TEKNIKA: JURNAL SAINS DAN TEKNOLOGI

Homepage journal: http://jurnal.untirta.ac.id/index.php/ju-tek/

Original research article

Designing IT Governance for SME digital transformation based on COBIT 2019 SME focus area

Mega Ayu Natalia [a, *], Rahmat Mulyana [b], Ridha Hanafi [a]

[a] *Department of Industrial Engineering, Telkom University, Bandung, Indonesia*
[b] *Departement of Computer and Systems Sciences, Stockholm University, Stockholm, Sweden*

ARTICLE INFO

Article history
Submitted 14 August 2024
Received in revised form 4 March 2025
Accepted 1 May 2025
Available online 1 June 2025

Keywords
Digital transformation
Design science research
IT Governance
COBIT 2019 SME focus area

Editor:
Bobby Kurniawan

Publisher's note:
The publisher remains neutral regarding jurisdictional claims in published maps and institutional affiliations, while the author(s) bear sole responsibility for the accuracy of content and any legal implications.

ABSTRACT

As Industry 4.0 advances, organizations must embrace digital transformation (DT) to remain competitive. However, inadequate IT Governance (ITG) often leads to DT failures. While ambidextrous ITG models, combining traditional and agile approaches, have proven effective for large banks, their applicability to small and medium enterprises (SMEs) remains unexplored. This study aims to recommend prioritized ITG solutions for SMEs and estimate improvements in capability maturity levels to ensure successful DT. Employing Design Science Research (DSR) across five stages—problem identification, requirement specification, design, demonstration, and evaluation—data were collected through semi-structured interviews and document analysis. Using COBIT 2019's SME focus area, the analysis identified three key Information Technology Governance and Management (ITGM) objectives: EDM03 (Ensured Risk Optimization), APO12 (Managed Risk), and MEA03 (Compliance with External Requirements), with an average capability maturity level of 3.38. Sixteen solutions, based on seven ITGM components, were developed and compiled into a roadmap to elevate the maturity level to 3.84. This research enriches COBIT 2019 literature, proposes a hybrid ITG framework for SMEs, and enhances web-based information systems, fostering operational efficiency, risk mitigation, regulatory compliance, and sustainable competitiveness for SMEs undergoing DT.

1. Introduction

The Industrial Revolution 4.0 has transformed how traditional businesses manage operations, aiming to enhance productivity, efficiency, and customer service through widespread technology and internet adoption. This is critical for organizations to sustain competitiveness by implementing Digital Transformation (DT) [1]. According to [2], DT is a process of fundamental change enabled by innovative digital technologies and the strategic utilization of key resources and capabilities, aiming to radically improve an entity and redefine its value proposition for

* Corresponding author
Email address: megaan091@gmail.com

DOI: http://dx.doi.org/10.62870/tjst.v21i1.28291

stakeholders. Additionally, DT is an ongoing process that seeks to improve an entity by triggering significant changes in its properties through a combination of information technology, computing, communications, and connectivity [3]. The increasing need for DT is driven partly by regulatory policies and partly by global changes triggered by the COVID-19 pandemic. This transformation can be achieved by adopting innovative digital technologies and strategically deploying core resources and capabilities. The primary purpose of DT is to create fundamental changes in entities such as organizations, business networks, industries, or corporations, while rearticulating the value offered to stakeholders [4].

To achieve successful DT, companies must develop new IT capabilities aligned with strategic priorities in the digital realm, encompassing four key elements: technology, governance, processes, and talent. To remain competitive in the DT era, organizations must possess sufficient speed and flexibility to seize emerging business opportunities identified and prioritized through digital technologies [5]. These technologies include social, mobile, analytics, cloud, and the Internet of Things (IoT), collectively referred to as SMACIT+, which also encompasses emerging technologies such as artificial intelligence, blockchain, robotics, and virtual reality. The integration and utilization of these technologies at individual, group, or societal levels have significant consequences for individuals, groups, and society [6].

Usaha Mikro Kecil dan Menengah (UMKM), or Small and Medium Enterprises (SMEs), as defined by [7], are business activities that expand employment, provide broad economic services to the community, contribute to income equalization, promote economic growth, and enhance national stability. According to [8] on Banking, Indonesia's banking structure comprises Commercial Banks and *Bank Perekonomian Rakyat* (BPR). Per [9] on the Development and Strengthening of the Financial Sector, Commercial Banks and BPRs differ in several aspects. Commercial Banks are limited liability companies, while BPRs may be limited liability companies or cooperatives. Commercial Banks have higher capital limits than BPRs [9]. Additionally, BPRs operate within a limited geographic area compared to Commercial Banks and focus on serving different market segments. Financial institutions offering services to micro-enterprises, such as national micro-banking units, BPRs, and BPRS, are classified as formal microfinance entities operating under banking regulatory laws [10]. Thus, BPRs can be considered SMEs in the banking sector due to their smaller scale compared to Commercial Banks.

As a financial service institution serving small and medium segments conventionally, the institution in focus does not provide payment traffic services. It must assess the implementation of good corporate governance. According to [11], Information Technology Governance (ITG) is defined as leadership, organizational structures, processes, and relational mechanisms that ensure an organization's IT sustains and extends its strategy and objectives. The institution requires an appropriate ITG framework to address the DT process. The COBIT 2019 framework, the latest version of COBIT, is suitable due to its design factors that enable precise alignment of ITG mechanisms with business goals, particularly in the SME context [12]. This research employs the COBIT 2019 SME Focus Area, which focuses on designing ITG for SMEs to achieve DT [13], [14].

Despite the importance of ITG, many Princeps 2 notes that many DT efforts fail due to inadequate ITG [15]. Previous research has explored Information Technology Governance and Management (ITGM) mechanisms influencing DT [5] and validated their impact. Studies have identified hybrid ITGM mechanisms, combining agile-adaptive and traditional approaches, that influence DT in Indonesia's banking and insurance industries. These mechanisms include both perceived effectiveness and ease of implementation [16]. Further research [4] measured the influence of these mechanisms, finding a moderate impact on DT and a strong influence of DT on organizational performance (OP). Other studies have investigated ambidextrous IT mechanisms critical to DT success in an award-winning Indonesian bank, including their impact on DT and OP [17]. According to Mulyana et al. [18], ambidextrous ITG refers to "a synergistic combination of agile-adaptive and traditional ITG mechanisms that balance the dynamics of exploration with the flexibility of innovation, adaptability, and exploitation with the stability of efficiency control, enabling organizations to optimize their digital and IT risks and resources toward value realization."

While hybrid ITG models combining traditional and agile approaches have proven effective for large banks, their applicability to SMEs remains untested. Previous research in banking has identified ITG mechanisms influencing DT and OP [19] and tested their influence model [20]. Studies using COBIT 2019 have underscored ITG's importance for DT in general [21], [22], as well as in IT services [23], DevOps [24], IT risk [25], and information security [26]. This research addresses a gap by analyzing the COBIT 2019 SME Focus Area's application to ITG challenges in DT for BPRs as SMEs in the banking sector. The framework's applicability in this context, particularly within banking, remains underexplored.

