

Ananda Viamianni

by D H

Submission date: 13-Jul-2023 10:47PM (UTC-0400)

Submission ID: 2130848459

File name: 6366-17059-1-RV.docx (481.42K)

Word count: 6083

Character count: 37783

COBIT 2019 INFORMATION SECURITY FOCUS AREA IMPLEMENTATION FOR REINSURCO DIGITAL TRANSFORMATION Ananda Viamianni¹, Rahmat Mulyana², Fitriyana Dewi³

¹Information Systems, School of Industrial Engineering, Telkom University

²Information Systems, School of Industrial Engineering, Telkom University

³Information Systems, School of Industrial Engineering, Telkom University

Email: ¹anandaviamianni@student.telkomuniversity.ac.id, ²rahmatmulyana@telkomuniversity.ac.id,
³fitriyanadewi@telkomuniversity.ac.id

(Received: dd mmm yyyy, Revised: dd mmm yyyy, Accepted: dd mmm yyyy)

Abstract

As information technology (IT) advancement evolves in Indonesia's insurance sector, organizations like ReinsurCo must accelerate their digital transformation (DT) to remain competitively viable. Although DT paves the way for new business models and operational improvements, the implementation often fails due to poor IT governance. Under the supervision of the State-Owned Enterprises Agency (SOE) and the Financial Services Authority (FSA), ReinsurCo must comply with regulations stating that SOEs must independently assess IT maturity to ensure information security. This research utilizes the five stages of Design Science Research (DSR): problem explication, requirement specification, design and development, demonstration, and evaluation. Data was collected through semi-structured interviews and both internal and external document triangulation. The data were then analyzed using the COBIT 2019 Information Security framework, implementing design factors prioritizing information technology governance and management (ITGM) objectives: APO13 Managed Security, DSS05 Managed Security Services, and BAI06 Managed IT Changes. Further analysis and identification were conducted to discover gaps against the seven component capabilities. These identified gaps were mapped into people, process, and technology aspects, which led to the creation of essential improvement recommendations. These recommendations were compiled into an implementation roadmap that can serve as a priority guide for ReinsurCo. This research is expected to be a reference for practitioners applying the COBIT 2019 Information Security framework in formulating strategic plans to address information security challenges.

Keywords: Digital Transformation, IT Governance, Information Security Management, COBIT 2019 Information Security, ReinsurCo

This is an open access article under the [CC BY](#) license.



*Corresponding Author: Author1

1. INTRODUCTION

In the past few years, the insurance sector in Indonesia has been experiencing rapid information technology (IT) advancements, which are driving insurance companies to adopt IT to enhance efficiency and broaden their service scope. However, this development has caused disruptions in numerous business sectors, forcing incumbent organizations to hasten their digital transformation (DT) to remain competitive [1]. The emergence of digital-born competitors, such as fintech companies, and the COVID-19 pandemic conditions are pressuring insurance companies to expedite DT implementation. DT is a fundamental change process triggered by

adopting innovative digital technologies, accompanied by strategic influences, resources, and core capabilities to radically enhance an entity's value (for example, an organization, business network, industry, or society) [2]. DT can be a crucial factor for incumbent organizations to maintain and increase market share in the face of technological disruption [3]. DT implementation can help organizations introduce more effective and efficient new business models, improve operational aspects, and provide a better and more innovative customer experience [4]. Moreover, DT can also enhance IT capabilities and product or service innovation, providing a competitive advantage in the industry [5].

However, implementing DT is complex, as failures often occur due to poor Information Technology Governance (ITG) [6]. Studies have shown that organizations frequently fail to provide structure and governance for DT projects due to a lack of alignment between business processes and ownership [6]. Therefore, organizations must establish effectiveness and alignment between IT and business by preparing mature ITG mechanisms [7].

ITG is an integral part of corporate governance that discusses definitions and implementation of processes, structures, and relational mechanisms to support business/IT alignment and create business value from business investments into IT [8]. ITG controls the formulation and implementation of IT strategies and ensures an alignment between business and IT conducted by the board, executive management, and IT management [9]. However, there are differences between IT management and ITG [8]. IT management is focused on providing effective IT services and products and managing IT operations [8] by ensuring that governance mechanisms have been implemented and governance guidelines have been correctly followed by the company [10]. On the other hand, ITG plays a crucial role in determining and distributing necessary mechanisms to ensure the organization achieves its IT suitability objectives for the present and future [10]. Despite this, ITG and IT management are interconnected and cannot operate separately. If a company wishes to grow and succeed, it not only needs to manage IT resources but also needs to implement them comprehensively within the company as part of the corporate governance structure [10]. In addition, organizations need to develop IT capabilities that align with digital strategic priorities involving four elements: technology, governance, processes, and talent [5].

