Jutisi: Jurnal Ilmiah Teknik Informatika dan Sistem Informasi
Jl. Ahmad Yani, K.M. 33,5 - Kampus STMIK Banjarbaru
Loktabat – Banjarbaru (Tlp. 0511 4782881), e-mail: puslit.stmikbjb@gmail.com
e-ISSN: 2685-0893
p-ISSN: 2089-3787

Using COBIT 2019 SME for Digital Transformation Governance of BPRDCo

Nai'la Rashikha[1*], Rahmat Mulyana[2], Ridha Hanafi[3]
[1,3]*Information System*, Telkom University, Bandung, Indonesia
[2]*Department of Computer and Systems Sciences (DSV)*, Stockholm University, Kista, Sweden
*e-mail *Corresponding Author:* nailarskh@student.telkomuniversity.ac.id

Abstract

Globalization has driven incumbent organizations to innovate through digital transformation (DT) to stay relevant. However, many DT efforts fail due to inadequate IT Governance (ITG). Ambidextrous ITG models using COBIT 2019 framework have demonstrated effectiveness in large banks. However, their applicability to small enterprises remains unexplored. This research aims to develop a prioritized ITG solution for SME and estimate the capability improvement of its maturity level for successful DT. The research followed five stages of Design Science Research (DSR), using COBIT 2019's SME focus area identified three key IT Governance and Management (ITGM) objectives: APO12 (Managed Risk), APO13 (Managed Security), and MEA03 (Compliance with External Requirements), with an average capability maturity level of 3.17. Thirteen essential solutions are recommended and compiled into an implementation roadmap, targeting a capability level increase to 3.86. This research contributes to ITG knowledge for DT at the SME level and practical implications for similar organizations.

Keywords: *Digital Transformation; Design Science Research; IT Governance; COBIT 2019 SME Focus Area; Bank.*

Abstrak

Globalisasi telah mendorong organisasi untuk berinovasi melalui Transformasi Digital (TD) agar tetap relevan. Namun, banyak upaya TD gagal karena Tata Kelola TI (TKTI) yang tidak memadai. Model TKTI hibrida yang menggunakan kerangka kerja COBIT 2019 telah menunjukkan efektivitas di bank-bank besar. Namun, penerapannya untuk usaha kecil masih belum dieksplorasi. Tujuan penelitian ini adalah untuk mengembangkan solusi TKTI yang diprioritaskan untuk UKM dan memperkirakan peningkatan kemampuan tingkat kematangannya untuk keberhasilan TD. Penelitian ini mengikuti lima tahap *Design Science Research* (DSR), menggunakan COBIT 2019 Area Fokus SME mengidentifikasi tiga tujuan utama Tata Kelola dan Manajemen TI (TKMTI): APO12 (*Managed Risk*), APO13 (*Managed Security*), dan MEA03 (*Managed Compliance with External Requirements*), dengan tingkat kematangan kemampuan rata-rata 3,17. Tiga belas solusi penting direkomendasikan dan disusun ke dalam roadmap implementasi, menargetkan peningkatan tingkat kemampuan menjadi 3,86. Penelitian ini berkontribusi pada pengetahuan TKTI untuk TD di tingkat UKM serta implikasi praktis untuk organisasi serupa.

Kata Kunci: *Transformasi Digital; Design Science Research; Tata Kelola TI; COBIT 2019 SME Focus Area; Bank.*

1. Introduction

In recent decades, globalization has increasingly pressured businesses to adapt by increasing integration efficiency through digital processes [1]. Based on SEA Digital Economy research by Google et al, the pandemic accelerated digital adoption, with 36% of consumers of digital services becoming new users and 90% intending to continue the habit post-pandemic [2]. This transformation highlights the growing significance of Digital Transformation (DT), which entails a fundamental change in an organization's form, function, or structure through digital technology to add value [3]. Information Technology (IT) is defined as "*all technologies used by organizations to collect, process, and disseminate information in all its forms*" [4]. Beyond traditional IT, digital technology also incorporates artificial intelligence, blockchain, robotics, virtual reality, and social media, mobile, analytics, cloud, and Internet of Things (IoT), which is often referred to as SMACIT [5]. Traditional business strategies and IT governance are being disrupted by the rapidly changing digital technology world.

In Indonesia, DT has become a national priority to encourage economic sectors to adapt amid the digital revolution as stated in the Indonesian Financial Services Sector Master Plan 2021-2025 [6]. The Financial Services Authority (OJK) has encouraged institutions like *Bank Perekonomian Rakyat* (BPR) to innovate by providing digital financial services. BPRDCo is a BPR providing financial services primarily to micro, small, and medium enterprises (MSMEs) in its local area. According to Law No. 4 of 2023, BPRs differ from commercial banks in that they have limited business activities and do not engage in payment traffic services like clearing and foreign exchange [7]. They also operate with less capital, with a minimum core capital of Rp6 billion [8] compared to Rp3 trillion for commercial banks [9]. As formal microfinance institutions under banking regulatory law [10], BPRs are considered SMEs within the banking sector due to their smaller scale compared to commercial banks. BPRDCo is one of the incumbent SME that is disrupted by digital technology. While DT is being pushed by the government, BPRDCo struggles with conventional IT systems that are not nearly agile and innovative enough to keep up with modern digital technologies. This creates a gap between BPRDCo's current IT practices and the ideal state of DT where IT governance (ITG) effectively aligns with business objectives to drive digital initiatives.

To address this gap, BPRDCo must shift from conventional IT systems to more agile and innovative governance models that can handle emerging technologies and drive value. Previous research has identified that ITG plays a crucial role in digital initiatives in organizations [11]. However, previous research has also shown that problems related to governance are the focus of organizational leaders in DT efforts because many organizations experience failure due to inadequate ITG [12]. Therefore, organizations need to implement ITG in DT efforts to create alignment between IT and business so that IT activities achieve organizational goals and comply with rules and policies [13]. To ensure that IT delivers strategic value, governance implementation needs to be supported by IT management that focuses on providing efficient and effective IT services and products [14]. Therefore, IT governance and management (ITGM) must operate in harmony to ensure alignment between business objectives and IT. COBIT 2019 has seven governance and management components consisting of forty objectives [15].

