

AGILE IT SERVICE MANAGEMENT DESIGN OF FINTECHCO DIGITALIZATION BASED ON COBIT 2019 DEVOPS FOCUS AREA

Achmad Fadhli Satriadi^{*1}, Rahmat Mulyana², Rokhman Fauzi³

¹Faculty of Industrial Engineering, Telkom University, Bandung, Indonesia

²Department of Computer and Systems Sciences, Stockholm University, Stockholm, Sweden

³Faculty of Industrial Engineering, Telkom University, Bandung, Indonesia

Email: ¹acfadhli@student.telkomuniversity.ac.id, ²rahmat@dsv.su.se, ³rokhmanfauzi@telkomuniversity.ac.id

(Article received: August 07, 2023; Revision: September 08, 2023; published: October 15, 2023)

Abstract

The Indonesian Financial Technology (Fintech) industry plays a pivotal role in driving digital technology advancements and propelling the nation's growth. The rapid development of Fintech presents a unique challenge for established financial companies, necessitating effective government regulation through a Sandbox approach. FintechCo, operating under the watchful eye of State-Owned Enterprises and the Financial Service Authority, must strike a delicate balance between their agile services and security risks. Hence, FintechCo necessitates an examination of optimal agile services through the utilization of five stages derived from the Design Science Research approach. This need arises to adhere to the Good Corporate Governance standards established by State-Owned Enterprises (SOE) and the Financial Services Authority (FSA). The cutting-edge COBIT 2019 DevOps Focus Area framework is employed for analysis. The research identifies three highest priority Governance and Management Objectives (GMOs): Managed Security Services (DSS05), Managed Problem (DSS03), and Managed Solution Identification and Build (BAI03). These GMOs are thoroughly evaluated, and comprehensive recommendations are provided based on their seven key components. There is an estimated 17% increase in the average capability score, from 2.82 to 3.30, across all three GMOs. The contribution of this study is twofold: to serve as a valuable knowledge resource for agile IT services in digitalization within organizations and to offer practical implications for FintechCo to enhance their digitalization. Furthermore, this research sets a precedent for the Fintech industry, signifying a benchmark for excellence and innovation.

Keywords: COBIT 2019 DevOps Focus Area, Design Science Research, Digitalization, Financial Technology, Indonesia, Information Technology Governance & Management.

1. INTRODUCTION

In this era, Information Technology (IT) is essential in developing education, economy, industry, and the country. This shift has led to the emergence of various challenges such as digitalization that need to be addressed to meet evolving needs. The ongoing process of digitalization is restructuring the dynamics between customers and businesses, necessitating fresh approaches for structuring and innovating business models [1]. There are many perceptions about digitalization, two of them are the utilization and implementation of digital technologies within the contexts of individuals, entities, or broader enterprises [2] and the transformation of interactions communications, business functions, and business models into the digital ones [3]. Setia [4] highlight that digitalization plays a pivotal role in the transformation journey of companies, as it improves customer relations, enhances IT-enabled business processes, and facilitates the delivery of online services.

IT has a significant role in the operational activities of a company [5]. The worldwide

momentum towards digital transformation has heightened the necessity for the proficient, streamlined processes and provision of software products, services, and solutions [6]. Because IT is very important and crucial in organizations, the use and development of IT must be agile. In business, agile organization is a strategy that helps to quickly adapt and respond to changes in the environment, such as evolving customer needs and advancements in technology [7]. The integration of Agile principles within the IT Governance framework has the potential to accelerate decision-making processes, reinforce business procedures, and augment organizational competitiveness [8]. Agile IT design requires regulations such as IT Governance (ITG), which focuses on monitoring IT assets, impacting business value, and mitigating IT-related risks [9]. This because ITG coordination is carried out under by the board, executive management, and IT management [10]. ITG also has a very important position in driving digital efforts within the organization [11].

The development of information technology impacts assimilation in every sector, one of which is the finance sector. The upward trajectory of financial and technological innovation has generated a heightened scholarly curiosity within this specific realm of study [12]. Over time, the financial and information technology sectors have merged under the name of Financial Technology (Fintech). The term 'Fintech' embodies a fusion of information technology and financial services, possessing the potential to transform business structures and facilitate entry into the industry [13]. Fintech has been attracting attention and acceptance rapidly in recent years [14]. The expectations of fintech itself cause significant challenges for several business organizations in implementing it. This is what causes the presence of fintech to be called digital disruption, where every business organization will try to compete with one another in developing it. One such manifestation of Fintech innovation in Indonesia is represented by FintechCo.

The world of finance hasn't been immune to the IT revolution. In fact, established incumbent financial companies have found themselves disrupted by this digital technology, compelling them to embrace Digital Transformation (DT) [15]. Digital technology disrupts incumbent companies due to its capacity to revolutionize traditional business models and processes. In the realm of finance, DT essentially means harnessing the power of fresh digital technologies like social media, mobile computing, and Internet of Things (IoT), with the goal to effect significant business enhancements. These include bettering customer interactions, streamlining operations, and bringing in groundbreaking business models. The objective of this transformation is not just to boost efficiency and improve customer service, but also to roll out innovative financial products. This changes the entire perspective of stakeholders towards traditional financial institutions, offering them a whole new interactive experience [16]. Nonetheless, the execution of digital transformation (DT) is a complex process, with frequent failures attributed to inadequate Information Technology Governance (ITG) [17]. Moreover, Incumbent companies require digital transformation to modernize outdated processes, enhance customer experiences, and remain competitive in the digital age. Starting from planning, system integration, governance, and other factors need to be considered for business organizations to be able to adopt fintech. By doing so, the organization can ensure that all aspects of its IT function are synchronized and in harmony with its overall objectives. Therefore, DevOps came as a means of culture shift toward collaboration between development, quality assurance, and operations [18]. DevOps practices promote a culture where development and operations teams work together, fostering shared ownership and responsibility. By shifting away from traditional

methods, organizations can foster effective collaboration among teams and employees, streamline the exchange of ideas and suggestions, and eliminate lengthy and cumbersome processes.

The fintech regulations are listed in Bank Indonesia Regulation No.18/40/PBI/2016 [19] about the Implementation of Payment Transaction Processing (PTP). According to Bank Indonesia, PTP is an innovation primarily related to fintech to meet the community's needs, especially in the payment system, both in terms of instruments, organizers, mechanisms, and infrastructure for implementing payment transaction processing. Other regulations were stated in Bank Indonesia Regulation Number 19/12/PBI/2017 [20] concerning implementing Financial Technology. This regulation contains the implementation of financial technology, which is divided into several categories: payment systems, market support, investment management, risk management, loans, financing, provision of capital, and other financial services. This regulation was made as a response to the development of Fintech in Indonesia. With this regulation, a stable, efficient, and safe financial system is hoped to be used for business organizations and the people of Indonesia. Furthermore, in POJK Number 13/POJK0.2/2018 [21] and PER-2/MBU/03/2023 [22], the basis for good governance defined as governance that applies the principles of openness, accountability, responsibility, independence, professionalism, and fairness in an integrated manner within conglomerate SOE.