ReinsurCo is a public service that operates in the reinsurance sector under the supervision of State-Owned Enterprises (SOE). The SOE Ministry provides guidelines through the Minister of State-Owned Enterprises Regulation (SOE) PER-2/MBU/03/2023 that guide good ITG standards in SOE operations, including the principle of information security. In addition, this regulation outlines the implementation of Good Corporate Governance (GCG) in SOE companies, which includes transparency, accountability, social responsibility, and good business ethics. This regulation aims to enhance the performance and transparency of SOE companies and encourage efficient and effective management to provide more significant benefits to the public and the state. On the other hand, regulation of the Financial Services Authority (FSA) Number 4/POJK.5/20221 added that insurance companies must ensure the security of all Non-Bank Financial Services Institution information, including consumer secrets and personal data, as well as affiliated parties. As a company under the supervision of the SOE and the Financial Services Authority (FSA), ReinsurCo needs to comply with

various regulations that have been given. One of ReinsurCo's efforts in implementing effective ITG is conducting its governance research. ReinsurCo's 2021 annual report shows that its ITG has matured. However, ReinsurCo still runs ITG processes traditionally, and traditional ITG practices are not necessarily effective in guiding DT [11]. The study found that new ITG mechanisms at ReinsurCo only accounted for 9%, while old ITG mechanisms were found to be as much as 91% [12]. Therefore, there is room for improvement, especially in facing DT challenges. This is also driven by Ministerial Regulation Number 21 of 2020 regarding measuring organizational readiness levels in the transformation towards the Indonesia Industry 4.0 Readiness Index (INDI 4.0). In assisting organizations in achieving INDI 4.0, the COBIT 2019 framework can control and maximize the value of information and technology to help organizations optimize their risks, realize potential benefits, and optimize resources [13]. In addition, to effectively implement ITG in an organization, it is necessary to build an ITG framework structure with international standards such as COBIT, ITIL, ISO, and others that can help achieve effective ITG [14]. COBIT 2019, in particular, is a significant driver of IT management in companies to be more responsive, flexible, and support innovation [15]. Therefore, the preparation of information security management is needed to improve ReinsurCo's IT readiness in facing DT.

This research uses the COBIT 2019 Information Security framework and aims to answer the following questions: What are the goals of information security ITGM needed by ReinsurCo? How to compile optimization recommendations for ITGM goals based on gap analysis of the seven components current capability and targets? Moreover, how to design essential optimizations on ITGM goals based on the results of the recommendation compilation? By aligning technology planning and organizational strategy, ReinsurCo can improve its performance and meet growing needs in the insurance industry.

2. RESEARCH METHODOLOGY

This study applies the design science research (DSR) framework in developing information security management for ReinsurCo's transformation. The conceptual model can be seen in Figure 1.

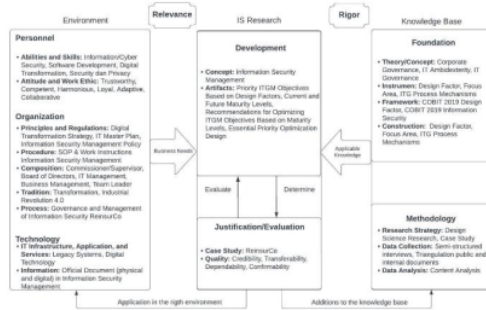


Figure 1 Research Methodology (Adapted from DSR Hevner [16])

The Conceptual Model comprises three parts: the environment, Information System (IS) research, and the knowledge base. These components aid in problem definition, determining relevant factors, and providing connections to facilitate mapping core issues [17]. The research flow used to produce optimization recommendations for ITGM objectives can be seen in Figure 2.

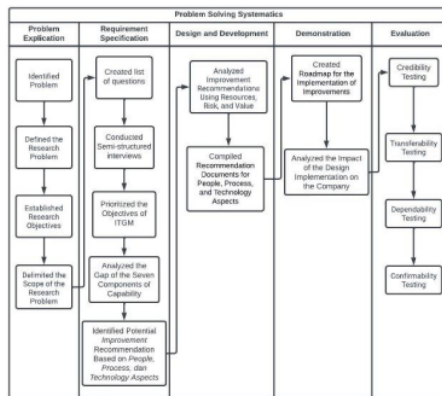


Figure 2 Research Flow

In the initial phase of the research, a problem explication was conducted to identify issues in the case study, establish the focus of the discussion, define objectives, and set limitations for the research process. Subsequently, the second phase entailed a requirement specification. This involved creating a list of questions to be used during semi-structured interviews to determine the goals of ITGM. Following establishing ITGM's goals, seven component capabilities were analyzed using the COBIT 2019 Information Security framework, and the company's gaps were identified to determine potential improvement recommendations categorized into people, process, and technology aspects. The third research phase was design and development, where the researcher analyzed the recommendations using resources, risk, and value to prioritize the implementation of the suggestions. The researcher then compiled improvement

recommendations. The fourth research phase was the demonstration, where an implementation roadmap was developed to identify strategic steps in applying the recommendations. An analysis of the impact of the design implementation on the company followed this. Throughout this research, testing was conducted in the evaluation phase using credibility testing to ensure the results were trustworthy [18], transferability testing was used to confirm the extent to which research results could be applied [18], dependability testing was used as an audit process for the research design strategy [18], and confirmability testing was used to evaluate the research results objectively [18].