This research aims to answer the following questions: How to compile IT governance solution recommendations based on the results of the assessment gap analysis on the scope of COBIT 2019 priority design factors SME focus areas for BPRDCo DT? How is the IT governance design based on the seven components of COBIT 2019 in SME focus areas for BPRDCo’ s DT? Furthermore, how can the estimated improvement of IT governance capabilities affect the DT of BPRDCo? This aims to improve BPRDCo’ s ITG and ensure its alignment with the company's strategy to achieve DT objectives. The findings of this research provide insights into the role of IT governance in facilitating DT for smaller companies particularly in the banking sector like BPRDCo.

2. Theoretical Foundation

The governance mechanism that affects DT, consists of agile/adaptive and traditional mechanisms defined as a hybrid/ambidextrous approach [16] proven to have a moderate influence on DT that affects organizational performance [17]. Mulyana et al. define ambidextrous IT governance mechanism 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*” [18]. There are seven key mechanisms that influence the success of DT [18]. Among these, four primary hybrid ITG mechanisms—namely, board and executive management, strategy and architecture, data and information, and internal and external collaboration—have a significant effect on the performance of organizations, which is entirely mediated by DT. The remaining three mechanisms—development and operations, risk and audit, and talent and culture—demonstrate a moderate influence [19].

While hybrid ITG models combining traditional and agile approaches have proven effective for large banks, their applicability to small enterprises remains untested. Prior studies conducted in the banking sector have determined the ITG processes influencing DT and OP [20], followed by a test of the influence model [21]. Furthermore, some prior ITG for DT studies have also used various COBIT 2019 approaches to prove the importance of ITG on DT in general [22], further using Deliver, Service, and Support domain[23] and other manuscripts with focus areas on IT services [24], IT risks [25], Information Security [26], and DevOps [27]. However, the COBIT 2019 SME Focus Area has yet to be thoroughly examined in this context, particularly within the banking sector. This study extends previous research by analyzing the application of the COBIT 2019 SME Focus Area framework to small and medium-sized enterprises, based on an analysis of the seven TKMTI components.

3. Methodology

This study employs the Design Science Research (DSR) framework, which explains how design science research is conducted in Information Systems by presenting a concise conceptual framework and providing clear guidelines for understanding, conducting, and evaluating research [28]. The conceptual model of the framework is depicted in Figure 1 through the adoption of Hevner's DSR. The model is composed of three primary components: the knowledge base, information system (IS) research, and environment.

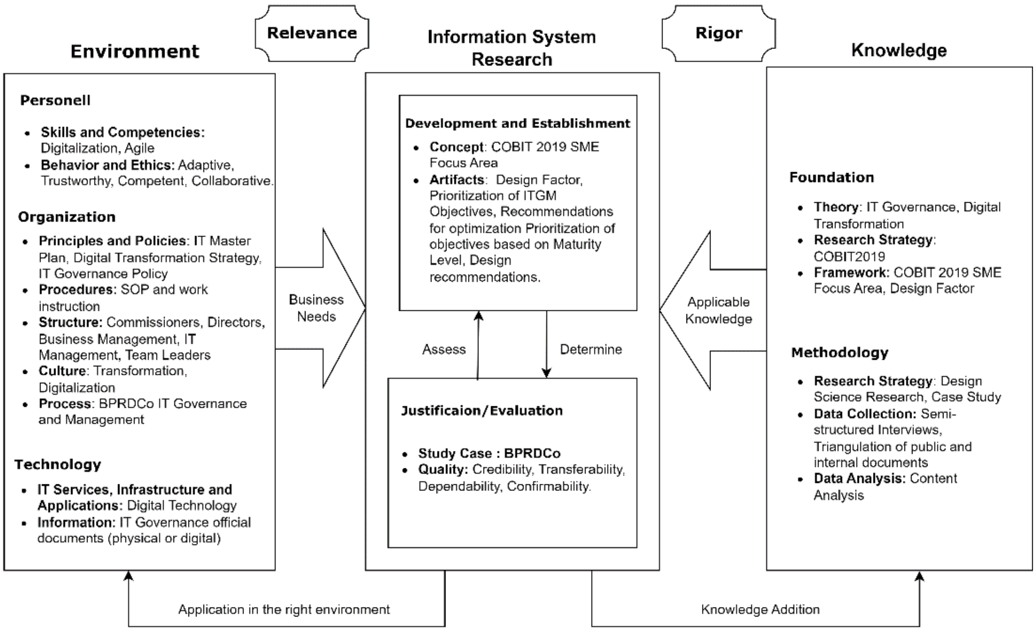
Environment
Relevance
Information System Research
Rigor
Knowledge
Personell
Skills and Competencies: Digitalization, Agile
Behavior and Ethics: Adaptive, Trustworthy, Competent, Collaborative.
Organization
Principles and Policies: IT Master Plan, Digital Transformation Strategy, IT Governance Policy
Procedures: SOP and work instruction
Structure: Commissioners, Directors, Business Management, IT Management, Team Leaders
Culture: Transformation, Digitalization
Process: BPRDCo IT Governance and Management
Technology
IT Services, Infrastructure and Applications: Digital Technology
Information: IT Governance official documents (physical or digital)
Business Needs
Development and Establishment
Concept: COBIT 2019 SME Focus Area
Artifacts: Design Factor, Prioritization of ITGM Objectives, Recommendations for optimization Prioritization of objectives based on Maturity Level, Design recommendations.
Assess
Determine
Justificaion/Evaluation
Study Case : BPRDCo
Quality: Credibility, Transferability, Dependability, Confirmability.
Applicable Knowledge
Foundation
Theory: IT Governance, Digital Transformation
Research Strategy: COBIT2019
Framework: COBIT 2019 SME Focus Area, Design Factor
Methodology
Research Strategy: Design Science Research, Case Study
Data Collection: Semi-structured Interviews, Triangulation of public and internal documents
Data Analysis: Content Analysis
Application in the right environment
Knowledge Addition

Figure 1 Research Method (adapted from Hevner [28])

In this study, five main stages of the DSR methodology are used to develop ITG solutions for BPRDCo’s DT, as shown in Figure 2.