To design agile information technology governance and management, this research uses the COBIT 2019 DevOps Focus Area framework approach as the initial standard. This study was undertaken by building upon prior research [23] that primarily concentrated on process components, thereby incorporating additional components from the Seven Components. By integrating these supplementary components, this research endeavors to achieve several objectives, including assessing the status of Agile Service within the framework of digitalization at FintechCo, formulating recommendations grounded in identified gaps, and evaluating the efficacy of these recommendations when applied within the current operational landscape of FintechCo.

2. METHODS

This study uses the Design Science Research framework that has been developed and optimized by Hevner [24] to support designing Agile Services at FintechCo. Design Science Research shown in Figure 1 explains the formulation of the problem, theories relevant to research, as well as the scope of research discussion which is divided into three (3) sections, namely Environment, Information System Research, and Knowledge.

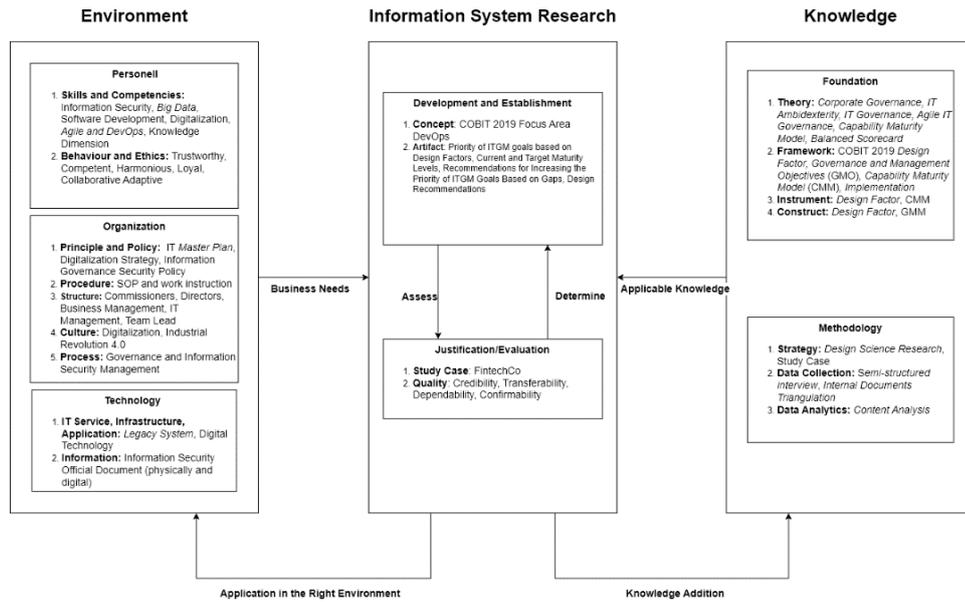


Figure 1. Design Science Research adopted from Hevner

The systematic research shown in Figure 2 explains the five (5) phases of systematic problem solving in this study. The first phase begins with Problem Identification, which describes problem identification, problem formulation, goal formulation, and problem definition formulation obtained through literature studies. The next phase is Requirements Determination, which explains the preparation for the interview phase, determining ITGM objectives, gap analysis, and determining recommendations based on Aspect: People, Process,

and Technology. Then proceed with the Designing and Constructing phase which consists of Resource, Risk, and Value analysis and preparation of recommendations based on Aspect: People, Process, and Technology. Next is the Demonstration phase, which consists of the phases of preparing a recommendation roadmap and determining the impact of the recommendations that have been prepared. The last phase is the Evaluation phase which is the phase of tests such as credibility, transferability, dependability, and confirmability[25].

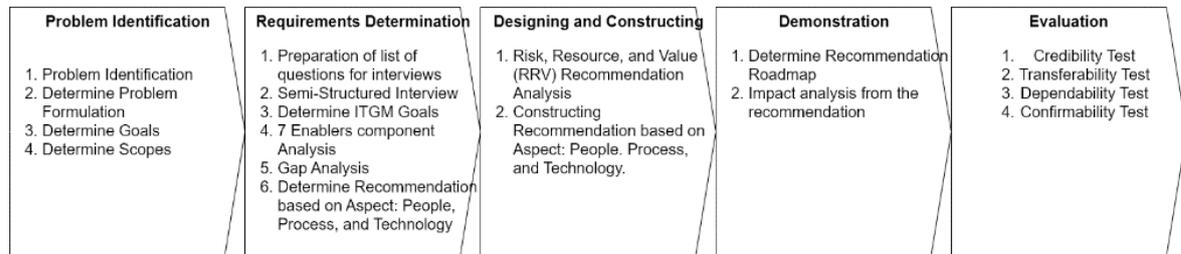


Figure 2. Systematic Research

3. RESEARCH RESULTS

3.1. ITGM Objectives Prioritization Result

The following is the prioritization based on the COBIT 2019 design factor toolkit [26] and the COBIT 2019 DevOps Focus Area [6]. The results of the two analyzes are multiplied and the results used to determine priorities.

Table 1. ITGM Objectives Prioritization Result

ITGM Objectives	Design Factor Score	Focus Area Score	Final Score
DSS05: Managed Security Services	80	2	160
DSS03: Managed Problems	50	3	150
BAI03: Managed Solutions Identification and Build	50	3	150

Based on Table 1, The Focus Area is value two (2) included in Secondary Relevance and is in the domain DSS05: Managed Security Services. Focus Areas have a value of three (3) including Primary Relevance and are found in two (2) domains, namely: DSS03: Managed Problems and BAI03: Managed Solutions Identification and Build. The three domains above were chosen because they have the highest score compared to the other domains.

3.2. Gap Analysis Result

A. Process Component

The results of the analysis carried out on the process components show that there are gaps in DSS05 with several gaps: DSS03 with one (1) gap, and BAI03 with two (2) gaps. The score obtained for

each ITGM Objectives is 2.9 for DSS05, 2.8 for DSS03, and 2.75 for BAI03. The following are the results of the analysis shown in Table 2.