This study fills this gap by analyzing its relevance to small banks, addressing the following questions: (1) How can ITG solutions be recommended based on a gap analysis of the COBIT 2019 SME Focus Area's priority design factors for DT in SMEs? (2) How can ITG be designed using the seven components of COBIT 2019 within the SME

Focus Area to support DT in SMEs? (3) Finally, how can the estimated improvement in ITG capability, based on the COBIT 2019 SME Focus Area, impact DT in SMEs? This research aims to align ITG practices with organizational strategy, enabling the institution to achieve its DT objectives. The proposed web-based solution drives DT by enhancing efficiency, technology integration, ITG flexibility, and business competitiveness, particularly for SMEs.

2. Material and method

This study adopts the Design Science Research (DSR) framework, which provides a concise and clear methodology for conducting and evaluating information systems research [27]. As shown in Fig. 1, DSR outlines problem formulation, relevant theories, and the scope of research discussion, divided into three sections: Environment, Information Systems Research, and Knowledge Base. The DSR method was selected because it systematically identifies problems, designs solutions based on the COBIT 2019 SME Focus Area, and evaluates their effectiveness, thereby enhancing the validity of the IT Governance (ITG) approach to support digital transformation (DT). Data were collected through semi-structured interviews and document analysis to ensure the solutions' relevance to organizational needs. Additionally, user involvement, including management and staff, was integrated into system development to ensure stakeholder inclusion, validate findings, and align solutions with operational conditions and organizational strategy.

Fig. 1 presents a framework adapted from Hevner [22]. This framework encompasses three scopes: Environment, Information Systems Research, and Knowledge Base. The Environment scope includes three components: People, Organization, and Technology. The Knowledge Base scope is divided into two categories: Foundations and Methodologies. Elements from the Environment and Knowledge Base scopes are synthesized to focus on Information Systems Research, which comprises two interdependent processes: Build/Develop and Justify/Evaluate. Fig. 2 illustrates the five stages of the research process in this study, adapted from [27].

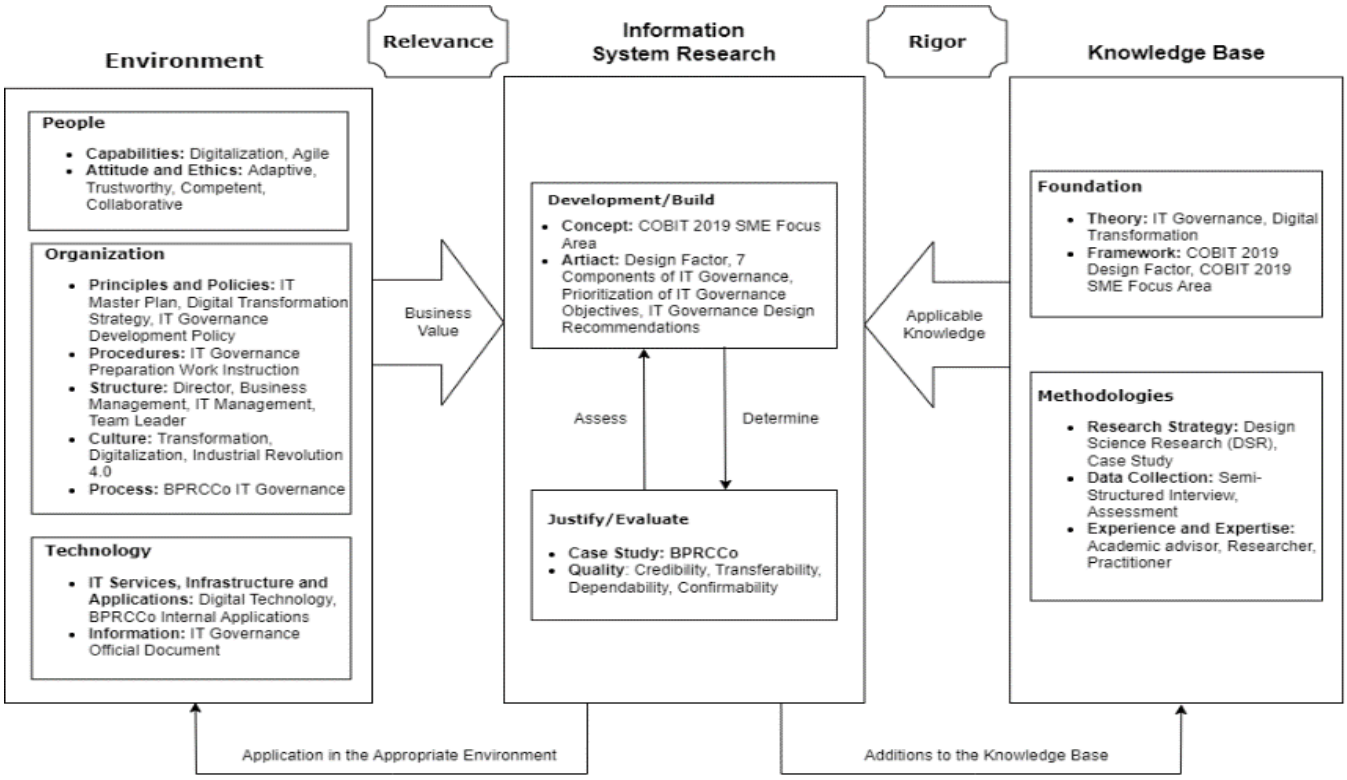

Fig. 1. Research method from Hevner.

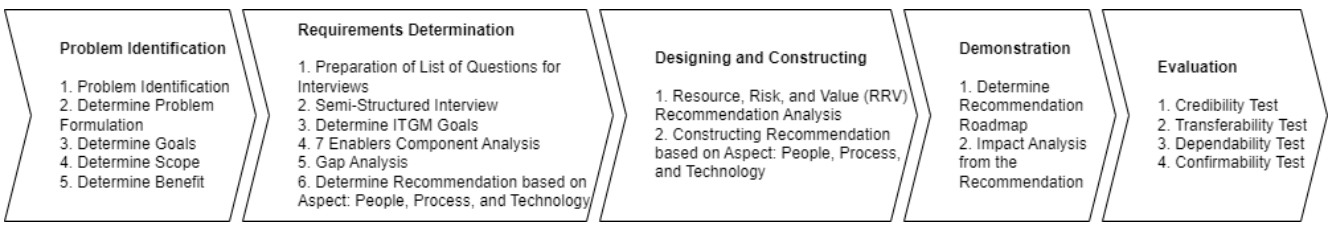

Fig. 2. Research process.

Table 1
Primary data.

