only), Not in SOE context
2. This Research: Combination of COBIT 2019 (Traditional) + DevOps, Propose IoT governance design, Assessed & validated using real case (EnergyCo), Covers 7 Governance Components grouped by People, Process, and Technology
3. Research Gap Addressed: Practical roadmap for IoT Governance, Recommendations prioritized based on Resource, Risk, and Value (RRV) analysis, Supports SOE transformation policy (BUMN, Kominfo)
Application in the Appropriate Environment
Addition to the Knowledge Base

Fig 1. Conceptual model, adapted from vom Brocke *et al.* [32]

http://dx.doi.org/10.30656/jsmi.v9i2.10803

problems. DSR steps include problem identification, solution design, demonstration, and evaluation. Fig. 1 represents the Design Science Research (DSR) methodology divided into three main components: Environment, IS Research, and Knowledge Base. The environment encompasses people, Organizations, and Technology, focusing on competencies, governance principles, and digital infrastructure. IS Research covers the development of the IoT governance model using COBIT 2019 and DevOps, assessing and specifying solutions, and evaluating the case study with a focus on Energic. The Knowledge Base supports the research foundation through theories and frameworks, with methodologies such as Design Science Research, case studies, and interviews. The research aims to enhance IoT governance, ensuring it contributes to digital transformation in the energy sector while delivering business value by optimizing processes and enhancing organizational agility.

3.2. Research process

The research employs a qualitative case study approach, focusing on Energy, a state-owned enterprise in the energy sector. This approach enables an in-depth examination of the challenges and opportunities associated with implementing IoT governance for digital transformation. The case study methodology enables us to study real-world applications and derive meaningful insights into how ambidextrous IT governance can be implemented in practice, addressing the specific regulatory and operational requirements of EnergyCo. This study employs a case study approach, as recommended by Yin [33], which is suitable for exploring complex contemporary phenomena within real-life contexts, particularly when the research seeks to answer “how” or “why” questions. The case study method is suitable for examining how EnergyCo implements ambidextrous IoT governance to support its digital transformation [33]. The positioning of this research in comparison to existing studies. While prior studies have explored IT governance using COBIT or agile transformation through DevOps, few have integrated both approaches to address the specific needs of IoT governance within state-owned enterprises. This study fills that gap by proposing an ambidextrous governance model that balances control and agility for digital transformation in the energy sector.

Fig. 2 illustrates a structured five-phase research process consisting of Problem Explanation, Requirement Determination, Design and Development, Demonstration, and Evaluation. In the first phase, Problem Explanation, the research problem was clearly identified, along with the research objectives, which were refined through an extensive literature review to establish the scope and boundaries of the study. The second phase, Requirement Determination, involved several key activities: creating a comprehensive list of research questions, conducting semi-structured interviews with key stakeholders at EnergyCo, determining the prioritization of IT governance objectives relevant to IoT, analyzing the seven components of capability within COBIT 2019’s DevOps focus area, and performing gap analysis to identify deficiencies. This phase also included evaluating potential improvement recommendations based on the analyzed gaps.

During the Design and Development phase, the research team drafted improvement recommendations, formulated detailed proposals addressing the people, process, and technology aspects, and prioritized these recommendations by considering Resources, Risks, and Value (RRV) to develop a feasible implementation plan. The Demonstration phase involved implementing a prototype governance solution, developing a comprehensive roadmap for deployment, and analysing the impact of the proposed design on the seven key components of IT governance relevant to IoT management. Finally, the Evaluation phase assessed the framework’s credibility, transferability, dependability, and confirmability through expert validation and iterative feedback, ensuring the reliability and applicability of the research outcomes.

3.3. Data collection

The data for this study were collected through semi-structured interviews and secondary data analysis. Semi-structured interviews were conducted with key stakeholders at EnergyCo (Table 2). These interviews allowed for flexibility in exploring the participants'

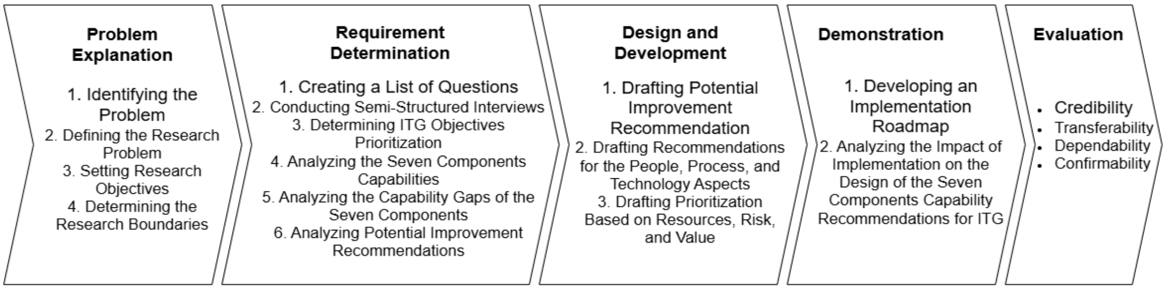
Problem Explanation
1. Identifying the Problem
2. Defining the Research Problem
3. Setting Research Objectives
4. Determining the Research Boundaries
Requirement Determination
1. Creating a List of Questions
2. Conducting Semi-Structured Interviews
3. Determining ITG Objectives Prioritization
4. Analyzing the Seven Components Capabilities
5. Analyzing the Capability Gaps of the Seven Components
6. Analyzing Potential Improvement Recommendations
Design and Development
1. Drafting Potential Improvement Recommendation
2. Drafting Recommendations for the People, Process, and Technology Aspects
3. Drafting Prioritization Based on Resources, Risk, and Value
Demonstration
1. Developing an Implementation Roadmap
2. Analyzing the Impact of Implementation on the Design of the Seven Components Capability Recommendations for ITG
Evaluation
• Credibility
• Transferability
• Dependability
• Confirmability

Fig 2. Research process

perspectives while ensuring alignment with the research questions [34]. Secondary data were obtained from publicly available reports, regulatory documents, and internal governance frameworks used by EnergyCo. Data saturation was reached after conducting a total of 3 interviews. This number was determined based on the point at which no new themes or insights emerged from the interviews. The data collection process ensured that both primary and secondary data were triangulated to strengthen the validity of the findings.

3.4. Data analysis

For the data analysis in this study, a qualitative content analysis approach is employed to identify patterns, relationships, and themes from the qualitative data obtained through semi-structured interviews and document analysis. This technique allows for an in-depth examination of the textual data to uncover the underlying structures and insights related to IoT governance and the implementation of ambidextrous IT governance. Content analysis helps systematically organize the data into categories and groups, facilitating the identification of key governance components and gaps in current practices. Additionally, the COBIT 2019 framework was used as a theoretical lens to analzse the alignment of IoT governance with EnergyCo's business objectives and regulatory requirements. The framework's Governance and Management Objectives (GMOs) were used to evaluate the existing IoT governance practices within EnergyCo and to identify potential gaps [18].