Table 2. Process Component Analysis Result

Management Practices	Achievement (%)	Capability Level
DSS05: Managed Security Services		
DSS05.01	100 Fully	2
	100 Fully	3
	100 Fully	4
DSS05.02	100 Fully	2
	100 Fully	3
	75 Largely	4
DSS05.03	89 Fully	2
	100 Fully	3
	100 Fully	4
DSS05.04	100 Fully	2
	90 Fully	3
	83 Largely	4
DSS05.05	88 Fully	2
	67 Largely	3
	50 Partially	4
DSS05.06	75 Largely	2
	88 Fully	3
	50 Partially	4
DSS05.07	88 Fully	2
	100 Fully	3
Total Capability Level Achieved		20
Average Score Level of Capability (Scale 0-5)		2.9
DSS03: Managed Problems		
DSS03.01	75 Largely	2
DSS03.02	100 Fully	2
DSS03.03	100 Fully	3
DSS03.04	100 Fully	2
	88 Fully	3
	50 Partially	4
	50 Partially	5
DSS03.05	100 Fully	2
	92 Fully	3
	100 Fully	4
Total Capability Level Achieved		14
Average Score Level of Capability (Scale 0-5)		2.8
BAI03: Managed Solutions Identification and Build		
BAI03.01	75 Largely	2
BAI03.02	95 Fully	2
	90 Fully	3
BAI03.03	70 Largely	2
	75 Largely	3
BAI03.04	88 Fully	3
BAI03.05	100 Fully	2
	100 Fully	3
BAI03.06	100 Fully	2
	100 Fully	3
	100 Fully	4
BAI03.07	83 Largely	2
	90 Fully	3
	50 Partially	4
BAI03.08	100 Fully	2
BAI03.09	90 Fully	3
BAI03.10	100 Fully	2
	100 Fully	3
	100 Fully	4
BAI03.11	100 Fully	3
BAI03.12	100 Fully	3
Total Capability Level Achieved		33
Average Score Level of Capability (Scale 0-5)		2.75

B. Policies, Principles, and Frameworks Component

This component explains the gaps related to policies, principles, and framework. In this component, FintechCo has no gaps regarding

policies, principles, and framework. The results of the analysis are shown in Table 3.

Table 3. Policies, principles, and frameworks analysis results

Relevance Policy, and Principle	Framework, Current State
DSS05: Managed Security Services	
Information security policy - Sets guidelines to protect corporate information and associated systems and infrastructure.	FintechCo already has policies in place to protect company information, systems and infrastructure. This is regulated in the Information Security Management Policy.
DSS03: Managed Problems	
Problem Resolution Policy – Documents rationale and provides guidance for addressing problems that result from incidents and identifying validated workarounds.	FintechCo already has a policy that regulates the management of security incidents, where every information security incident will be recorded and reported, and incident analysis must consider several criteria so that corrective and preventive actions can be prioritized.
BAI03: Managed Solutions Identification and Build	
Maintenance Policy - Defines proper support of software and hardware components to ensure longer asset life, increase employee productivity and maintain an acceptable user experience.	FintechCo already has a policy regarding computer management that includes software (application standards, end-user applications, OS), hardware (use of personal computers, removable media), and platforms (cloud, database).
Software development policy - Standardizes software development across the organization by listing all protocols and standards to be followed.	FintechCo already has policies regarding application standards and application system development standards that must be verified and validated to ensure that the inputs used and the outputs are correct, complete, and appropriate.
System and service acquisition policy - Provides procedures to assess, review and validate requirements for acquisition of system and services.	FintechCo has established procedures for identification, collection, acquisition and preservation of information within incident management procedures.

C. Culture, Ethics, and Behavior Component

In this component, a gap was found in BAI03. Table 4 displays the results of the analysis on the culture, ethics, and behavior components. This component affect people at organization.

Table 4. Culture, ethics, and behavior component analysis results

Key Culture Elements	Current State
DSS05: Managed Security Services	
Create a culture of awareness regarding user responsibility to maintain security and privacy practices.	FintechCo already has a guideline for security and privacy in daily practice with an Information Security Management Policy and has implemented awareness of information security.
DSS03: Managed Problems	
Support a culture of proactive problem management (detection, action and prevention) with clearly defined	FintechCo has set a policy that requires each user to record every information security incident and report

Key Culture Elements	Current State
roles and responsibilities. Ensure a transparent and open environment for reporting problems by providing independent reporting mechanisms and/or rewarding people who bring problems forward.	it to the Service Desk. This was determined to be able to assist monitoring and support the needs of investigations in the future. FintechCo also conducts technical compliance testing through regular vulnerability assessments
BAI03: Managed Solution Identification and Build	
Ensure agile and scalable delivery of digital services; engage an ecosystem of partners with whom the organization can work or set up a bimodal IT structure with digital factories, agile leaders and teams, continuous flow, and a mindset toward improvement.	FintechCo already has an Agile Project Management program as implemented in their Risk Assessment. Currently FintechCo is also working with several digital companies such as AWS and Google Cloud Platform.
Establish an open, unbiased culture that fairly and objectively evaluates alternatives when investigating potential new solutions (including whether to build or buy).	FintechCo does not yet have an open and impartial culture of evaluating and investigating potential new solutions

D. Application, Infrastructure, and Service Component

This component shows the gaps related to the application, infrastructure, and services that exist in FintechCo. Complete results are shown in Table 5 below.

Table 5. Application, infrastructure, and service component analysis result

Application, Infrastructure, and Service	Current State
DSS05: Managed Security Services	
Directory Services	Using Microsoft Single Sign On (SSO)

Table 6. Organization structure analysis results

COBIT Structure	Organization	Management Objective	Current State
Chief Officer	Technology	BAI03, DSS03	The company already has a Chief Technology Officer who is responsible for identifying technology trends as well as developing and managing the company's technology architecture.
Chief Officer	Information	BAI03, DSS05, DSS03	There is an IT Steering Committee, where members of the committee consist of representatives from the Chief Information Officer, Chief Information Security Officer, and Chief Digital Officer
Chief Security Officer	Information	DSS05	
Chief Digital Officer		BAI03	
Executive Committee		DSS03	
Steering Committee		BAI03	
Business Owners	Process	BAI03, DSS05	Business Process Owners reside in each unit head but mostly in IT Big Data & Analytic Group
Portfolio Manager		BAI03	FintechCo does not yet have a Portfolio Manager role responsible for ensuring that the management system is fully integrated into the portfolio of programs, projects and services.
Business Manager	Continuity	BAI03	FintechCo does not yet have a Business Continuity Manager responsible for managing, designing, overseeing, and assessing an enterprise's business continuity capability, to ensure that the enterprise's critical functions continue to operate following disruptive events.
Project Office	Management	BAI03	FintechCo does not yet have a Project Continuity Manager who is responsible for Ensuring that projects related to DevOps are initiated, planned, and executed in accordance with the management system.
Head Development		BAI03, DSS05, DSS03	There is a Development Center Group and a Test & Quality Assurance Unit which are responsible for designing solutions, solution components, conducting QA, and change management
Program Manager		BAI03	
Project Manager		BAI03	

