Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)
Volume 4, Number 10, 2025, DOI 10.58471/esaprom.v4i10
ESSN 2828-9463 (Online)
https://ejournal.seaninstitute.or.id/index.php/esaprom

Evaluation of IT Governance With a Focus on Business Application Continuity Using the Cobit 2019 Framework : A Case Study in XYZ Group

Bagus Firmansyah[1], Heru Purnomo Ipung[2], Mohammad A Soetomo[3]
Master Of Information Technology, Faculty Of Engineering And Information Technology, Swiss German University

Article Info
Keywords:
IT Governance, COBIT 2019, Business Application Continuity, Capability Assessment.

ABSTRACT
This study aims to evaluate the current state of IT governance at XYZ Group, identify capability gaps against best practices, and propose an improved governance model based on the COBIT 2019 framework. A mixed-method approach was applied, combining qualitative interviews with IT stakeholders and quantitative capability assessments across key governance objectives, including EDM03 (Ensured Risk Optimization), APO12 (Managed Risk), APO13 (Managed Security), BAI10 (Managed Configuration), DSS04 (Managed Continuity), and DSS05 (Managed Security Services). The capability assessment revealed that governance all process areas are at a capability level 2 Partially Achieved and lowest with EDM03 scoring 11.1%, indicating the process is not yet achieved according to COBIT 2019 standards. To validate the proposed governance framework, a validation was conducted involving both academic and industry experts. The results confirmed that the framework is relevant, feasible, and strategically aligned with XYZ Group's IT goals. This research contributes a tailored governance solution focused on strengthening business application continuity, offering a practical reference for mid-sized organizations navigating similar challenges.

Corresponding Author:
Bagus Firmansyah
Master Of Information Technology, Faculty Of Engineering And Information Technology, Swiss German University

INTRODUCTION

In the current era of rapid digital disruption, organizations are increasingly reliant on business applications to support operational continuity, decision-making, and customer engagement. However, many enterprises, especially those with organically grown IT portfolios, face significant challenges in maintaining these applications continuity and ensuring they remain adaptable to future demands. This thesis, aims to address these challenges through a comprehensive framework integrating governance and design application architecture.

The importance of this research stems from the growing complexity of IT systems and the necessity to maintain business agility while minimizing technical debt and operational risk. According to Gartner (2023), over 70% of digital transformation initiatives fail to achieve business value due to poor application lifecycle governance. This is further supported by Al-Faifi et al. (2022), who emphasize that long-term continuity in application portfolios requires integrated planning across IT governance.

Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)
Volume 4, Number 10, 2025, DOI 10.58471/esaprom.v4i10
ESSN 2828-9463 (Online)
https://ejournal.seaninstitute.or.id/index.php/esaprom

The need for this thesis is especially evident in organizations like the XYZ Group, which has accumulated a diverse set of business applications over the years. These include core applications vital to business processes (e.g., ERP, CRM) and non-core applications that support internal functions such as HR, procurement, and administration. Without centralized planning and continuous governance.

A real-world example highlighting the urgency of this issue occurred in 2022, when XYZ's sales platform experienced prolonged downtime due to database scalability issues. This incident not only affected revenue but also undermined customer trust. Analysis revealed the absence of formal governance and monitoring mechanisms confirming the need for a business application continuity.

XYZ Group is an institution that oversees various strategic business units in the education, healthcare, and employment solutions sectors. With a wide scope of units and close to 9,000 employees, XYZ plays an important role as a value chain supporter of AHEMCE (Astra Heavy Equipment, Mining, Construction, and Energy). In the midst of rapid business growth, XYZ faces challenges in maintaining the continuity of enterprise application systems that support various business processes across units.

As the reliance on digital information systems increases, the need for a system that is always available, can continue to run in conditions of disruption (continuity), and is customer-oriented is becoming increasingly crucial. System failures or IT service disconnections have a direct impact on services, human resource management, and operations run by XYZ Group.

In Astra's work culture known as *the 8 Astra Behavioral Values*, Customer Focus is an important pillar that requires all group entities, including XYZ, to always prioritize customer satisfaction. In the context of enterprise applications, this means that the system must be able to support services that are fast, precise, and responsive to the needs of both internal and external users. In line with that, in the 2023 yearbook of PT United Tractors Tbk, the Company stated that the Company continues to develop and maximize digitalization and digital-based innovation to improve service quality and provide more value for customers, increase work effectiveness and productivity, and create other business opportunities("Annual Report-United-Tractors-2023-Final.pdf," n.d.).

The determining factor for this thesis is the strategic vision of XYZ Group to scale its operations digitally across Indonesia. To support this vision, the organization requires a future-proof application strategy that ensures agility. Therefore, this research seeks to design an framework based on COBIT 2019 for governance. By addressing the intersection of these frameworks within the context of XYZ Group, the study contributes both theoretically and practically to the development of a more effective and adaptable IT strategy for mid-sized enterprises.

The increase in XYZ Group's business causes the need for Business Applications to support operations to also increase, this can be seen by the many application developments carried out, along with that, the risk of continuity and dependence on IT systems becomes critical, for that it is necessary to have a control that ensures that the risks that arise can be anticipated using existing standards/practices. So that IT continues to be present not only to develop business applications but also to think about how to maintain system continuity to

Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)
Volume 4, Number 10, 2025, DOI 10.58471/esaprom.v4i10
ESSN 2828-9463 (Online)
https://ejournal.seaninstitute.or.id/index.php/esaprom

support the XYZ Group's business. This study aims to Identify the extent to which IT risk management practices have been implemented. Find gaps between current conditions and best practices. It is the basis for planning for improving IT governance more effectively.

RESEARCH METHODS

This research explain research method using COBIT 2019 to create a structured approach.

Framework Overview

This research is based on the concept of Enterprise Governance of IT (EGI&T) which emphasizes the importance of alignment between business strategy and the use of information technology. EGI&T was chosen because it can provide clear direction in managing risk, ensuring continuity of application services, and maintaining information security at XYZ Group.

As the main framework, this study uses COBIT 2019. Through the *Goal Cascade* mechanism, stakeholder needs are translated into Enterprise Goals (EG), then downgraded to Alignment Goals (AG), and finally produce six main Governance and Management Objectives (GAMO): EDM03, APO12, APO13, BAI10, DSS04, and DSS05.

Each GAMO is further elaborated into practices and activities **as** defined by COBIT 2019. This is the basis for evaluating in three stages:

1. Capability Assessment – assesses the extent to which practices/activities have been implemented in XYZ.
2. Gap Analysis – compares the current condition with the target condition.
3. Design Improvement Roadmap – compiles the improvement stages towards *Fully Achieved conditions*.

Thus, this research framework is not only theoretical, but also applicable, because it connects the needs of stakeholders with concrete actions that organizations need to take to improve application governance.

