Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control
Journal homepage: http://kinetik.umm.ac.id
ISSN: 2503-2267
Vol. 10, No. 4, November, Pp. 561-574

Ambidextrous blockchain governance to strengthen BankCo's digital transformation through COBIT 2019 traditional and DevOps

Salsabill Nur Aisyah[1], Rahmat Mulyana[*2], Tien Fabrianti Kusumasari[1]
Information Systems, Faculty of Industrial Engineering, Telkom University, Bandung, Indonesia[1]
Department of Computer and System Sciences, Stockholm University, Stockholm, Sweden[2]

Article Info
Keywords:
Ambidextrous Blockchain Governance, Digital Transformation, COBIT 2019, DevOps, APO12, Design Science Research, Case Study, Banking

Article history:
Received: June 14, 2025
Accepted: July 31, 2025
Published: November 01, 2025

Cite:
S. N. Aisyah, R. Mulyana, and T. F. Kusumasari, "Ambidextrous Blockchain Governance to Strengthen BankCo's Digital Transformation through COBIT 2019 Traditional and DevOps", *KINETIK*, vol. 10, no. 4, Nov. 2025.
https://doi.org/10.22219/kinetik.v10i4.2361

*Corresponding author.
Rahmat Mulyana
E-mail address:
rahmat@dsv.su.se

Abstract
The adoption of blockchain in banking accelerates digital transformation by enhancing transparency and operational efficiency. However, it also brings with it governance issues pertaining to accountability, compliance, and system integrity within a highly regulated environment. This study addresses these challenges by developing a blockchain governance solution based on ambidextrous approach within COBIT 2019's Traditional and DevOps Focus Areas. A governance model was built and evaluated through iterative steps. Until saturation was reached, information was gathered through key stakeholder interviews and checked with internal documentation such as yearly reports, risk frameworks, and policy records. The ambidextrous COBIT 2019 framework was used in the analysis for all seven governance components. Governance and Management Objectives (GMOs) were prioritized based on design factors, national regulations (POJK No.11/2022 and SOE Minister Regulation No.PER-2/MBU/03/2023), and insights from prior studies. APO12: Managed Risk was identified as the most prioritized GMO. A capability gap analysis revealed missing leadership roles, overlapping security responsibilities, and underdeveloped risk management practices. Recommendations include formalizing key governance roles and strengthening risk management process for blockchain and DevOps environments. These enhancements are expected to increase the maturity level of APO12 from 3.5 to 4.1, thereby improving BankCo's risk management, compliance, and innovation capabilities. Ultimately, the findings contribute to continuous digital innovation by aligning risk management practices with strategic performance goals and adaptive control mechanisms rooted in emerging technology principles.

1. Introduction

Digital transformation has become a top priority in various industries, including the banking industry, as well as the worldwide surge in digital technologies [1], [2]. In the face of ever-changing market obstacles, firms are motivated to innovate by operational efficiency and performance optimization. [3]. One of the prominent technologies is blockchain, which is known for its ability to create a permanent, transparent, and decentralized system of record [4]. The use of blockchain enables the integration of reporting systems, automation of accounting processes, and real-time management of transaction data across institutions. Moreover, in the context of Industry 4.0, blockchain supports strengthening transparency and interoperability among financial actors, while addressing key challenges such as data privacy and reliance on centralized infrastructure [5]. Blockchain not only supports the efficiency of business processes through smart contracts that execute agreements without intermediaries [6], but also increases data privacy, reduces the risk of errors [7], and reduces the likelihood of fraud [8].

There are challenges associated with the deployment of blockchain technology, though, particularly when it comes to regulatory ambiguity [9], concerns over data security [10], and the need for information technology (IT) governance that ensures reliability, accountability, and security [11]. IT governance becomes a critical factor to ensure that digital innovations remain within the control of the organization and do not pose systemic risks. Within this framework, an ambidextrous governance approach becomes relevant, combining stable and structured governance with the adaptive flexibility of Agile and DevOps approaches [12]. From the technical side, blockchain governance includes the design and management of tokens, transactions, and secure and efficient interoperability protocols [13]. This ambidextrous approach is considered capable of bridging the need for innovation exploration with the existence of stability exploitation in organizations undergoing digital transformation [14].

COBIT 2019 as a global framework in IT governance provides an integrated approach, from measuring, controlling, to evaluating the performance of an organization's IT governance and management [15]. ISACA has also

introduced the COBIT 2019 Focus Area for DevOps, which combines Agile and Lean principles to accelerate disruptive innovations such as blockchain, without sacrificing control and quality [16]. By combining the formal COBIT 2019 framework and agile DevOps, the Ambidextrous IT Governance approach was born [17], which supports IT development in a balanced way between innovation and stability [18].

In the banking industry, the requirement for thorough IT governance has been governed by official rules such as POJK No. 11/POJK.03/2022 [19] on the use of IT in commercial banks and SOE Minister Regulation No.PER-2/MBU/03/2023, which suggests the importance of sound corporate governance, including in the management of technology and innovation [20]. Both regulations emphasize strategy alignment, value creation, risk and resource management, and performance evaluation in IT governance [21]. However, digital transformation in the banking sector faces major challenges, such as complex IT management, blockchain ecosystem security, strict regulatory compliance, and complicated technology migration processes [22]. This transformation is crucial to address the dynamics of customer behavior, increasing competitive intensity, and rapid regulatory changes [23].

Governance is responsible for ensuring operational success. This points to the importance of IT governance as a key component in corporate governance [24], which goals to maximize IT's utilization as a strategic asset for the company [25], [26]. This governance implements performance assessment, risk management, resource management, and strategic alignment to strike a balance between risk control and value development [27], [28]. In the context of blockchain, governance establishes a structure of roles, responsibilities, policies, and control mechanisms to ensure security, compliance, and alignment with business objectives [29]. ISACA created COBIT 2019, a common framework for IT governance and management that attempts to maximize company value via the management of IT resources and risks. The framework is adaptive because of its factor design and focus areas that can be tailored to specific organizational needs [30]. In the financial sector, COBIT 2019 has proven effective as a comprehensive IT governance model in improving operational efficiency, maintaining information security, and ensuring regulatory compliance [31].