2.1 Data Collection

The data for this research was collected using two methods. First, semi-structured interviews to gather verbal data. Second, internal and external document triangulation, where data was collected and analyzed to gain a more comprehensive understanding of the data being processed.

2.2 Data Analysis

The collected data was then analyzed to determine the priority of design factors, focus areas, and ITGM process mechanisms. The priority of these three categories was then calculated to produce the final priority of ITGM objectives. Based on these ITGM objective priorities, an assessment was conducted using the seven components of COBIT 2019 Information Security capabilities: process components, organizational structure components, people, skills and competence components, policy and procedure components, information components, culture, ethics, and behavior components, and services, infrastructure, and application components. The research results were then used to devise potential improvements mapped to people, processes, and technology aspects.

2.3 Evaluation

The results of this research were then evaluated based on justifications/evaluations, including credibility tests, transferability tests, dependability tests, and confirmability tests [18].

3. RESULTS AND DISCUSSION

This research involved data collection and processing of helpful information throughout the study. The data collected can be divided into two types: primary data, which consists of general risks and current internal conditions, and secondary data, which includes the organizational structure, company profile, annual performance reports, company strategic plans, and related regulations.

3.1 Results of ITGM Goals Prioritization

The prioritization of ITGM goals was determined based on the multiplication of priorities of the 40 ITGM goals identified from the design factor analysis [19]. Subsequently, the focus area of information security used the COBIT 2019 Information Security framework, which includes core categories, namely APO13 and DSS05, and relevant categories, which are considered to be related to the ITGM goals with the core categories, even if they do not have a direct relationship with the focus area [20]. In addition, ITG process mechanisms affect DT [21], [22]. The results of the ITGM goals prioritization can be seen in Table 1

Table 1 Analysis Results of ITGM Goal Priorities

ITGM Goals	Design Factor Assessment	Focus Area Assessment	Mechanism Assessment	Final Score
APO13	80	2	5	800
DSS05	75	2	5	750
BAI06	95	1	4	380

3. 2 Results of the Process Component Assessment and Gap Analysis

The results of the process component assessment for the priority ITGM objectives can be seen in Table 2.

Table 2 Assessment Results of Process Component Capabilities

Management Practices	Achievement	Capability Level
APO13 Managed Security		
APO13.01	100 % Fully	2
APO13.02	100 % Fully	3
	100 % Fully	4
APO13.03	100 % Fully	4
	100 % Fully	5
Total Capability Level Achieved		18
Capability Score		3,3
DSS05 Managed Security Services		
DSS05.01	100 % Fully	2
	100 % Fully	3
DSS05.02	100 % Fully	2
	100 % Fully	3
	100 % Fully	4
DSS05.03	89 % Fully	2
	100 % Fully	3
DSS05.04	100 % Fully	2
	83 % Largely	3
	0 % None	4
DSS05.05	100 % Fully	2
	100 % Fully	3
DSS05.06	100 % Fully	2
	100 % Fully	3
DSS05.07	75 % Largely	2
	100 % Fully	3
Total Capability Level Achieved		32
Capability Score		2
BAI06 Managed IT Changes		
BAI06.01	100 % Fully	2
	100 % Fully	3
BAI06.02	100 % Fully	2
	33 % Partially	3
	100 % Fully	4
BAI06.03	100 % Fully	4
BAI06.04	100 % Fully	2
	100 % Fully	3
Total Capability Level Achieved		16

Management Practices	Achievement	Capability Level
Capability Score		1,9

The gap assessment on the process components refers to the strategic planning of ReinsurCo, as stated in the annual report. This report established a minimum maturity value target of score 3, utilizing the COBIT 2019 framework. This aligns with the pre-existing regulations of the Ministry of State-Owned Enterprises, which guide such enterprises to assess IT maturity independently and set a target score of 3 using the COBIT framework [23]. Consequently, the gap findings for the ITGM objective DSS05 amounted to 2 gaps; for the ITGM objective BAI06, there was one gap.

3. 3 Results of the Organizational Structure Component Assessment and Gap Analysis

The results of the organizational structure component assessment for the priority ITGM objectives can be seen in Table 3.