3.5. Research validity and reliability

To ensure the validity and reliability of the research, multiple methods were employed. The triangulation of data sources (interviews, regulatory documents, and internal reports) enhanced the robustness of the findings. In terms of reliability, the research adhered to consistent procedures for data collection, including standardized interview questions and clear guidelines for secondary data analysis. A second researcher also reviewed the coding process to minimize bias and ensure consistency in identifying themes.

To ensure that this engineering-oriented research produces measurable outcomes, several Key Performance Indicators (KPIs) were defined to evaluate the effectiveness and impact of the proposed IoT governance model. These KPIs are formulated as follows:

1. Capability level improvement calculated through pre- and post-assessment.
2. Classification of improvement recommendations based on Resource × Risk × Value (RRV) formula, where each component is rated from 1 to 3, resulting in a total score ranging from 3 to 18.
3. Total number of improvement recommendations, classified by priority using the Resource × Risk × Value (RRV).
4. Validation effectiveness, determined through stakeholder approval.
5. Coverage across the COBIT-based Governance components.

These indicators confirm that the research outputs are not only conceptually robust but also quantifiably aligned with the needs of digital transformation.

3.6. Ethical considerations

This study adhered to ethical guidelines for research, ensuring that all participants were fully informed about the purpose of the study, their rights, and the confidentiality of their responses. All interviews were conducted with the participants' informed consent, and the data were anonymized to protect their privacy. Additionally, the study complied with standards to ensure ethical research practices throughout the process.

Table 2. Primary data

Interviewees	Position	Discussion	Date
Interviewee 1	President Director	Discussed IT governance, the company's developing technology status, and the introduction of the research topic.	March,12 2025
Interviewee 2	IT Architecture Manager	Described developing technology and IT governance procedures in relation to the business's operations.	March, 12 2025
Interviewee 3	Internal Staff IT	Discussed IT governance in more detail from the standpoints of internal execution and operations.	March, 12 2025
Interviewee 4	STI Field (Corporate IT Subfield)	Discussed challenges and solutions in managing corporate IT systems	May, 16 2025
Interviewee 5	Application Services Division (EnergyCo Business Process Outsourcing Subfield)	Discussed the integration of IT governance with business process outsourcing and future improvements	May, 16 2025

http://dx.doi.org/10.30656/jsmi.v9i2.10803

Table 3. Secondary data

Document	Description
EnergyCo Profile	Overview of EnergyCo's business operations, mission, vision, and core values.
EnergyCo Organizational Structure	Details on EnergyCo's organizational hierarchy, departments, and leadership structure.
EnergyCo Annual Report	A comprehensive report covering EnergyCo’s financial performance, key achievements, and future plans.
EnergyCo Sustainability Report	Information on EnergyCo’s sustainability initiatives, environmental impact, and social responsibility.
Corporate Governance Guidelines	Set of principles and practices governing EnergyCo’s operations and compliance with regulatory standards.
Corporate Ethics Guidelines	Guidelines outlining the ethical standards expected from EnergyCo employees and management.
Regulation	Relevant laws and regulations that EnergyCo must comply with in its operations and business practices.

Data was gathered through interviews with 5 (five) interviewees during the period March-May 2025. Table 2 displays the secondary data utilized to complement the primary data in evaluating EnergyCo’s situation and to identify areas requiring improvement. Five interviewees participated in semi-structured interviews from March to May 2025 to collect data. Table 3 illustrates the iterative process of triangulating the interviews with internal secondary documents until data saturation was attained. This ensured that, as suggested by Fusch & Ness [35], no new themes or insights emerged. This approach improved the study's validity and reliability [36]. Design elements were prioritized, and DevOps emphasis areas were categorized as part of the data analysis process. After that, the Governance and Management Objectives (GMOs) were evaluated by combining relevant regulations with pertinent literature. After assessing the maturity levels of the seven governance components, capability gaps were found, and practical suggestions for improvement were developed. A systematic implementation plan and effect evaluation of the out-comes of prioritizing these recommendations according to factors including value, risks, and resources

4. RESULTS AND DISCUSSION

4.1. GMO prioritization result

The GMO prioritization was carried out by considering multiple factors, including regulatory frameworks, COBIT 2019 design factors, DevOps, AI insights, and the impact of IT service management. These parameters were weighted to determine their relative importance in supporting EnergyCo's IoT governance framework. The following table presents the prioritized GMOs, highlighting the most critical areas for enhancing IoT governance in line with EnergyCo's digital transformation goals.

The Accumulated score of 94 for ITGM objective DSS05—Managed Security Services (Table 4). In determining the design, several stages must be completed. First, the priority of IT Governance and Management (ITGM) objectives is established by calculating the influence of design factors, IT governance mechanisms that impact digital transformation (TD), and relevant literature on activities that affect IT service management.

The priority scores are derived from four main parameters: the Design Factors from COBIT 2019, which scored 90; the DevOps Focus Area [11], which scored 67 within COBIT 2019; regulatory frameworks, including ICT Minister No. 5/2021, which scored 100; and SOE Minister No.PER-2/MBU/03/2023 scored 100. Additionally, insights from three previous studies on IoT [27], [29] are integrated and scored 100. These scores are calculated by averaging the weights of these parameters, ensuring a balanced approach that aligns regulatory compliance, governance models, and academic insights.

The scores were obtained through a multi-criteria rating of each Governance and Management Objective (GMO) against four parameter groups: COBIT 2019 design factors, the COBIT 2019 DevOps focus area, national regulations (ICT Minister No. 5/2021 and SOE Minister No. PER-2/MBU/03/2023), and prior IoT-governance research. Each parameter was first scored on a 0–100 scale using expert judgment based on its relevance and impact on IoT governance at EnergyCo. The accumulated score for each GMO was then calculated as the arithmetic mean of these parameter scores. DSS05 (Managed Security Services) obtain the highest accumulated score (94), indicating that it is simultaneously highly constrained by regulation, strongly supported by existing design factors, and relatively less mature in terms of DevOps-oriented

http://dx.doi.org/10.30656/jsmi.v9i2.10803

Table 4. GMO prioritization result

ITGM Objective	COBIT 2019 Design Factor [17]	COBIT 2019 Focus Area DevOps [11]	ICT Minister No.5/2021	SOE Minister No.PER-2/MBU/03/2023	Previous Research			Accumulated Score
					IoT Governance Paper 1 [30]	IoT Governance Paper 2 [31]	IoT Governance Paper 3 [28]	
DSS05—Managed Security Services	90	67	100	100	100	100	100	94

capability level improvement and coverage of DSS05 governance components serve as the primary indicators of success. Within DSS05, the development effort specifically targets practices that are most affected by the comparatively lower DevOps score, such as automated security monitoring and continuous vulnerability management.