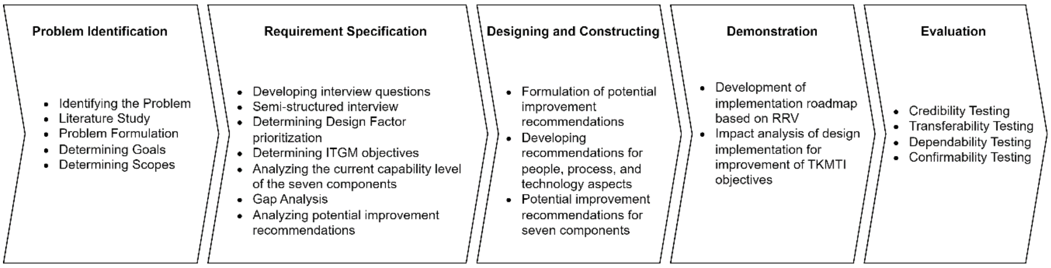
Problem Identification
Identifying the Problem
Literature Study
Problem Formulation
Determining Goals
Determining Scopes
Requirement Specification
Developing interview questions
Semi-structured interview
Determining Design Factor prioritization
Determining ITGM objectives
Analyzing the current capability level of the seven components
Gap Analysis
Analyzing potential improvement recommendations
Designing and Constructing
Formulation of potential improvement recommendations
Developing recommendations for people, process, and technology aspects
Potential improvement recommendations for seven components
Demonstration
Development of implementation roadmap based on RRV
Impact analysis of design implementation for improvement of TKMTI objectives
Evaluation
Credibility Testing
Transferability Testing
Dependability Testing
Confirmability Testing

Figure 2. Research Process

The first stage, Problem Identification, involves understanding the research problem through literature review, problem formulation, goal setting, and defining the study's scope. Requirement Specification follows, focusing on developing specific requirements by creating interview questions, conducting semi-structured interviews, prioritizing design factors, identifying IT Governance and Management (ITGM) objectives, analyzing current capabilities, performing gap analysis, and recommending improvements. To ensure the quality of qualitative research, achieving data saturation is crucial, which can be accomplished through methods such as interviews and further ensured by data triangulation [29]. The semi-structured interviews were performed using a predefined list of questions. Table 1 presents the details of the interviews conducted.

Table 1 Interview Details

Date	Duration	Interviewee	Position
March 18, 2024	30 Minutes	Interviewee 1	Deputy Head of IT
	15 Minutes	Interviewee 2	Head of IT Operational and Security
	15 Minutes	Interviewee 3	Head of IT Development
May 16, 2024	25 Minutes	Interviewee 1	Deputy Head of IT
	10 Minutes	Interviewee 2	Head of IT Operational and Security
	10 Minutes	Interviewee 3	Head of IT Development

The data collection process followed an iterative approach, with data being gathered and analyzed repeatedly to ensure depth and accuracy. Triangulation was used as suggested by Fuchs and Ness [29] to further improve the validity and dependability of the results. This involved utilizing multiple sources, including access to a range of internal and public documents such as the Company Profile, Governance Report, Sustainability Report, Organizational Structure, Risk Profile, IT Audit Report, Business Continuity Plan, IT Standard Operating Procedures, ISMS Guidelines and Procedures, IT Development Plan, and relevant regulations. Data collection continued until saturation is reached, when there is enough data to conduct a second research and additional coding is no longer feasible [29]. In the Designing and Constructing stage, potential improvement recommendations are formulated, and strategies are developed for people, processes, and technology, targeting gaps identified in the previous phase. The Demonstration phase involves implementing the designed solutions, creating an implementation roadmap based on resources, risk, and value, and analyzing the impact of these solutions on ITGM objectives. Finally, Evaluation assesses the research outcomes based on credibility, transferability, dependability, and confirmability to ensure that the findings are credible, applicable, reliable, and verifiable [30]. This structured approach ensures a comprehensive and methodical research process from problem identification to solution evaluation.

4. Discussion

4.1. ITGM Objectives Prioritization Result

This stage determines the main objectives of ITGM based on regulations, design factors, SME area focus, and ITGM process mechanism. The results of these considerations result in the priority of ITGM goals.

Table 2. Prioritization Result

Control	Regulations	Design Factor	SME Focus Area	Previous research	Final Score
MEA03: Managed Compliance with External Requirements	100	90	80	100	95
APO12: Managed Risk	100	85	80	100	94
APO13: Managed Security	100	85	80	100	94

Based on Table 2, it can be observed that the primary objective of ITGM with the highest priority is MEA03: Managed Compliance with External Requirements, with a final score of 95. Furthermore, APO12: Managed Risk and APO13: Managed Security also receive high priority, each with a final score of 94. These results demonstrate a strong focus on the aspects of compliance, risk, and security within the IT governance management framework at BPRDCo.

4.2. Gap Analysis Result

1) Process Component

The following Table 3 evaluates the capability of the process components by assessing the achievement levels of each activity related to IT governance management (ITGM) objectives. This assessment is based on COBIT 2019 guidelines tailored for SMEs [31].

Table 3. Process Component

Management Practices	Achievement	Capability Level
APO12: Managed Risk		
APO12.01	100% (Fully)	2
	100% (Fully)	3
	100% (Fully)	4
APO12.02	90% (Fully)	3
	50% (Partially)	4
	100% (Fully)	5
APO12.03	100% (Fully)	2
	100% (Fully)	3
	100% (Fully)	4
APO12.04	83% (Largely)	3
	100% (Fully)	4
APO12.05	100% (Fully)	2
	100% (Fully)	3
APO12.06	100% (Fully)	3
	100% (Fully)	4
	100% (Fully)	5
Capability Level Score		2
APO13: Managed Security		
APO13.01	100% (Fully)	2
APO13.02	75% (Largely)	3
	100% (Fully)	4
APO13.03	100% (Fully)	4
	100% (Fully)	5
Capability Level Score		2
MEA03: Managed Compliance with External Requirements		
MEA03.01	100% (Fully)	2
	75% (Largely)	3
MEA03.02	100% (Fully)	3
MEA03.03	100% (Fully)	3
	100% (Fully)	4
	100% (Fully)	5
MEA03.04	83% (Largely)	3
	100% (Fully)	4
Capability Level Score		2

The table displays the percentage of achievement and corresponding capability levels for each activity. The results indicate varying levels of capability, with some areas fully achieving the set objectives and others requiring further development to reach higher capability levels.