Table 3 Assessment Results of Organizational Structure Component Capabilities

COBIT Organizational Structure	ITGM Objectives	Current Condition
Chief Information Officer	APO13, DSS05, BAI06	IT Director
Chief Technology Officer	APO13	
Chief Information Security Officer	APO13 DSS05	
Enterprise Risk Committee	APO13	Risk Monitoring Committee
Business Process Owners	APO13, DSS05, BAI06	Head of IT Division
Project Management Office	APO13	IT Planning & QA Officer
Program Manager	BAI06	Not available
Project Manager	BAI06	Not available
Head Architect	APO13	Not available
Head Human Resources	DSS05	Head of Human Resources and General Affairs Division
Head Development	APO13, DSS05, BAI06	Head of IT Application & Development Department
Head IT Operations	APO13, DSS05, BAI06	Head of IT Infrastructure & Operation Department
Head IT Administration	APO13	Head of Planning & QA Officer Department
Services Manager	APO13 BAI06	Infrastructure & Operational Officer
Information Security Manager	APO13, DSS05, BAI06	
Business Continuity Manager	BAI06	Business Continuity Management

COBIT Organizational Structure	ITGM Objectives	Current Condition
Privacy Officer	DSS05 BAI06	Legal & Compliance Division

Based on the assessment of the capability of the organizational structure component, it was found that ReinsurCo still needs to map the roles of Program Manager, Project Manager, and Head Architect, indicating three gaps.

3.4 Results of the Information Components Assessment and Gap Analysis

The results of the analysis and evaluation of the information components with the priority of ITGM goals can be seen in Table 4.

Table 4 Assessment Results of Information Component Capabilities

Management Practices	Information Output	Current Condition
APO13 Managed Security		
APO13.01	ISMS Scope Statement IS Policy	MPTI and RJPP documents MPTI and RJPP documents
APO13.02	IS Risk Treatment Plan IS Business Case	Project Charter, MPTI, Development and Implementation Procedure, and Risk Register documents Audit Result Report document
APO13.03	IS Review Reports	Information Security Review Report document
DSS05 Managed Security Services		
DSS05.01	IS Management Reports IS Security Services Catalog	Audit Result Report document IT Services Catalog document
DSS05.02	Connectivity Security Policy Results Of Penetration Test	MPTI and IT Policy documents Penetration Test Report document
DSS05.03	Security Policies for Endpoint Devices	MPTI, SLA, OLA, and Asset List documents
DSS05.04	Results of Reviews of User Accounts Approved User Access Rights	Access Rights Review Results document RACI Chart document
DSS05.05	Access Logs Approved Access Requests	Access Log document RACI Chart document
DSS05.06	Access Privileges Inventory of Sensitive Documents and Devices	User Menu and Admin Menu Comparison document Sensitive Information and Device Inventory document
DSS05.07	Security Incident Tickets Security Incident Characteristics	Incident List document Incident List document

Management Practices	Information Output	Current Condition
	Security Event Logs IS Management Reports	Incident List document Incident List document
BAI06 Managed IT Changes		
BAI06.01	Impact Assessments	Change Management SOP
BAI06.02	Post-Implementation IS Review of Emergency Changes	Not Available
BAI06.03	Updated Change Request Status Reports	Managed Engine documentation
BAI06.04	Change Documentation	Managed Engine documentation

One gap was identified based on the evaluation of information component capabilities: ReinsurCo still needs a document for post-implementation security evaluation of emergency changes.

3.5 Results of the People, Skills, and Competencies Component Assessment and GAP Analysis

The results of the assessment of people, skills, and competencies components in the priority of ITGM objectives can be seen in Table 5.

Table 5 Assessment Results of People, Skills, and Competence Component Capabilities

Skills	Current Condition
APO13 Managed Security	
Information Security	ISO 27001 Training and Certification, installation of anti-malware and anti-virus, access rights restriction, and MAC address checks
Information Security Strategy Development	ISO 27001 Training and Certification, installation of anti-malware and anti-virus, access rights restriction, and MAC address checks
DSS05 Managed Security Services	
Information Security	ISO 27001 Training and Certification, installation of anti-malware and anti-virus, access rights restriction, and MAC address checks
Information Security Management	Activation of anti-malware and anti-virus, access rights restriction, MAC address checks, ISO 27001, penetration training, and certification have been carried out.
Penetration Testing	Regular penetration tests are conducted, and prevention detection technology is used to detect and prevent security incidents. Penetration test results have also been reported regularly.
Security Administration	Documentation of incoming-outgoing data and management of related documents, identification of sensitive data, new access control procedure and policy creation, and related documentation of anti-virus

Skills	Current Condition
	configurations, switch settings, and data center access rights.
BAI06 Managed IT Changes	
Changes Management	Application of ITG training, COBIT 2019 certification, and a helpdesk that handles SDP application and change management.
Changes Support	ITG training, competence dictionary and training plan, COBIT 2019 certification, and a helpdesk that manages the SDP application and change management.

One gap was found based on the assessment results of people, skills, and competencies components. ReinsurCo has not conducted further exploration related to the information security framework to enhance information security.

3.6 Results of the Policy and Procedures Components Assessment and GAP Analysis

The results of the policy and procedure components assessment for priority ITGM objectives can be seen in Table 6.

Table 6 Analysis Results of Policy and Procedure Component Assessment

Policy	Current Condition
APO13 Managed Security	
Information Security and Privacy Policy	ISMS Scope Statement, ISMS Policy, and ISO 27001
DSS05 Managed Security Services	
Information Security Policy	Don't have a policy for secure disposal device to protect information
BAI06 Managed IT Changes	
IT Change Management Policy	Formal Standard Policy and Helpdesk Policy

Based on the policy and procedure components assessment, a single gap was identified: ReinsurCo still needs a policy for securely disposing of devices to protect the information stored on those devices.