To assess the effectiveness and practical impact of the proposed IoT governance model, a set of Key Performance Indicators (KPIs) was evaluated during the research. These KPIs provide measurable evidence of the improvements achieved through the implementation of the governance framework. The following results were obtained:

1. Capability level improvement
   The average capability level for the DSS05 (Managed Security Services) domain is projected to increase from a baseline of 3.29 to a target level of 3.86 after the full implementation of the recommended improvements.
2. RRV-based recommendation prioritization
   Each recommendation was prioritized using the Resource × Risk × Value (RRV) formula. In this framework, each dimension Resource, Risk, and Value is scored from 1 (low) to 3 (high), resulting in a final score between 3 to 18. Recommendations scoring 10–18 were considered medium priority, while those scoring 1–9 were categorized as low priority. This method enabled structured decision-making regarding implementation focus and resource allocation.
3. Governance Improvement Recommendations
   A total of seven improvement recommendations were generated. Based on the RRV (Resource × Risk × Value) analysis, the recommendations are classified into medium- and low-priority categories.
4. Validation Effectiveness
   All proposed recommendations were validated through expert judgment involving both internal stakeholders from EnergyCo and an external IoT governance expert. The validation reached 100% approval, signifying consensus on the practical feasibility, strategic alignment, and potential benefits of the proposed improvements.
   During the validation workshop, the experts not only confirmed the overall relevance of the proposed IoT governance framework but also provided several critical comments. First, they highlighted the need to formalize key roles, such as CISO and Privacy Officer, which were initially implied but not explicitly defined in the framework. Second, they suggested refining the improvement recommendations by linking them more clearly to specific DSS05 management practices and to measurable KPIs. Third, they emphasized the importance of incorporating continuous security awareness activities into the DevOps pipeline rather than treating them as isolated training events. Based on this feedback, the framework and roadmap were revised by explicitly adding the missing roles, restructuring the recommendations around DSS05 practices, and integrating security awareness into the people-related initiatives. After these revisions and confirmation, all experts agreed that the framework was feasible, aligned with EnergyCo's context, and sufficiently actionable, as reflected in the 100% approval score.
5. Governance coverage
   The governance model successfully covered all seven governance components as defined by COBIT 2019's Governance and Management Objectives (GMOs). This includes dimensions such as processes, organizational structure, policies, information, culture, people, skills, and technology infrastructure, achieving 100% component alignment.

4.2. Analysis and gaps

4.2.1. *Process component*

The process component capabilities are assessed by examining the degree to which DSS05 and other key governance actions related to GMOs have been implemented (Table 5). The capability rating approach of COBIT, which represents achievement in several ratings, is used in this study. The COBIT rating system is used to evaluate capability levels**.** The actual state of each management practice within the evaluated Governance and Management is then mapped using the capability levels: Not Achieved (N) for 0% to 14% achievement, Partially (P) for 15% to 50%, Largely (L) for 51% to 85%, and Fully (F) for 86% to 100%. The outcomes of this capability level mapping serve as the foundation for both developing pertinent improvement suggestions and performing a gap analysis between the existing situation and the desired capability levels that EnergyCo expects.

Table 5. Capability level value

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

Table 6 analysis results show gaps in several DSS05 Process component practices, including DSS05.01, DSS05.02, and DSS05.07. Examining the Organization Structure component is the next step in the investigation. The comprehensive evaluation of the present condition of the Organization Structure component at EnergyCo (Table 7).

4.2.2. *Organization structure component*

The assessment of the organizational structure component refers to the organizational structure component within the COBIT 2019 DevOps Focus Area for each TKMTI objective. The roles that EnergyCo must fulfill within the organizational structure to achieve its objectives. System design and architecture management are handled by Architecture & Information Technology Security, which designs and oversees the technology infrastructure.

Table 7 presents the organizational structure of EnergyCo, showing how most of the key governance roles from COBIT 2019 are effectively covered, even though some roles like Chief Information Officer (CIO) and Chief Information Security Officer (CISO) are not explicitly listed. These roles are managed by departments such as Information Technology Systems and Architecture, as well as Information Technology Security, which handle critical areas including IT strategy, security, product management, and operational systems. However, certain roles, such as Privacy Officer, Release Manager, and Automation Manager, are not formally established, and their functions are distributed across multiple departments. This flexibility works in the current structure, but formalizing these roles would further improve clarity and governance, particularly as EnergyCo continues its digital transformation journey.

4.2.3. *Information component*

This section addresses the information components related to the DSS05 output flows that ensure the efficacy and integrity of enterprise IoT governance and strategic alignment. Table 8 summarizes EnergyCo's practices related to DSS05, as per COBIT 2019. It demonstrates that most key practices, such as malware prevention, network security, and endpoint security, are in place, with policies and regular evaluations being implemented. The company tracks security incidents, conducts penetration tests, and ensures proper access management for both physical and IT assets. However, EnergyCo could further improve in areas such as inventory management for sensitive documents and more detailed threat evaluations to better align with the full scope of governance and security practices outlined

Table 6. Process component

Management Practice	Achievement (%)	Capability Level
DSS05—Managed Security Services		
DSS05.01 Protect against malicious software.	100% F (Fully)	2
	92% F (Fully)	3
	50% P (Partially)	4
DSS05.02 Manage network and connectivity security.	100% F (Fully)	2
	50% P (Partially)	3
DSS05.03 Manage endpoint security.	100% F (Fully)	2
	75% L (Largely)	3
	75% L (Largely)	4
DSS05.04 Manage user identity and logical access.	100% F (Fully)	2
	92% F (Fully)	3
	83% L (Largely)	4
DSS05.05 Manage physical access to I&T assets.	100% F (Fully)	2
	100% F (Fully)	3
	75% L (Largely)	4
DSS05.06 Manage sensitive documents and output devices.	100% F (Fully)	2
	75% L (Largely)	3
	100% F (Fully)	4
DSS05.07 Manage vulnerabilities and monitor the infrastructure for security-related events.	25% P (Partially)	2