Combining DevOps with IT governance frameworks has become a strategic approach in driving more efficient, automated, and collaborative software development [32]. DevOps itself is a collection of principles that integrate the role of developers in the entire software lifecycle [16]. On the other hand, ambidextrous IT governance presents a balance between exploration—focuses on innovation, adaptation, and agility—and exploitation that emphasizes efficiency, control, and stability. Research from the national banking industry shows that successful digital transformation and enhanced organizational performance are driven by a combination of traditional and adaptive IT governance systems [25]. Related research also confirms that explorative and exploitative approaches have a positive impact on business achievement [33]. In an era of technological disruption and dynamic regulation, an ambidextrous approach is key for organizations to maintain stability while continuing to innovate through a blend of agile practices and traditional governance mechanisms [17].

Previous studies tend to discuss traditional IT control frameworks or agile development models separately. There is a lack of integrated governance models that explicitly combine the structured controls of COBIT 2019 with the agility and speed of DevOps, particularly in highly regulated industries such as banking [17]. Additionally, there is limited empirical research available that implements this ambidextrous governance approach to address specific blockchain challenges in real-world organizational environments in Indonesia [34]. This governance framework transforms ethical principles such as transparency into operational roles and structures, and integrates the RRV (resources, risks, values) perspective to support strategic decisions and innovation. This framework bridges external compliance with internal digital transformation needs, while filling gaps in literature [35].

This research focuses on digital transformation and suggests an ambidextrous blockchain governance architecture for the banking industry. This framework's design refers to both the DevOps concepts of the ISACA Focus Area and the Governance and Management Objectives (GMO) in COBIT 2019, which combine to create a balance between a formalized governance structure and the need for innovative flexibility [12]. With this methodology, the study offers conceptual and applicative contributions in the development of new technology governance relevant to the banking ecosystem in Indonesia. This study uses BankCo—a national bank currently undergoing digital transformation and actively implementing blockchain technology as part of its digital innovation efforts—as a case study. The main question to be answered is: *"How can an ambidextrous blockchain governance model based on COBIT 2019 and DevOps principles drive the success of digital transformation in banking institutions?"*

2. Research Method

A conceptual model serves as the foundation for the research's methodology, which designs solutions and evaluates results in the context of information systems using the Design Science Research (DSR) methodology. DSR provides systematic guidelines for understanding problems, producing artifacts, and carrying out assessments of scientific efficacy [36]. As shown in Figure 1, the DSR framework is composed of three interdependent components: the environment, which captures the contextual factors such as people, organizational structures, and technology; the information systems research process, which includes the iterative activities of building and evaluating artifacts; and the knowledge base, which provides theoretical and methodological foundations.

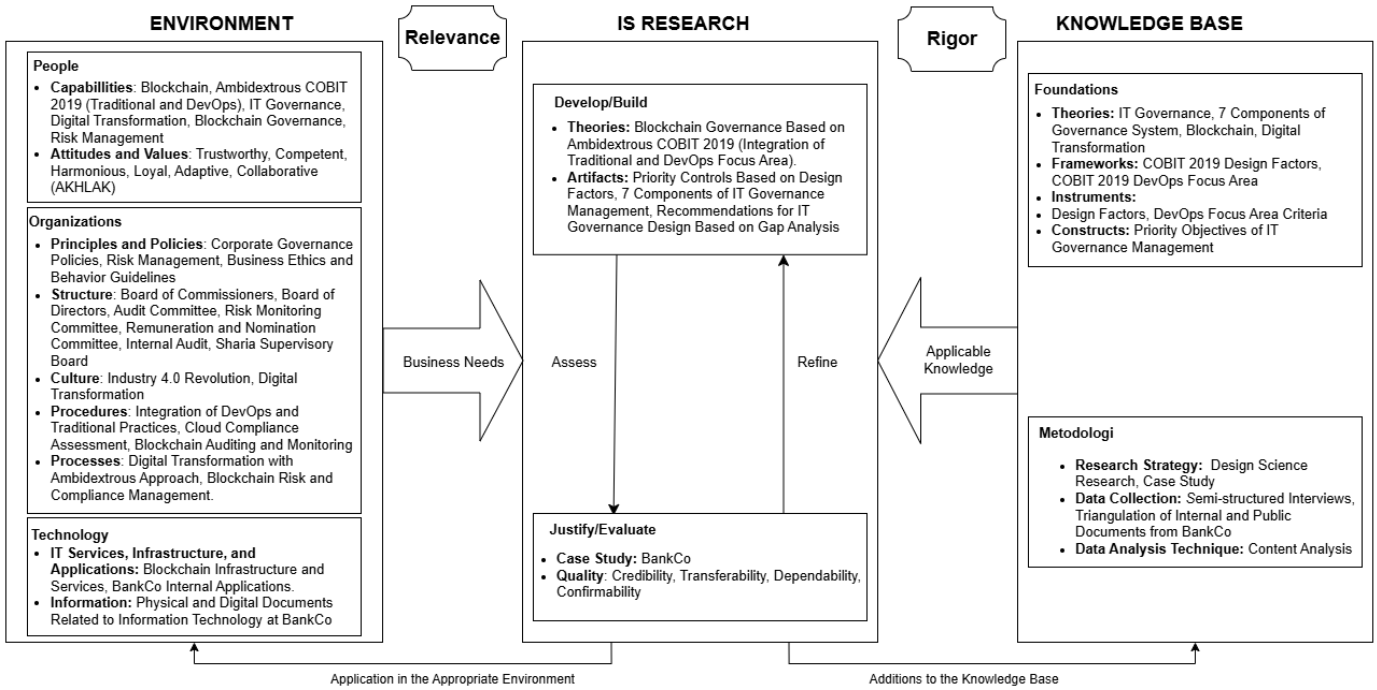

Figure 1. Research on Design Science, adapted from Hevner

Figure 1 illustrates the DSR framework applied in this research to develop a blockchain governance model adapted to the context of BankCo. The environment component captures contextual relevance by reflecting digital capabilities, transformation strategies, and formalized governance practices, including policies, structural roles, and supporting technologies. The IS research component implements the DSR cycle through iterative development and evaluation processes, producing governance artifacts such as design factors and blockchain oversight objectives developed using COBIT 2019 Traditional and DevOps, and verified through case-based assessments applying credibility, transferability, reliability, and confirmability.