Problem Identification

The research begins by identifying core challenges related to the continuity and alignment of business applications, This step leverages internal documentation reviews and uncover pain points . These findings are also visualized in the fishbone (Ishikawa) diagram in Chapter 1.

Observation & Interview

The interview was conducted by asking questions to explore various information about the problems and needs of IT management in the XYZ Group and to collect data directly by observing the activities.

Standard Benchmark

This phase observed practices against a chosen standard, Map each observed activity/process to the relevant COBIT governance objectives (e.g., EDM/other governance objectives) and identify required practices/controls (GAMO).

Proposed Framework Chapter 2 / Governance Layer

This layer try to align application especially with goals Benchmarked using COBIT 2019.

Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)
Volume 4, Number 10, 2025, DOI 10.58471/esaprom.v4i10
ESSN 2828-9463 (Online)
https://ejournal.seaninstitute.or.id/index.php/esaprom

This research uses Enterprise Governance of IT (EGIT) based on the COBIT 2019 framework. The results *of the Goal Cascade* in Chapter 2, page 29 until 32, have set six Governance and Management Objectives (GAMO) as the main scope, namely: EDM03 (Ensured Risk Optimization), APO12 (Managed Risk), APO13 (Managed Security), BAI10 (Managed Configuration), DSS04 (Managed Continuity), and DSS05 (Managed Security Services).

Each GAMO is then analyzed in more detail through practices and activities as defined in COBIT 2019. This is done to ensure that research not only stops at an objective level, but also assesses the real actions that the organization must take to achieve the desired level of capability.

EDM03 – Ensured Risk Optimization

1. Key practices: Establish risk tolerance, directing risk management activities, ensure ongoing evaluation of IT risks
2. Key activities: Risk appetite documentation, reporting to management, and compliance monitoring.

APO12 – Managed Risk

1. Key practices: IT risk identification, business impact analysis, risk monitoring.
2. Key activities: creating a risk register, conducting periodic risk assessments.

APO13 – Managed Security

1. Key practices: security policy management, access control, awareness & training.
2. Key activities: creating app security policies, access audits, awareness campaigns.

BAI10 – Managed Configuration

1. Key practices: application & infrastructure configuration management, baseline controls.
2. Key activities: CMDB updates, change reviews, configuration validation.

DSS04 – Managed Continuity

1. Main practices: service continuity plan, DRP/BCP trials, evaluation of test results.
2. Key activities: creating BCPs, simulating disaster recovery, updating procedures.

DSS05 – Managed Security Services

1. Key practices: day-to-day security operations, incident monitoring, incident response.
2. Key activities: application log monitoring, incident analysis, attack reporting.

By detailing the practices and activities in each GAMO, this study has a structured evaluation basis for:

1. Capability Assessment → assess the extent to which this practice/activity has been carried out at XYZ.
2. Gap Analysis → compare current conditions with expected targets.

The Improvement Roadmap → outline gradual improvement steps towards *Fully Achieved*.

Evaluation

Capability Assesment

To assess the quality, effectiveness, and completeness of the proposed continuity application governance framework based on best practices and academic standards. To ensure consistency, the following indicators are used:

Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)
Volume 4, Number 10, 2025, DOI 10.58471/esaprom.v4i10
ESSN 2828-9463 (Online)
https://ejournal.seaninstitute.or.id/index.php/esaprom

1. Assessed based on six COBIT 2019 governance objectives
2. Evaluation criteria include clarity of roles, policy alignment, and governance process capability.

Each dimension is scored using The Guttman scale assesses each activity of the components of the governance and management process. If the activity has been performed, then it is granted a score of 1 if otherwise, it is granted a score of 0 (Nachrowi et al., 2020). filled by domain experts and internal IT stakeholders company within XYZ Group. The Purpose is to Quantify capability level of each process.

Data Collection

These indicators were assessed using:

1. Interviews and questionnaires with IT managers, application owners, and risk management staff at XYZ Group.
2. Document review of IT governance policies, application continuity plans, and incident reports.

Gap Analysis

A gap analysis is performed by comparing the current state (from the benchmarks) with the desired future state defined by best practices.

This analysis enables clear identification of areas needing improvement.

Validation

The final stage of this research methodology focuses on evaluating the effectiveness and validating the feasibility of the proposed governance. This ensures that the design not only aligns with best practices but also fits the organizational context of XYZ Group.

a. Document Review

After the evaluation of the proposed design is completed in the previous stage, the final stage of this research is validation. Which one to verify whether the proposed framework is relevant, feasible, and applicable within XYZ Group context.

b. FGD
   1. With academic and industry experts
   2. Experts evaluate the clarity and strategic fit of the framework
   3. Iterative refinement based on expert

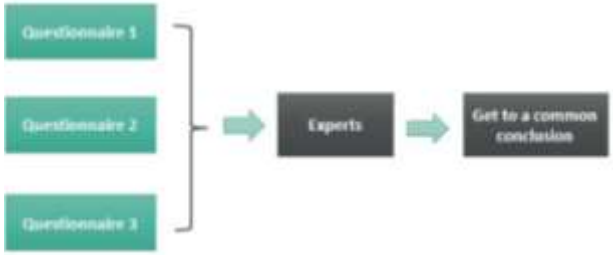


Figure 3. 1 Validation Process

The validation method uses a five-point Likert scale which assesses the aspects of feasibility, clarity, and relevance framework (Lamm et al., 2020). This method was chosen because it is simple and can measure respondents' perceptions quantitatively. However, it should be noted that the use of the Likert scale has the potential for bias, specifically polarity

Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)
Volume 4, Number 10, 2025, DOI 10.58471/esaprom.v4i10
ESSN 2828-9463 (Online)
https://ejournal.seaninstitute.or.id/index.php/esaprom

(answers tend to be extreme on the side of strongly agree or strongly disagree). Therefore, the validation results will be interpreted carefully and complemented by a qualitative analysis of the respondents' comments. The validation is conducted using a combination of document review and Focus Group Discussion (FGD) to obtain structured and iterative feedback from experts in IT governance, both from academic and industry backgrounds.

Design Improvement

Based on the gap findings, an improvement design recommendation is proposed. The improvement base on after validation form expert review.

RESULT and DISCUSSION

Introduction

This chapter presents the findings based on the problem identification stage, where a fishbone (Ishikawa) diagram was developed to analyze the root causes contributing to the Business Application Continuity in XYZ Group. Form the basis for experimentation, gap identification, and framework improvement through the application of COBIT. As mentioned in chapter 1, IT governance is needed to be able to support organizational growth and meet stakeholder expectations. This governance must be able to guarantee that every application used.