http://dx.doi.org/10.30656/jsmi.v9i2.10803

Table 7. Organization structure component

COBIT Organization Structure	Management Objective	Current State
DSS05—Managed Security Services		
Chief Information Officer	DSS05	The responsibilities of the CIO are managed by Vice President of Information Technology Systems, overseeing IT strategy, policies, and technology alignment.
Chief Information Security Officer	DSS05	The CISO role is managed by the Architecture & Information Technology Security team, responsible for overseeing IT security and risk management.
Business Process Owners	DSS05	The role is managed by the Directorate of Networks & Infrastructure and Information Technology Systems, which ensure IT processes align with business needs.
Head Human Resources	DSS05	The Director of Human Capital and Administration is responsible for managing HR functions, including talent development and employee welfare.
Head Development	DSS05	Product and service development responsibilities are managed by the Vice President of Information Technology Systems, ensuring innovation and IT service delivery.
Head IT Operations	DSS05	IT operations management is overseen by the Vice President of Infrastructure and Data Services, ensuring the smooth operation of systems and infrastructure.
Information Security Manager	DSS05	Information security is managed by Architecture & Information Technology Security, which is responsible for handling the implementation of security policies and controls.
Privacy Officer	DSS05	Privacy management is handled by the Information Security team, ensuring compliance with data protection regulations.
Product Owner/Manager	DSS05	Product management for IT is handled by Information Technology Systems, which oversees the development and lifecycle management of digital products and services.
Software Development Manager	DSS05	Software development and application management responsibilities are handled by the Vice President of Information Technology Systems, overseeing the creation and maintenance of software applications.
Testing Manager	DSS05	Software testing is managed by Information Technology Systems, ensuring quality control and testing of applications.
Systems Operations Manager	DSS05	Systems operations and infrastructure maintenance are managed by the Vice President of Infrastructure and Data Services, ensuring operational continuity and system maintenance.
Release Manager	DSS05	Software release management is handled by Information Technology Systems, overseeing software releases and deployments.
Automation Manager	DSS05	Process and system automation responsibilities are handled by Information Technology Systems, implementing automation solutions across IT operations.
Systems Architecture Manager	DSS05	System design and architecture management are handled by Architecture & Information Technology Security, which designs and oversees the technology infrastructure.

in COBIT 2019.

4.2.4. *People, skills, and competencies component*

The People, Skills, and Competencies component is analyzed based on the DSS05 domain, with details summarized in Table 9**.** The outline EnergyCo's key skills and competencies in Information Security. The company has implemented robust cybersecurity practices, including a strong cybersecurity organization (CSIRT), adherence to ISO 27001 standards, and regular penetration testing to identify and address vulnerabilities. EnergyCo also has a well-established security administration function that oversees access controls and manages security events. While the company is aligned with best practices, improving transparency on the outcomes of penetration testing and further formalizing specific security measures could enhance its overall security governance.

4.2.5. *Policies and procedures component*

The policies and procedures component is analyzed based on DSS05 domain to assess the adequacy of compliance and risk policies (Table 10).

Table 8. Information component

Management Practice	**Information Output**	**Current State**
DSS05—Managed Security Services		
DSS05.01 Protect against malicious software.	Malicious software prevention policy	EnergyCo has established a malicious software prevention policy, which includes regular updates to software defenses and anti-malware tools.
	Evaluations of potential threats	EnergyCo performs regular threat evaluations, but specific documentation regarding potential threats is not fully detailed.
DSS05.02 Manage network and connectivity security.	Connectivity security policy	EnergyCo has a comprehensive network connectivity security policy that defines security measures for data transmission and connectivity.
	Results of penetration tests	EnergyCo performs penetration tests, and the results are used to assess vulnerabilities in the network infrastructure and improve security.
DSS05.03 Manage endpoint security	Security policies for endpoint devices	EnergyCo has endpoint security policies in place to protect devices such as laptops, desktops, and mobile devices from security threats and unauthorized access.
DSS05.04 Manage user identity and logical access.	Results of reviews of user accounts and privileges	EnergyCo conducts reviews of user accounts and privileges periodically, ensuring that access rights are up-to-date and compliant with internal policies.
	Approved user access rights	The company ensures that approved user access rights are managed based on the periodic reviews of user accounts, ensuring that only authorized users have access to sensitive systems.
DSS05.05 Manage physical access to I&T assets.	Access logs	EnergyCo maintains access logs for all physical access to IT assets, including server rooms, data centers, and other critical infrastructure.
	Approved access requests	EnergyCo reviews and approves access requests to critical IT assets, ensuring only authorized personnel can access them.
DSS05.06 Manage sensitive documents and output devices.	Access privileges	EnergyCo applies access privileges to sensitive documents and output devices, restricting access to authorized personnel only.
	Inventory of sensitive documents and devices	There is no explicit inventory management for sensitive documents and devices, though policies on access control for such items are in place.
DSS05.07 Manage vulnerabilities and monitor the infrastructure for security-related events.	Security incident tickets	EnergyCo uses a ticketing system to manage and track security incidents, ensuring that incidents are addressed and resolved in a timely manner.
	Security incident characteristics	EnergyCo maintains security event logs to track all security events related to IT infrastructure, which helps in monitoring threats and vulnerabilities.
	Security event logs	EnergyCo analyzes security incident characteristics to identify patterns and root causes, allowing for proactive risk mitigation in future incidents.

http://dx.doi.org/10.30656/jsmi.v9i2.10803

Table 9. People, skills, and competencies component

Skills	Current State
DSS05—Managed Security Services	
Information Security	EnergyCo has a robust cybersecurity framework, including policies for malicious software prevention and incident response. The company's cybersecurity organization CSIRT was established to manage risks related to cyber threats.
Information Security Management	EnergyCo manages information security through regular updates to cybersecurity policies and effective implementation of ISO 27001 standards. The company's IT Master Plan and policies are aligned with business goals, ensuring effective protection of company data.
Penetration Testing	EnergyCo conducts penetration tests to assess vulnerabilities in their infrastructure. These tests are essential for enhancing security measures, though specific details on test results are not fully documented.
Security Administration	EnergyCo has a dedicated security administration team responsible for managing access control systems, ensuring secure access to sensitive data and IT assets, and monitoring security events and incidents. The team works with internal and external stakeholders to maintain a secure environment.
Information Security	EnergyCo has a robust cybersecurity framework, including policies for malicious software prevention and incident response. The company's cybersecurity organization CSIRT was established to manage risks related to cyber threats.
Information Security Management	EnergyCo manages information security through regular updates to cybersecurity policies and effective implementation of ISO 27001 standards. The company's IT Master Plan and policies are aligned with business goals, ensuring effective protection of company data.

The outline EnergyCo's Information Security Policy, which is designed to ensure the protection of corporate information, systems, and infrastructure. The company adheres to ISO 27001 standards and has established a Cybersecurity Incident Response Team (CSIRT) to handle cyber threats. EnergyCo is also in compliance with the Cyber and Cryptography Agency of Indonesia (BSSN), registering its policy to strengthen its cybersecurity posture and mitigate potential risks.

4.2.6. *Culture, ethics, and behavior component*

Table 11 evaluates the culture, ethics, and behavior component to see how organizational conduct and values facilitate the successful application of DSS05, especially when it comes to IoT governance. The Culture, Ethics, and Behavior component within EnergyCo underscores the company's dedication to cultivating a culture of security and privacy awareness. The Corporate Code of Conduct is actively socialized among employees and partners to reinforce ethical behaviour, with a focus on maintaining information security and confidentiality. This effort is supported by continuous training, awareness programs, and a strong ethical framework that guides all business practices.