Application, Infrastructure, and Service	Current State
Email Filtering Systems	There is a policy related to email management, including email filtering
Identity and Access Management System	Using Microsoft Single Sign On (SSO)
Security Awareness Services	Security awareness training has been conducted
Security Information and Event Management (SIEM) Tools	No tools related to SIEM were found
Security Operations Center (SOC) Services	No SOC services found
Third-Party Security Assessment Services	Using FintechCo's IT Audit Final Report
URL Filtering Systems	There is a policy regarding URL management, including URL filtering
DSS03: Managed Problems	
Problem tracking/resolution system	Fintech does not yet have a Problem Management Catalog which functions as a tool for a problem tracking/resolution system.
BAI03: Managed Solution Identification and Build	
Digital services	Amazon Web Services, Google Cloud Platform
Solution evaluation and selection services	DevOps uses Gitlab; project management using JIRA and Confluence; Continuous Improvement/Development using Ansible. For DevOps and CI/CD activities used on AWS
Testing tools and services	

E. Organization Structure Component

In the results of the analysis of the organization structure components, there is a gap with the number three (3). FintechCo does not yet have roles such as Business Continuity Manager, Project Management Office and Portfolio Manager. The result shown in Table 6.

COBIT Structure	Organization	Management Objective	Current State
Relationship Manager		BAI03	FintechCo has an existing B2B and B2C unit, which is tasked with overseeing and managing the internal interface and communications between the business and I&T functions.
Service Manager		BAI03, DSS03	The Service Management Unit is responsible for overseeing the IT service management process and aligning service levels with business requirements.
Information Manager	Security	BAI03, DSS05, DSS03	The IT Security Policy, Compliance, and Control unit are accountable for both information security and corporate IT.
Privacy Officer		BAI03, DSS05	
Head Architect		BAI03	The IT Architecture Unit is in charge of developing, managing, implementing, and providing guidance on the company's IT architecture.
Head IT Operations		BAI03, DSS05, DSS03	The IT Infrastructure Unit is tasked with managing the company's IT infrastructure, including record-keeping and IT administration.
Head IT Administration		BAI03	
Head Human Resources		DSS05	The Human Resources department is responsible for human resource planning and policy development.

F. Information Component

The results of the information component analysis at FintechCo show gaps in reports such as penetration testing reports, user access review

reports, issues closure reports, and problem management catalogs that are not yet available. The results are shown in Table 7.

Table 7. Information component analysis result

Management Practice	Information Output	Current State
DSS05: Managed Security Services		
DSS05.01 - Protect against malicious software.	Malicious software prevention policy	FintechCo already has a policy regarding the handling of malicious software (malicious code, viruses)
	Evaluations of potential threats	The framework and methodology used by FintechCo anticipate threats, weaknesses, impacts, and risk management (possibility of fraud, security threats, and related business risks).
DSS05.02 - Manage network and connectivity security.	Connectivity Security Policy	Fintech already has policies related to connectivity security that are regulated in the Information Security Management Policy
	Results Of Penetration Tests	FintechCo has conducted penetration testing, but found no reports related to penetration testing
DSS05.03 - Manage endpoint security.	Security Policies for Endpoint Devices	FintechCo already has policies related to security for endpoint devices that are regulated in the Information Security Management Policy
DSS05.04 - Manage user identity and logical access.	Results of Reviews of User Accounts and Privileges	There are no report documents related to user access review
	Approved User Access Rights	There is an Access Control Procedure policy
DSS05.05 - Manage physical access to I&T assets.	Access Logs	
	Approved Access Requests	
DSS05.06 - Manage sensitive documents and output devices.	Access Privileges	FintechCo already has a policy regarding access rights set out in CHAPTER VIII Access Settings
	Inventory Of Sensitive Documents and Devices	FintechCo already has a policy regarding access rights set out in CHAPTER VIII Access Settings
DSS05.07 - Manage vulnerabilities and monitor the infrastructure for security-related events.	Security Incident Tickets	FintechCo has utilized the Service Desk for tickets regarding security incidents
	Security Incident Characteristics	FintechCo has utilized Service Desk to classify security incidents
	Security Event Logs	FintechCo has a record of security incidents, this is regulated in Chapter VII Operational and Communication Management
DSS03: Managed Problems		
DSS03.01 - Identify and classify problems.	Problem classification scheme	FintechCo does not yet have a problem classification scheme
	Problem status reports	FintechCo already has a policy regarding every issue of information security incidents that must be recorded and reported to the Service Desk
	Problem register	FintechCo does not yet have a Problem Management Catalog to record the problems found.
DSS03.02 - Investigate and diagnose problems.	Problem resolution reports	
	Root causes of problems	FintechCo has set a policy that requires each user to record every information security incident and report it to the Service Desk. This was determined to be able to assist monitoring and support the needs of investigations in the future.
DSS03.03 - Raise known errors.	Proposed solutions to known errors	
	Known error records	
DSS03.04 - Resolve and close problems.	Communication of knowledge learned	Information regarding incidents reported to the Service Desk will be shared with the appropriate parties
	Closed problem records	FintechCo doesn't have any reports of Problem Closure yet.

Management Practice	Information Output	Current State
DSS03.05 - Perform proactive problem management.	Identified sustainable solutions Problem resolution monitoring reports	All activities on Fintech are recorded and stored. Information on these activities will be used to assess the Business Continuity Plan
BAI03: Managed Solutions Identification and Build		
BAI03.01 - Design high-level solutions.	Approved high-level design specification	FintechCo already has an architectural design that meets the needs of the RPO (Recovery Point Objective refers to how much data loss a company application can tolerate)
BAI03.02 - Design detailed solution components.	Internal and external SLAs	FintechCo already has a policy towards internal and external parties.
	Approved detailed design specification	FintechCo already has an architectural design that meets RPO needs with consideration and testing of applications, databases, cloud, network.
BAI03.03 - Develop solution components.	Feasibility study report	FintechCo already has a policy regarding approval of requirements by sponsors such as risk mitigation requirements relating to supplier access to organizational assets must be agreed with suppliers and documented
	Approvals of requirements and proposed solutions by sponsor	
BAI03.04 - Procure solution components.	Approved acquisition plan	FintechCo's current acquisition plan is the current acquisition of cloud subscriptions (GCP and AWS) through partnership channels
	Updates to asset inventory	FintechCo already has a policy on asset inventory
BAI03.05 - Build solutions.	Integrated and configured solution components	FintechCo already has a policy regarding solution integration such as integrated risk and opportunity handling
BAI03.06 - Perform quality assurance (QA).	Quality review results, exceptions and corrections Quality assurance plan	FintechCo already has a Test & Quality Assurance Unit to handle IT changes and transitions
BAI03.07 - Prepare for solution testing.	Test procedures	
	Test plan	
BAI03.08 - Execute solution testing.	Test result communications	FintechCo already has procedures and test plans such as incident management procedures.
	Test result logs and audit trails	
BAI03.09 - Manage changes to requirements.	Record of all approved and applied change requests	FintechCo already has a policy regarding recording every change to their application system.
	Maintenance plan	
BAI03.10 - Maintain solutions.	Updated solution components and related documentation	The plan for testing, maintenance and re-assessments as in the Business Continuity Plan is carried out regularly by FintechCo.
	Updated service portfolio	
BAI03.11 - Define IT products and services and maintain the service portfolio.	Service definitions	FintechCo has set policies regarding formal change control procedures that must be defined and carried out precisely, every change in the system will be reviewed and tested to ensure there are no negative impacts on operations or security.