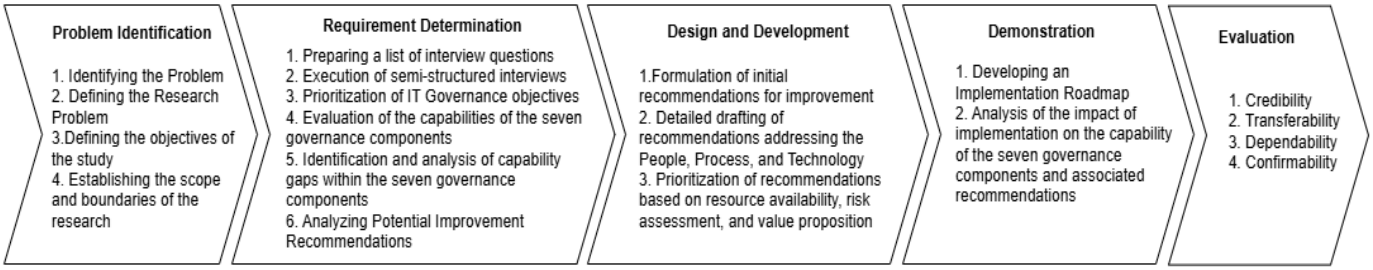

Figure 2. Research Process

Figure 2 illustrates the research flow with its five methodical stages, namely problem identification, requirement determination, solution design and development, demonstration, and performance evaluation [37]. This research employs a case study methodology as suggested by Yin [38], which is appropriate for investigating intricate contemporary phenomena inside real-life situations, particularly when the inquiry aims to address "how" or "why" concerns. The case study method is appropriate for examining how BankCo implements ambidextrous blockchain governance to support its digital transformation. The first stage began by clearly identifying the core problem and research objectives, then deepening the understanding through a thorough literature review to ensure the focus of the research is aligned with the context and real needs [37].

The second stage is requirement determination, concentrating on gathering information to fully comprehend the research problem. Key BankCo officials participated in semi-structured interviews conducted both in-person and online over several sessions to gather primary data. In addition, secondary data were used to enrich the analysis. Table 1 presents the primary data.

Table 1. Primary Data

Respondent	Positions	Date
Respondent 1 (R1)	IT Strategic Planning & Governance Officer	March – May 2025
Respondent 2 (R2)	Digital & Operation Risk Management Officer	
Respondent 3 (R3)	IT Security Officer	
Respondent 4 (R4)	IT Strategic Planning & Development Officer	
Respondent 5 (R5)	Internal Audit Officer	

Table 1 shows that semi-structured interviews were the main technique used in this study to collect primary data with key participants, namely the VP of IT Strategic Planning & Governance and the Digital & Operation Risk Management, conducted via Microsoft Teams to explore relevant information. In addition, Table 2 shows the secondary data.

Table 2. Secondary Data

Secondary data	Description
BankCo Profile	Provides an overview of BankCo's general profile.
BankCo Annual Report 2024	Contains information regarding financial performance, achievements, and strategies implemented during the fiscal year.
BankCo Sustainability Report 2024	Details BankCo's efforts and initiatives in achieving social, environmental, and economic sustainability goals.
Regulations	Includes regulations relevant to BankCo's business activities and operations.

The data collection process utilized both primary and secondary data. This strategy was applied to obtain information that was not only in-depth and comprehensive but also highly valid through the triangulation process, by comparing multiple sources to enhance the precision and reliability of the study's findings.

The third stage, design and development, includes an in-depth analysis of improvement recommendations by considering the dimensions of resource, risk, and value. The results of the analysis were then formulated into structured recommendations with a comprehensive approach through three main perspectives, namely the people aspect, the process aspect, and the technology aspect.

The fourth stage is the demonstration phase, which includes the development of a roadmap to guide the timing of the implementation of improvements, as well as pre- and post-implementation impact analysis to evaluate the efficiency of the suggested solution.

The fifth stage is evaluation, which is carried out using the four primary characteristics of qualitative research, namely credibility, transferability, dependability, and confirmability. These four aspects are used to evaluate the research's quality and dependability before the procedure is deemed finished [37]. Using the criteria of credibility, transferability, dependability, and confirmability, the evaluation is conducted through a case study at BankCo [39].

Design factor prioritization and DevOps target area classification were integrated into the data analysis. Following that, relevant research and legal requirements are combined to evaluate the Governance and Management Objectives (GMO). Data credibility was assured by cross-referencing interview results with internal documentation. Iterations of data gathering and analysis were conducted until saturation was achieved and no meaningful information was found [40]. Maturity levels for each of the seven governance components are used to find competence gaps and create recommendations for practical improvements. A structured implementation roadmap and implementation impact were the results of further prioritizing these recommendations based on risk, value, and resource considerations.

3. Results and Discussion

The DevOps Focus Area design criteria of COBIT 2019, IT governance and management's (ITGM) main goals, the governance process mechanisms, and the current regulatory standards were all used to thoroughly examine the gathered data. These analytical dimensions served as the basis for evaluating the relevance and urgency of ITGM goals, which were further explored using the seven main elements of the COBIT 2019 DevOps Focus Area: information flows, organizational structures, process mechanisms, human capital, skills and competencies, procedural frameworks and governing principles, ethical and cultural behavior, service capabilities, infrastructure readiness, and application architecture.

3.1 GMO Prioritization Result

The prioritization displayed in Table 3 is the result of integrating various references, including COBIT 2019 Design Factors and DevOps Focus Areas from ISACA [41], [42], regulations such as POJK No.11/2022 [19] and SOE Minister Regulation No.PER-2/MBU/03/2023 [20], as well as findings from previous research [43], [44], [45]. Every source provides a weighted score that represents its degree of significance and impact on blockchain governance prioritization.

The final score was determined through a weighted average calculation, resulting in a balanced prioritization based on a combination of regulatory demands, governance framework, and conceptual findings from the research.

Table 3. GMO Prioritization Result

Factor Considered	GMO Prioritization
	APO12-Managed Risk
COBIT 2019 Design Factor [30]	70
COBIT 2019 DevOps Focus Area [41]	33
POJK No. 11/2022 [19]	100
SOE Minister Regulation No.2/2023 [20]	100
Blockchain Governance Paper 1 [43]	100
Blockchain Governance Paper 2 [44]	100
Blockchain Governance Paper 3 [45]	100
Final Score	**86**

Based on the accumulated weighting results in Table 3, the top priority in GMO is APO12—Managed Risk, with a final score of 86. The weights from the many sources indicated in the table were merged to create this score, which represents the combined impact of prior Blockchain governance research, pertinent laws, and COBIT 2019 design factor.