3.7 Results of the Culture, Ethics, and Behavior Component Assessment and GAP Analysis

The results of the culture, ethics, and behavior components assessment for the priority ITGM objectives can be seen in Table 7.

Table 7 Assessment Results of Culture, Ethics, and Behavior Components

Key Cultural Elements	Current Conditions
APO13 Managed Security	
Cultivating a culture of security and privacy awareness to encourage desired behavior and the implementation of security and privacy policies in daily practice	There is a comprehensive IT governance and security process initiative implemented using maturity measurements and ISO20000 and ISO27001 standards. Guidelines and management for data and IT security have been approved by the board

Key Cultural Elements	Current Conditions
	of directors and the application of Information Security Management System (ISMS) is socialized through the board of directors' appeal to all employees.
DSS05 Managed Security Services	
Creating a user-awareness culture in maintaining security and privacy practices	There is a comprehensive IT governance and security process initiative implemented using maturity measurements and ISO20000 and ISO27001 standards.
BAI06 Managed IT Changes	
Leaders should promote a culture of continuous improvement in IT solutions and services, considering the impact of technological changes on the company, managing risks and costs, and evaluating benefits and suitability with IT strategies and company objectives	There is socialization and implementation of initiatives related to understanding of comprehensive IT governance and processes.

No gaps were found based on the assessment of the culture, ethics, and behavior components. ReinsurCo has implemented cultures according to the COBIT 2019 reference.

3.8 Results of the Service, Infrastructure, and Application Components Assessment and GAP Analysis

The results of assessing the service, infrastructure, and application components for the priority objectives of ITGM can be seen in Table 8.

Table 8 Assessment Results of Services, Infrastructure, and Applications Components

Service, Infrastructure, and Application	Current Condition
APO13 Managed Security	
Configuration Management Tools	BitLocker Windows System, Firewall, Privileged User, and Fortinet.
Security and Privacy Awareness Services	Cybersecurity Summit 2021 Training, ISO 27001, FireEye, and Traffic Filtering Firewall. ISO 27001 Assessment.
Third-party Security Assessment Services	
DSS05 Managed Security Services	
Directory Services	Single Sign-On (SSO). Fortinet.
Email Filtering Systems	Data Management and IT Security Guidelines.
Identity and Access Management System	Dissemination of Information Security Posters and Articles.
Security Awareness Services	Fortinet.
Security Information and Event Management (SIEM) Tools	Not Available
Security Operations Center (SOC) Services	ISO 27001 Assessment.
Third-Party Security Assessment Services	Fortinet, IT Policies and Procedures.
URL Filtering Systems	
BAI06 Managed IT Changes	

Service, Infrastructure, and Application	Current Condition
IT Change Management Tools	Software Development Plan (SDP), Change Management
Release Management Tools	GIT
Testing Tools and Services	Not Available

Two gaps were identified based on assessing the service, infrastructure, and application components. That is, ReinsurCo still needs SOC services and testing tools and services.

3.9 Potential Improvements

Potential Improvements aim to determine the most suitable improvement strategy for ReinsurCo's current condition based on the gap analysis results of seven component capabilities. These improvements consist of three potential improvement aspects: people, process, and technology.

Table 9 Potential Improvements in People Aspect

Component Capability	Type	Potential Improvement
APO13 Managed Security		
Organizational Structure	Responsibility	Adding the responsibility of Head Architect.
People, Skills, and Competence	Skill & Awareness	Enhancing knowledge, experience, and individual abilities in exploring information security standards and frameworks.
DSS05 Managed Security Services		
Organizational Structure	Responsibility	Adding the responsibility of Program Manager.
	Responsibility	Adding the responsibility of Project Manager.

Potential improvements in the people aspect for the ITGM objectives APO13 Managed Security and BAI06 Managed IT Changes are explained in Table 9.

Table 10 Potential Improvements in Process Aspect

Component Capability	Type	Potential Improvement
DSS05 Managed Security Services		
Process	Policy	Establishing a policy basis related to regular access rights management.
	Policy	Establishing a policy basis related to regular event log reviews.
BAI06 Managed IT Changes		
Process	Procedures	Creating procedures to address emergency changes and maintenance without sacrificing information security.
Information	Record	Creating information documents related to post-implementation

Component Capability	Type	Potential Improvement
Policy and Procedures	Procedures, Policy	information security for emergency changes.
		Creating procedures and adding policies related to the safe disposal of devices.
	Policy	Establishing a policy basis related to regular access rights management.
	Policy	Establishing a policy basis related to regular event log reviews.

Potential improvements in the process aspect for the ITGM objectives DSS05 Managed Security Services and BAI06 Managed IT Changes are explained in Table 10.