4.2.7. *Services, infrastructure, and application components*

To accomplish the ITGM goal, the service, application, and infrastructure for each management practice are listed in Table 12 DSS05. The outlines the service, application, and infrastructure components critical to achieving the ITGM objective DSS05-Managed Security Service at EnergyCo. The company has implemented a comprehensive suite of security services, including email filtering systems, SIEM tools, and a Security Operations Center (SOC). EnergyCo also emphasizes the importance of identity and access management and runs continuous security awareness services to maintain a secure environment. These measures, along with third-party security assessments and URL filtering systems, ensure that the organization is prepared to manage security risks effectively.

Table 10. Policies and procedures component

Policy	Current State
DSS05—Managed Security Services	
Information security policy (Establish guidelines for protecting corporate information and related systems and infrastructure)	EnergyCo has a strong information security policy, aligned with ISO 27001 standards. The policy is focused on cybersecurity and includes the establishment of a cybersecurity organization (CSIRT) to manage cyber threats and ensure business continuity. The policy covers the protection of assets and data, with compliance registered with the Cyber and Cryptography Agency of Indonesia (BSSN)

http://dx.doi.org/10.30656/jsmi.v9i2.10803

Table 11. Culture, ethics, and behavior component

Key Culture Elements	Current State
DSS05—Managed Security Services	
Create a culture of awareness regarding user responsibility to maintain security and privacy practices.	EnergyCo emphasizes the importance of security and privacy awareness across the organization. The Corporate's Code of Conduct requires all employees to comply with ethical practices and responsibilities, which includes maintaining information security and confidentiality. EnergyCo also fosters a culture of integrity and awareness through training programs and regular socialization of the Code of Conduct.

4.3. Potential improvement

Based on the findings of the gap analysis in the preceding step, a three-part examination of possible enhancements was conducted: people, process, and technology. In addition to the components, types, and potential gaps, the following are the key findings of the analysis. Table 13 identifies specific gaps in EnergyCo's governance practices across the People, Process, and Technology aspects:

People Aspect: There is a need to formalize roles such as CISO, Product Owner, and Privacy Officer to clarify responsibilities and strengthen governance over cybersecurity and privacy. Additionally, there is a gap in penetration testing and security administration competencies. Increasing focus on cybersecurity training for employees, particularly through workshops and certification programs, will help address this gap and align with the governance of DevOps and IoT.

Process Aspect: Gaps exist in the inventory management of sensitive documents and devices, as well as the absence of clear procedures for conducting security incident evaluations and threat assessments. Establishing formal policies and procedures for inventory management and risk assessments will improve consistency in managing these areas, particularly in the context of IoT security and DevOps environments.

Technology Aspect: EnergyCo needs to integrate SIEM and SOC tools with its legacy IT systems to enhance real-time monitoring and response capabilities. Additionally, expanding endpoint security features to include advanced malware protection, mobile device management (MDM), and network segmentation will help ensure better protection, especially for IoT devices and within DevOps pipelines. By addressing these gaps, EnergyCo can strengthen its DSS05 practices and improve its overall security posture, aligning with COBIT 2019 standards for a comprehensive Managed Security Service framework.

4.4. Resource, risk, and value (RRV) analysis

The priorities were determined by summing the total scores of all suggested improvements. The recommendations with the highest scores were categorized as top priorities and grouped into three

Table 12. Services, infrastructure, and application component

Services, Infrastructure	Current State
DSS05—Managed Security Services	
Directory services	EnergyCo utilizes directory services to manage and authenticate users within its IT infrastructure, ensuring access control across systems.
Email filtering systems	EnergyCo employs email filtering systems to block phishing attempts and malware from entering the organization, enhancing communication security.
Identity and access management system	EnergyCo implements a comprehensive Identity and Access Management (IAM) system to manage user identities and access rights across various systems.
Security awareness services	EnergyCo runs security awareness programs for employees, focusing on the importance of data protection and security best practices.
Security information and event management (SIEM) tools	EnergyCo utilizes advanced security monitoring systems to oversee its infrastructure, although the use of specific SIEM tools is not highlighted.
Security operations center (SOC) services	There is no specific mention of a SOC (Security Operations Center). However, EnergyCo likely has centralized incident response capabilities.
Third-party security assessment services	EnergyCo engages third-party security assessments to identify vulnerabilities and strengthen the organization's cybersecurity posture.
URL filtering systems	EnergyCo implements URL filtering systems to block access to malicious websites and prevent employees from visiting harmful or unauthorized sites.

http://dx.doi.org/10.30656/jsmi.v9i2.10803

Table 13. Potential improvement

Component	Type	Gap	Potential Improvement
DSS05—Managed Security Services			
People Aspect			
Organizational Structure	Roles	CISO, Product Owner, and Privacy Officer roles are not explicitly defined in the organization.	EnergyCo should formalize roles such as CISO, Product Owner, and Privacy Officer to clarify responsibilities and improve governance over cybersecurity and privacy, particularly in IoT Governance.
People, Skills, and Competencies Component	Skill & Awareness	No detailed penetration testing skills or security administration competencies documented for employees.	Increase the focus on cybersecurity training for staff, particularly for roles in penetration testing and security administration, through workshops and certification programs, ensuring alignment with DevOps security practices and IoT security.
Culture, Ethics, and Behavior Component	Communicat ion	Security awareness communication is infrequent and not standardized across all teams.	Implement a regular security awareness campaign across departments with periodic refresher courses and internal communications to raise awareness about security responsibilities, fostering a DevOps security culture and integrating IoT security awareness.
Process Aspect			
Principles, Policies, and Procedures Component	Policy	Inventory management of sensitive documents and devices is not well defined or documented.	Establish a formal inventory management policy for sensitive documents and output devices, ensuring regular audits, categorization, and access control of these assets, aligning with IoT Governance and ensuring compliance across the organization.
Information	Procedure	No clear procedures for conducting security incident evaluations and threat assessments.	Develop and implement standardized procedures for assessing security incidents and evaluating potential threats, ensuring consistent and thorough risk management practices across DevOps environments and IoT security.
Technology Aspect			
Service, Infrastructure, and Application Component	Tools	SIEM and SOC tools do not fully integrate with legacy IT Systems.	Integrate SIEM and SOC tools with older IT infrastructure and systems to enhance real-time monitoring, automate threat detection, and improve incident response times, boosting IoT security monitoring.
	Features	Endpoint security measures do not cover all types of devices or possible attack vectors.	Expand endpoint security features, including advanced malware protection, mobile device management (MDM), and network segmentation, to provide a comprehensive defense strategy for all endpoints, particularly in DevOps pipelines and IoT environments.