2) Information Component

The following Table 4 shows the information output of each management practice that must be met to achieve the ITGM objectives. The gap analysis for the information component evaluates BPRDCo's current practices in risk management, information security, and compliance with external requirements. The following table highlights these gaps and suggests areas for improvement.

Table 4. Information Component

Management Practice	Information Output	Current State
APO12: Managed Risk		
APO12.01 Collect Data.	Identified risk issues and factors	Risk Assessment, Information Asset Risk Register
	Data on risk events and contributing factors	Incident Management Log.
APO12.02 Analyze risk.	Risk analysis results	Information Asset Risk Register
APO12.03 Maintain a risk profile.	Documented risk profile, including status of risk management actions	Risk Profile Report
APO12.04 Articulate risk.	Risk analysis and risk profile reports for stakeholders	Risk Profile Report
	Results of third-party risk assessments	External Audit

Management Practice	Information Output	Current State
APO12.05 Define a risk management action portfolio.	Project proposals for reducing risk	BPRDCo has not yet developed a project proposal to mitigate risk.
APO12.06 Respond to risk.	Risk impact communication	Risk Profile Report
	Risk-related root causes	Root-cause analysis - Audit Findings Working Paper
APO13 Managed Security		
APO13.01 Establish and maintain an information security management system (ISMS)	ISMS scope statement	ISMS Guidelines and Procedures
	ISMS policy	ISMS Guidelines and Procedures
APO13.02 Define and manage an information security risk treatment plan.	IS risk treatment plan	ISMS Guidelines and Procedures, Information Asset Risk Register, Risk Profile Result Report, Incident response procedure and BCP.
	IS business cases	ISMS Guidelines and Procedures
APO13.03 Monitor and review the information security management system (ISMS).	Recommendations for improving the information security management system (ISMS)	Internal Audit Report and ISO27001 Audit Report.
	ISMS audit reports	Internal audit and ISO27001 audit.
MEA03 Managed Compliance with External Requirements		
MEA03.01 Identify external compliance requirements.	Log of required compliance actions	Log legal, regulatory, and contractual requirements.
	Compliance requirements register	List of regulatory requirements.
MEA03.02 Optimize response to external requirements.	Communications of changed compliance requirements	Electronic media, circulars, or socialization.
	Updated I&T policies and procedures	Latest policies, procedures and standards.
MEA03.03 Confirm external compliance.	Compliance confirmations	BPRDCo Internal Audit Report
	Identified compliance gaps	BPRDCo Internal Audit Report
MEA03.04 Obtain assurance of external compliance.	There are no small and medium enterprise specific outputs for this practice.	

Note: □ Gap

While the company has established procedures and reports for managing risks and maintaining an ISMS, there are areas that require further development, such as creating risk mitigation project proposals.

3) Organization Structure Component

The following Table 5 shows the roles that must be met to achieve ITGM goals. The gap analysis for the organization structure component assesses BPRDCo's current organizational roles and their alignment with COBIT framework objectives. The following table details these organizational gaps and identifies areas for improvement.

Table 5. Organization Structure Component

COBIT Organization Structure	Objective	Current State
General Manager	MEA03	Operations Director - BPRDCo has an operations director role as the highest-ranking function responsible for the overall operational management of the company.
Operations Manager	MEA03	
Financial Manager	MEA03	Head of PBK and Tax - BPRDCo has Head of PBK and Tax role that manages and oversees the company's financial activities
Business Process Owners	APO12, APO13, MEA03	The Head of Department/Unit at BPRDCo holds a role responsible for the overall performance of a process in achieving objectives and driving process improvements.
Head of IT	APO12, APO13, MEA03	IT Division Head - BPRDCo has an IT division head role responsible for setting the I&T strategy as well as planning, resourcing and managing the delivery of I&T services and solutions to support corporate objectives.
Security Expert	APO12, APO13,	Security Officer - BPRDCo has a security officer role responsible for the information security management and IT risk management aspects of the company.
IT Development Coordinator	APO12, APO13, MEA03	Head of IT Development - BPRDCo has the role of Head of IT Development who is responsible for developing new products from planning to implementation, as well as performing Bug fixing.

COBIT Organization Structure	Objective	Current State
IT Operations Coordinator	APO12, APO13, MEA03	Head of IT Operations & Security - BPRDCo has the role of Head of IT Operations & Security who is responsible for managing IT operations and running security for the security of the company's information systems.
Privacy Officer	APO12, APO13, MEA03	BPRDCo does not yet have a privacy officer role responsible for monitoring privacy risks, business impact and coordinating compliance with privacy policies.
Legal Department	MEA03	Legal Staff - BPRDCo has a legal staff role responsible for providing guidance on legal and regulatory matters.
Compliance or Quality	MEA03	Compliance Division - BPRDCo has a division responsible for the implementation of the compliance function that is independent of the operational function.
Audit	MEA03	Internal Audit - BPRDCo has an Internal Audit Unit that is responsible for the provision of internal audits.

Note: ▨ Gap

While BPRDCo has established key roles there are gaps including the absence of roles like Privacy Officer, which are crucial for comprehensive privacy compliance.

4) People, Skills, and Competencies Component

The following Table 6 shows the skills that must be met to achieve ITGM goals.

Table 6. People, Skills, and Competencies Component

Key Culture Elements	Current State
APO12 Managed Risk	
Business Risk Management	Risk management training and coaching
Information Assurance	Information Security Policy - ISMS Guidelines and Procedures
Risk Management	BPRDCo does not yet have training and certification programs related to IT risk management
APO13 Managed Security	
Information security	The company has conducted training and ISO27001: 2013 certification, but not all company staff have implemented information security awareness.
Information Security Strategy Development	Security Operations Center (SOC).
MEA03 Managed Compliance with External Requirements	
Information Security	The company has conducted training and ISO27001:2013. certification

Note: ▨ Gap

The gap analysis of the people, skills, and competencies component reveals several critical areas for improvement within BPRDCo's current state of risk management and information security. The assessment highlights the need for enhanced training and certification programs, particularly in IT risk management and the implementation of information security awareness among all staff.