G. People, Skills, and Competencies Component

Table 8 shows that FintechCo have gaps on BAI03 regarding documentation production and

systems design that still based only on Microsoft Visio.

Table 8. People, skills, and competencies component analysis result

Skills	Current State
DSS05: Managed Security Services	
Information Security	Fintech has implemented antivirus installation, access rights settings, and awareness training related to information security
Information Security Management	FintechCo has implemented management in antivirus installation, management of access rights restrictions, and awareness management by conducting awareness training related to information security.
Penetration Testing	FintechCo has conducted penetration testing related to information security and system security.
Security Administration	Security-related administration at FintechCo has been regulated in the FintechCo Information Security Management Policy.
DSS03: Managed Problems	
Business risk management	Decree of the Board of Directors of the Company No. 01/FKN-01/KD/VIII/2019 concerning Business Continuity Plan Policy
Information assurance	Already contained in the Information Security Management Policy
Risk management	Already contained in the Decision of the Board of Directors of Risk Management using COSO and ERM
BAI03: Managed Solution Identification and Build	
Application development	FintechCo manages its Application Development based on COBIT EDM, PBRM and related PBI
Business process testing	FintechCo manages its Business Process Testing based on PBI, EU, Fund Transfer PBI, PBI, PPTP, PP PSTE
Component integration	FintechCo manages its Component Integration based on the Decision of the Risk Management Directors using COSO and ERM
Database design	FintechCo manages and uses its Database Design based on AWS, SuSE Linux, PSQL
Documentation production	FintechCo manages its Documentation Production using only Microsoft Office Visio
Hardware design	FintechCo manages its Hardware Design based on UML, EA, JIRA
Porting/software configuration	FintechCo manages its Software Configuration using Java, CI/CD, Ansible

Programming/software development	FintechCo manages its Software Development based on Agile, SDLC, DevOps and uses Java, PSQL, AWS CI/CD
Release and deployment	FintechCo manages its Release And Deployment based on AWS
Solution architecture	FintechCo manages its Solution Architecture using Microsoft Office Visio, AWS, JIRA
Solution deployment	FintechCo manages its Solution Deployment using Ansible, AWS CI/CD, AWS ECS, JIRA
Systems design	FintechCo manages its Systems Design using only Microsoft Office Visio
Systems development management	FintechCo manages its Systems Development Management based on AWS CI/CD
Systems engineering	
Systems installation/decommissioning	FintechCo manages its Systems Engineering using UML, EA, JIRA
Systems integration	
Testing	
User experience design	FintechCo manages its Testing using Microsoft Project, JIRA

3.3. Potential Improvement

The goal of potential improvement is to pinpoint what changes are necessary to fill any identified gaps.

The changes in potential improvement are divided into three (3) aspect, which are People, Process, and Technology. Below are the results of potential improvements shown in Table 9.

Table 9. Potential improvements

No.	Component	Type	Potential Improvement
People Aspect			
BAI03: Managed Solution Identification and Build			
1	Organization Structure	Roles, Responsibilities	Added the role of Business Continuity Manager who is responsible for managing, designs, oversees and/or assesses an enterprise's business continuity capability, to ensure that the enterprise's critical functions continue to operate following disruptive events.
2	Organization Structure	Roles, Responsibilities	Adding the role of Portfolio Manager responsible for guiding portfolio management, ensuring selection of correct programs and projects, managing and monitoring programs and projects for optimal value, and realizing long-term strategic objectives effectively and efficiently.
3	Organization Structure	Roles, Responsibilities	FintechCo does not yet have a Project Management Office role
4	Culture, Ethics, and Behavior	Communication; Skills & Awareness	Conduct training or create and execute a well-thought-out communication strategy that consistently reinforces the significance of quality and continuous improvement initiatives in a regular and impactful manner. The purpose of this recommendation is about the importance of open communication when evaluating and investigating potential new solutions.
5	People, Skills, and Competencies	Skills & Awareness	Conduct training to improve and develop skills in Documentation Production
6	People, Skills, and Competencies	Skills & Awareness	Conduct training to improve and develop skills in System Design
Process Aspect			
DSS05: Managed Security Services			
1	Process	Policy	Adding points regarding regular physical information security awareness training to information security management policies CHAPTER VI Physical and Environmental Management
2	Process	Procedure	Develop procedures for deleting or destroying sensitive documents owned by the company
3	Information	Record	Create a User Access Review Report template
4	Information	Record	Create a penetration testing report template that is function as a documentation tool for the penetration testing carried out.
DSS03: Managed Problem			
1	Process	Record	Create a Problem Management Catalog template that functions to store records or entries for each problem that has been identified and logged within the organization.
2	Information	Record	Create a Problem Closure or Problem Resolution Report template that contains a detailed summary and results of problems solved within an organization
BAI03: Managed Solution Identification and Build			
1	Process	Record	Create a documentation report template about Solution Component that complies with standards. The documentation is useful in providing clear and consistent information on each component of the solution.
2	Process	Policy	Create and add IT Strategic Plan policies that serve as the basis for all processes and activities for planning the future of the company's IT.
Technology Aspect			
DSS05: Managed Security Services			
1	Application, Infrastructure, and Service	Tools	Define the right and suitable tools such as AZURE sentinel, Splunk enterprise, IBM Qradar that can collect, analyze and manage security information and events that occur in the IT environment
DSS03: Managed Problem			
1	Application, Infrastructure, and Service	Tools	Create a Problem Management Catalog template that functions to store records or entries for each problem that has been identified and logged within the organization.

3.4. Resource, Risk, and Value (RRV) Analysis

Potential improvements that have been determined then be compiled in a roadmap that has been prioritized based on resource, risk, and value (RRV) analysis. RRV analysis gives a score of three (3) with the criteria: if the required resource comes from internal sources, the risk impacts one unit in the company, and the value of the implementation impacts all units in the company. Next, the RRV analysis gives a score of two (2) with the criteria: if the required resources come from internal and external, the risk impacts several units in the company, and the value of the implementation impacts several units in the company. And finally, the RRV analysis gives a score of one (1) with the criteria: if the required resource comes from an external source, the risk impacts all units in the company, and the value of the implementation impacts one unit in the company. Following are the results of the roadmap priority analysis based on the RRV shown in Table 10.