Conclude the Governance System Design

The conclusion of the governance system design is derived from the mapping of COBIT 2019 Governance and Management Objectives relevant to the research scope. This section outlines the identified sub-processes, associated activities, and their assessed capability levels. Each sub-process is evaluated based on its role in ensuring effective governance and risk optimization, providing a clear overview of the organization's current governance posture and areas for improvement.

1. EDM03 Ensured risk optimization

Safeguard the organization so that IT-related risks remain within its defined risk appetite and tolerance, while their effect on enterprise value is recognized and controlled, and the likelihood of compliance breaches is reduced.

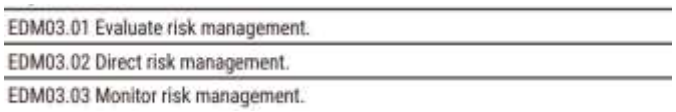


Figure 4. 1 Derived Practice EDM03

2. PO12 Managed risk

Embed IT risk governance into the enterprise-wide risk management process, ensuring that the management efforts achieve an optimal balance between associated costs and expected benefits.

Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)
Volume 4, Number 10, 2025, DOI 10.58471/esaprom.v4i10
ESSN 2828-9463 (Online)
https://ejournal.seaninstitute.or.id/index.php/esaprom

APO12.01 Collect data.
APO12.02 Analyze risk.
APO12.03 Maintain a risk profile.
APO12.04 Articulate risk.
APO12.05 Define a risk management action portfolio.
APO12.06 Respond to risk.

Figure 4. 2 Derived Practice APO12

3. APO13 Managed security

Ensure that both the frequency and consequences of information security incidents remain within the organization's defined risk appetite.

APO13.01 Establish and maintain an information security management system (ISMS).
APO13.02 Define and manage an information security and privacy risk treatment plan.
APO13.03 Monitor and review the information security management system (ISMS).

Figure 4. 3 Derived Practice APO13

4. BAI10 Managed configuration

Ensure that adequate details on service assets are available to support effective service management, while also evaluating the consequences of modifications and addressing service-related incidents.

BAI10.01 Establish and maintain a configuration model.
BAI10.02 Establish and maintain a configuration repository and baseline.
BAI10.03 Maintain and control configuration items.
BAI10.04 Produce status and configuration reports.
BAI10.05 Verify and review integrity of the configuration repository.

Figure 4. 4 Derived Practice BAI10

5. DSS04 Managed continuity

In the face of significant disturbances (such as threats, opportunities, or sudden demands), the enterprise must be able to adapt quickly, maintain operational continuity, and preserve the availability of resources and information within tolerable limits.

DSS04.01 Define the business continuity policy, objectives and scope.
DSS04.02 Maintain business resilience.
DSS04.03 Develop and implement a business continuity response.
DSS04.04 Exercise, test and review the business continuity plan (BCP) and disaster response plan (DRP).
DSS04.05 Review, maintain and improve the continuity plans.
DSS04.06 Conduct continuity plan training.
DSS04.07 Manage backup arrangements.
DSS04.08 Conduct post-resumption review.

Figure 4. 5 Derived Practice DSS04

6. DSS05 Managed security services

Reduce the adverse effects of information security weaknesses and incidents on business operations.

Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)
Volume 4, Number 10, 2025, DOI 10.58471/esaprom.v4i10
ESSN 2828-9463 (Online)
https://ejournal.seaninstitute.or.id/index.php/esaprom

DSS05.01 Protect against malicious software.
DSS05.02 Manage network and connectivity security.
DSS05.03 Manage endpoint security.
DSS05.04 Manage user identity and logical access.
DSS05.05 Manage physical access to I&T assets.
DSS05.06 Manage sensitive documents and output devices.
DSS05.07 Manage vulnerabilities and monitor the infrastructure for security-related events.

Figure 4. 6 Derived Practice DSS05

Evaluation

1. Capability Assesment

Measurement questionnaires that have been prepared previously distributed to the target respondents who have been determined based on the mapping of the RACI table. After being given time, the questionnaires were collected against for analysis. The calculated results from this questionnaire will be used to assess the capability level.

a. Here is a table image of the RACI Chart of the control objectives EDM03 Ensured risk optimization.

B. Component: Organizational Structures								
Key Governance Practice	Board	Executive Committee	Chief Executive Officer	Chief Risk Officer	Chief Information Officer	I&T Governance Board	Enterprise Risk Committee	Chief Information Security Officer
EDM03.01 Evaluate risk management.	A	R	R	R	R	R	R	
EDM03.02 Direct risk management.	A	R	R	R	R	R	R	
EDM03.03 Monitor risk management.	A	R	R	R	R	R	R	R
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**							
COSO Enterprise Risk Management, June 2017	6. Governance and Culture—Principle							
King IV Report on Corporate Governance for South Africa, 2016	Part 2: Fundamental concepts—Definition of corporate governance							

Figure 4. 7 RACI for EDM03

Based on the RACI for EDM03 table, the following is a description of the selection of respondents in XYZ Group:

Table 4. 1 Functional EDM03 RACI

No	Functional Cobit Structure	Functional XYZ Structure
1	Board	VP Fuction Group (Represent of Ketua XYZ)
2	Executive Committee	VP Function Group
3	Chief Executive Officer	VP Function Group
4	Chief Risk Officer	Head of Internal Control & Risk Management
5	Chief Information Officer	Head of IT System & Infrastructure
6	I&T Governance Board	Head of Internal Control & Risk Management
7	Enterprise Risk Committee	Head of Internal Control & Risk Management
8	Chief Information Security Officer	Head of Internal Control & Risk Management

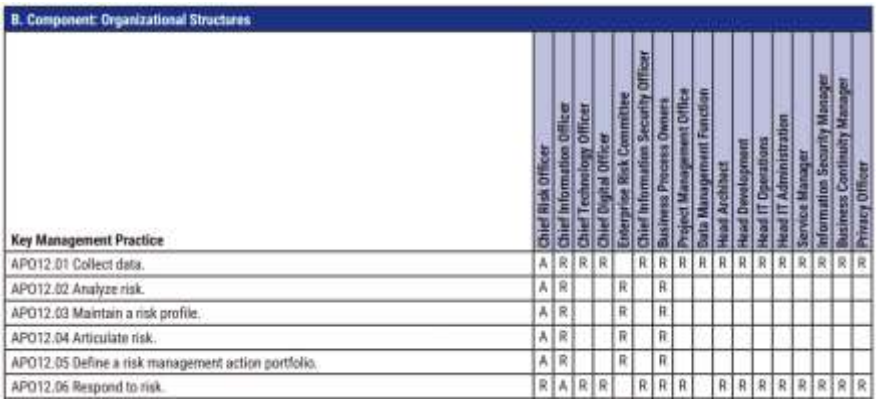
From the RACI Chart conversion table above, the respondents were as follows:

Table 4. 2 Respondent EDM03

No	Responden	Jumlah
1	VP Function Group	1
2	Head of Internal Control & Risk Management	1
3	Head of IT System & Infrastructure	1
	Total	4

b. Here is a table image of the RACI Chart of the control objectives APO12 Managed risk.

Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)
Volume 4, Number 10, 2025, DOI 10.58471/esaprom.v4i10
ESSN 2828-9463 (Online)
https://ejournal.seaninstitute.or.id/index.php/esaprom



B. Component: Organizational Structures Key Management Practice	Chief Risk Officer	Chief Information Officer	Chief Technology Officer	Chief Digital Officer	Enterprise Risk Committee	Chief Information Security Officer	Business Process Owners	Project Management Office	Data Management Function	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
APO12.01 Collect data.	A	R	R	R		R	R	R	R	R	R	R	R	R	R	R	R
APO12.02 Analyze risk.	A	R			R		R										
APO12.03 Maintain a risk profile.	A	R			R		R										
APO12.04 Articulate risk.	A	R			R		R										
APO12.05 Define a risk management action portfolio.	A	R			R		R										
APO12.06 Respond to risk.	R	A	R	R		R	R	R		R	R	R	R	R	R	R	R

Figure 4. 8 RACI for APO12

Based on the RACI for APO12 table, the following is a description of the selection of respondents in XYZ Group:

Table 4. 3 Functional APO12 RACI

No	Functional Cobit Structure	Functional XYZ Structure
1	Chief Risk Officer	Head of Internal Control & Risk Management
2	Chief Information Officer	Head of IT System & Infrastructure
3	Chief Technology Officer	Head of IT System & Infrastructure
4	Chief Digital Officer	Head of IT System & Infrastructure
5	Enterprise Risk Committee	Head of IT System & Infrastructure
6	Chief Information Security Officer	Head of Internal Control & Risk Management
7	Business Process Owners	VP Function Group
8	Project Management Office	Head of IT System & Infrastructure
9	Data Management Function	Head of IT System & Infrastructure
10	Head Architect	Head of IT System & Infrastructure
11	Head Development	Head of IT System & Infrastructure
12	Head IT Operations	Head of IT System & Infrastructure
13	Head IT Administration	Head of IT System & Infrastructure
14	Service Manager	Head of IT System & Infrastructure
15	Information Security Manager	Head of IT System & Infrastructure
16	Business Continuity Manager	Head of Internal Control & Risk Management

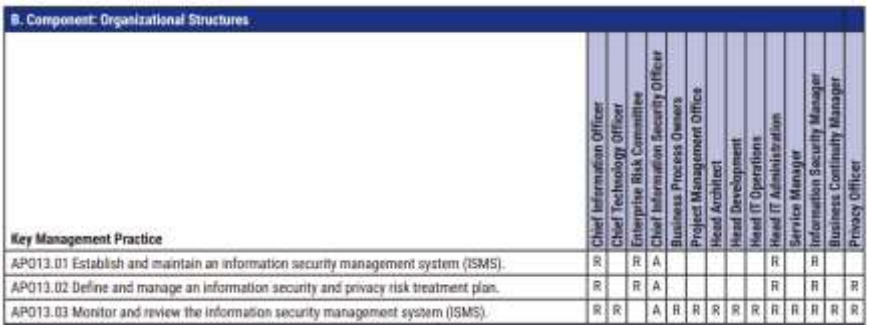
From the RACI Chart conversion table above, the respondents were as follows:

Table 4. 4 Respondent APO12

No	Responden	Jumlah
1	VP Function Group	1
2	Head of Internal Control & Risk Management	1
3	Head of IT System & Infrastructure	1
	Total	3

c. Here is a table image of the RACI Chart of the control objectives APO13 Managed security.

Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)
Volume 4, Number 10, 2025, DOI 10.58471/esaprom.v4i10
ESSN 2828-9463 (Online)
https://ejournal.seaninstitute.or.id/index.php/esaprom



B. Component: Organizational Structures	Chief Information Officer	Chief Technology Officer	Enterprise Risk Committee	Chief Information Security Officer	Business Process Owners	Project Management Office	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
Key Management Practice														
APO13.01 Establish and maintain an information security management system (ISMS).	R		R	A						R		R		
APO13.02 Define and manage an information security and privacy risk treatment plan.	R		R	A						R		R		R
APO13.03 Monitor and review the information security management system (ISMS).	R	R		A	R	R	R	R	R	R	R	R	R	R

Figure 4. 9 RACI for APO13

Based on the RACI for APO13 table, the following is a description of the selection of respondents in XYZ Group:

Table 4. 5 Functional APO13 RACI

No	Functional Cobit Structure	Functional XYZ Structure
1	Chief Information Officer	Head of IT System & Infrastructure
2	Chief Technology Officer	Head of IT System & Infrastructure
3	Enterprise Risk Committee	Head of Internal Control & Risk Management
4	Chief Information Security Officer	Head of Internal Control & Risk Management
5	Business Process Owners	VP Function Group
6	Project Management Office	VP Function Group
7	Head Architect	Head of IT System & Infrastructure
8	Head Development	Head of IT System & Infrastructure
9	Head IT Operations	Head of IT System & Infrastructure
10	Head IT Administration	Head of IT System & Infrastructure
11	Service Manager	Head of IT System & Infrastructure
12	Information Security Manager	Head of Internal Control & Risk Management
13	Business Continuity Manager	Head of Internal Control & Risk Management
14	Privacy Officer	Head of Internal Control & Risk Management
15	Chief Information Officer	Head of IT System & Infrastructure
16	Business Continuity Manager	Head of Internal Control & Risk Management
17	Privacy Officer	Head of Internal Control & Risk Management

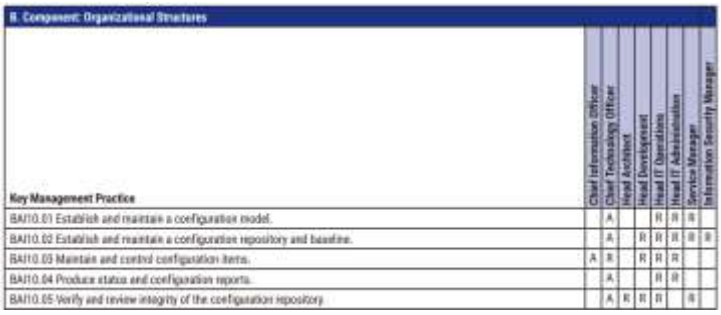
From the RACI Chart conversion table above, the respondents were as follows:

Table 4. 6 Respondent APO13

No	Responden	Jumlah
1	VP Function Group	1
2	Head of Internal Control & Risk Management	1
3	Head of IT System & Infrastructure	1
	Total	3

d. Here is a table image of the RACI Chart of the control objectives BAI10 Managed configuration.

Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)
Volume 4, Number 10, 2025, DOI 10.58471/esaprom.v4i10
ESSN 2828-9463 (Online)
https://ejournal.seaninstitute.or.id/index.php/esaprom



B. Component: Organizational Structures									
Key Management Practice	Chief Information Officer	Chief Technology Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	
BAI10.01 Establish and maintain a configuration model.		A			R	R	R		
BAI10.02 Establish and maintain a configuration repository and baseline.		A		R	R	R	R	R	
BAI10.03 Maintain and control configuration items.	A	R		R	R	R			
BAI10.04 Produce status and configuration reports.		A			R	R			
BAI10.05 Verify and review integrity of the configuration repository.		A	R	R	R		R		

Figure 4. 10 RACI for BAI10

Based on the RACI for BAI10 table, the following is a description of the selection of respondents in XYZ Group:

Table 4. 7 Functional for BAI10

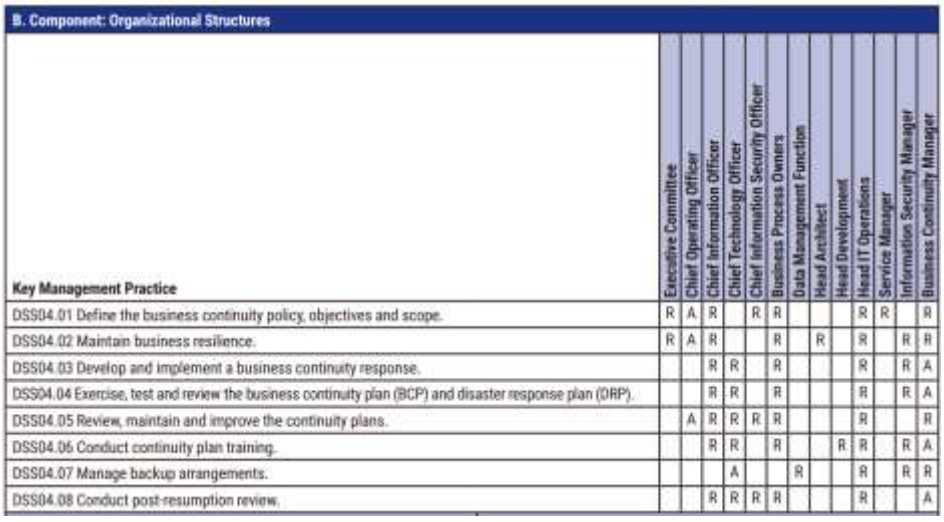
No	Functional Cobit Structure	Functional XYZ Structure
1	Chief Information Officer	Head of IT System & Infrastructure
2	Chief Technology Officer	Head of IT System & Infrastructure
3	Head Architect	Head of IT System & Infrastructure
4	Head Development	Head of IT System & Infrastructure
5	Head IT Operations	Head of IT System & Infrastructure
6	Head IT Administration	Head of IT System & Infrastructure
7	Service Manager	Head of IT System & Infrastructure
8	Information Security Manager	Head of Internal Control & Risk Management

From the RACI Chart conversion table above, the respondents were as follows:

Table 4. 8 Respondent BAI10

No	Responden	Jumlah
1	Head of Internal Control & Risk Management	1
2	Head of IT System & Infrastructure	1
	Total	2

e. Here is a table image of the RACI Chart of the control objectives DSS04 Managed continuity.



B. Component: Organizational Structures															
Key Management Practice	Executive Committee	Chief Operating Officer	Chief Information Officer	Chief Technology Officer	Chief Information Security Officer	Business Process Owners	Data Management Function	Head Architect	Head Development	Head IT Operations	Service Manager	Information Security Manager	Business Continuity Manager		
DSS04.01 Define the business continuity policy, objectives and scope.	R	A	R		R	R				R	R		R		
DSS04.02 Maintain business resilience.	R	A	R			R		R		R		R	R		
DSS04.03 Develop and implement a business continuity response.			R	R		R				R		R	A		
DSS04.04 Exercise, test and review the business continuity plan (BCP) and disaster response plan (DRP).			R	R		R				R		R	A		
DSS04.05 Review, maintain and improve the continuity plans.		A	R	R	R	R				R			R		
DSS04.06 Conduct continuity plan training.			R	R		R			R	R		R	A		
DSS04.07 Manage backup arrangements.				A			R			R		R	R		
DSS04.08 Conduct post-resumption review.			R	R	R	R				R			A		

Figure 4. 11 RACI for DSS04

Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)
Volume 4, Number 10, 2025, DOI 10.58471/esaprom.v4i10
ESSN 2828-9463 (Online)
https://ejournal.seaninstitute.or.id/index.php/esaprom

Based on the RACI for DSS04 table, the following is a description of the selection of respondents in XYZ Group:

Table 4. 9 Functional DSS04

No	Functional Cobit Structure	Functional XYZ Structure
1	Executive Committee	VP Function Group (Represent of Ketua XYZ)
2	Chief Operating Officer	VP Function Group
3	Chief Information Officer	Head of IT System & Infrastructure
4	Chief Technology Officer	Head of IT System & Infrastructure
5	Chief Information Security Officer	Head of Internal Control & Risk Management
6	Business Process Owners	VP Function Group
7	Data Management Function	Head of IT System & Infrastructure
8	Head Architect	Head of IT System & Infrastructure
9	Head Development	Head of IT System & Infrastructure
10	Head IT Operations	Head of IT System & Infrastructure
11	Service Manager	Head of IT System & Infrastructure
12	Information Security Manager	Head of Internal Control & Risk Management
13	Business Continuity Manager	Head of Internal Control & Risk Management

From the RACI Chart conversion table above, the respondents were as follows:

Table 4. 10 Respondent DSS04

No	Responden	Jumlah
1	VP Function Group	1
2	Head of Internal Control & Risk Management	1
3	Head of IT System & Infrastructure	1
	Total	3

f. Here is a table image of the RACI Chart of the control objectives DSS05 Managed security services.