3.2 Gap Analysis

3.2.1 Process Component

The competence of the process component was assessed by examining each step in the context of the selected IT Governance and Management (ITGM) objectives. The target levels were determined based on the organization's strategic goals. This section focuses on the APO12 Risk Management objective, as presented in Table *4*.

Table 4. Process Component

Management Practices	Achievement (%)	Capability Level
APO12: Managed Risk		
APO12.01 Collect data	100% Fully	2
	75% Largely	3
	100% Fully	4
APO12.02 Analyze risk	92% Fully	3
	50% Partially	4
	100% Fully	5
APO12.03 Maintain a risk profile	100% Fully	2
	100% Fully	3
	75% Largely	4
APO12.04 Articulate risk	88% Largely	3
	100% Fully	4
APO12.05 Define a risk management action portfolio	100% Fully	2
	100% Fully	3
APO12.06 Respond to risk	75% Largely	3
	100% Fully	4
	100% Fully	5

The results shown in Table *4* indicate that four gaps were identified within the APO12 practices—specifically in APO12.1 Collect Data, APO12.2 Analyze Risk, APO12.3 Maintain a Risk Profile, and APO12.5 Define a Risk Management Action Portfolio.

3.2.2 Organizational Structure Component

The organizational structure, which serves as the primary decision-making body within the business, is assessed in this section. Table 5 summarizes the results of the evaluation of BankCo's organizational structure.

Table 5. Organization Structure Component

COBIT Organization Structure	Current State
Chief Information Officer	The IT Director leads the strategic planning and management of all aspects of information technology.
Chief Risk Officer	Held by the Director of Risk Management who leads the strategic and operational risk control in the company.
Chief Digital Officer	The SEVP of Digital Business directs digital product innovation and digital transformation initiatives.
Chief Technology Officer	The CTO position is formally called the IT Operations Manager who handles the technical and operational aspects.
Chief Information Security Officer	Held by the IT Security Manager who is in charge of developing policies and managing information security risks.
Information Security Manager	Tasks are aligned with the IT Security Manager, focusing on the implementation of security controls and policy compliance.
Business Continuity Manager	This role falls under the Operational Risk Management Division which handles business resilience to disruptions.
Head Development	The application development unit resides in the IT Directorate which manages the design and maintenance of digital solutions.
Head Architect	A Chief IT Architect position is in place and functioning in line with technology architecture design responsibilities.
Head IT Administration	The IT Administration Unit provides administrative support and technical services for IT operations.
Project Management Office	IT Directorate and manage project execution and risk oversight in digital initiatives.
Head IT Operations	Manage daily IT infrastructure and service operations within the scope of the IT Operations function.
Business Process Owners	Certain business units are designated as process owners with responsibility for IT performance and risk.
Service Manager	This role is located on the IT Operations team, which handles the management of IT services, operations, and support.
Privacy Office	Held by the Data Management & Analytics function that ensures data privacy and regulatory compliance.
Enterprise Risk Committee	The Director of Risk Management, who oversees corporate risk governance overall, heads the committee.
Data Management Function	Implemented by the Data Management & Analytics team that ensures data quality and supports business analysis.

Table 5 shows that most of the key roles in IT governance and risk management are established and functional, with no significant role gaps. However, there is no specialized unit to handle new technologies such as blockchain. The integration of risk management in the rapid DevOps cycle has also not been optimized, causing the mitigation process to be reactive. Additionally, the efficacy of risk control and system resilience may be weakened in blockchain and DevOps systems due to the absence of real-time risk management.

3.2.3 Information Component

At this stage, the assessment of the information component was carried out using the current state of information available at BankCo. The present state of the bank is described in detail in Table 6.

Table 6. Information Component

Management Practice	Information Output	Current State
APO12.01 Collect data	Emerging risk issues and factors	IT & Digital Risk, Regulatory Compliance Risk and Third-Party Integration
	Data on risk events and contributing factors	Information Asset Risk Register and Risk Assessment
	Data on the operating environment relating to risk	Incident Management Log
APO12.02 Analyze risk	Risk analysis results	Register of Information Asset Risk
	I&T risk scenarios	Regulatory Compliance Risk and Third-Party Integration

Management Practice	Information Output	Current State
	Scope of risk analysis efforts	No specific Blockchain available yet by still combining with other technologies in IT & Digital Risk
	Aggregated risk profile, including status of risk management actions	Report on Risk Profiles
APO12.03 Maintain a risk profile	Documented risk scenarios by line of business and function	These are generally available for technology areas in IT & Digital Risk, Regulatory Compliance Risk and Third-Party Integration
	Risk analysis and risk profile reports for stakeholders	Risk Profile Report
	Results of third-party risk assessments	External Audit
APO12.04 Articulate risk	Opportunities for acceptance of greater risk	BankCo has formulated and documented a Risk Appetite Statement (RAS) that organizes the handling of risks
APO12.05 Define a risk management action portfolio	Project proposals for reducing risk	The risk management document already contains a project proposal from BankCo to reduce the risk
	Risk impact communication	Reports on IT risk and incident escalation
APO12.06 Respond to risk	Risk-related root causes	Incident reports and risk assessments
	Risk-related incident response plans	Reporting risk and responsiveness to the IT team based on key risk indicators

As shown in Table 6, according to the assessment's findings, BankCo is lacking two crucial components: specified risk scenarios for each function and business line and a documented scope of risk analysis activities.

3.2.4 People, Skills, and Competencies Component

Table *7* shows the stage where the focus is on assessing the People, Skills, and Competencies component. The objective is to evaluate if human resource capabilities match the roles and responsibilities required to enable ITGM deployment.

Table 7. People, Skills, and Competencies Component

Skills	Current State
Business risk management	Internal training, workshops, and risk certification
Information assurance	There are specialized domains of Information and Cyber Security and Data Privacy that govern data security and reliability
Risk management	BankCo currently has a risk management framework that covers digital, cyber, third-party, and emerging risks, including potential risks from blockchain implementation

According to the evaluation results of the People, Skills, and Competencies component in Table *7*, BankCo has effectively met all skill requirements, and no gaps were found.