Table 11 Potential Improvements in Technology Aspect

Component Capability	Type	Potential Improvement
DSS05 Managed Security Services		
Services, Infrastructure, and Applications	Tools	Provision of SOC services.
BAI06 Managed IT Changes		
Services, Infrastructure, and Applications	Tools	Provision of device testing tools.

Potential improvements in the technology aspect for the ITGM objectives DSS05 Managed Security Services and BAI06 Managed IT Changes are explained in Table 11.

3.10 Roadmap Implementation Based on Resource, Risk, and Value Analysis

The resource, risk, value (RRV) analysis is employed to prioritize implementing potential improvements. This prioritization considers evaluating resources, risks, and value through categorization into low, medium, and high levels. The following are the results of the RRV analysis for 11 potential improvements, as presented in Table 12.

Table 12 Results of the Resource, Risk, and Value Analysis

Potential Improvement	Value	Implementation priority
People Aspect		
Enhancing individuals' knowledge, experience, and ability to explore further applicable standards and frameworks of information security within the company	12	1
Adding responsibilities for the Project Manager	12	2
Adding responsibilities for the Program Manager	9	3
Adding responsibilities for the Head Architect	6	4
Process Aspect		

Potential Improvement	Value	Implementation priority
Creating specific information documents regarding post-implementation information security for emergency changes	12	1
Establishing a foundational policy to be complied with in managing access rights regularly by ReinsurCo	9	2
Establishing a foundational policy to be complied with in conducting regular reviews of event logs concerning potential incidents	9	3
Creating procedures and detailing steps in dealing with emergency changes and maintenance without sacrificing information security	9	4
Creating procedures and adding policies related to secure device disposal	9	5
Technology Aspect		
Determining the right tool following information security regulations for software and application testing tools	12	1
Determining the right tool following information security regulations by providing a SOC service that can be used to monitor, detect, analyze, and respond to real-time security threats	6	2

4. DESIGN AND RECOMMENDATIONS

4.1 People Aspect Recommendations

The design for the people aspect yields recommendations involving additional responsibilities for several parties at ReinsurCo, such as the Head of the IT Division, the Information Technology Planning & Quality Assurance Department, and the Information Technology Application Development Department. Firstly, the Head of the IT Division is responsible for system architecture and application development, which includes designing technical designs, ensuring the fulfilment of functional and non-functional requirements, and supervising software development project execution. Secondly, the Information Technology Planning & Quality Assurance Department holds responsibilities for managing and supervising overall significant IT program development, encompassing planning, organizing, executing, and controlling projects. Thirdly, the Information Technology Application Development Department is responsible for developing IT project plans, covering objectives, schedules, budgets, and required resources. Additionally, recommendations include enhancing individual skills through training and certification of various information security standards and frameworks to protect company assets from vulnerabilities, such as NIST SP 800-5, Certified Information System Security Professional (CISSP), Certified Information Security Manager (CISM), and

CIS Critical Security Control training and certification.

4.2 Process Aspect Recommendations

The design for the process aspect results in two recommendations in the form of Standard Operating Procedure (SOP) documents for emergency changes and information security maintenance. These provide detailed guidelines for identifying emergency changes from incidents for conducting tests and evaluations related to information security and for SOP documents for safely disposing of devices to ensure that no longer used devices cannot be reused or misused. Furthermore, a recommendation design includes a post-implementation information security report for emergency changes, serving as a reporting tool and effectiveness evaluation of the implemented emergency actions. Additionally, there are three policy addition recommendations: periodic access rights monitoring policies, periodic event log monitoring policies, and device disposal policies. Firstly, a periodic access rights monitoring policy aims to detect and prevent unauthorized access, protecting the organization from internal and external security threats. Secondly, the policy of periodic event log monitoring serves to identify potentially risky activities, enabling quick actions in response to potential threats. Thirdly, the policy for device disposal ensures that all sensitive data and information have been correctly erased before disposal to prevent devices from being reused and misused, contributing to the organization's information security.

4.3 Technology Aspect Recommendations

The design for the technology aspect results in recommendations in the form of a proposed tools document detailing the advantages, disadvantages, costs, and system operations that the company can implement. These recommendations are based on the Gartner Magic Quadrant Leaders [24], [25]. In this regard, recommendations for devices in the implementation of SOC services, namely Splunk, and software and application testing tools, namely Synk, are provided. First, as a SOC service, Splunk has advantages such as quickly detecting threats and identifying and assessing information security risks. Furthermore, Splunk is suitable for organizations with large data volumes and offers visualization features that can assist users in understanding information security data. Secondly, Synk, as a software and application testing tool, can test software and applications against potential information security threats by detecting and rectifying information security vulnerabilities. Synk also can integrate with code repositories like GitHub and GitLab, which ReinsurCo has used.

4.4 Implementation Roadmap

The implementation roadmap is designed to guide the execution of the designed recommendations.

Based on the RRV analysis results, the recommendations with the highest scores can be implemented first. The implementation design in Table 13 can be initiated from Q4 (October – December) 2023 up to Q3 (July-September) 2024.