B. Component: Organizational Structures									
Key Management Practice	Chief Information Officer	Chief Information Security Officer	Business Process Owners	Head Human Resources	Head Development	Head IT Operations	Information Security Manager	Privacy Officer
DSS05.01 Protect against malicious software.		A	R	R	R	R	R	
DSS05.02 Manage network and connectivity security.		A			R	R	R	
DSS05.03 Manage endpoint security.		A			R	R	R	
DSS05.04 Manage user identity and logical access.		A	R			R	R	R
DSS05.05 Manage physical access to I&T assets.		A				R	R	R
DSS05.06 Manage sensitive documents and output devices.	A					R		R
DSS05.07 Manage vulnerabilities and monitor the infrastructure for security-related events.		A				R	R	R

Figure 4. 12 RACI for DSS05

Based on the RACI for DSS05 table, the following is a description of the selection of respondents in XYZ Group:

Table 4. 11 Functional DSS05

No	Functional Cobit Structure	Functional XYZ Structure
1	Chief Information Officer	Head of IT System & Infrastructure
2	Chief Information Security Officer	Head of Internal Control & Risk Management
3	Business Process Owners	VP Function Group
4	Head Human Resources	Head of IT System & Infrastructure
5	Head Development	Head of Internal Control & Risk Management

Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)
Volume 4, Number 10, 2025, DOI 10.58471/esaprom.v4i10
ESSN 2828-9463 (Online)
https://ejournal.seaninstitute.or.id/index.php/esaprom

6	Head IT Operations	VP Function Group
7	Information Security Manager	Head of IT System & Infrastructure
8	Privacy Officer	Head of IT System & Infrastructure

From the RACI Chart conversion table above, the respondents were as follows:

Table 4. 12 Respondent DSS05

No	Responden	Jumlah
1	VP Function Group	1
2	Head of Internal Control & Risk Management	1
3	Head of IT System & Infrastructure	1
	Total	3

2. Analysis activity of Capability Levels

Capability level analysis is an evaluation of the extent to which the company has met the standards of good IT management. However, the purpose of this assessment is not only to measure how well a company is managing IT, but also to raise awareness of the importance of improving IT management as well as identifying priorities in efforts to improve IT capabilities. The level of capability in question is a representation of the maturity of the IT process in the company, which is measured quantitatively using values or numbers. The determination of the level of capability in each IT process will be carried out by paying attention to the scale that has been determined, starting from level 1 (one) to level 5 (five). The guide used in determining this level is the COBIT 2019 guidebook which contains the Governance and Management Objective. Using this guide, it is hoped that it can help determine the appropriate level of capability for each IT activity carried out in the company. In Cobit 2019, the Capability Assessment starts from Level 2. Because according to the information at level 1 (Perform) means that every company must have carried out an objective process but there is no structure in managing it.

Table 4. 13 Capability Level Cobit 2019

Level	Name	Process Attribut ID	Keterangan
0	Incomplete		The process is not implemented or fails to achieve its purpose. There is no recognizable outcome.
1	Performed	PA 1.1 - Process Performance	The process is executed and achieves its process purpose, but there is no structured approach to manage it.
2	Managed	PA 2.1 – Performance Management PA 2.2 – Work Product Management	The process is planned, monitored, and adjusted. Work products are appropriately established, controlled, and maintained.
3	Established	PA 3.1 – Process Definition PA 3.2 – Process Deployment	The process follows a defined and standardized method that is documented, communicated, and improved over time.
4	Predictable	PA 4.1 – Process Measurement PA 4.2 – Process Control	The process operates within defined limits to achieve its outcomes. Performance is measured and controlled with quantitative techniques.
5	Optimizing	PA 5.1 Process Innovation PA 5.2 – Process Optimization	The process is continuously improved based on quantitative feedback and from learning and innovation.

In analyzing the activity, the questionnaire is divided into several stages according to the level of ability that has been identified through the rating of the activity process. The assessment of these activities was carried out by referring to 144 standards that have been

Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)
Volume 4, Number 10, 2025, DOI 10.58471/esaprom.v4i10
ESSN 2828-9463 (Online)
https://ejournal.seaninstitute.or.id/index.php/esaprom

set, namely COBIT 2019. After filling out the questionnaire, the activities that have reached the maximum level of capability can be further analyzed to determine the next level of capability that the company will achieve. This aims to find out the extent to which the company has met the standards of good IT management, as well as to identify priorities in efforts to improve IT capabilities. Thus, the level of the company's activity capabilities can be identified more clearly. The following is a rating of process activities in determining capability levels.

Table 4. 14 Rating Process Capability

Skala	Keterangan	Pencapaian (%)
N	*Not Achieved*	0% – 14%
P	*Partially Achieved*	15% – 49%
L	*Largely Achieved*	50% – 84%
F	*Fully Achieved*	85% – 100%

If all attributes on a level get:

1. A score of F, then the process is considered to have reached that level and can be evaluated for the next level.
2. A score of P or L, then the process has not met that level and is stated to have only reached the previous level.

The management and calculation of questionnaire data to determine the level of ability of each activity was carried out using the Guttman Scale formula (Nachrowi et al., 2020). This formula is used to calculate and process the data obtained from the questionnaire that has been filled out by the respondents. By using this formula, it is hoped that it can help determine the level of activity ability more accurately. The formula is as follows:

$$CC = \frac{\Sigma CLa}{\Sigma Po} \; x \; 100\%$$

Description

CC : Achievement value of governance and management capability level

∑CLa : The total amount of governance and management value

∑Po : The total number of governance and management activities

In practice, COBIT assessment is based on, work product:

1. It is supporting evidence that the activity was carried out (Process Attribut 2.2: Performed).
2. If it's not available, then the activity is arguably not actually done — meaning that level 1 can't be fully reached.

Ideally, the availability of work products and the validation of capability results are interrelated.

Capability Level Calculation

Capability Calculation EDM03 Level 2

a. EDM03 (Respondent 1)

The calculation of the capability level process in the EDM03 objective process at XYZ Group is evaluated in stages, or starting from the capability level that has been determined in the COBIT 2019 Framework module. The following are the results of the calculation of

Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)
Volume 4, Number 10, 2025, DOI 10.58471/esaprom.v4i10
ESSN 2828-9463 (Online)
https://ejournal.seaninstitute.or.id/index.php/esaprom

questionnaire data that has been distributed in the form of the Guttman Scale value of each respondent.