3.2.5 Principles, Policies, and Procedures Component

Table *8* presents the analysis of the Principles, Policies and Procedures component with reference to the existing conditions in BankCo. The objective is to identify how well the principles and rules align with ITGM's ideal standards and to evaluate the consistency of the policy and procedure implementation in supporting BankCo's objectives.

Table 8. Principles, Policies, and Procedures Component

Policy	Current State
Enterprise risk policy	Enterprise risk policies covering strategic, operational, compliance, and general digital risks
Fraud risk policy	General policy for fraud risk prevention and handling

The analysis of this component, as presented in

Table *8*, highlights a gap in the Fraud Risk Policy, which requires further development and refinement.

3.2.6 Culture, Ethnics, and Behavior Component

Table *9* shows that the Culture, Ethics and Behavior component is assessed with reference to the actual cultural environment at BankCo. This evaluation aims to understand how well the organizational culture and behavioral values are embedded within the company.

Table 9. Culture, Ethnics, and Behavior Component

Key Culture Elements	Current State
To support a transparent and participatory risk culture, senior management should set direction and demonstrate visible and genuine support for incorporation of risk practices throughout the enterprise. Management should encourage open communication and business ownership for I&T-related business risk. Desirable behaviors include aligning policies to the defined risk appetite, reporting risk trends to senior management and risk governing bodies, rewarding effective risk management, and proactively monitoring risk and progress on the risk action plan.	As part of the application of corporate governance that incorporates the principles of transparency, BankCo has implemented risk management procedures into place.

The evaluation findings for this component are shown in
Table *9*. It was found that BankCo has met all cultural and ethical elements as recommended by COBIT 2019, with no gaps identified.

3.2.7 Service, Infrastructure, and Application Component

As shown in Table 10, these components were assessed by examining the real conditions of service delivery, infrastructure, and applications at BankCo. The objective was to measure the suitability, availability, and capability of the technology used to support the implementation of ITGM.

Table 10. Service, Infrastructure, and Application Component

Service, Infrastructure, and Application	Current State
Crisis management services	BankCo has crisis management services that cover operational, digital and cyber risks such as SIEM
Governance, risk and compliance (GRC) tools	BankCo implements GRC framework to manage IT risk
Risk analysis tools	BankCo makes use of risk scoring, risk heatmaps, and Risk Control Self-Assessment (RCSA)
Risk intelligence services	BankCo utilizes general intelligence services to monitor IT and cyber risks, such as threat intelligence

The analysis, summarized in Table 10, reveals a notable gap around Risk Intelligence Services, indicating the need for further enhancement in this domain.

The implementation of blockchain technology is driving digital transformation in the banking industry, resulting in for flexible and strong IT governance. BankCo, as a case study, faced challenges in aligning technological innovation with operational stability, especially when integrating a dynamic DevOps approach [32]. This study highlights the significance of an ambidextrous governance framework based on COBIT 2019 that can effectively build blockchain governance by integrating DevOps approaches with traditional focus areas [30], [34]. The findings reinforce previous studies that highlighted the urgency of structural roles, risk management, and synergy between development and operations in dealing with blockchain governance challenges [43], [44], [45]. The research also reveals the unique context at BankCo, including the lack of integration between functions as well as automation limitations that have not been covered by conventional frameworks. By bringing together theoretical approaches, this research provides insights for the development of contextualized and applicable blockchain governance, especially in supporting sustainable digital transformation in the Indonesian banking industry.

3.3 Potential Improvement

The next stage was to develop improvement strategies according to the findings of the seven capacity components' gap analysis and ITGM priority APO12. Table 11 highlights the three main aspects that need to be strengthened—people, process, and technology—as well as the types of improvements that are relevant for each component.

Table 11. Potential Improvement

Component	Type	Potential Improvement
Aspect: People		
Organization structure	Communication	Strengthen the organizational structure with cross-functional collaboration and real-time communication between DevOps, security, and risk teams
Aspect: Process		
Process	Record	Adding a recording system for risk events, incidents, and impacts specific to blockchain technology.
Process	Procedures	Adding separate procedures to identify, measure, and monitor Blockchain-specific KRIs
Process	Policy	Adding a Risk Appetite Statement policy specific to Blockchain technology
Process	Procedures	Create specific procedures for incident handling and risk response based on blockchain technology
Principles, Policies, and Procedures Component	Policy	Establish policies for preventing and handling fraud risks based on digital technology and Blockchain
Information	Policy	Create clear guidelines for the application and risk management of blockchain technology to avoid it being grouped together with other IT and digital risks
Information	Procedures	Create specific procedures to identify, analyze, and mitigate blockchain risks, including procedures for managing compliance, third-party integration, and blockchain audits
Aspect: Technology		
Service, Infrastructure, and Application	Technology	Adding blockchain specific monitoring features to the existing intelligence platform

Table 11 shows gaps in BankCo's governance related to blockchain integration, incident handling procedures, and relevant risk response. Specific mechanisms for risk mitigation, compliance management, third-party integration, and auditing of blockchain systems are also needed to ensure accountable and adaptive governance.

3.4 Resource, Risk, and Value (RRV) Analysis

Table *12* shows the RRV calculation, presenting the scores and categories for Resource, Risk, and Value (RRV) analysis to facilitate efficient resource allocation and decision-making in a project [46]. The assessment of resource aspects includes the involvement of internal and external personnel to support the implementation of solutions [47], while the risk assessment is based on the potential impact of failure, both limited to one work unit and on an organizational scale [48]. On the other hand, the value aspect reflects the level of contribution of the solution to improving performance, ranging from the scope of operational units to the entire institution. These three aspects are classified on a weight scale of Low (1-9), Medium (10-18), and High (19-27) [47].