Table 10. RRV analysis results for roadmap prioritization

No.	Potential Improvement	Final Score	Category
Aspect: People			
1	Conduct training or create and execute a well-thought-out communication strategy that consistently reinforces the significance of quality and continuous improvement initiatives in a regular and impactful manner. The purpose of this recommendation is about the importance of open communication when evaluating and investigating potential new solutions.	27	High
2	Adding the role of the Project Management Office which is responsible for supporting program and project managers and for gathering, assessing and reporting information about the conduct of programs and constituent projects	12	Medium
3	FintechCo does not yet have a Business Continuity Manager who is responsible for managing, designs, oversees and/or assesses an enterprise's business continuity capability, to ensure that the enterprise's critical functions continue to operate following disruptive events	9	Low
4	Conduct training to improve and develop skills in Documentation Production	8	Low
5	Conduct training to improve and develop skills in Systems Design	6	Low
6	Adding the role of Portfolio Manager responsible for	6	Low

No.	Potential Improvement	Final Score	Category
	guiding portfolio management, ensuring selection of correct programs and projects, managing and monitoring programs and projects for optimal value, and realizing long-term strategic objectives effectively and efficiently.		
Aspect: Process			
1	^Create a User Access Review Report template	27	High
2	Create a penetration testing report template that is useful as a documentation tool for the penetration testing carried out.	27	High
3	Adding points regarding regular physical information security awareness training to information security management policies Chapter VI Physical and Environmental Management	18	Medium
4	Create a documentation report template about Solution Component that complies with standards. The documentation is useful in providing clear and consistent information on each component of the solution.	18	Medium
5	Develop procedures for deleting or destroying sensitive documents owned by the company	9	Low
6	Create and add IT Strategic Plan policies that serve as the basis for all processes and activities for planning the future of the company's IT.	6	Low
7	Create a Problem Closure or Problem Resolution Report template that contains a detailed summary and results of problems solved within an organization	4	Low
8	Create a Problem Management Catalog template that functions to store records or entries for each problem that has been identified and logged within the organization.	3	Low
Aspect: Technology			
1	Define the right and suitable tools such as AZURE sentinel, Splunk enterprise, IBM Qradar that can collect, analyze and manage security information and events that occur in the IT environment	6	Low

3.5. Implementation Roadmap

The following is an overview of the implementation roadmap designed based on the RRV analysis shown in Table 11.

Table 11. Roadmap implementation of the designed recommendation

Recommendation	Roadmap Timeline (Quarter)							
	2024				2025			
	1	2	3	4	1	2	3	4
People Aspect								
Conduct training or create and execute a well-thought-out communication strategy that consistently reinforces the significance of quality and continuous improvement initiatives in a regular and impactful manner. The purpose of this recommendation is about the importance of open communication when evaluating and investigating potential new solutions (27 - High)								
Adding the role of the Project Management Office which is responsible for supporting program and project managers and for gathering, assessing and reporting information about the conduct of programs and constituent projects (12 – Medium)								
FintechCo does not yet have a Business Continuity Manager who is responsible for managing, designs, oversees and/or assesses an enterprise's business continuity capability, to ensure that the enterprise's critical functions continue to operate following disruptive events (9 - Low)								
Conduct training to improve and develop skills in Documentation Production (8 - Low)								
Conduct training to improve and develop skills in Systems Design (6 - Low)								
Adding the role of Portfolio Manager responsible for guiding portfolio management, ensuring selection of correct programs and projects, managing and monitoring programs and projects for optimal value, and realizing long-term strategic objectives effectively and efficiently (6 - Low)								
Process Aspect								
Create a User Access Review Report template (27 - High)								
Create a penetration testing report template that is useful as a								

Recommendation	Roadmap Timeline (Quarter)							
	2024				2025			
	1	2	3	4	1	2	3	4
documentation tool for the penetration testing carried out (27 - High)								
Adding points regarding regular physical information security awareness training to information security management policies - Physical and Environmental Management (18 - Medium)								
Create a documentation report template about Solution Component that complies with standards. The documentation is useful in providing clear and consistent information on each component of the solution (18 - Medium)								
Develop procedures for deleting or destroying sensitive documents owned by the company (9 - Low)								
Create and add IT Strategic Plan policies that serve as the basis for all processes and activities for planning the future of the company's IT (6 - Low)								
Create a Problem Closure or Problem Resolution Report template that contains a detailed summary and results of problems solved within an organization (4 - Low)								
Create a Problem Management Catalog template that functions to store records or entries for each problem that has been identified and logged within the organization (3 - Low)								
Technology Aspect								
Define the right and suitable tools such as Azure sentinel, Splunk enterprise, IBM Qradar that can collect, analyze and manage security information and events that occur in the IT environment (6 - Low)								

3.6. Impact Estimation of Recommendations on FintechCo

The following is an estimate of the impact of the recommendations designed for the gaps found in each component. The process component shows the increasing score on all GMOs after the recommendations. The estimated result of process component is shown in Table 12. With these

recommendations, the capability score on the three GMOs is estimated to increase, for DSS05, from 2.9 to 3.6; DSS03 from 2.8 to 3.2; and BAI03 from 2.75 to 3.1. There is an estimated average of 17% increase in the average capability score, from 2.82 to 3.30, across all three GMOs

Table 12. Impact estimation on process component

ITGM Objectives	Previous Capability Level	Estimated Capability After Recommendation
DSS05: Managed Security Services	2.90	3.60
DSS03: Managed Problems	2.80	3.20
BAI03: Managed Solution Identification and Build	2.75	3.10
Average Capability	2.82	3.30

The recommendations on the organization structure component give 3 (three) roles and responsibilities: Portfolio Manager, Business Continuity Manager, and Project Management Office. The recommendations on the information component give template guidelines for reports and documentation documents. FintechCo also received a training and certification recommendation on the culture, ethics, and behavior component, and the people, skills, and competencies component. Lastly, on the application, technology, and services component, FintechCo received recommendations as solutions for the missing tools and documents. Below is the estimated impact result of the recommendation given to FintechCo, shown in Table 13.