areas: people, process, and technology. This categorization serves as a framework for executing the recommendations. Table 14 evaluates three primary aspects: the resources required, the risk impact in the event of failure, and the potential value of performance improvements. Each of these aspects is rated as Low, Medium, or High, and the overall score is calculated using the formula Score = Resource × Risk × Value. Based on the score, improvements are categorized into three priority levels: Low (1–9), Medium (10–18), and High (19–27). This categorization enables EnergyCo to prioritize and focus resources on initiatives with the greatest impact. Based on the RRV (Resource × Risk × Value) analysis, the prioritization results showed that four initiatives were classified as medium priority, and three as low-priority initiatives.

http://dx.doi.org/10.30656/jsmi.v9i2.10803

Table 14. Resources, risk, and value (RRV) analysis

Potential Improvement	Final Score	Category
Establish a formal inventory management policy for sensitive documents and output devices, ensuring regular audits categorization, and access control of these assets.	18	Medium
EnergyCo should formalize roles such as CISO, Product Owner, and Privacy Officer to clarify responsibilities and improve governance over cybersecurity and privacy.	12	Medium
Increase the focus on cybersecurity training for staff, particularly for roles in penetration testing and security administration, through workshops and certification programs.	12	Medium
Expand endpoint security features to include advanced malware protection, mobile device management (MDM), and network segmentation	12	Medium
Implement a regular security awareness campaign with periodic refresher courses.	8	Low
Develop and implement standardized procedures for security incident evaluations and threat assessments defense strategy for all endpoints.	6	Low
Integrate SIEM and SOC tools with older IT infrastructure and systems to enhance real-time monitoring, automate threat detection, and improve incident response times.	3	Low

4.5. Implementation roadmap

Table 15 outlines the implementation plan for key initiatives set for 2026 and 2027. These initiatives are designed to tackle the improvements identified through the RRV analysis. They provide a structured approach to enhancing organizational capabilities and addressing the identified gaps.

The EnergyCo's approach to improving its workforce, processes, and technology over the period of 2026 to 2027. The plan begins with strengthening key roles and providing necessary training, followed by updates to internal processes and the adoption of cutting-edge technologies.

4.6. Impact of recommendation implementation

Table 16 shows the impact of the improvement implementation on EnergyCo through a comparison of capability levels before and after the improvement was implemented. The implementation of the suggested recommendations is expected to significantly enhance the average capability of the DSS05 Process component, increasing it from 3.29 to 3.86. The benefits of these improvements extend beyond just the process component. This represents a significant improvement of approximately 18.24%, reflecting enhanced governance maturity across key components, including security processes, organizational roles, and

Table 15. Implementation roadmap

Potential Improvement	2026				2027			
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Establish a formal inventory management policy for sensitive documents and output devices, ensuring regular audits categorization, and access control of these assets.	■	■						
EnergyCo should formalize roles such as CISO, Product Owner, and Privacy Officer to clarify responsibilities and improve governance over cybersecurity and privacy.		■	■					
Increase the focus on cybersecurity training for staff, particularly for roles in penetration testing and security administration, through workshops and certification programs.			■	■				
Expand endpoint security features to include advanced malware protection, mobile device management (MDM), and network segmentation				■	■			
Implement a regular security awareness campaign with periodic refresher courses.				■	■			
Develop and implement standardized procedures for security incident evaluations and threat assessments defense strategy for all endpoints					■	■		
Integrate SIEM and SOC tools with older IT infrastructure and systems to enhance real-time monitoring, automate threat detection, and improve incident response times.						■	■	

http://dx.doi.org/10.30656/jsmi.v9i2.10803

risk management practices. The increase also indicates a stronger alignment with COBIT 2019 standards, suggesting that the implemented governance model contributes meaningfully to EnergyCo's digital transformation objectives.

The baseline value of 3.29 was obtained from a COBIT 2019 process-assessment workshop with EnergyCo's IT governance team, using the standard capability rating criteria. The estimated post-implementation level of 3.86 was derived through scenario-based assessment in which the same experts evaluated the expected effect of each recommendation on the relevant DSS05 management practices. The value of 3.86 should therefore be interpreted as a target capability level rather than an empirically measured outcome, and it will need to be validated in a follow-up assessment once the roadmap has been fully executed.

The previous capability level scores were assigned by EnergyCo's IT governance team and process owners during a facilitated COBIT 2019 assessment workshop, based on consensus scoring of each DSS05 management practice. The estimated capability level

Table 16. Estimation impact of recommendations

Management Practice	Previous Capability Level	Estimated Capability Level
DSS05.01 Protect against malicious software.	4	4
DSS05.02 Manage network and connectivity security.	3	4
DSS05.03 Manage endpoint security.	3	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.	3	4
DSS05.07 Manage vulnerabilities and monitor the infrastructure	2	3
Average Capability	3.29	3.86

Table 17. Estimation impact on the governance component

Before Implementation State	After Implementation State
CISO, Product Owner, and Privacy Officer roles are not explicitly defined in the organization.	EnergyCo formalizes roles like CISO, Product Owner, and Privacy Officer to clarify responsibilities and improve governance over cybersecurity and privacy, supporting IoT Governance.
No detailed penetration testing or security administration competencies documented for employees.	EnergyCo increases focus on cybersecurity training for staff, particularly for roles in penetration testing and security administration, through workshops and certification programs, ensuring alignment with DevOps security practices.
Security awareness communication is infrequent and not standardized across all teams.	EnergyCo implements a regular security awareness campaign across departments, with periodic refresher courses and internal communications to raise awareness about security responsibilities, aligning with DevOps practices.
Inventory management of sensitive documents and devices is not well defined or documented.	EnergyCo establishes a formal inventory management policy for sensitive documents and output devices, ensuring regular audits, categorization, and access control, improving IoT Governance by managing connected device security.
No clear procedures for conducting security incident evaluations and threat assessments.	EnergyCo develops and implements standardized procedures for assessing security incidents and evaluating potential threats, ensuring consistent and thorough risk management practices across DevOps and IoT environments.
SIEM and SOC tools are not fully integrated with legacy IT systems.	EnergyCo integrates SIEM and SOC tools to monitor and manage security information and incidents within the IT environment, improving IoT security monitoring across all connected devices.
Endpoint security measures do not cover all types of devices or possible attack vectors.	EnergyCo expands endpoint security features, including advanced malware protection, mobile device management (MDM), and network segmentation, to provide a comprehensive defense strategy for all endpoints, particularly in IoT environments and DevOps pipelines.

http://dx.doi.org/10.30656/jsmi.v9i2.10803

scores were then derived by the researchers, along with the same experts, in a follow-up session. In this session, the expected impact of each prioritized recommendation on the capability levels was evaluated and agreed upon.