Table 12. RRV Analysis

Potential Improvement	Final Score	Priority
Aspect: People		
Strengthen the organizational structure with cross-functional collaboration and real-time communication between DevOps, security, and risk teams	12	Medium
Aspect: Process		
Adding a recording system for risk events, incidents, and impacts specific to blockchain technology.	12	Medium
Adding separate procedures to identify, measure, and monitor Blockchain-specific KRIs	12	Medium

Potential Improvement	Final Score	Priority
Adding a Risk Appetite Statement policy specific to Blockchain technology	18	Medium
Create specific procedures for incident handling and risk response based on blockchain technology	6	Low
Establish policies for preventing and handling fraud risks based on digital technology and Blockchain	6	Low
Create clear guidelines for the application and risk management of blockchain technology to avoid it being grouped together with other IT and digital risks	18	Medium
Create specific procedures to identify, analyze, and mitigate blockchain risks, including procedures for managing compliance, third-party integration, and blockchain audits	12	Medium
Aspect: Technology		
Adding blockchain specific monitoring features to the existing intelligence platform	3	Low

Table *12* identifies the items as "Medium" and "Low," with a score of 18 being the highest and 3 being the lowest. Priorities have been determined by assigning respective scores to resources, risks, and improving overall value.

3.5 Implementation Roadmap

The implementation roadmap for the major projects scheduled for 2026 and 2027 is shown in

Table *13*. By offering an organized method for strengthening organizational capabilities and filling in identified gaps, the potential improvements discovered in the RRV) analysis are the focus of these initiatives. The strategy to accomplish these objectives is shown in the table. This ensures that significant modifications are effectively integrated into the organization's strategic plan.

Table 13. Implementation Roadmap

Recommendation	2026				2027			
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Aspect: People								
Strengthen the organizational structure with cross-functional collaboration and real-time communication between DevOps, security, and risk teams								
Aspect: Process								
Adding a recording system for risk events, incidents, and impacts specific to blockchain technology								
Adding separate procedures to identify, measure, and monitor Blockchain-specific KRIs								
Adding a Risk Appetite Statement policy specific to Blockchain technology								
Create specific procedures for incident handling and risk response based on blockchain technology								
Establish policies for preventing and handling fraud risks based on digital technology and Blockchain								
Create clear guidelines for the application and risk management of blockchain technology to avoid it being grouped together with other IT and digital risks								
Create specific procedures to identify, analyze, and mitigate blockchain risks, including procedures for managing compliance, third-party integration, and blockchain audits								
Aspect: Technology								
Adding blockchain specific monitoring features to the existing intelligence platform								

As shown in

Table *13*, the roadmap takes two years to develop, from 2026 to 2027, divided into four quarters each year. The recommendations can begin to be implemented from the first quarter of 2026 to the second quarter of 2027.

3.6 Estimated Impact of Recommendations on BankCo

Table 14 shows the measurable increase in process capability that results when important recommendations are put into practice. Competency levels indicate better adherence to risk management effectiveness.

Table 14. Estimated Impact of Recommendation Process Component

Management Practice	Previous Capability level	Estimated Capability After Recommendation
APO12.01 Collect data	3	4
APO12.02 Analyze risk	4	5
APO12.03 Maintain a risk profile	4	4
APO12.04 Articulate risk	4	4
APO12.05 Define a risk management action portfolio	3	3
APO12.06 Respond to risk	3	5
Total Amount	21	25
Total Score	3,5	4,1

As shown in

Table 14, the GMO APO12 capability level increased from 3.5 to 4,1 indicating improved compliance with risk management effectiveness in BankCo.

Table *15* shows the estimated impact on Organizational Structure, Information, People, Policies, and Procedures, and Services, Infrastructure, and Applications Components.

Table 15. Impact of Recommendation Implementation

Pre-Implementation	Post-Implementation
Process Component	
Capability level 3.5	Capability level 4
Adding a recording system for risk events, incidents, and impacts specific to blockchain technology.	Blockchain specific record keeping systems are available, making monitoring, auditing, and impact analysis easier
Adding separate procedures to identify, measure, and monitor Blockchain-specific KRIs	Specialized procedures available for blockchain KRIs, improving detection speed and accuracy
Adding a Risk Appetite Statement policy specific to Blockchain technology	Create a clear RAS for blockchain, increasing the clarity of acceptable risk limits
Create specific procedures for incident handling and risk response based on blockchain technology	Establishment of blockchain-specific handling procedures, improving mitigation response
Organization Structure Component	
Strengthen the organizational structure with cross-functional collaboration and real-time communication between DevOps, security, and risk teams	Improve efficiency, minimize errors through automation, and accelerate the handling of risk vulnerabilities
Information Component	
Create specific policies related to the use and risk management of blockchain technology, so that they are no longer grouped together in general with other IT & Digital Risk	Independent blockchain policies, making it easier to manage compliance and control
Create specific procedures to identify, analyze, and mitigate blockchain risks, including procedures for managing compliance, third-party integration, and blockchain audits	Detailed procedures, strengthening the blockchain risk management process
Principles, Policies, and Procedures Component	
Establish policies for preventing and handling fraud risks based on digital technology and Blockchain	There is a blockchain specific fraud prevention policy, enhancing protection and supervision.
Service, Infrastructure, and Application Component	
Adding blockchain specific monitoring features to the existing intelligence platform	Blockchain monitoring feature available, enabling real-time monitoring

Table *15* shows the governance improvements after the recommendations were implemented, including blockchain-specific risk logging, KRIs and RAS procedures, and faster incident handling. Business roles were clarified, policies were separated from general IT risks, and real-time monitoring features were added to support stronger oversight and control.

3.7 Discussion

This research identifies significant institutional challenges faced by technology-enabled financial organizations, particularly in the context of complex blockchain integration. While existing governance frameworks comply with regulations, traditional methods are not enough to satisfy the dynamic needs of innovation. This emphasizes the need for a shift towards adaptive and ambidextrous governance models that combine regulatory compliance with innovative flexibility. Research from BankCo demonstrates that the difficulties presented by blockchain technology have not been adequately addressed by either fully control-based or totally agile governance frameworks, including undefined systemic risks and inherent ethical dilemmas. This methodological gap's appearance indicates that operational responsiveness and structural stability must be reconciled. The ambidextrous blockchain governance model proposed in this research integrates the DevOps methodology of COBIT Focus Areas with the control concepts of COBIT 2019, thus aligning with national regulations such as POJK No.11/2022 and SOE Minister Regulation No.PER-2/MBU/03/2023.