Respondent	Position	Discussion
R1	Head of IT	IT policies, procurement, development processes, technology adoption, and methodologies
R2	Head of Risk Management	Risk management policy, risk analysis process, and risk implementation at BPRCCo
R3	Head of Compliance	Policies and procedures, regulatory, and regulatory compliance processes
R4	Compliance Staff	Policies and procedures, regulatory, and regulatory compliance processes
R5	Human Resources Staff	Personnel (central and branch employees, payroll process, and training program)
R6	Administration Staff	BPRCCo profile and administration
R7	Expert ITGDT BPR	Evaluation of research analysis results

Table 2
Secondary data.

Data	Description
BPRCCo Profile	The overview of the BPRCCo
BPRCCo Governance Implementation Report	The BPRCCo's annual governance report to related institutions
BPRCCo Organizational Structure	The organizational structure of the BPRCCo
BPRCCo Policy and Procedure Documents	The collection of policy and procedure documents at BPRCCo

Table 3
ITGM Objectives prioritization result.

ITGM objectives	(1)	(2)	(3)	(4)	Final score
MEA03: Managed Compliance with External Requirements	100	100	80	100	97
EDM03: Ensured Risk Optimization	100	95	80	100	96
APO12: Managed Risk	100	75	80	100	93

Note: (1) Regulation POJK 75 and SEOJK 15, (2) COBIT 2019 Design Factor, (3) COBIT 2019 SME Focus Area, (4) Past Research

Fig. 2 outlines the step-by-step research process as follows. First, the problem identification stage involves identifying issues related to IT Governance (ITG) preparation through a literature review to define the problem, objectives, research scope, and benefits. Second, the requirement specification stage includes preparing a list of questions for semi-structured interviews. According to [28], interviews were conducted until data saturation was achieved, focusing on capturing perspectives on specific topics. Individual perspectives were explored in depth, while group perspectives provided broader insights. This approach enabled efficient data collection within a short time frame. Data were collected from BPRCCo, a banking company. Data collection is categorized into two types: primary data, obtained directly from primary sources, and secondary data. Semi-structured interviews served as the primary data collection method. Primary data are presented in Table 1, detailing the systematic offline and online interviews conducted.

The study involved seven respondents who assisted the researcher in assessing BPRCCo's current state, conducting a gap analysis of the seven components of the governance system, identifying the potential governance system, and determining potential improvements. Table 2 presents the secondary data used to support the primary data in evaluating BPRCCo's condition to formulate improvement recommendations. The third stage, designing and constructing, involves analyzing improvement recommendations based on resources, risk, and value, and preparing recommendations for people, processes, and technology. The fourth stage, demonstration, includes preparing an improvement implementation roadmap and analyzing the effects of the draft improvement recommendations. The fifth stage, evaluation, tests credibility, transferability, dependability, and confirmability [29].

3. Results and discussion

3.1. Problem identification

This research began by identifying problems in the banking sector, particularly in small and medium enterprises (SMEs), specifically *Bank Perkreditan Rakyat* (BPR). The problem identification process involved determining the scope, objectives, and benefits of the research. The research scope focuses on BPRCCo, a company operating under the supervision of the *Otoritas Jasa Keuangan* (OJK), which conducts conventional banking activities.

Table 4
Process component analysis result.

Management practices		Achievement	Capability	
Objective	Sub-objective		Level	Achieve
EDM03	EDM03.01 Evaluate risk management.	100% (Fully)	2	4
		100% (Fully)	3	
	EDM03.02 Direct risk management.	100% (Fully)	2	
		100% (Fully)	3	
	EDM03.03 Monitor risk management.	100% (Fully)	2	
		100% (Fully)	3	
		100% (Fully)	4	
APO12	APO12.01 Collect data	100% (Fully)	2	2
		100% (Fully)	3	
		75% (Largely)	4	
	APO12.02 Analyze risk.	100% (Fully)	3	
		100% (Fully)	4	
		100% (Fully)	5	
	APO12.03 Maintain a risk profile.	100% (Fully)	2	
		100% (Fully)	3	
		100% (Fully)	4	
	APO12.04 Articulate risk.	100% (Fully)	3	
		100% (Fully)	4	
	APO12.05 Define a risk management action portfolio.	100% (Fully)	2	
		0% (Not Achieved)	3	
	APO12.06 Respond to risk.	100% (Fully)	3	
		100% (Fully)	4	
		100% (Fully)	5	
MEA03	MEA03.01 Identify external compliance requirements.	100% (Fully)	2	2
		100% (Fully)	3	
	MEA03.02 Optimize response to external requirements.	100% (Fully)	3	
	MEA03.03 Confirm external compliance.	75% (Largely)	3	
		100% (Fully)	4	
		100% (Fully)	5	
	MEA03.04 Obtain assurance of external compliance.	100% (Fully)	3	
		50% (Partially)	4	

The COBIT 2019 SME Focus Area framework was employed to develop Information Technology Governance (ITG) for Digital Transformation (DT) at BPRCCo. Additionally, the COBIT 2019 Design Toolkit was used, applying design factor analysis (factors one to ten) to prioritize IT Governance and Management (ITGM) objectives. The assessment of three ITGM objectives serves as a benchmark to evaluate BPRCCo's current condition and determine the target capability level.

3.2. Problem identification

3.2.1. ITGM objectives prioritization result

The final prioritization of IT Governance and Management (ITGM) objectives is determined based on four factors: the sequence of design factors, the SME Focus Areas from the COBIT 2019 SME Focus Area framework, regulations outlined in OJK [30], [31], and findings from previous research. Table 3 presents the final prioritization results. The highest prioritization score is achieved by MEA03: Managed Compliance with External Requirements, with an accumulated weight of 97. The second-highest score is achieved by EDM03: Ensured Risk Optimization, with an accumulated weight of 96. The third-highest score is achieved by APO12: Managed Risk, with an accumulated weight of 93.

Table 4 indicates that each management practice within EDM03: Ensured Risk Optimization, APO12: Managed Risk, and MEA03: Managed Compliance with External Requirements has a capability level based on the COBIT 2019 SME Focus Area framework. The process component assessment shows that each practice has achieved a certain level of performance. The organizational structure of BPRCCo was evaluated with reference to the COBIT 2019 SME Focus Area framework and the Skills Framework for the Information Age 8 [32].