Table 17 provides a comparison of the status before and after the implementation for the People, Process, and Technology aspects. The improvements to EnergyCo's governance components focus on formalizing key roles, such as CISO and Privacy Officer, enhancing cybersecurity training for staff, and improving security awareness across departments. It also outlines the implementation of a formal inventory management policy for sensitive assets, standardized procedures for evaluating security incidents, and the improved integration of SIEM tools and SOC services for real-time monitoring. Additionally, endpoint security will be strengthened with advanced malware protection and MDM, boosting the company's overall governance and security posture.

4.7. Research implication

The results of this study have both theoretical and practical implications. Theoretically, this research contributes to the development of IoT governance by offering an ambidextrous governance model that integrates both traditional COBIT 2019 and agile DevOps principles, an approach that has been rarely explored in previous studies. This combination addresses the complexity of managing IoT environments, especially within state-owned enterprises in the energy sector. Practically, the findings provide a structured governance model tailored to the operational context of EnergyCo, enabling more effective management of digital transformation initiatives. The RRV-based prioritization ensures that improvement efforts are directed toward areas with the highest strategic impact. The results also offer insights into aligning governance components across people, process, and technology dimensions, supporting decision-makers in enhancing governance maturity and agility simultaneously.

4.8. Discussion

The evaluation results across EnergyCo's governance components highlight meaningful insights that reinforce and extend prior literature. Compared to existing studies in related work, particularly those by [1], this study confirms that ambidextrous governance mechanisms, which balance control and agility, are indeed crucial for supporting digital transformation. However, the current research distinguishes itself by specifically applying these mechanisms to IoT governance in the energy sector, an area that has received limited attention. For instance, prior studies such as Sedrati *et al*. [28] and Morar *et al*. [27] proposed structured IoT governance frameworks but lacked real-world validation within SOEs. This study bridges that gap by applying and evaluating such a framework within EnergyCo using Design Science Research, thus offering an evidence-based model tailored for energy-sector SOEs. Additionally, the study confirms the need to formalize roles such as CISO and Privacy Officer, also emphasized in governance maturity models, including NIST SP 800-213A [31], while revealing that such roles are often informally distributed across departments, which affects clarity and accountability in IoT risk management.

Furthermore, this paper contributes by showing that DevOps principles, particularly in the form of continuous security integration and shared responsibility, align well with IoT governance needs. This aligns with the findings of Wiedemann *et al*. [20] and Plant et al. [21], who advocated for internal control and agility in DevOps environments. However, unlike previous research, this study directly integrates DevOps into a COBIT 2019-based governance framework and tests it through a real-world case, making it a practical contribution rather than a purely conceptual one. In terms of methodological contribution, this research extends the work of Fusch & Ness [35] by applying data saturation principles in qualitative interviews and triangulating the insights with internal documents, enhancing the study's validity. The structured prioritization of GMOs based on regulatory and design factor alignment also provides a replicable approach for similar organizations.

In summary, this paper's key contribution lies in developing a hybrid governance model that balances stability and agility, tailored to the regulatory and operational context of state-owned energy enterprises. It not only validates the relevance of ambidextrous IT governance for IoT but also advances prior literature by offering a contextual and operationalized framework for digital transformation in highly regulated environments. In addition to theoretical and practical contributions, the findings of this study are also measurable through well-formulated Key Performance Indicators (KPIs). Each KPI was evaluated using clear calculation methods rather than relying solely on descriptive interpretation. For instance, the improvement in capability level was determined through pre- and post-assessment scores using COBIT 2019, while the prioritization of governance improvement recommendations was guided by the RRV (Resource × Risk × Value) formula. Furthermore, the full validation from internal and external stakeholders, along with the complete coverage of COBIT 2019 governance components, demonstrates that the proposed framework is both comprehensive and implementable in real-world contexts.

The successful implementation of DevOps in the banking and telecommunications sectors, driven by faster time-to-market, enhanced automation of compliance, and improved service security, demonstrates that organizations can simultaneously pursue exploration (agility and innovation) and exploitation (control and risk management) through ambidextrous IT governance mechanisms. In banking, for example, institutions like J.P. Morgan and BRI achieved operational excellence by integrating DevOps practices with strong governance frameworks, ensuring that rapid development did not compromise regulatory compliance or system reliability. This dual capability is particularly relevant for state-owned energy enterprises, which face increasing demands for efficiency, digital innovation, and reliability under strict regulatory environments. As shown in BRI's transformation journey, balancing agile initiatives (such as DevOps and digital product teams) with traditional governance (including risk and audit functions) has enabled sustainable digital outcomes. This approach could be adapted in the energy sector to accelerate smart grid deployment, optimize operations, and ensure energy system resilience [1].

5. CONCLUSION

This research addresses a critical gap in the IoT governance literature by proposing a hybrid governance framework that integrates COBIT 2019 principles with adaptive DevOps practices. Existing studies have rarely combined these two approaches, especially in the context of state-owned enterprises (SOEs) within the energy sector. By focusing on EnergyCo, this study demonstrates how the proposed framework supports digital transformation while ensuring regulatory compliance, mitigating risk, and promoting operational agility. The findings align with the research objectives, particularly in strengthening governance through formalized roles, cybersecurity training, and the enhancement of security tools tailored to IoT environments.

Despite these contributions, the study is limited by its single-case design and the use of qualitative validation. These factors may constrain the generalizability of the results to broader organizational contexts. Future research is encouraged to replicate this model across different industries, explore cross-organizational adoption, and evaluate the real-time effectiveness of this approach in managing dynamic IoT-related risks. The framework and recommendations provided here offer a practical foundation for SOEs seeking to innovate securely while maintaining governance discipline in the face of emerging technologies.

ACKNOWLEDGMENT

We would like to extend our deepest gratitude to all those who supported us throughout the course of this research. A special thank you to EnergyCo for providing the necessary resources and funding that made this research possible.

REFERENCES

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

[2] H. D. Phi, V. P. Thi Hai, T. N. Duy, and V. N. Van, “The Impact of Digital Transformation on the Competitive Advantage of Businesses: Case Study of Businesses Providing Logistic Services in HCMC, Vietnam,” *Int. J. Manag. Econ. Invent.*, vol. 10, no. 07, pp. 3366–3379, Jul. 2024, doi: 10.47191/ijmei/v10i7.07.

[3] P. C. Verhoef *et al.*, “Digital transformation: A multidisciplinary reflection and research agenda,” *J. Bus. Res.*, vol. 122, pp. 889–901, 2021, doi: 10.1016/j.jbusres.2019.09.022.

[4] W. Shao, “The Role of Digital Transformation in Enhancing Organizational Agility and Competitive Advantages: A Strategic Perspective,” *Adv. Econ. Manag. Polit. Sci.*, vol. 154, no. 1, pp. 115–120, Jan. 2025, doi: 10.54254/2754-1169/2024.19552.