This research contributes theoretically by articulating the dual-mode model into an applicable empirical framework, addressing the limitations of previous philosophical approaches that lack technical guidance [37]. Different from macro frameworks that are not integrated with IT systems such as COBIT 2019, this model is able to translate ethical principles such as fairness and transparency into concrete roles, processes, and organizational structures [26]. Its added value also lies in embedding the RRV principle for strategic decision-making that considers feasibility, compliance, and value creation [46]. The integration of blockchain governance controls in Traditional COBIT and DevOps structures allows organizations to bridge external audit demands and internal innovation capacity, reflecting an important leap in the literature [15], [32], [37].

Particularly, the redefinition of blockchain governance as an integrated system that supports institutional resilience and ethical adaptability in digital banking offers a more applicable approach than previous abstract models. With a roadmap that matches BankCo's maturity level and regulatory needs, as well as the establishment of oversight functions, accountability mechanisms, and standardized procedures for bias and ethics testing, the model has shown to improve the APO12 maturity score from 3.5 to 4.1. These findings confirm that blockchain governance can serve as a strategic lever in accountable and innovative digital transformation. The research also provides practical recommendations for policymakers and industry players, emphasizing the importance of institutionalizing blockchain governance as a core function, establishing cross-functional risk councils, and strengthening decision-making clarity through the development of dedicated RAS and blockchain-based fraud prevention policies.

4. Conclusion

This research has a concerning set of limitations, including possible bias and a scope limited to the BankCo case study. The integration of the ambidextrous COBIT 2019 framework with DevOps principles provides a systematic approach in improving IT governance to support blockchain-based digital transformation. Emphasis on the APO12 Managed Risk domain and addressing gaps in people, processes, and technology successfully drove an increase in GMO capability from level 3.5 to 4, even though the organization's strategic goals still require constant improvement.

Presenting an IT governance strategy that integrates traditional DevOps principles with contemporary practices to facilitate end-to-end blockchain-based transformation in the banking industry is the research's scholarly contribution. The results contribute to the literature of research on emerging technology governance by emphasizing how crucial adaptive governance is when handling digital disruption. Practically, this COBIT 2019 and DevOps-based approach provides an applicable framework that can be modified and applied by other industries facing similar challenges, especially with reference to efficiency, compliance, and risk management during the digital transformation process.

The effective adoption of this framework, however, is potentially hampered by the complexity of banking technology and the ever-changing regulatory dynamics that demand continuous contextual adjustments. Future research is recommended to expand empirical tests across industries, analyze how emerging technologies like artificial intelligence can be incorporated into risk management, and assess how blockchain can improve operational security and transparency within an adaptive governance framework.

References

[1] D. Jabborova, D. Mamurova, K. K. Umurova, U. Ulasheva, S. X. Djalolova, and A. Khurramov, “Possibilities of Using Technologies in Digital Transformation of Sustanable Development,” *E3S Web of Conferences*, vol. 491, p. 01002, Feb. 2024. https://doi.org/10.1051/e3sconf/202449101002

[2] E. J. Omol, “Organizational digital transformation: from evolution to future trends,” Jul. 04, 2024, *Emerald Publishing*. https://doi.org/10.1108/DTS-08-2023-0061

[3] E. Ali Alqararah, M. Shehadeh, and H. Yaseen, "The Role of Digital Transformation Capabilities in Improving Banking Performance in Jordanian Commercial Banks," *Journal of Risk and Financial Management*, vol. 18, no. 4, Apr. 2025. https://doi.org/10.3390/jrfm18040196

[4] T.-G. Budisteanu, "Blockchain and the Banking Sector: Benefits, Challenges and Perspectives," *Open J Soc Sci*, vol. 13, no. 03, pp. 288–300, 2025. https://doi.org/10.4236/jss.2025.133019

[5] M. Javaid, A. Haleem, R. P. Singh, R. Suman, and S. Khan, "A review of Blockchain Technology applications for financial services," Jul. 01, 2022, *Elsevier B.V*. https://doi.org/10.1016/j.tbench.2022.100073

[6] J. Park, S. Jeong, and K. Yeom, "Smart Contract Broker: Improving Smart Contract Reusability in a Blockchain Environment," *Sensors*, vol. 23, no. 13, Jul. 2023. https://doi.org/10.3390/s23136149

[7] Dr. A. Muayad and M. Abumandil, "Role of Smart Contract Technology Blockchain Services in Finance and Banking Systems: Concept and Core Values," *SSRN Electronic Journal*, 2022. https://dx.doi.org/10.2139/ssrn.4078566

[8] Rupali Gangarde, "Exploring the Role of Blockchain in Preventing Cyber Fraud in Financial Systems," *Computer Fraud and Security*, pp. 123–130, Dec. 2024. https://doi.org/10.52710/cfs.81

[9] C. L. Reyes and J. P. Cutler, "Ready Layer One: Functional Regulation For Blockchain Infrastructure," 2025. http://dx.doi.org/10.2139/ssrn.5145302

[10] H. A. Nahi *et al.*, "Blockchain Network for Regulation Decentralized E-Government Systems," *Data and Metadata*, vol. 4, Jan. 2025. https://doi.org/10.56294/dm2025201

[11] H. Mewha, "Blockchain Wakes: Balancing the Light and Dark Sides of Blockchain Through Global Regulation," 2023. https://doi.org/10.1017/9781108609708.007

[12] S. Baertschi, L. Guenthardt, R. Sabani, and M. Krey, "A Method for the Adoption of DevOps in the Banking Industry," in *2023 International Conference on Information Management (ICIM)*, IEEE, Mar. 2023, pp. 31–36. https://doi.org/10.1109/ICIM58774.2023.00012

[13] L. Lesavre, P. Varin, and D. Yaga, "Blockchain networks :Token Design and Management Overview," Feb. 2024. https://doi.org/10.6028/NIST.IR.8301

[14] R. Mulyana, L. Rusu, and E. Perjons, "Key Ambidextrous IT Governance Mechanisms Influence on Key Ambidextrous IT Governance Mechanisms Influence," *in Proc. PACIS, 2024*, 2024.

[15] ISACA, *COBIT 2019 Framework: Introduction and Methodology*. 2018.

[16] ISACA, "COBIT Focus Area: DevOps," 2021.

[17] R. Mulyana, "IT Governance Influence on Digital Transformation, Ph.D. dissertation," IEEE, Stockholm University, 2025.