Table 13 Implementation Roadmap

Recommendations	2023		2024	
	Q4	Q1	Q2	Q3
People Aspect				
Conducting training and certification for information security framework	■			
Executing the responsibility of Project Manager in the IT Application Development Department		■		
Executing the responsibility of Program Manager in the IT Planning & Quality Assurance Department			■	
Executing the responsibility of Head Architect in the IT Division				■
Process Aspect				
Implementing post-implementation emergency change information security document	■			
Implementing periodic access rights management policy		■		
Implementing a policy of periodic incident log review			■	
Implementing an SOP for emergency changes and information security maintenance				■
Implementing SOP and policy for device disposal				■
Technology Aspect				
Implementing Synk as a software and application testing tool	■			
Implementing Splunk as a SOC service		■		

4.5 Impact of the Design

From the research conducted, the influence of the design on the proposed recommendations was found for each of the seven component capabilities presented in Table 14. The estimation of the design impact can be used to determine the level of change that occurred when ReinsurCo implemented the recommendations designed in this study.

Table 14 Impact of Design Before and After Improvement

Before Improvement	After Improvement
Process Component	
2,4	3
Organizational Structure Component	
No Program Manager responsibilities	Implementation of Program Manager responsibilities in the Information Technology Application Development Department
No Project Manager responsibilities	Implementation of Project Manager responsibilities in the Information Technology Application Development Department
No Head Architect responsibilities	Implementation of Head Architect responsibilities in the IT Division Head
Information Component	

Before Improvement	After Improvement
No post-implementation security assessment document for emergency changes	Post-Implementation Emergency Change Security Report Document
People, Skills, and Competence Component	
No deeper exploration regarding other information security standards and frameworks	Application of other information security standards and frameworks, such as NIST SP 800-53 training, CISSP, CISM, CIS Critical Security Controls
Policies and Procedures Component	
No policy for regular access rights monitoring	A policy for regular access rights review is in place
No policy for regular event log monitoring	A policy for regular event log review is in place
Services, Infrastructure, and Applications Component	
No SOC services	SOC services such as Splunk are available
No software or application testing tools	Software or application testing tools such as OWASP ZAP are available

5. CONCLUSIONS

In the process of developing an information security management system for the transformation of ReinsurCo using COBIT 2019 Information Security, three priority goals for information security (ITGM) were identified: APO13 Managed Security, DSS05 Managed Security Services, and BAI06 Managed IT Changes. An analysis of the seven components of capability and gap assessment was carried out on these three ITGM goals to derive optimization recommendations which were then mapped into the aspects of people, process, and technology. In terms of the people aspect, the recommendations include additions to the job descriptions for positions such as the Head Architect, Project Manager, and Program Manager to align with the current conditions at ReinsurCo, and the enhancement of individual capabilities through training aimed at expanding knowledge about information security standards and frameworks. Regarding the process aspect, recommendations include implementing standard operating procedures (SOP) to ensure more effective and efficient operations at ReinsurCo, adding policy documents, and documentation of information to facilitate administrative processes. Meanwhile, for the technology aspect, the recommendations involve the documentation of proposed tools that assist the company in detecting, analyzing, and responding to security threats in real-time, as well as software and application testing tools to minimize potential risks. This optimization design for ITGM goals has produced an implementation roadmap and, as a result of the proposed recommendations, an increase in the maturity level of ITGM capabilities of APO13 Managed Security, DSS05 Managed Security Services, and BAI06 Managed IT Changes by 0.6 or 25% from the previous capability level of ReinsurCo. ReinsurCo's capability has increased from 2.4 (before improvements) to 3 (after improvements) on the process components of these three ITGM goals. This

study is expected to serve as a reference for practitioners in designing a company's strategic plan by applying the COBIT 2019 Information Security framework for information security management system design. Additionally, the results of this study are intended to provide ReinsurCo with a reference for reviewing and evaluating company conditions. By considering the essential recommendation results, the company can prepare strategies to face the challenges and changes in the digital era.