Table 13. Impact estimation on organization structure, information, culture, people, and application component

Previous State	State After Recommendation
Organization Structure Component	
BAI03: Managed Solution Identification and Build	
FintechCo does not yet have a Portfolio Manager role responsible for ensuring that the management system is fully integrated into the portfolio of programs, projects and services.	Portfolio Manager role and responsibilities fulfilled
FintechCo does not yet have a Business Continuity Manager responsible for managing, designing, overseeing, and assessing an enterprise's business continuity capability, to ensure that the enterprise's critical functions continue to operate following disruptive events.	Business Continuity Manager role and responsibilities fulfilled
FintechCo does not yet have a Project Management Office who is responsible for Ensuring that projects related to DevOps are initiated, planned, and executed in accordance with the management system.	Project Management Office role and responsibilities fulfilled
Information Component	
DSS05: Managed Security Services	
FintechCo has conducted penetration testing, but found no reports related to penetration testing	Guidelines for penetration testing results reports

There are no report documents related to user access review	User Access Review Report Document has been made
DSS03: Managed Problem	
FintechCo does not yet have a problem classification scheme	Problem Management Catalogue Document
FintechCo does not yet have a Problem Management Catalog to record the problems found.	Problem Management Catalogue Document
FintechCo doesn't have any reports of closing issues yet.	Problem Closure Document
Culture, Ethics, and Behavior Component	
BAI03: Managed Solution Identification and Build	
FintechCo does not yet have an open and impartial culture of evaluating and investigating potential new solutions	With training and certification being held as well as establishing effective and consistent communication governance, it is hoped that it will be able to close the Culture, Ethics and Behavior Component gap at FintechCo.
People, Skills, and Competencies Component	
BAI03: Managed Solution Identification and Build	
Competence of Documentation Production is still based only on Microsoft Visio	With training and certification recommendation being held, it is hoped that the employee at FintechCo can improve their skills on Documentation Production.
Competence of Systems Design is still based only on Microsoft Visio	With training and certification recommendation being held, it is hoped that the employee at FintechCo can improve their skills on Systems Design
Application, Infrastructure, and Service Component	
DSS05: Managed Security Services	
No tools related to SIEM were found	Splunk Enterprise [27]
Security Operations Center (SOC) Services	Splunk Enterprise [27]
DSS03: Managed Problem	
Fintech does not yet have a Problem Management Catalog which functions as a tool for a problem tracking/resolution system.	Problem Management Catalogue Document has been made

4. DISCUSSION

Entering the Fintech sector, a hotbed of innovation, where pioneering companies like FintechCo are born in the digital era. These startups typically boast modest assets and lower inherent risks, affording regulators the opportunity to grant them more flexibility through the Regulatory Sandbox approach [20]. This newfound freedom calls for a different approach to IT governance and management - one that is agile, adaptive, and aligns seamlessly with their dynamic environment. For these Fintech companies, the pursuit of swift digitalization, rapid customer experience enhancements, and sustainable control over their operations necessitates

a holistic focus on robust development and operations (DevOps) [21].

The findings from prior research [23] had an emphasis on the process component. These findings solely recognized discrepancies linked to practices and activities within business processes. Consequently, in the context of this study, the elements encompassing the Seven Components were incorporated to pinpoint gaps in areas including information, culture, competencies, organizational structure, policies, and infrastructure. To address these gaps and bolster FintechCo's IT agile services, we have formulated recommendations encompassing three essential aspects: people, process, and technology. In the people aspect, our research has led us to propose additional roles and responsibilities, essential to fortify the organization's resilience, including a dedicated Business Continuity Manager, Portfolio Manager, and Project Management Office. In the process aspect, our tailored recommendations center on designing Standard Operating Procedures (SOPs), report templates, and critical policies that were previously absent. By providing these guidelines, we empower FintechCo to navigate challenges with efficiency and effectiveness, ensuring they stay ahead of the competition. Furthermore, the technology aspect of our recommendations is a pivotal pillar in enhancing FintechCo's performance. By identifying suitable applications and tools, we equip FintechCo with the necessary resources to thrive in the digital age, making the most of emerging technologies to deliver unparalleled customer experiences. With these recommendations, the capability score on the three GMOs is estimated to increase, for DSS05, from 2.9 to 3.6; DSS03 from 2.8 to 3.2; and BAI03 from 2.75 to 3.1. There is a 17% increase in the average capability score, from 2.82 to 3.30, across all three GMOs.

The crux of this study lies in revealing the function of the Design Science Research approach, expertly leveraging ISACA's latest framework - the COBIT 2019 DevOps Focus Area. Through meticulous research and analysis, this study presents a compelling solution tailor-made for the disruptive financial industry, with the Fintech sector as a shining example. By adopting this framework, FintechCo and its peers in the financial industry can harness the potency of agile-adaptive IT governance and management, fostering a transformative environment that propels their growth and success.

The path to digital transformation in the financial realm is multifaceted, demanding both conventional stability and agile innovation. This research demonstrates that by embracing a balanced approach and leveraging the COBIT 2019 DevOps Focus Area, financial institutions can confidently embark on their digital journey, outpacing competition, and delivering unparalleled customer experiences. The future of the financial industry is

poised for disruption, and the Fintech sector is leading the way with a dynamic, agile, and adaptive vision for growth and progress.

5. CONCLUSION

Throughout this study, we believe have shed light on the challenges and opportunities faced by a leading financial technology organization, FintechCo. As we delve into the implications and potential improvements, it is crucial to acknowledge certain limitations that may restrict the generalization of our findings to other organizations. However, these limitations serve as steppingstones for future research endeavors, aimed at exploring a wider range of financial technology firms, ensuring a more comprehensive understanding of the industry's dynamic landscape.

Drawing from 2019 COBIT DevOps Focus Area framework, we have pinpointed three highest prioritized IT Governance and Management (ITGM) objectives: Managed Security Services (DSS05), Managed Problems (DSS03), and Managed Solution Identification and Build (BAI03). Identifying a total of fifteen gaps within these objectives has granted us unparalleled insight into areas ripe for improvement, thereby fostering digital transformation excellence within FintechCo.

As we reflect on the impact of our research, it is evident that the potential improvements identified have practical implications for FintechCo and the wider financial technology community. By aligning its operations with the recommendations, FintechCo can not only maintain the continuity of its digitalization but also bolster its position in the industry, setting new standards for excellence and innovation. In addition, this study also acts as a guiding light, illuminating the path to success for FintechCo and inspiring other financial technology organizations to embrace transformative change. By staying attuned to the ever-evolving landscape of digitalization and agile IT services, FintechCo can unlock its true potential, leading the industry towards a future brimming with unprecedented possibilities. As we embark on this journey of advancement and innovation, we anticipate that our research will serve as a catalyst, propelling FintechCo and its peers towards a future characterized by ingenuity and resilience growth.