[18] Achmad Fadhli Satriadi, R. Mulyana, and R. Fauzi, "Agile IT Service Management Design of Fintechco Digitalization Based on COBIT 2019 Devops Focus Area," *Jurnal Teknik Informatika (Jutif)*, vol. 4, no. 5, pp. 1165–1177, Oct. 2023. https://doi.org/10.52436/1.jutif.2023.4.5.1304

[19] OJK, "Peraturan Otoritas Jasa Keuangan Nomor 11/POJK.03/2022 Tahun 2022 tentang Penyelenggaraan Teknologi Informasi Oleh Bank Umum," 2022.

[20] BUMN, "Peraturan Menteri Badan Usaha Milik Negara Nomor PER-2/MBU/03/2023 Tahun 2023 tentang Pedoman Tata Kelola dan Kegiatan Korporasi Signifikan Badan Usaha Milik Negara," 2023. Accessed: Jul. 28, 2025.

[21] M. Safiullah and S. R. Paramati, "The impact of FinTech firms on bank financial stability," *Electronic Commerce Research*, vol. 24, no. 1, pp. 453–475, Mar. 2024.

[22] S. Wang, M. Asif, M. F. Shahzad, and M. Ashfaq, "Data privacy and cybersecurity challenges in the digital transformation of the banking sector," *Comput Secur*, vol. 147, p. 104051, Dec. 2024. https://doi.org/10.1016/j.cose.2024.104051

[23] F. Seyedjafarrangraz, C. De Fuentes, and M. Zhang, "Mapping the global regulatory terrain in digital banking: a longitudinal study across countries," *Digital Policy, Regulation and Governance*, Nov. 2024.

[24] R. Mulyana, L. Rusu, and E. Perjons, "IT Governance Mechanisms Influence on Digital Transformation: A Systematic Literature Review," *AMCIS*, 2021.

[25] 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," Oct. 2023.

[26] R. Dhillon and P. Sivabalan, "Exploring dimensions of governance for different types of blockchain systems," *British Accounting Review*, 2025.

[27] A. Joshi, L. Bollen, H. Hassink, S. De Haes, and W. Van Grembergen, "Explaining IT governance disclosure through the constructs of IT governance maturity and IT strategic role," *Information & Management*, vol. 55, no. 3, pp. 368–380, Apr. 2018. https://doi.org/10.1016/j.im.2017.09.003

[28] N. H. A. Alnor *et al.*, "The role of bank governance in managing the risks associated with banking institutions," *International Journal of Advanced and Applied Sciences*, vol. 11, no. 4, pp. 194–206, Apr. 2024. https://doi.org/10.21833/ijaas.2024.04.021

[29] M. M. Ibrahimy, A. Norta, and P. Normak, "Blockchain-based governance models supporting corruption-transparency: A systematic literature review," Jun. 01, 2024, *Zhejiang University*. https://doi.org/10.1016/j.bcra.2023.100186

[30] ISACA, *COBIT 2019 Design guide designing an information and technology governance solution*. 2018.

[31] K. Leonardo and R. Latuperissa, "Information Technology Governance Design in Trading Companies Using the COBIT 2019 Framework," *Journal of Information Systems and Informatics*, vol. 6, no. 3, pp. 1466–1483, Sep. 2024. https://doi.org/10.51519/journalisi.v6i3.798

[32] A. Alić, A. Traljić, and D. Đonko, "Methodology for Evaluating the Impact of DevOps Principles," in *2025 24th International Symposium INFOTEH-JAHORINA (INFOTEH)*, IEEE, Mar. 2025, pp. 1–6. https://doi.org/10.1109/INFOTEH64129.2025.10959292

[33] Y. Alam, S. N. Azizah, and C. Caroline, "Digital Transformation in Banking Management: Optimizing Operational Efficiency and Enhancing Customer Experience," *International Journal of Management Science and Information Technology*, vol. 5, no. 1, pp. 46–55, Jan. 2025. https://doi.org/10.35870/ijmsit.v5i1.3646

[34] 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, Dec. 2024. https://doi.org/10.1016/j.digbus.2024.100083

[35] Project Management Institute, *A Guide to the Project Management Body of Knowledge (PMBOK® Guide) - Seventh Edition and the Standard for Project Management*. Project Management Institute, 2021.

[36] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design Science in Information Systems Research 1," 2004. https://doi.org/10.2307/25148625

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

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

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

[40] P. Fusch and L. Ness, "Are We There Yet? Data Saturation in Qualitative Research," *The Qualitative Report*, Sep. 2015. https://doi.org/10.46743/2160-3715/2015.2281

[41] ISACA, *COBIT Focus Area: DevOps Using COBIT 2019*. 2021
[42] ISACA, *COBIT 2019 Framework Governance and Management Objectives*. 2019. Accessed: Mar. 10, 2025
[43] G. Laatikainen, M. Li, and P. Abrahamsson, "A system-based view of blockchain governance," *Inf Softw Technol*, vol. 157, May 2023. https://doi.org/10.1016/j.infsof.2023.107149
[44] R. van Pelt, S. Jansen, D. Baars, and S. Overbeek, "Defining Blockchain Governance: A Framework for Analysis and Comparison," *Information Systems Management*, vol. 38, no. 1, pp. 21–41, 2021. https://doi.org/10.1080/10580530.2020.1720046
[45] E. Tan, S. Mahula, and J. Crompvoets, "Blockchain governance in the public sector: A conceptual framework for public management," *Gov Inf Q*, vol. 39, no. 1, Jan. 2022. https://doi.org/10.1016/j.giq.2021.101625
[46] Project Management Institute, *A Guide to the Project Management Body of Knowledge (PMBOK® Guide) – Seventh Edition and The Standard for Project Management*, 7th ed. 2021. Accessed: Jun. 06, 2025.
[47] C. E. Otero, L. D. Otero, I. Weissberger, and A. Qureshi, "A Multi-criteria Decision Making Approach for Resource Allocation in Software Engineering," in *2010 12th International Conference on Computer Modelling and Simulation*, IEEE, 2010, pp. 137–141. https://doi.org/10.1109/UKSIM.2010.32
[48] F. Marle and T. Gidel, "A multi-criteria decision-making process for project risk management method selection," *International Journal of Multicriteria Decision Making*, vol. 2, no. 2, p. 189, 2012. https://doi.org/10.1504/IJMCDM.2012.046948