The recapitulation of the results of the calculation of Level 2 questionnaire data by respondent 1 which was distributed to the Board of XYZ represented by the VP Function Group can be seen in the table below:

Table 4. 15 Results and Data Processing of Capability Questionnaire EDM03 Respondent 1

EDM03 – Ensured Risk Optimization					
Level	Process	Activity	Yes	No	Score
2	EDM03.01	1	-	V	0
		2	-	V	0
		3	-	V	0
		4	-	V	0
	EDM03.02	1	-	V	0
		2	-	V	0
		3	-	V	0
		4	-	V	0
	EDM03.03	1	V	-	1
		Total			1
		Capability Level			11,1%

The results of capability level 2 EDM03 in respondent 1 are as follows:

$$CC = \frac{\Sigma CLa}{\Sigma Po} \; x \; 100\%$$

$\boldsymbol{CC}$ = 1/9 × $\mathbf{100}$%

$\boldsymbol{CC}$ = 11,1%

Based on the results of the calculation of questionnaire data from respondent 1, it was found that the capability at level 2 EDM03 had a capability level value of 11,1%.

b. EDM03 (Responden 2)

Table 4. 16 Results and Data Processing of Capability Questionnaire EDM03 Respondent 2

EDM03 – Ensured Risk Optimization					
Level	Process	Activity	Yes	No	Score
2	EDM03.01	1	-	V	0
		2	-	V	0
		3	-	V	0
		4	-	V	0
	EDM03.02	1	-	V	0
		2	-	V	0
		3	-	V	0
		4	-	V	0
	EDM03.03	1	V	-	1
		Total			1
		Capability Level			11,1%

The results of capability level 2 EDM03 in respondent 2 are as follows:

$$CC = \frac{\Sigma CLa}{\Sigma Po} \; x \; 100\%$$

$\boldsymbol{CC}$ = 1/9 × $\mathbf{100}$%

$\boldsymbol{CC}$ = 11,1%

Based on the results of the calculation of questionnaire data from respondent 2, it was found that the capability at level 2 EDM03 had a capability level value of 11,1%.

Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)
Volume 4, Number 10, 2025, DOI 10.58471/esaprom.v4i10
ESSN 2828-9463 (Online)
https://ejournal.seaninstitute.or.id/index.php/esaprom

c. EDM03 (Responden 3)

Table 4. 17 Results and Data Processing of Capability Questionnaire EDM03 Respondent 3

EDM03 – Ensured Risk Optimization					
Level	Process	Activity	Yes	No	Score
2	EDM03.01	1	-	V	0
		2	-	V	0
		3	-	V	0
		4	-	V	0
	EDM03.02	1	-	V	0
		2	-	V	0
		3	-	V	0
		4	-	V	0
	EDM03.03	1	V	-	1
		Total			0
		Capability Level			11,1%

The results of EDM03 capability level 2 in respondent 3 are as follows:

$$CC = \frac{\Sigma CLa}{\Sigma Po} \; x \; 100\%$$

$\boldsymbol{CC}$ = 1/9 × $\mathbf{100}$%

$\boldsymbol{CC}$ = 11,1%

Based on the results of the calculation of questionnaire data from respondent 3, it was found that the capability at level 2 EDM03 had a capability level value of 11.1%.

Capability Calculation Recap - EDM03

Based on the results of the evaluation of questionnaire data from each respondent consisting of 3 (Three) respondents, the recapitulation and results of EDM03 capability level 2 are as follows:

Table 4. 18 EDM03 Capability Calculation Recap

Evaluation ID	: EVA-1
Objective	: EDM03 – Ensured Risk Optimization
Evaluation Date	: Juli, 25 2025
Capability Level	: 2
Information	: Not Achieved

Process	Responden	Number of Activity Values	Total Activity	Capability Value
EDM03	R1	1	9	11,1%
	R2	1	9	11,1%
	R3	1	9	11,1%
Total		3	27	33,3%
Capability Level Objective Results				11,1%

EDM03 Level 2 Objective Capability Results

$CLi = R1 + R2 + R3 \,/\, \sum R$

CLi = 11,1% + 11,1% + 11,1% / 3

CLi = 33,3%/3

CLi = 11,1%

Based on the results of the calculation above, it shows that the objective process: EDM03 – Ensured Risk Optimization on Capability has a capability level of 11.1%. This shows that the company's capability level is in the category of Not Achieved level (0-15%), Thus, it can be concluded that the capability level objective process EDM03 is at level 2, and not continued to level 3.

Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)
Volume 4, Number 10, 2025, DOI 10.58471/esaprom.v4i10
ESSN 2828-9463 (Online)
https://ejournal.seaninstitute.or.id/index.php/esaprom

Work of Product EDM03 - Ensured Risk Optimization

The following are the results of the work (Work of Product) for the EDM03 Ensured Risk Optimization process objectives which have been adjusted to the output of COBIT 2019 at XYZ Group:

Table 4. 19 Work of Product EDM03

Work of Product				
EDM03	Output	Exist	Proof	%
EDM03.01 Evaluate risk management	Risk appetite guidance	-	-	0%
	Evaluation of risk management activities	V	Document Top Risk & Operasional Risk XYZ. in Appendix A	100%
	Approved risk tolerance levels	-	-	0%
EDM03.02 Direct risk management	Approved process for measuring risk management	-	-	0%
	Key objectives to be monitored for risk management	V	Document Top Risk & Operasional Risk XYZ. in Appendix A	100%
	Risk management policies	-	-	0%
EDM03.03 Monitor risk management	Remedial actions to address risk management deviations	V	Document Top Risk & Operasional Risk XYZ. in Appendix A	100%
	Risk management issues for the board	-	-	0%
	Summary			300%
	Normalize			37,5%

It can be seen from the table above, there are 8 outputs or document evidence provided by COBIT 2019, for the EDM03 process objective has an average evidence value of 37,5%, which means that EDM03 is at the Partially Achieved level (15% – 49%) and there are 3 from 8 outputs that are not available in the XYZ Group.

APO124.3.3.2 Capability Calculation APO12 Level 2

1. APO12 (Responden 1)

The calculation of the capability level process in the APO12 objective process at XYZ Group is evaluated in stages, or starting from the capability level that has been determined in the COBIT 2019 Framework: Governance and Management Objective module. The following are the results of the calculation of questionnaire data that has been distributed in the form of the Guttman Scale value of each respondent.

The recapitulation of the results of the questionnaire data calculation by respondent 1 which was distributed to the VP Function Group can be seen in the table below:

Table 4. 20 Results and Data Processing of Capability Questionnaire APO12 Respondent 1

APO12 – Managed Risk					
Level	Process	Activity	Yes	No	Score
2	APO12.01	1	-	V	0
		2	-	V	0
	APO12.03	1	-	V	0
		2	-	V	0
		3	-	V	0
	APO12.05	1	V	-	1
		Total			1
		Capability Level			16,6%

Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)
Volume 4, Number 10, 2025, DOI 10.58471/esaprom.v4i10
ESSN 2828-9463 (Online)
https://ejournal.seaninstitute.or.id/index.php/esaprom

The results of the Level 2 APO12 capability in respondent 1 are as follows:

$$CC = \frac{\Sigma CLa}{\Sigma Po} \; x \; 100\%$$

CC = 1/6 × 100%

CC = 16.6%

Based on the results of the calculation of questionnaire data from respondent 1, it was found that the capability at level 2 of APO12 had a capability level value of 16.6%.