Table 5
People, skills, and competencies component analysis result

Objective	Skills	Current State
EDM03	Business Risk Management	BPRCCo has the skills for pre-defined business risk management analysis.
	Risk Management	There is a Risk Management Team in BPRCCo that has the competency for risk management.
APO12	Business Risk Management	BPRCCo has the skills for predefined business risk management analysis.
	Information Assurance	BPRCCo has implemented measures to protect information systems, especially in the IT Team.
	Risk Management	BPRCCo does not yet have a training and education program related to risk management.*
MEA03	Information Security	BPRCCo does not yet have a compliance training and education program.*

Note: * means improved

Table 6
Principles, policies, and procedures component analysis result

Relevance principles, policies, and procedures	Current State
EDM03 Enterprise risk policy - Defines at a strategic, tactical and operational level how enterprise risk should be organized and managed in accordance with the company's business objectives. This policy should support the principles of enterprise risk governance and outline risk management activities.	BPRCCo has a risk management policy that regulates the identification, collection, analysis, and maintenance of risk profile.
MEA03 Compliance policy - Identify regulatory, contractual, and internal compliance requirements. Describes the process for assessing compliance with regulatory, contractual, and internal requirements. Lists roles and responsibilities for various activities in the process and provides guidance on metrics to measure compliance. Obtain compliance reports and confirm compliance or corrective actions to address compliance gaps in a timely manner.	BPRCCo does not yet have governance procedures that cover compliance requirements.*

Note: * means improved

3.2.2. Gap analysis result

This evaluation focused on the organizational structure as the primary decision-making entity in the company. Table A1 (see Appendices) reveals gaps in the organizational structure, specifically the absence of a Security Manager and a Legal role at BPRCCo. Table A2 in Appendices identifies gaps in the information component, indicating that BPRCCo has not fully implemented the follow-up plan for the findings related to the management practices in EDM03, APO12, and MEA03.

Table 5 shows that the management practices EDM03 Ensured Risk Optimization, APO12 Managed Risk, and MEA03 Managed Compliance with External Requirements all revealed gaps in the 'people, skills, and competencies' component. Specifically, BPRCCo lacks training and education programs related to risk management and compliance. This finding is supported by a respondent who stated, "Our bank only involves the head of the section to attend training but has not included the staff below him." This statement illustrates the current deficiency in BPRCCo's risk management skills.

Similarly, Table 6 indicates that these same management practices (EDM03, APO12, and MEA03) revealed gaps in the 'principles, policies, and procedures' component, as BPRCCo does not yet have governance procedures that cover compliance requirements. This is corroborated by Compliance staff, who explained that BPRCCo lacks such governance procedures. During an interview, a respondent further confirmed this, mentioning, "We [at] BPRCCo do not yet have a procedure that regulates activities and processes related to compliance, but we will design it for next year along with the OJK regulations released regarding this matter." This statement is reflected in the gap analysis of the 'principles, policies, and procedures' component.

Table 7 highlights that these management practices also identified gaps in the 'culture, ethics, and behavior' component. BPRCCo staff lack risk-related awareness, including an understanding of internal and external risk factors for each team, and are not aware of established policies, procedures, and applicable regulatory compliance.

Table 7
Culture, ethics, and behavior component analysis result

No	Objective	Key culture elements	Current state
1	EDM03	Promote an I&T risk-aware culture at all levels of the organization and proactively empower the company to identify, report, and improve I&T risks, opportunities, and potential business impacts. Senior management sets direction and demonstrates real and genuine support for risk practices. In addition, management should clearly define risk appetite and ensure appropriate levels of debate as part of business-as-usual activities. Desirable behaviors include encouraging employees to raise issues or negative outcomes and demonstrating transparency with respect to I&T risks. Business owners should accept ownership of I&T risks where applicable and demonstrate a genuine commitment to I&T risk management by providing adequate resources.	BPRCCo has implemented a proactive culture in the identification, reporting and potential business impact on the company.
2	APO12	To support a transparent and participatory risk culture, senior management must set direction and demonstrate real and genuine support for the incorporation of risk practices across the enterprise. Management should encourage open communication and business ownership for IT-related business risks. Expected behaviors include aligning policies with established risk appetite, reporting risk trends to senior management and risk governing bodies, rewarding effective risk management, and proactively monitoring risks and progress on risk action plans.	BPRCCo staff do not yet have an awareness of risk analysis to determine the internal and external risk factors for each team.*
3	MEA03	Promote a compliance-conscious culture, including zero tolerance for non-compliance with legal and regulatory requirements.	BPRCCo staff do not have an awareness of all the provisions that have been made and authorized in the form of policies, procedures, and compliance with applicable regulations. *

Note: * means improved

Table 8
Services, infrastructure, and application component analysis result

No	Objective	Services, infrastructure, and application	Current state
1	EDM03	Risk Management System	ISMS (Information System Management System), Data Center
2	APO12	Crisis Management Services	Disaster Recovery, Data Center
		Governance, Risk and Compliance (GRC) Tools	Statement of Applicable (SOA) ISO 27001:2022
		Risk Analysis Tools	OJK and BI Forms
		Risk Intelligence Services	Does not yet have an application related to risk intelligence
3	MEA03	Regulatory Watch Services	Do not yet have an application to support the compliance process*
		Third-Party Compliance Assessment Services	ISO 27001:2022 compliance and Assessment Consultant

Note: * means improved

Furthermore, Table 8 indicates that EDM03, APO12, and MEA03 found gaps in the 'services, infrastructure, and application' component. BPRCCo lacks:

- applications to mitigate risks related to incident handling management,
- services or software for managing governance and compliance,
- applications or services for assessing, monitoring, and overseeing risks related to BPRCCo, and
- applications to support the monitoring of findings, follow-up, and compliance.

3.2.3. Potential improvement

Finally, Table A3 (see Appendices) presents potential improvements across three aspects (people, process, and technology) for EDM03 Ensured Risk Optimization, APO12 Managed Risk, and MEA03 Managed Compliance with External Requirements. These improvements address seven components from COBIT 2019 and are categorized by these three aspects: People, Process, and Technology.

Table 9
Impact estimation on process component capability level

ITGM Objective	Previous capability level	Estimated capability after recommendation
EDM03 Ensured Risk Optimization	10	10
APO12 Managed Risk	23	25
MEA03 Managed Compliance with External Requirements	11	15
Total Amount	44	50
Total Score	3.38	3.84

Table 10
Impact estimation on Organization Structure, Information, People, Skill, and Competencies, Principles, Policies, and Procedures, Culture, Ethics, and Behavior, Service, Infrastructure, and Application Component

Component	Previous State	State after Recommendation
Organization Structure	BPRCCo has a manager responsible for all aspects of IT security management. However, the Bank only has a network security section/team. The bank does not have a general IT security role head.	IT Security role and responsibilities fulfilled
	BPRCCo does not currently have a role responsible for guidance on legal and regulatory matters.	Legal role and responsibilities fulfilled
Information	The working papers of the plan are responsive to implementation. However, during the execution of BPRCCo, not all of these plans were implemented as planned, so there is no report recording the gap follow-up.	Gap Follow-up Monitoring Record Report Document.
People, Skills, and Competencies	BPRCCo does not yet have a training and education program related to risk management.	Risk Management Training
	BPRCCo does not yet have a training and education program related to compliance.	Compliance Training
Principles, Policies, and Procedures	BPRCCo does not yet have IT governance procedures that include compliance requirements.	IT Governance Procedure
Culture, Etchics, and Behavior	BPRCCo staff do not have an awareness of risk analysis to determine the internal and external risk factors for each team.	Risk Management Awareness
	BPRCCo staff do not have an awareness of all the provisions that have been made and ratified in the form of policies, procedures, and compliance with applicable regulations.	Compliance Awareness
Services, Infrastructure, and Applications	Disaster Recovery, Data Center Statement of Applicable (SOA) ISO 27001:2022	Disaster Recovery, Data Center, SIEM Statement of Applicable (SOA) ISO 27001:2022, Compliance 360, SAP GRC
	Does not yet have an application related to risk intelligence	FICO Score, Tableau, SAS Risk Management
	Does not yet have an application to support the compliance process	Complysci, Auditboard

3.3. Designing and constructing

Table A4 (see Appendices) shows the prioritization of improvements based on the final value obtained from the results of the analysis of resources, risk, and value for each potential improvement to three aspects: people, process, and technology by considering the criteria for assessing resources [33], risks [34], and values [35].