REFERENCES

- [1] J. Johansson, P. Söderholm, V. Parida, C. Kostenius, J. Frishammar, and Å. Ericson, "ADDRESSING SOCIETAL CHALLENGES," p. 3, 2018.
- [2] A. Frenzel-Piasentin, J. C. Muench, M. Bruckner, and D. J. Veit, "Digitization or Digitalization?-Toward an Understanding of Definitions, Use and Application in IS Research Crowdfunding Decision-Making

- View project Sustainably Digital View project,” Americas Conference on Information Systems, 2021, p. 10. [Online]. Available: <https://www.researchgate.net/publication/354402700>
- [3] T. A. Branca, B. Fornai, V. Colla, M. M. Murri, E. Streppa, and A. J. Schröder, “The challenge of digitalization in the steel sector,” *Metals (Basel)*, vol. 10, no. 2, p. 1, Feb. 2020, doi: 10.3390/met10020288.
- [4] T. Niemand, C. Rigtering, A. Kallmünzer, S. Kraus, and S. Matijas, *Association for Information Systems AIS Electronic Library (AISeL) ENTREPRENEURIAL ORIENTATION AND DIGITALIZATION IN THE FINANCIAL SERVICE INDUSTRY: A CONTINGENCY APPROACH*. 2017. [Online]. Available: http://aisel.aisnet.org/ecis2017_rp/70
- [5] S. Vejseli, A. Rossmann, and T. Connolly, “IT Governance and Its Agile Dimensions: Exploratory Research in the Banking Sector,” *Hawaii International Conference on System Science*, p. 1, 2019.
- [6] ISACA, *COBIT Focus Area: DevOps*. [Online]. Available: www.isaca.org
- [7] M. Janssen and H. van der Voort, “Agile and adaptive governance in crisis response: Lessons from the COVID-19 pandemic,” *Int J Inf Manage*, vol. 55, Dec. 2020, doi: 10.1016/j.ijinfomgt.2020.102180.
- [8] S. Vejseli, A. Rossmann, and K. Garidis, “Association for Information Systems Association for Information Systems The Concept of Agility in IT Governance and its Impact on Firm The Concept of Agility in IT Governance and its Impact on Firm Performance Performance,” 2022. [Online]. Available: https://aisel.aisnet.org/ecis2022_rp/98
- [9] S. De Haes, L. Caluwe, T. Huygh, and A. Joshi, “Governing Digital Transformation Guidance for Corporate Board Members,” 2020. [Online]. Available: <http://www.springer.com/series/10101>
- [10] S. De Haes, W. Van Grembergen, A. Joshi, and T. Huygh, “COBIT as a Framework for Enterprise Governance of IT,” in *Management for Professionals*, Springer Nature, 2020, pp. 125–162. doi: 10.1007/978-3-030-25918-1_5.
- [11] R. Mulyana, L. Rusu, and E. Perjons, “IT Governance Mechanisms Influence on Digital Transformation: A Systematic Literature Review A Systematic Literature Review,” Americas’ Conference on Information System (AMCIS), 2021, pp. 1–10. [Online]. Available: <https://aisel.aisnet.org/amcis2021>
- [12] O. Pakhnenko, P. Rubanov, D. Hacar, and V. Yatsenko, “Digitalization of financial services in European countries: Evaluation and comparative analysis,” *Journal of International Studies*, vol. 14, no. 2, pp. 267–282, 2021, doi: 10.14254/2071-8330.2021/14-2/17.
- [13] I. Adhitya and W. Chrismastianto, “ANALISIS SWOT IMPLEMENTASI TEKNOLOGI FINANSIAL TERHADAP KUALITAS LAYANAN PERBANKAN DI INDONESIA,” 2017. [Online]. Available: www.eMarketer.com
- [14] I. Mavlutova, T. Volkova, A. Natrins, A. Spilbergs, I. Arefjevs, and I. Miahkykh, “Financial Sector Transformation in the Era of Digitalization,” *Studies of Applied Economics*, vol. 38, no. 4, p. 2, 2021, doi: 10.25115/eea.v38i3%20(1).4055.
- [15] R. Mulyana, L. Rusu, and E. Perjons, “IT Governance Mechanisms that Influence Digital Transformation: A Delphi Study in Indonesian Banking and Insurance Industry,” Pacific Asia Conference on Information Systems (PACIS), 2022.
- [16] R. Mulyana, L. Rusu, and E. Perjons, “How Hybrid IT Governance Mechanisms Influence Digital Transformation and Organizational Performance in the Banking and Insurance Industry of Indonesia,” Lisbon: Information Systems Development (ISD) Conference, 2023, pp. 1–12.
- [17] N. Obwegeser, T. Yokoi, M. Wade, and T. Voskes, “7 Key Principles to Govern Digital Initiatives,” 2020. [Online]. Available: <https://mitsmr.com/2UWvNEs>
- [18] C. Ebert, G. Gallardo, J. Hernantes, and N. Serrano, “SOFTWARE TECHNOLOGY DevOps.”
- [19] Bank Indonesia, *PERATURAN BANK INDONESIA NO. 18/40/PBI/2016 TENTANG PENYELENGGARAAN PEMROSESAN TRANSAKSI PEMBAYARAN*. 2016.
- [20] Bank Indonesia, *Peraturan Bank Indonesia (PBI) No. 19/12/PBI/2017 tentang Penyelenggaraan Teknologi Finansial*. 2017.
- [21] Otoritas Jasa Keuangan, *Peraturan Otoritas Jasa Keuangan (POJK) Nomor 13/POJK.02/2018 tentang Inovasi Keuangan Digital*. 2018.
- [22] Menteri BUMN, *Peraturan Menteri Badan Usaha Milik Negara (BUMN) Republik Indonesia Nomor Per-2/MBU/03/2023 tentang Pedoman Tata Kelola dan Kegiatan Korporasi Signifikan Badan Usaha Milik*

Negara. 2023.

- [23] P. M. Dewi, R. Fauzi, and R. Mulyana, "Perancangan Tata Kelola Teknologi Informasi Untuk Transformasi Digital Di Industri Perbankan Menggunakan Framework COBIT 2019 Domain Build, Acquire And Implement: Studi Kasus Bank XYZ," 2019.
- [24] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design Science in Information Systems Research," 2004. [Online]. Available: <https://www.jstor.org/stable/25148625>
- [25] A. K. Shenton, "Strategies for ensuring trustworthiness in qualitative research projects," *Education for Information*, vol. 22, no. 2, pp. 63–75, 2004, doi: 10.3233/EFI-2004-22201.
- [26] ISACA, *Implementing and Optimizing an Information and Technology Governance Solution*. 2018. [Online]. Available: <http://linkd.in/ISACAOOfficial>
- [27] Gartner, "Gartner Magic Quadrant & Critical Capabilities," 2023. <https://www.gartner.com/en/research/magic-quadrant> (accessed Jul. 28, 2023).