6. REFERENCES

- [1] K. S. R. Warner and M. Wäger, "Building dynamic capabilities for digital transformation: An ongoing process of strategic renewal," *Long Range Plann.*, vol. 52, no. 3, pp. 326–349, Jun. 2019, doi: 10.1016/j.lrp.2018.12.001.
- [2] C. Gong and V. Ribiere, "Developing a unified definition of digital transformation," *Technovation*, vol. 102, Apr. 2021, doi: 10.1016/j.technovation.2020.102217.
- [3] V. Gurbaxani and D. Dunkle, "Gearing up for successful digital transformation," *MIS Quarterly Executive*, vol. 18, no. 3, pp. 209–220, 2019, doi: 10.17705/2msqe.00017.
- [4] J. Jewer and N. Van Der Meulen, "Governance of Digital Transformation: A Review of the Literature," 2022, [Online]. Available: <https://hdl.handle.net/10125/80144>
- [5] R. Mulyana, L. Rusu, and E. Perjons, "IT Governance Mechanisms Influence on Digital Transformation: A Systematic Literature Review," in *Proc. 27th Annu. Am. Conf. Inf. Syst.*, Twenty-Seventh Americas' Conference on Information Systems (AMCIS), 2021, pp. 1–10. [Online]. Available: <https://aisel.laisnet.org/amcis2021>
- [6] N. Obwegeser, T. Yokoi, M. Wade, and T. Voskes, "7 Key Principles to Govern Digital Initiatives," 2020. [Online]. Available: <https://mitsmr.com/2UWvNEs>
- [7] S. Vejseli and A. Rossmann, "The Impact of IT Governance on Firm Performance A Literature Review," in *AISeL Electronic Library (AISeL)*, Langkawi, 2017.
- [8] S. De Haes, L. Caluwe, T. Huygh, and A. Joshi, *Governing Digital Transformation*. Springer, 2020, doi: <https://doi.org/10.1007/978-3-030-30267-2>.
- [9] S. De Haes and W. Van Grembergen, "IT Governance and Its Mechanisms," *Information systems control journal*, no. 1, pp. 27–33, 2004.
- [10] R. Pereira and M. M. Da Silva, "Towards an integrated IT governance and IT management framework," in *Proceedings of the 2012 IEEE 16th International Enterprise Distributed Object Computing Conference, EDOC 2012*, 2012, pp. 191–200. doi: 10.1109/EDOC.2012.30.
- [11] N. Robbiyani, R. Mulyana, and L. Abdurrahman, "Pengujian Model Pengaruh Tata Kelola TI Terhadap Transformasi Digital dan Kinerja Asuransi C," *Explore: Jurnal Sistem Informasi dan Telematika*, vol. 13, no. 2, p. 95, Dec. 2022, doi: 10.36448/jsit.v13i2.2712.
- [12] F. A. Pahrevi, R. Mulyana, L. Ramadani, and J. S. Informasi, "Analisis Pengaruh Tata Kelola TI terhadap Transformasi Digital dan Kinerja Asuransi C," *Jurnal Sistem Informasi dan Telematika (Telekomunikasi, Multimedia dan Informatika)*, vol. 13, 2022.
- [13] S. F. Bayastura, S. Krisdina, and A. P. Widodo, "Analisis Dan Perancangan Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 2019 Pada PT.XYZ," *JIKO (Jurnal Informatika dan Komputer)*, vol. 4, 2021, doi: 10.33387/jiko.
- [14] P. M. Dewi, R. Fauzi, and R. Mulyana, "Perancangan Tata Kelola Teknologi Informasi Untuk Transformasi Digital Di Industri Perbankan Menggunakan Framework COBIT 2019 Dengan Domain Build, Acquire and Implement: Studi Kasus Bank XYZ," *e-Proceeding of Engineering*, vol. 8, no. 5, p. 9672, 2021.
- [15] ISACA, *COBIT 2019 Framework: Introduction and Methodology*. USA, 2018.
- [16] 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>
- [17] A. Hevner and S. Chatterjee, *Design Research in Information Systems*, vol. 22. in Integrated Series in Information Systems, vol. 22. Boston, MA: Springer US, 2010, doi: 10.1007/978-1-4419-5653-8.
- [18] 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.
- [19] ISACA, *Designing and Information and Technology Governance Solution*. 2018.
- [20] ISACA, *COBIT Focus Area: Information Security*. 2020. [Online]. Available: www.isaca.org
- [21] 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 *Information Systems Development (ISD) Conference*, Lisbon: Association for Information Systems (AIS), 2023.
- [22] 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)*, no. AI-IS-ASIA, pp. 1–16, Jun. 2022.
- [23] Kementerian Badan Usaha Milik Negara, *Peraturan Menteri Badan Usaha Milik Negara tentang Panduan Penyusunan Pengelolaan Teknologi Informasi Badan Usaha Milik Negara*. Indonesia: jdih.bumngoi.d: 4 hlm., 2013.
- [24] A. K. Kavanagh, T. Bussa, and G. Sadowski, "Magic Quadrant for Security Information and Event Management," Feb. 2020. [Online]. Available: <https://www.gartner.com/doc/reprints?id=1-1YEDHXVD&ct=200219&st=sb>
- [25] M. Horvath, D. Gardner, Bhat Manjunath, R. Chugh, and A. Zhao, "Magic Quadrant for Application Security Testing," May 2023.

Ananda Viamianni

ORIGINALITY REPORT

4%

SIMILARITY INDEX

3%

INTERNET SOURCES

1%

PUBLICATIONS

1%

STUDENT PAPERS

PRIMARY SOURCES

1	netmarket.oss.aliyuncs.com Internet Source	1%
2	ejournal.unkhair.ac.id Internet Source	1%
3	Submitted to Universitas Brawijaya Student Paper	1%
4	investor.jasamarga.com Internet Source	1%

Exclude quotes On

Exclude bibliography On

Exclude matches < 1%

Ananda Viamianni

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10