3.4. Demonstration

Table A5 (see Appendices) presents the implementation roadmap designed for the suggested recommendations, which stem from potential improvements. The roadmap's development considered resource, risk, and value analysis, with prioritization guided by the priorities in Table A4. The roadmap itself is structured into four quarters over one year; however, the estimated implementation of these recommendations across people, process, and technology aspects is projected to take two years, from 2025 to 2026.

Table 9 illustrates the pre- and post-improvement capability levels. The capability level for EDM03 Ensured Risk Optimization shows no change, and it is noted that BPRCCo does not have a gap in the process components for this objective. APO12 Managed Risk exhibits an increased capability level, from 23 to 25, while MEA03 Managed Compliance with External Requirements increases from 11 to 15. Such increases are realized if BPRCCo fulfills all recommendations for each management practice, as specified by the COBIT 2019 SME Focus Area.

Drawing from the COBIT 2019 SME Focus Area, which includes components such as Organization Structure, Information, People, Skills, and Competencies, Principles, Policies, and Procedures, Culture, Ethics, and Behavior, and the Service, Infrastructure, and Application Component, the estimated design influence based on recommendations for BPRCCo is detailed below in Table 10.

3.5. Evaluation

In this study, there are four criteria for examining qualitative method research data to be tested by testing credibility, transferability, dependability, and confirmability [29]. Credibility is a key factor in evaluation techniques that prioritize internal validity. It involves researchers conducting measurements and checks to ensure the research aligns with its intended purpose [29]. In this study, credibility is demonstrated by presenting findings or gaps within BPRCCo, for which improvements were subsequently designed to be adoptable and implementable by the research object, BPRCCo. Transferability relates to the external validity of a study, assessing the extent to which findings can be accurately and effectively applied to other contexts or settings. In this investigation, external validity was addressed by formulating recommendations based on potential improvements. These recommendations are organized according to appropriate guidelines, illustrating how the findings can be extrapolated to other scenarios within information security management. The applicability of the designed improvements, based on research findings and including potential enhancements, to BPRCCo or similar contexts demonstrates transferability in this study [29].

Research is considered dependable (or reliable) if it can be replicated under similar conditions (context, methodology), yielding consistent results [29]. In this study, dependability is supported by comprehensive research documentation, including interview questions, transcripts, appendices of assessment results (using COBIT 2019 SME Focus Area framework tools), and documentation of suggested improvements for BPRCCo. This detailed documentation aims to ensure that the research process is transparent and could, in principle, lead to consistent analysis if replicated. Confirmability is a fundamental criterion in evaluation methodologies that emphasize objectivity. Research objectivity is considered achieved if the findings are grounded in the data and can be corroborated by others, rather than stemming solely from the researcher's biases or perspectives [29]. In this study, confirmability is addressed through the clear articulation of the research scope, methods, and identified gaps at BPRCCo. Furthermore, the research process and findings have been verified by relevant parties, including BPRCCo representatives, ITGDT BPR experts, and peer reviewers, to ensure the results are supported by the evidence.

3.6. Discussions

This research confirms that effective ITG mechanisms are critical to the digital transformation of SMEs such as BPRs. This finding is in line with previous research conducted on large banks, which also highlights ITG's crucial role in successful DT; this study affirms its importance for BPRs. BPRCCo faces challenges in implementing ambidextrous or hybrid ITG, mainly due to limited human and financial resources. However, with the right approach that combines agile methodologies for rapid development and traditional approaches to ensure operational stability, BPRCCo can improve its efficiency and responsiveness.

The results of this study make an important contribution to the understanding of how an ambidextrous approach can be adapted and applied in organizations with limited resources. This approach demonstrates the importance of flexibility and customization of IT policies to suit different scales of organizations. As such, this research paves the way for BPRCCo to implement more effective strategies to address the challenges of DT, maximize the potential of existing resources, and improve its competitiveness in the digital age.

However, the proposed ambidextrous approach still has limitations in scalability and adaptation to regulatory changes, particularly for resource-constrained SME banks. Further testing across various sectors is needed to ensure its broad effectiveness. Future developments may include the integration of artificial intelligence for decision automation and enhanced interoperability with other digital banking systems.

4. Conclusions

This study has several limitations, including potential bias due to its single case study design, limited generalizability beyond BPRCCo's specific banking context, inherent researcher subjectivity, and conclusions that may primarily apply to BPRs or similar entities. The research analysis identified three priority controls for BPRCCo: EDM03 (Ensured Risk Optimization), APO12 (Managed Risk), and MEA03 (Managed Compliance with External Requirements). The capability level before improvement was 3.38, which increased to 3.84 post-improvement, representing a gain of 0.46. Potential areas for further improvement include the people, process, and technology aspects.

This research is expected to enrich the ITG knowledge base for SME digital transformation and offer valuable practical insights for the management of similar organizations. It contributes to the literature by analyzing the application of ITG in the digital transformation (DT) of SMEs, particularly within the small-scale banking sector. Practically, the findings—leveraging COBIT 2019—can be applied to other industries facing similar challenges in risk management, regulatory compliance, and operational efficiency. However, the proposed solutions and frameworks may have limitations in terms of adaptability to rapid regulatory changes and integration with highly advanced banking technologies.

Future research directions include testing the approach across a broader range of case studies, exploring the use of AI for risk management, and investigating blockchain integration to enhance security and operational transparency.

Declaration statement

Mega Ayu Natalia: Conceptualization, Methodology, Writing-Original Draft, Collecting data, Writing-Review & Editing. **Rahmat Mulyana**: Conceptualization, Methodology, Writing-Review. **Ridha Hanafi**: Conceptualization, Methodology, Writing-Review.

Acknowledgement

The author extends the highest appreciation and sincere gratitude to:

- The expertise, for the willingness to serve as a subject matter expert and for providing insights and professional opinions that greatly assisted in the development of the framework and interpretation of the research findings.
- BPRCCo, for granting permission, data support, and access to information necessary for conducting the audit and collecting field data.
- The Research Team, fellow colleagues involved in this research process, for their cooperation, dedication, and collaborative spirit which played an important role in the successful implementation of this study.

The author acknowledges that this paper is still far from perfect. Therefore, the author welcomes any constructive suggestions and criticisms for future improvement.

Disclosure statement

This manuscript is submitted with the assurance that there is no conflict of interest, and that it conforms to the journal's ethical requirements and publication policies.