5) Policies, Principles, and Procedures Component

The following Table 7 outlines the policies required to meet ITGM goals. The gap analysis for the policies, principles, and procedures component assesses BPRDCo's existing policies and their alignment with industry standards. The following table details these gaps and suggests areas for enhancement.

Table 7. Policies, Principles, and Procedures Component

Policy	Current State
APO12: Managed Risk	
There are no small and medium enterprise-specific principles, policies and procedures for this objective [31].	
APO13: Managed Security	
Information security and privacy policy	BPRDCo already has ISMS Guidelines and Procedures that regulate information security policies. However, there is no privacy aspect yet.
MEA03: Managed Compliance with External Requirements	
Compliance Policy	BPRDCo Compliance Policy.

Note: ▨ Gap

While the company has established information security guidelines and a compliance policy, there are notable gaps, such as the absence of privacy policies.

6) Culture, Ethics, and Behavior Component

The following Table 8 shows the elements that must be met to achieve the ITGM objectives. The gap analysis for the Culture, Ethics, and Behavior component examines BPRDCo's current cultural practices and their alignment with risk management, security, privacy, and compliance principles. The following table highlights these areas and identifies opportunities for improvement.

Table 8. Culture, Ethics, and Behavior Component

Key Culture Components	Current State
APO12 Managed Risk	
A transparent and collaborative risk culture, where senior management should set the direction and support for alignment of risk practices.	BPRDCo has implemented practices related to risk management as one aspect of corporate governance that applies the principle of Transparency.
APO13 Managed Security	
Establish a culture of security and privacy awareness that encourages desirable behavior and implementation of security and privacy policies in daily practice. Provide sufficient security and privacy guidance, indicate security and privacy champions, and proactively support and communicate security and privacy programs, innovations and challenges.	Information security guidelines are in place and communicated, but there are still gaps in their implementation and effectiveness.
MEA03 Managed Compliance with External Requirements	
Promote a compliance-aware culture, including zero tolerance of noncompliance with legal and regulatory requirements.	The compliance division conducts ongoing socialization and training to all work units regarding the latest regulations.

Note: ▨ Gap

While efforts have been made to establish a transparent risk culture and promote compliance awareness, there are gaps in the consistent implementation and effectiveness of these practices.

7) Application, Infrastructure, and Service Component

The following Table 9 shows the elements that must be met to achieve the ITGM objectives. The gap analysis for the application, infrastructure, and service component reveals BPRDCo's current capabilities and identifies areas needing improvement. The following table details these gaps and areas for enhancement.

Table 9. Application, Infrastructure, and Service Component

Application, Infrastructure, and Service	Current State
APO12 Managed Risk	
Crisis management services	DRC, BCP, SIEM
Governance, risk and compliance (GRC) tools	BPRDCo has not yet using tools for governance, risk, and compliance
Risk analysis tools	Risk Assessment
Risk intelligence services	BPRDCo has not yet using risk intelligence services tool intelligence services
APO13 Managed Security	
Configuration management tools	CMDB
Security and privacy awareness services	ISMS ISO training and coaching
Third-party security assessment services	ISO 27001:2013 Assessment
MEA03 Managed Compliance with External Requirements	
Regulatory Watch services	Veritas
Third-party compliance assessment services	External Audit, ISO 27001:2013 Assessment

Note: ▨ Gap

While some tools and services are in place, such as crisis management and configuration management tools, significant gaps remain in governance, risk, and compliance tools, and risk intelligence services. Additionally, security and privacy measures, as well as third-party assessments, need broader implementation.

4.3 Potential Improvement

After conducting a gap analysis on seven capability components against three priority ITGM objectives, namely APO12, APO13, and MEA03. The next step is to analyze the improvements or enhancements needed by BPRDCo based on the results of the identified gaps. In Table 10 there are three aspects of potential improvement, namely people, process, and technology aspects along with the type of improvement for each component.

Table 10. Potential Improvement

Component	Gap	Type	Potential Improvement
People Aspect			
APO12 Managed Risk, APO13 Managed Security, and MEA03 Managed Compliance with External Requirements			
Organization Structure	BPRDCo does not yet have a Privacy Officer role	Roles, Responsibility	Adding the role of a Privacy Officer who is responsible for monitoring privacy risks, business impact, and coordinating compliance with privacy policies.
APO12 Managed Risk			
People, Skills, and Competencies	BPRDCo does not yet have a training and certification program related to risk management	Skills & Awareness	Implement training and certification programs related to IT risk management for company employees.
APO13 Managed Security			
Culture, Ethics, and Behavior	The company has conducted socialization and training on ISO27001, but not all staff have implemented all clauses.	Skills & Awareness	Conduct awareness programs to increase employee awareness of ISO27001 as an information security management practice.
Process Aspect			
APO12 Managed Risk			
Process	Has not fully included information on control effectiveness, gaps, inconsistencies, redundancies, remediation status, and impact on risk profile.	Procedure	Adding points related to the provision of reporting the results of risk assessment and risk profile in BPRDCo risk assessment guidelines and procedures.
Process	BPRDCo does not yet have specific procedures related to risk control evaluation	Procedure	Adding regular control testing processes to evaluate the efficacy of risk controls.
Process	Has not fully managed risk mitigation actions as a project	Policy	Add or update policies related to risk mitigation management that require risk mitigation/control actions with high IR ratings to be managed as projects, including guidance on project workflows and approvals.
APO13 Managed Security			
Process	Has not fully developed a proposal for implementation of the information security risk management plan that includes funding considerations and allocation of roles and responsibilities.	Procedure	Add procedures for developing risk treatment plan implementation proposals supported by business cases.
		Record	Risk treatment plan proposal along with business case
	There is no aspect of the application of privacy in the current ISMS guidelines and procedures.	Policy	Add or update privacy-related policies to complement and align existing ISMS policies in your company
MEA03 Managed Compliance with External Requirements			
Process	There is no effectively maintained log of legal, regulatory and contractual requirements.	Policy	Adding a policy of mapping legal and regulatory requirements to the company's standard procedures to ensure the company's standards remain in line with the latest regulations.
	There is no documentation/statement regarding aspects of compliance with third party regulations on the supplier/vendor evaluation form.	Procedure	Add provisions to vendor and third-party management procedures to ensure third party compliance with regulations.
Technology Aspect			
APO12 Managed Risk			
Services, Infrastructure, and Applications	Not yet using tools for governance, risk, and compliance assistance	Tools	Define services or applications to assist with enterprise IT governance, risk and compliance.
	Not yet using risk intelligence services tool	Tools	Define services or applications to help identify, measure, manage, and mitigate risk.