[5] J. Zhang, Y. Ye, C. Hu, and B. Li, “Architecture design and demand analysis on application layer of standard system for ubiquitous power Internet of Things,” *Glob. Energy Interconnect.*, vol. 4, no. 3, pp. 304–314, Jun. 2021, doi: 10.1016/j.gloei.2021.07.001.

[6] J. Sakhnini, H. Karimipour, A. Dehghantanha, R. M. Parizi, and G. Srivastava, “Security aspects of Internet of Things aided smart grids: A bibliometric survey,” *Internet of Things*, vol. 14, p. 100111, Jun. 2021, doi: 10.1016/j.iot.2019.100111.

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

[8] S. Zhang, “Research on the impact of digital transformation on enterprise innovation,” in *International Review of Economics & Finance*, vol. 90, Elsevier, 2024, pp. 544–551. doi: 10.2991/978-2-38476-257-6_65.

[9] J. Jöhnk, P. Ollig, P. Rövekamp, and S. Oesterle, “Managing the complexity of digital transformation—How multiple concurrent initiatives foster hybrid ambidexterity,” *Electron. Mark.*, vol. 32, no. 2, pp. 547–569, Jun. 2022, doi: 10.1007/s12525-021-00510-2.

http://dx.doi.org/10.30656/jsmi.v9i2.10803

[10] J. Zhen, C. Cao, H. Qiu, and Z. Xie, "Impact of organizational inertia on organizational agility: the role of IT ambidexterity," *Inf. Technol. Manag.*, vol. 22, no. 1, pp. 53–65, Mar. 2021, doi: 10.1007/s10799-021-00324-w.

[11] ISACA, *COBIT Focus Area: DevOps*. 2019. [Online]. Available: https://www.scribd.com/document/906261743/COBIT-Focus-Area-DevOps-Using-COBIT-2019

[12] D. Henriques, R. Pereira, I. S. Bianchi, R. Almeida, and M. M. da Silva, "How IT Governance can assist IoT project implementation," *Int. J. Inf. Syst. Proj. Manag.*, vol. 8, no. 3, pp. 25–45, Sep. 2021, doi: 10.12821/ijispm080302.

[13] 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.

[14] G. Vial, "Understanding digital transformation: A review and a research agenda," *J. Strateg. Inf. Syst.*, vol. 28, no. 2, pp. 118–144, Jun. 2019, doi: 10.1016/j.jsis.2019.01.003.

[15] Abhimanyu Ahluwalia, "Leveraging IoT for Smart Grids and Energy Management in Electrical Systems: Applications, Benefits, and Challenges," *J. Electr. Syst.*, vol. 20, no. 2, pp. 2802–2809, Apr. 2024, doi: 10.52783/jes.6853.

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

[17] S. Vejseli, A. Rossmann, and K. Garidis, "The Concept of Agility in IT Governance and its Impact on Firm Performance," *ECIS2022 Res. Pap.*, no. 98, pp. 6–18, 2022, [Online]. Available: https://aisel.aisnet.org/ecis2022_rp/98/

[18] ISACA, *COBIT 2019 Framework - Introduction and Methodology*. 2019. [Online]. Available: https://books.google.co.id/books/about/COBIT_2019_Framework.html?id=PmmDuQEACAAJ&redir_esc=y

[19] L. Jaime and J. Barata, "How can FLOSS Support COBIT 2019? Coverage Analysis and a Conceptual Framework," *Procedia Comput. Sci.*, vol. 219, no. 2022, pp. 680–687, 2023, doi: 10.1016/j.procs.2023.01.339.

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

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

[22] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Comput. Networks*, vol. 76, pp. 146–164, Jan. 2015, doi: 10.1016/j.comnet.2014.11.008.

[23] V. A. F. Almeida, D. Doneda, and M. Monteiro, "Governance Challenges for the Internet of Things," *IEEE Internet Comput.*, vol. 19, no. 4, pp. 56–59, Jul. 2015, doi: 10.1109/MIC.2015.86.

[24] C. Stephen Ball and D. Degischer, "IoT implementation for energy system sustainability: The role of actors and related challenges," *Util. Policy*, vol. 90, no. May, p. 101769, Oct. 2024, doi: 10.1016/j.jup.2024.101769.

[25] K. Boeckl *et al.*, "Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks," *Nistir 8228*, p. 44, 2019, [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2019/nist.ir.8228.pdf

[26] P. Sethi and S. R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications," *J. Electr. Comput. Eng.*, vol. 2017, pp. 1–25, 2017, doi: 10.1155/2017/9324035.

[27] B. Morar, Y. Barkawie, R. Balakrishnan, M. Khasawneh, J. Bangara, and H. A. Baker, "IoT Governance - Governance framework," 2021. [Online]. Available: https://www.deloitte.com/content/dam/assets-zone2/middle-east/en/docs/industries/technology-media-telecommunications/2024/me_IoT-Governance.pdf

[28] A. Sedrati, A. Mezrioui, and A. Ouaddah, "IoT-Gov: A structured framework for internet of things governance," *Comput. Networks*, vol. 233, no. May, p. 109902, Sep. 2023, doi: 10.1016/j.comnet.2023.109902.

[29] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks," *J. Inf. Secur. Appl.*, vol. 38, pp. 8–27, Feb. 2018, doi: 10.1016/j.jisa.2017.11.002.

[30] A. Sedrati, A. Mezrioui, and A. Ouaddah, "IoT

Governance: A state of the Art and a Comparative analysis," in *2022 13th International Conference on Information and Communication Systems (ICICS)*, IEEE, Jun. 2022, pp. 76–81. doi: 10.1109/ICICS55353.2022.9811219.

[31] National Institute of Standards and Technology, "Essay: Planning for Updating IoT Cybersecurity Guidance for theFederal Government (NIST SP 800-213 and NIST SP 800-213A)," 2021. [Online]. Available: https://www.nist.gov/system/files/documents/2025/06/03/Essay Update to 800-213 2025-06-03.pdf

[32] J. vom Brocke, A. Hevner, and A. Maedche, "Introduction to Design Science Research," in *Design Science Research. Cases*, no. November, 2020, pp. 1–13. doi: 10.1007/978-3-030-46781-4_1.

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

[34] J. Mackiewicz, "A Mixed-Method Approach," in *Writing Center Talk over Time*, New York: Routledge, 2018. | Series: Routledge research in writing studies: Routledge, 2018, pp. 37–60. doi: 10.4324/9780429469237-3.

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

[36] H. Morgan, "Using Triangulation and Crystallization to Make Qualitative Studies Trustworthy and Rigorous," *Qual. Rep.*, vol. 29, no. 7, pp. 1844–1856, Jul. 2024, doi: 10.46743/2160-3715/2024.6071.