Funding statement

The study was completed without reliance on funding from any external sources.

Data availability statement

All relevant data supporting the conclusions of this research are provided within the article and accompanying supplementary materials.

AI Usage Statement

Generative AI and AI-assisted tools were used to enhance the language and readability of this manuscript. The authors have reviewed and revised all AI-generated content to ensure its accuracy and alignment with the research. The authors remain fully responsible for the work's scientific content, conclusions, and integrity, and disclose the use of AI to ensure transparency and adherence to publisher guidelines.

References

[1] G. Khaerunnisa, R. Mulyana, and L. Abdurrahman, "Pengujian Pengaruh Tata Kelola TI Terhadap Transformasi Digital dan Kinerja Asuransi A Menggunakan Structural Equation Modeling," *J. Ilm. Penelit. dan Pembelajaran Inform.*, vol. 8, no. 2, pp. 381–392, Jun. 2023, doi: 10.29100/jipi.v8i2.3469.

[2] C. Gong and V. Ribiere, "Developing a unified definition of digital transformation," *Technovation*, vol. 102, Apr. 2021, Art. no. 102217, doi: 10.1016/j.technovation.2020.102217.

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

[4] R. Mulyana, L. Rusu, and E. Perjons, "How Hybrid IT Governance Mechanisms Influence Digital Transformation and Organizational Performance in the Banking and Insurance Industry of Indonesia," in *Proc. 2023 Int. Conf. Inf. Syst. Dev.*, 2023.

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

[6] I. Sebastian et al., "How Big Old Companies Navigate Digital Transformation," *MIS Q. Exec.*, vol. 16, no. 3, pp. 197–213, Sep. 2017.

[7] Republic of Indonesia, "Undang-Undang Republik Indonesia Nomor 20 Tahun 2008 tentang Usaha Mikro, Kecil, dan Menengah," 2008.

[8] Republic of Indonesia, "Undang-Undang Republik Indonesia Nomor 10 Tahun 1998 tentang Perbankan," 1998,

[9] Republic of Indonesia, "Undang-Undang Republik Indonesia Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan," 2023.

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

[11] S. De Haes and W. Van Grembergen, "IT Governance and Its Mechanisms," 2004. [Online]. Available: https://blog.dinamika.ac.id/erwin/files/2013/02/jpdf041-ITGovernanceandIts.pdf

[12] D. Utomo et al., "Leveraging COBIT 2019 to Implement IT Governance in SME Context: A Case Study of Higher Education in Campus A," *CommIT J.*, vol. 16, no. 2, pp. 129–141, Jun. 2022, doi: 10.21512/commit.v16i2.8172.

[13] ISACA, *COBIT® 2019 Framework: Introduction and Methodology*, 2019. [Online]. Available: https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004Ko9cEAC.

[14] ISACA, *COBIT for Small and Medium Enterprises*, 2021. [Online]. Available: https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004L2noEAC.

[15] N. Obwegeser et al., "7 Key Principles to Govern Digital Initiatives," 2020. [Online]. Available: https://mitsmr.com/2UWvNEs.

[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 *Proc. PACIS 2022*, 2022.

[17] R. Mulyana, L. Rusu, and E. Perjons, "Key Ambidextrous IT Governance Mechanisms for Successful Digital Transformation: A Case Study of Bank Rakyat Indonesia (BRI)," *Digit. Bus.*, vol. 4, no. 2, Dec. 2024, Art. no. 100083, doi: 10.1016/j.digbus.2024.100083.

[18] 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 *Proc. PACIS 2024*, 2024.

[19] F. Luthfia, R. Mulyana, and L. Ramadani, "Analisis Pengaruh Tata Kelola TI Terhadap Transformasi Digital dan Kinerja Bank B," *ZONAsi: J. Syst. Inf.*, vol. 4, no. 2, 2022.

[20] T. Z. Nurafifah, R. Mulyana, and L. Abdurrahman, "Pengujian Model Pengaruh Tata Kelola TI Terhadap Transformasi Digital dan Kinerja Bank A," *J. Inf. Syst. Res. (JOSH)*, vol. 4, no. 1, pp. 73–82, Oct. 2022, doi: 10.47065/josh.v4i1.2257.

[21] O. T. P. Poetry, "Perancangan Tata Kelola Teknologi Informasi untuk Digital di Industri Perbankan Menggunakan Framework COBIT 2019 dengan Domain, Deliver, Service, and Support: Studi Kasus Bank XYZ," 2021. [Online]. Available: https://openlibrarypublications.telkomuniversity.ac.id/index.php/engineering/article/view/15776.

[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," 2021.

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

[24] N. Riznawati, R. Mulyana, and A. F. Santoso, "Pendayagunaan COBIT 2019 DevOps dalam Merancang Manajemen Pengembangan TI Agile pada Transformasi Digital BankCo," *SEIKO: J. Manag. Bus.*, vol. 6, no. 2, pp. 2023–223, 2023.

[25] Y. W. Dwi, M. Dewi, R. Mulyana, and A. F. Santoso, "Penggunaan COBIT 2019 I&T Risk Management untuk Pengelolaan Risiko Transformasi Digital BankCo," 2023.

[26] A. Rahmadana, R. Mulyana, and A. F. Santoso, "Pemanfaatan COBIT 2019 Information Security dalam Merancang Manajemen Keamanan Informasi pada Transformasi BankCo," 2023.

[27] R. Santosa and D. Irawan, "Studi Risiko TI pada Sektor Keuangan," *Jurnal Sistem Informasi Bisnis*, vol. 6, no. 2, 2021, hlm. 34–45, doi: 10.31933/jsib.v6i2.210.

[28] P. I. Fusch and L. R. Ness, "Are We There Yet? Data Saturation in Qualitative Research," *Qual. Rep.*, vol. 20, no. 9, pp. 1408–1416, 2015. [Online]. Available: http://www.nova.edu/ssss/QR/QR20/9/fusch1.pdf.

[29] A. K. Shenton, "Strategies for ensuring trustworthiness in qualitative research projects," *Educ. Inf.*, vol. 22, no. 2, pp. 63–75, 2004, doi: 10.3233/EFI-2004-22201.

[30] Otoritas Jasa Keuangan, "POJK NOMOR 75/POJK.03/2016 Tentang Standar Penyelenggaraan Teknologi Informasi Bagi Bank Perkreditan Rakyat dan Bank Pembiayaan Rakyat Syariah," 2016. [Online]. Available: https://ojk.go.id/id/kanal/perbankan/regulasi/peraturan-ojk/Pages/POJK-tentang-Standar-Penyelenggaraan-Teknologi-Informasi-bagi-Bank-Perkreditan-Rakyat-dan-Badan-Pembiayaan-Rakyat-Syariah.aspx

[31] Otoritas Jasa Keuangan, "SEOJK NOMOR 15/SEOJK.03/2017 Tentang Standar Penyelenggaraan Teknologi Informasi Bagi Bank Perkreditan Rakyat dan Bank Pembiayaan Rakyat Syariah," 2017. [Online]. Available: https://ojk.go.id/id/kanal/perbankan/regulasi/surat-edaran-ojk/Pages/Surat-Edaran-Otoritas-Jasa-Keuangan-Nomor-15-SEOJK.03-2017-.aspx

[32] SFIA Foundation, "SFIA 8: The Framework Reference," 2021. [Online]. Available: https://www.sfia-online.org

[33] J. Song, A. Martens, and M. Vanhoucke, "Using Earned Value Management and Schedule Risk Analysis with resource constraints for project control," *Eur. J. Oper. Res.*, vol. 297, no. 2, pp. 451–466, 2022, doi: 10.1016/j.ejor.2021.05.036.