4.4 Resource, Risk, and Value (RRV) Analysis

The following Table 11 presents the scores and categories for potential improvements identified through the Resource, Risk, and Value (RRV) analysis. This analysis provides insight into where BPRDCo can focus its efforts to optimize resource management, mitigate risks, and enhance overall value. The table categorizes the identified potential improvements as "Medium" and “Low”.

Table 11 RRV Analysis

No	Potential Improvement	Final score	Category
1	Added a policy of mapping legal and regulatory requirements with standard company procedures to ensure company standards remain compliant with the latest regulations	18	Medium
2	Adding points related to the provisions for reporting risk assessment results and risk profile in BPRDCo’s risk assessment guidelines and procedures.	18	Medium
3	Add or update privacy-related policies	18	Medium
4	Adding a Privacy Officer role	18	Medium
5	Added procedures for developing proposals for the implementation of risk treatment plans supported by business cases	12	Medium
6	Holding awareness programs to increase employee awareness related to ISO27001 as an information security management practice	12	Medium
7	Prepare a risk treatment plan proposal along with a business case	12	Medium
8	Define services or applications to help identify, measure, manage, and mitigate risk	12	Medium
9	Adding control testing procedures that are carried out on a regular/periodic basis as a form of testing the effectiveness of risk control	12	Medium
10	Add or update policies related to risk mitigation management that require risk mitigation/control actions with high IR ratings to be managed as projects, including guidance on project workflows and their approvals	9	Low
11	Implement training and certification programs related to IT risk management for company employees	8	Low
12	Define services or applications to help with corporate governance, risk, and compliance	6	Low
13	Add provisions to vendor and third-party management procedures to ensure third-party compliance with regulations	6	Low

4.5 Implementation Roadmap

The following Table 12 outlines the implementation roadmap for key initiatives planned for 2025 and 2026. These initiatives are designed to address the potential improvements identified in the Resource, Risk, and Value (RRV) analysis, providing a structured approach to enhancing organizational capabilities and addressing identified gaps. The table illustrates the phased approach to achieving these goals, ensuring that critical changes are effectively integrated into the organization's strategic plan.

Table 12. Implementation Roadmap

Initiatives	2025				2026			
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
People Aspect								
Add the Privacy Officer role.		■						
Implement risk management training and certification programs.			■					
Holding an awareness program on risk management practices.				■				
Process Aspect								
Add a policy for mapping legal and regulatory requirements with standard company procedures.	■							
Add provisions related to the reporting of risk assessment and risk profile results.		■						
Develop or update privacy-related policies.			■					
Establish procedures for developing proposals for risk treatment plan implementation.				■				
Formulate risk treatment plan proposals.				■				
Add control testing procedures.					■			
Develop or update policies related to risk mitigation management.						■		
Add provisions to vendor and third-party management procedures.							■	
Technology Aspect								
Define services or applications to support corporate IT governance, risk, and compliance.			■					
Define services or applications to help identify, measure, manage, and mitigate risk.				■				

4.6 Recommendations Impact on BPRDCo

The following Table 13 provides a detailed comparison of the process component capability values for the ITGM objectives both prior to and following the improvements. The average capability score before the enhancements was 3.17, whereas, after the improvements, it increased to 3.86. This represents a significant increase of 0.69 in the capability levels associated with the three ITGM objectives.

Table 13. Estimation of Impact on Process Component

ITGM Objectives	Previous Capability Level	Estimated Capability Level
APO12: Managed Risk	3.5	4.17
APO13: Managed Security	3	3.67
MEA03: Managed Compliance with External Requirements	3	3.75
Average Capability	3.17	3.86

The following Table 14 outlines the state of organizational structure, information, people, skills and competencies, culture, ethics and behavior, principles, policies and procedures, and services, infrastructure, and applications components before and after the implementation of recommended IT governance improvements at BPRDCo. The estimation of these components serves as a baseline for understanding the impact of implementing the suggested improvements on BPRDCo's overall governance capabilities.

Table 14. Estimation of Impact on Governance Component

Previous State	State After Recommendation
Organization Structure Component	
APO12, APO13, MEA03	
There is no role for a Privacy Officer who is responsible for monitoring the risks and business impacts of privacy laws and coordinating the implementation of policies and activities that ensure compliance with privacy directives.	Privacy Officer role and responsibilities fulfilled.
Information Component	
APO13	
ISMS Guidelines and Procedures, Risk Register Information Assets, Risk Profile Report Results, Incident response procedures and BCP.	ISMS Guidelines and Procedures, Risk Register Information Assets, Risk Profile Report Results, Incident response procedures and BCP, and RTP Proposal.
People, Skills and Competencies Component	
APO12	
BPRDCo does not yet have a training and certification program related to IT risk management.	- Certified in Risk and Information Systems Control (CRISC) oleh ISACA. - ISO3100:2018 Risk Management - Certified Enterprise Risk Management (ERM)
Culture, Ethics, and Behavior	
APO13	
The company has conducted training and certification ISO27001:2013, but not all company staff have implemented information security awareness.	- Training and workshops ISO27001 - Modul E-learning ISO27001 - Information security newsletter - Information security drill according to ISO27001 standards
Principles, Policies, and Procedures	
There is no aspect of the application of privacy in the current ISMS guidelines and procedures.	Information Security and Privacy Guidelines and Procedures.
Services, Infrastructure, and Applications	
Not using tools for governance, risk, and compliance.	Software and GRC platform
Not yet using a risk intelligence services tool.	Software Risk Intelligence

The comparison of the previous state with the state after recommendations highlights enhancements across multiple areas. Notably, the introduction of a Privacy Officer, the inclusion of risk treatment proposals, and the adoption of advanced training and certification programs. Additionally, the focus on information security awareness and the integration of software tools for governance, risk, and compliance further strengthens BPRDCo's ability to manage IT risks effectively. These improvements are expected to result in a more compliant and resilient IT governance structure that supports the bank's digital transformation objectives.