[34] S. Tangprasert, "A Study of Information Technology Risk Management of Government and Business Organizations in Thailand using COSO-ERM based on the COBIT 5 Framework," *J. Appl. Sci. (Thailand)*, vol. 19, pp. 13–24, Jun. 2020, doi: 10.14416/j.appsci.2020.01.002.

[35] S. Jagannathan and A. Sorini, "A Cybersecurity Risk Analysis Methodology for Medical Devices," in *Proc. 2015 IEEE Symp. Product Compliance Eng. (ISPCE)*, 2015, pp. 1–6, doi: 10.1109/ISPCE.2015.7138706.

Authors information

Mega Ayu Natalia is a student majoring in Information Systems, Telkom University, Indonesia. Her reasearch interests include IT governance and digital transformation.

Rahmat Mulyana is a PhD researcher and lecturer at the Department of Computer and Systems Sciences (DSV), Stockholm University, Sweden. His research interests include IT governance, risk management, audit and assurance, digital transformation, enterprise architecture, and information security and privacy management.

Ridha Hanafi is a Professional Lecturer and Researcher in Information Systems, Universitas Telkom, Indonesia. He received the doctoral degree from Universitas Pendidikan Indonesia, Indonesia. His research interests include enterprise architecture and IT governance & management.

Appendices

Table A1
Organization structure component analysis result

COBIT Post	Objective	Current State
Board	EDM03	President Director - BPRCCo has a Board or group of executives and/or directors who are responsible for corporate governance and have full control over its resources.
Executive Committee	EDM03	Board of Commissioners - The Company has a group of senior executives involved in managing the portfolio of IT-enabled Investments, IT services and IT assets, ensuring that value is delivered, and risk is managed. This committee is usually chaired by a board member.
Financial Manager	EDM03, MEA03	Consumer Credit Director - BPRCCo has managers responsible for all aspects of finance, including financial risks and controls and reliable and accurate accounts.
General Manager	EDM03, MEA03	Chief Operating Officer - BPRCCo has the highest functioning section responsible for the total management of the company.
Operations Manager	EDM03, MEA03	
Head of IT	EDM03, APO12, MEA03	Head of IT - BPRCCo has in place a manager responsible for aligning IT and business strategies and is accountable for planning, resourcing and managing the delivery of IT services and solutions and solutions to support corporate objectives.
Security Manager	EDM03	Infrastructure & Network Security - BPRCCo has a manager responsible for all aspects of IT security management. However, the Bank only has a network security section/team. The bank does not have a general IT security role head.*
Business Process Owners	APO12, MEA03	Head of Operations, Head of Marketing, Head of Billing - BPRCCo has a section that is responsible for the performance of a process in realizing its objectives, driving process improvements and approving process changes.
Security Expert	APO12	Security Expert / Head of IT - BPRCCo has a role that is responsible for the security management aspects of the company.
IT Development Coordinator	APO12, MEA03	Application & System Development - BPRCCo has a role that is responsible for the process of developing IT-related solutions.
IT Operations Coordinator	APO12, MEA03	Network Infrastructure & Security - BPRCCo has a role responsible for the IT operational environment and infrastructure.
Privacy Officer	APO12, MEA03	Risk Management - BPRCCo has a role responsible for monitoring the risks and business impact of privacy laws and for guiding and coordinating the implementation of policies and activities that ensure compliance.
Legal Department	MEA03	Legal Department - BPRCCo does not currently have a role responsible for guidance on legal and regulatory matters.*
Compliance or Quality	MEA03	Compliance - BPRCCo has a function within the company responsible for all external compliance guidance.
Audit	MEA03	Internal Audit Unit - BPRCCo has the role of being responsible for the provision of internal audit.

Note: * means improvement

Table A2
Information component analysis result

Objective	Information Output	Current State
EDM03.01 Evaluate Risk Management	Risk Appetite Guidance	BPRCCo currently has a risk appetite that is recognized and approved by the board.
	Evaluation of Risk Management Activities	BPRCCo has conducted an evaluation of its risk management activities.
	Approved Risk Tolerance Levels	The Risk Management Team at BPRCCo has assessed the level of each risk.
EDM03.02 Direct Risk Management	Approved Process for Measuring Risk Management	BPRCCo involves the board of commissioners to approve and evaluate risk management policies.
	Key Objectives to be Monitored for Risk Management	The Risk Monitoring Committee of BPRCCo has monitored the implementation of risk management activities.
	Risk Management Policies	BPRCCo has risk management policies, risk management procedures, and risk limit setting.
EDM03.03 Monitor Risk Management	Remedial Actions to Address Risk Management Deviations	BPRCCo corrects risk management deviations that have been mitigated.
	Risk Management Issues for the Board	The Risk Monitoring Committee reports to the Board of Commissioners on various risks and potential risks faced

Table A2
Information component analysis result

Objective	Information Output	Current State
		by BPRCCo and the implementation of risk management by the Board of Directors.
APO12.01 Collect data.	Identified Risk Issues and Factors	BPRCCo determines the current conditions to find out what factors influence the occurrence of risks.
	Data on Risk Events and Contributing Factors	BPRCCo records incidents and incident factors and/or problems that occur.
APO12.02 Analyze risk.	Risk Analysis Results	BPRCCo has a risk register to keep up to date on the combined risk scenarios that are occurring.
APO12.03 Maintain a risk profile.	Documented Risk Profile, Including Status of Risk Management Actions	BPRCCo has a risk profile to identify the current condition of the company.
APO12.04 Articulate risk.	Risk Analysis and Risk Profile Reports for Stakeholders	BPRCCo conveys risk scenarios via email with the aim that relevant stakeholders can understand the risks to make decisions.
	Results of Third-Party Risk Assessments	BPRCCo has evaluated the assessment of third parties.
APO12.05 Define a risk management action portfolio.	Project Proposals for Reducing Risk	BPRCCo has developed a document to attach possible strategic opportunities to reduce the Bank's risk.
APO12.06 Respond to risk.	Risk Impact Communication	The working papers of the plan are responsive to be implemented, but during execution not all plans are responsive to be implemented as planned.*
	Risk-Related Root Causes	The company has recorded the cause and follow-up findings.
MEA03.01 Identify external compliance requirements.	Log of Required Compliance Actions	BPRCCo records the current state of all relevant legal, regulatory, and contractual requirements, their impact, and required actions.
	Compliance Requirements Register	BPRCCo maintains an overall list of harmonized and integrated external compliance requirements for the company.
MEA03.02 Optimize response to external requirements.	Communications of Changed Compliance Requirements	If there are changes to requirements and compliance, approved policy, standards and procedures documents can be socialized to the teams involved via email or can be presented online.
	Updated I&T Policies and Procedures	BPRCCo has updated policies and/or procedures when there is a change in new legal requirements.
MEA03.03 Confirm external compliance.	Compliance Confirmations	BPRCCo has a compliance letter that contains the status of each regulatory regulation.
	Identified Compliance Gaps	BPRCCo's Compliance Team evaluates the company's processes and activities based on regulatory compliance.