4.7 Discussion of Study Results

The rapid advancement and integration of digital technologies are causing significant disruptions, fundamentally challenging traditional business models. Incumbent organizations, long reliant on conventional IT systems and governance, face a pressing need to adapt. To navigate this disruption, organizations must adopt more agile and flexible governance models. BPRs encounter challenges in implementing ambidextrous or hybrid IT governance due to constraints human and financial resources. However, with an appropriate approach that combines agile methodologies for rapid development and traditional methods for operational stability, BPRs can enhance both efficiency and responsiveness.

This study confirms the critical role of ITG mechanisms in supporting digital transformation DT within SMEs. These findings align with previous research on large banks, which indicates that ITG is essential for achieving digital success. Building on prior studies that have explored the use of the COBIT 2019 framework to support DT in banking institutions [24] [25] [26] [27], this research further demonstrates the relevance of the COBIT 2019 approach within the SME focus area [31], specifically for small-scale banking companies like BPRDCo. This research offers new insights into how the ambidextrous approach can be adapted and implemented in organizations with limited resources, such as SMEs, and highlights the flexibility and adaptability of IT governance that can be applied across different organizational sizes.

5. Conclusion

This study has limitations, including the potential for bias in data analysis and interpretation, which may affect the conclusions drawn. Additionally, the design is prepared specifically for the BPRDCo case study, so the identification results may not be fully applicable to other industries. Therefore, future researchers are advised to be mindful of the subjective nature of the interpretation process in this study and pay attention to the organizational context when interpreting or applying these findings.

The application of COBIT 2019's SME Focus Area framework provides a structured approach to enhancing ITG in SMEs like BPRDCo. Based on the results of prioritization based on related regulations, COBIT 2019 design factors for SME focus areas and governance mechanisms that support DT, three priority ITGM objectives in BPRDCo are obtained, namely APO12 Managed Risk, APO13 Managed Security, and MEA03 Managed Compliance with External Requirements. Based on the results of the gap analysis of the seven capability components in the SME focus area, a governance improvement design was carried out that includes three aspects, namely people, process, and technology. The results of the improvement on the ITGM objectives produce a roadmap for the implementation and influence of the recommendations. The implementation of the improvement design enhanced BPRDCo's capability levels. The pre-implementation assessment showed an average capability score of 3.17, which increased to 3.86 post-implementation. This 0.69-point increase reflects the effectiveness of the proposed solutions in enhancing ITG practices. The improvement in capability levels is indicative of better alignment between IT and business objectives, improved risk management, and enhanced compliance with external requirements.

By leveraging the COBIT 2019 framework, this study enhances the ITG knowledge base, specifically tailored for supporting DT at the SME level. Furthermore, this research serves as a beacon guiding SMEs in the banking industry towards successful digital transformation. By adapting to the rapidly changing digital landscape and optimizing their IT services, SMEs can realize their full potential with opportunities for unprecedented growth and innovation.

References

[1] S. Kraus, P. Jones, N. Kailer, A. Weinmann, N. Chaparro-Banegas, and N. Roig-Tierno, “Digital Transformation: An Overview of the Current State of the Art of Research,” *Sage Open*, vol. 11, no. 3, pp. 1–15, Sep. 2021, doi: https://doi.org/10.1177/21582440211047576.

[2] Google, Temasek, and Bain, “e-Conomy SEA 2020,” 2020.

[3] C. Gong and V. Ribiere, “Developing a Unified Definition of Digital Transformation,” *Technovation*, vol. 102, p. 102217, Apr. 2021, doi: 10.1016/J.TECHNOVATION.2020.102217.

[4] S. Sarosa and D. Zowghi, “Strategy for Adopting Information Technology for SMEs: Experience in Adopting Email Within an Indonesian Furniture Company,” *Electronic Journal of Information Systems Evaluation (EJISE)*, vol. 6, no. 2, pp. 165–176, 2003.

[5] I. M. Sebastian, K. G. Moloney, J. W. Ross, N. O. Fonstad, C. Beath, and M. Mocker, “How big old companies navigate digital transformation,” *MIS Quarterly Executive*, vol. 16, no. 3, pp. 197–213, 2017, [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85028657634&partnerID=40&md5=1f34a6b050d9ab3df9189ccfb00905b0

[6] OJK, “Master Plan Sektor Jasa Keuangan Indonesia 2021-2025,” 2020. [Online]. Available: www.ojk.go.id

[7] Indonesia, “Undang-Undang (UU) Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan,” 2023.

[8] OJK, “Peraturan Otoritas Jasa Keuangan Nomor 5 /POJK.03/2015 Tentang Kewajiban Penyediaan Modal Minimum dan Pemenuhan Modal Inti Minimum Bank Perkreditan Rakyat,” 2015.

[9] OJK, “Peraturan Otoritas Jasa Keuangan Republik Indonesia Nomor 12 /POJK.03/2020 Tentang Konsolidasi Bank Umum,” 2020.

[10] BRIN and BKF, “Ekosistem Lembaga Pembiayaan Mikro,” 2022. Accessed: Aug. 15, 2024. [Online]. Available: https://fiskal.kemenkeu.go.id/files/berita-kajian/file/1674547577_laporan_akhir_ekosistem_lembaga_pembiayaan_mikro_27122022.pdf

[11] R. Mulyana, L. Rusu, and E. Perjons, “IT Governance Mechanisms Influence on Digital Transformation: A Systematic Literature Review,” in *AMCIS 2021 Proceedings:* , Association for Information Systems (AIS), 2021, pp. 1–10. [Online]. Available: https://aisel.aisnet.org/amcis2021/adv_info_systems_general_track/adv_info_systems_general_track/19/

[12] N. Obwegeser, T. Yokoi, M. Wade, and T. Voskes, “7 Key Principles to Govern Digital Initiatives,” *MIT Sloan Manag Rev*, vol. 61, no. 3, pp. 1–9, 2020, Accessed: Nov. 04, 2023. [Online]. Available: https://mitsmr.com/2UWvNEs

[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] R. Peterson, “Crafting Information Technology Governance,” *Information Systems Management*, vol. 21, no. 4, pp. 7–22, 2004, doi: 10.1201/1078/44705.21.4.20040901/84183.2.

[15] ISACA, *COBIT 2019 Framework: Introduction & Methodology*. 2018. Accessed: Jan. 06, 2024. [Online]. Available: www.isaca.org

[16] R. Mulyana, L. Rusu, and E. Perjons, “IT Governance Mechanisms that Influence Digital Transformation: A Delphi Study in Indonesian Banking and Insurance Industry,” in *PACIS 2022 Proceedings*, Association for Information Systems (AIS), 2022, pp. 7–11. Accessed: Oct. 28, 2023. [Online]. Available: https://aisel.aisnet.org/pacis2022/267

[17] 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,” pp. 1–12, 2023, Accessed: Oct. 28, 2023. [Online]. Available: https://urn.kb.se/resolve?urn=urn:nbn:se:su:diva-222626

[18] R. Mulyana, L. Rusu, and E. Perjons, “Key Ambidextrous IT Governance Mechanisms for Successful Digital Transformation: A Case Study of Bank Rakyat Indonesia (BRI),” *Digital Business*, vol. 4, no. 2, p. 100083, 2024, doi: https://doi.org/10.1016/j.digbus.2024.100083.

[19] R. Mulyana, L. Rusu, and E. Perjons, “Key Ambidextrous IT Governance Mechanisms Influence on Digital Transformation and Organizational Performance in Indonesian Banking and Insurance,” in *PACIS 2024 Proceedings*, 2024, p. 7. Accessed: Jul. 09, 2024. [Online]. Available: https://aisel.aisnet.org/pacis2024/track15_govce/track15_govce/7

[20] F. Luthfia, Rahmat Mulyana, and L. Ramadani, “Studi Kasus Pengaruh Tata Kelola TI Terhadap Transformasi Digital dan Kinerja Bank B,” *ZONAsi: Jurnal Sistem Informasi*, vol. 4, no. 2, pp. 100–116, Oct. 2022, doi: 10.31849/zn.v4i2.11085.

[21] T. Nurafifah, R. Mulyana, and L. Abdurrahman, “Pengujian Model Pengaruh Tata Kelola TI Terhadap Transformasi Digital dan Kinerja Bank A,” *Journal of Information System Research (JOSH)*, vol. 4, no. 1, pp. 73–82, Oct. 2022, doi: 10.47065/josh.v4i1.2257.

[22] D. A. Permana, R. Fauzi, and R. Mulyana, “Perancangan Tata Kelola Teknologi Informasi untuk Transformasi Digital di Industri Perbankan Menggunakan Framework COBIT 2019 Domain Align, Plan, and Organise: Studi Kasus di Bank XYZ,” *eProceedings of Engineering*, vol. 8, no. 5, pp. 9664–9671, 2021.

[23] O. T. Poetry, R. Fauzi, and R. Mulyana, “Perancangan Tata Kelola Teknologi Informasi untuk Digital di Industri Perbankan Menggunakan Framework COBIT 2019 dengan

Domain, Deliver, Service, and Support: Studi Kasus Bank XYZ," *eProceedings of Engineering*, vol. 8, no. 5, pp. 9684–9692, 2021.

[24] Bq. D. Tarbiyatuzzahrah, R. Mulyana, and A. F. Santoso, "Penggunaan COBIT 2019 GMO dalam Menyusun Pengelolaan Layanan TI Prioritas pada Transformasi Digital BankCo," *JTIM : Jurnal Teknologi Informasi dan Multimedia*, vol. 5, no. 3, pp. 218–238, Oct. 2023, doi: 10.35746/jtim.v5i3.400.

[25] Y. W. D. M. D. Dewi, R. Mulyana, and A. F. Santoso, "Penggunaan COBIT 2019 I&T Risk Management untuk Pengelolaan Risiko Transformasi Digital BankCo," *Jutisi : Jurnal Ilmiah Teknik Informatika dan Sistem Informasi*, vol. 12, no. 3, pp. 1366–1380, 2023, doi: http://dx.doi.org/10.35889/jutisi.v12i3.1488.

[26] A. Rahmadana, R. Mulyana, and A. F. Santoso, "Pemanfaatan COBIT 2019 Information Security Dalam Merancang Manajemen Keamanan Informasi Pada Transformasi BankCo," *Jutisi : Jurnal Ilmiah Teknik Informatika dan Sistem Informasi*, vol. 12, no. 3, pp. 1226–1239, 2023, doi: http://dx.doi.org/10.35889/jutisi.v12i3.1513.

[27] N. Riznawati, R. Mulyana, and A. F. Santoso, "Pendayagunaan COBIT 2019 DevOps dalam Merancang Manajemen Pengembangan TI Agile pada Transformasi Digital BankCo," *SEIKO : Journal of Management & Business*, vol. 6, no. 2, pp. 2023–223, 2023, doi: https://doi.org/10.37531/sejaman.v6i2.5519.

[28] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design Science in Information Systems Research," *MIS Quarterly*, vol. 28, no. 1, pp. 75–105, 2004, doi: 10.2307/25148625.

[29] P. Fusch and L. Ness, "Are We There Yet? Data Saturation in Qualitative Research," *Walden Faculty and Staff Publications*, vol. 20, no. 9, pp. 1408–1416, Feb. 2015, Accessed: Aug. 09, 2024. [Online]. Available: https://scholarworks.waldenu.edu/facpubs/455

[30] A. Shenton, "Strategies for Ensuring Trustworthiness in Qualitative Research Projects," *Education for Information*, vol. 22, pp. 63–75, Jul. 2004, doi: 10.3233/EFI-2004-22201.

[31] ISACA, *COBIT for Small and Medium Enterprises*. 2021. [Online]. Available: www.isaca.org