Table A3
Potential Improvement

No	Aspect	Component	Type	Potential Improvement
1	People (EDM03, APO12, MEA03)	Organization Structure	Roles and Responsibility	Added an IT Security role responsible for all aspects of IT security management.
2	People (EDM03, APO12, MEA03)	Organization Structure	Roles and Responsibility	Add a Legal role responsible for guidance on legal and regulatory issues.
3	People (EDM03, APO12, MEA03)	People, Skills, and Competencies	Skills & Awareness	Create a training program or townhall related to risk management.
4	People (EDM03, APO12, MEA03)	People, Skills, and Competencies	Skills & Awareness	Create a training program or townhall related to compliance with external policies, procedures, and regulations.
5	People (EDM03, APO12, MEA03)	Culture, Ethics, and Behavior	Skills & Awareness	Create awareness in the form of media posters or videos related to risk awareness in organizations channeled through email.
6	People (EDM03, APO12, MEA03)	Culture, Ethics, and Behavior	Skills & Awareness	Create awareness in the form of media posters or videos related to awareness of compliance with internal and external provisions that have been authorized by BPRCCo.

Table A3
Potential Improvement

No	Aspect	Component	Type	Potential Improvement
7	Process (APO12)	Process	Policy	Create an IT Quality Management program that contains findings, recommendations, and follow-ups which will then be reported to relevant parties.
8	Process (APO12)	Process	Procedures	Add provisions related to conducting internal and external risk analysis with a time scale of 1 (one) time per 3 (three) months in risk management procedures.
9	Process (APO12)	Process	Procedures	Adding provisions on the scale of evaluation of company processes and activities against regulators 1 (one) time per 3 (three) months in governance procedures.
10	Process (APO12)	Process	Procedures	Adding provisions related to the process of monitoring and reporting compliance status to relevant internal parties in the governance procedures.
11	Process (APO12)	Principles, Policies, and Procedures	Procedures	Add procedures containing provisions, processes, and sub-processes in implementing compliance governance.
12	Process (APO12)	Information	Record	Adding supervisory records based on the execution of the follow-up plan of the findings.
13	Technology (APO12)	Services, Infrastructure, and Application	Tools	Adding tools that can assist BPRCCo in minimizing risks related to incident handling management.
14	Technology (APO12)	Services, Infrastructure, and Application	Tools	Adding software that has the function to manage the Bank's governance and compliance.
15	Technology (APO12)	Services, Infrastructure, and Application	Tools	Adding applications that include risk assessment, monitoring, and supervision features at BPRCCo.
16	Technology (APO12)	Services, Infrastructure, and Application	Tools	Adding applications to support the process of monitoring compliance with regulations.

Table A4
RRV analysis result for roadmap prioritization

No	Aspect	Potential Improvement	Score	Category
1	People	Add an IT Security role that is responsible for all aspects of IT security management.	18	Medium
2	People	Create a training program or townhall related to risk management.	12	Medium
3	People	Create training programs or townhalls related to compliance with external policies, procedures, and regulations.	12	Medium
4	People	Add a Legal role responsible for guidance on legal and regulatory issues.	9	Low
5	People	Create awareness in the form of media posters or videos related to risk awareness in organizations channeled through email.	9	Low
6	People	Create awareness in the form of media posters or videos related to awareness of compliance with internal and external provisions that have been authorized by BPRCCo.	9	Low
7	Process	Add procedures containing provisions, processes, and sub-processes in implementing compliance governance.	18	Medium
8	Process	Create an IT Quality Management program that contains findings, recommendations, and follow-ups that will then be reported to relevant parties.	18	Medium
9	Process	Adding provisions on the scale of evaluation of the company's processes and activities against regulators 1 (one) time per 3 (three) months to the governance procedures.	18	Medium
10	Process	Adding provisions related to conducting internal and external risk analysis with a time scale of 1 (one) time per 3 (three) months in the risk management procedure.	18	Medium
11	Process	Adding supervisory records based on the execution of the follow-up plan of the findings.	12	Medium
12	Process	Adding provisions related to the process of monitoring and reporting compliance status to relevant internal parties to the governance procedures.	6	Low
13	Technology	Add tools that can assist BPRCCo in minimizing risks related to incident handling management.	12	Medium
14	Technology	Adding software that has the function to manage bank governance and compliance.	9	Low
15	Technology	Adding applications that include risk assessment, monitoring, and supervision features at BPRCCo.	6	Low
16	Technology	Adding applications to support the process of monitoring compliance with regulations.	6	Low

Table A5
Roadmap implementation of the designed recommendation

Recommendation	Category	Roadmap Timeline							
		2025				2026			
		Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
People Aspect									
Add an IT Security role that is responsible for all aspects of IT security management.	Medium								
Create a training program or townhall related to risk management.	Medium								
Create training programs or townhalls related to compliance with external policies, procedures, and regulations.	Medium								
Add a Legal role responsible for guidance on legal and regulatory issues.	Low								
Create awareness in the form of media posters or videos related to risk awareness in organizations channeled through email.	Low								
Create awareness in the form of media posters or videos related to awareness of compliance with internal and external provisions that have been authorized by BPRCCo.	Low								
Process Aspect									
Add procedures containing provisions, processes, and sub-processes in implementing compliance governance.	Medium								
Create an IT Quality Management program that contains findings, recommendations, and follow-ups that will then be reported to relevant parties.	Medium								
Adding provisions on the scale of evaluation of the company's processes and activities against regulators 1 (one) time per 3 (three) months to the governance procedures.	Medium								
Adding provisions related to conducting internal and external risk analysis with a time scale of 1 (one) time per 3 (three) months in the risk management procedure.	Medium								
Adding supervisory records based on the execution of the follow-up plan of the findings.	Medium								
Adding provisions related to the process of monitoring and reporting compliance status to relevant internal parties to the governance procedures.	Low								
Technology Aspect									
Add tools that can assist BPRCCo in minimizing risks related to incident handling management.	Medium								
Adding software that has the function to manage bank governance and compliance.	Low								
Adding applications that include risk assessment, monitoring, and supervision features at BPRCCo.	Low								
Adding applications to support the process of monitoring compliance with regulations.	Low								