2. APO12 (Respondent 2)

The recapitulation of the results of the questionnaire data calculation by respondent 2 which was distributed to the Head of Internal Control & Risk Management can be seen in the table below:

Table 4. 21 Results and Data Processing of Capability Questionnaire APO12 Respondent 2

APO12 – Managed Risk					
Level	Process	Activity	Yes	No	Score
2	APO12.01	1	-	V	0
		2	-	V	0
	APO12.03	1	-	V	0
		2	-	V	0
		3	-	V	0
	APO12.05	1	V	-	1
		Total			1
		Capability Level			16,6%

The results of the Level 2 APO12 capability in respondent 2 are as follows:

$$CC = \frac{\Sigma CLa}{\Sigma Po} \; x \; 100\%$$

$\boldsymbol{CC}$ = 1/6 × $\mathbf{100}$%

$\boldsymbol{CC}$ = 16,6%

Based on the results of the calculation of questionnaire data from respondent 2, it was found that the capability at level 2 of APO12 had a capability level value of 16.6%.

3. APO12 (Respondent 3)

The recapitulation of the results of the questionnaire data calculation by respondent 3 which was distributed to the Head of IT System & Infrastructure can be seen in the table below:

Table 4. 22 Results and Data Processing of Capability Questionnaire APO12 Respondent 3

APO12 – Managed Risk					
Level	Process	Activity	Yes	No	Score
2	APO12.01	1	-	V	0
		2	-	V	0
	APO12.03	1	-	V	0
		2	-	V	0
		3	-	V	0
	APO12.05	1	V	-	1
		Total			1
		Capability Level			16,6%

The results of the Level 2 APO12 capability in respondent 3 are as follows:

$$CC = \frac{\Sigma CLa}{\Sigma Po} \; x \; 100\%$$

Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)
Volume 4, Number 10, 2025, DOI 10.58471/esaprom.v4i10
ESSN 2828-9463 (Online)
https://ejournal.seaninstitute.or.id/index.php/esaprom

CC = 1/6 × **100**%
CC = 16,6%

Based on the results of the calculation of questionnaire data from respondent 3, it was found that the capability at level 2 of APO12 had a capability level value of 16.6%.

Capability Calculation Recap – APO12

Based on the results of the evaluation of questionnaire data from each respondent consisting of 3 (Three) respondents, the recapitulation and results of capability level 2 APO12 are as follows:

Table 4. 23 Capability Calculation Recap APO12

Evaluation ID : EVA-2
Objective : APO12 – Managed Risk
Evaluation Date : Juli, 25 2025
Capability Level : 2
Information : Partially Achieved

Proses	Responden	Number of Activity Values	Total Activity	Capability Value
APO12	R1	1	6	16,6%
	R2	1	6	16,6%
	R3	1	6	16,6%
Total		3	20	49.8%
Result Capability Level Objective				16,6%

Result Capability Objective APO12
CLi = R1 + R2 + R3 / ∑R
CLi = 16.6% + 16.6% + 16.6% / 3 x 100%
CLi = 49.8 / 3 x 100%
CLi = 16.6%

Based on the calculation results above, it shows that the objective process: APO12 – Managed Risk in Capability has a capability level of 16.6%. This shows that the company's capability level is in the category of Partially Achieved level (15% - 49%), Thus, it can be concluded that the capability level objective process APO12 is at level 2, and is not continued to level 3.

Work of Product APO12 – Managed Risk

The following are the work results (Work of Product) for the EDM03 Ensured Risk Optimization process objectives which have been adjusted to the output of COBIT 2019 at XYZ Group:

Table 4. 24 Work of Product APO12

APO12	Work of Product Output	Exist	Proof	%
APO12.01 Collect data	Emerging risk issues and factors	V	Document Top Risk & Operasional Risk XYZ. in Appendix A	100%
	Data on risk events and contributing factors	V	Document Top Risk & Operasional Risk XYZ. in Appendix A	100%
	Data on the operating environment relating to risk	-	-	0%
APO12.02 Analyze risk	Risk analysis results	-	-	0%
	Risk analysis results	-	-	0%

Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)
Volume 4, Number 10, 2025, DOI 10.58471/esaprom.v4i10
ESSN 2828-9463 (Online)
https://ejournal.seaninstitute.or.id/index.php/esaprom

APO12	Work of Product Output	Exist	Proof	%
	Scope of risk analysis efforts	-	-	0%
APO12.03 Maintain a risk profile	Aggregated risk profile, including status of risk management actions	-	-	0%
	Documented risk scenarios by line of business and function	-	-	0%
APO12.04 Articulate risk	Risk analysis and risk profile reports for stakeholders	-	-	0%
	Results of third-party risk assessments	-	-	0%
	Opportunities for acceptance of greater risk	-	-	0%
APO12.05 Define a risk management action portfolio	Project proposals for reducing risk	-	-	0%
	Risk impact communication	-	-	0%
APO12.06 Respond to risk	Risk-related root causes	-	-	0%
	Risk-related incident response plans	-	-	0%
	Summary			200%
	Normalize			13%

It can be seen from the table above, there are 15 outputs or document evidence provided by COBIT 2019, for the APO12 process objective has an average evidence value of 13,3%, which means that APO12 is at the Not Achieved level (0% – 14%) and there are 13 from 15 outputs that are not available in the XYZ Group.

Capability Calculation APO13 Level 2

A. APO13 (Responden 1)

The calculation of the capability level process in the APO13 objective process at XYZ Group is evaluated in stages, or starting from the capability level that has been determined in the COBIT 2019 Framework: Governance and Management Objective module. The following are the results of the calculation of questionnaire data that have been distributed in the form of Guttman Scale values from each respondent.

Table 4. 25 Results and Data Processing of Capability Questionnaire APO13 Respondent 1

APO13 – Manage Security					
Level	Process	Activity	Yes	No	Score
1	APO13.01	1	V	-	1
		2	V	-	1
		3	V	-	1
		4	V	-	1
		5	V	-	1
		6	V	-	1
		7	V	-	1
		Total			7
		Capability Level			100%

The result of the Level 2 capability of APO13 in respondent 1 is with the following formula:

$$CC = \frac{\Sigma CLa}{\Sigma Po} \; x \; 100\%$$

$\boldsymbol{CC}$ = 7/7 × $\mathbf{100}$%

$\boldsymbol{CC}$ = $\mathbf{100}$%

Based on the results of the questionnaire data calculation from respondent 1, it was found that the capability at level 2 of APO13 has a capability level value of 100%.

Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)
Volume 4, Number 10, 2025, DOI 10.58471/esaprom.v4i10
ESSN 2828-9463 (Online)
https://ejournal.seaninstitute.or.id/index.php/esaprom

B. APO13 (Responden 2)

The calculation of the capability level process in the APO13 objective process at XYZ Group is evaluated in stages, or starting from the capability level that has been determined in the COBIT 2019 Framework: Governance and Management Objective module. The following are the results of the calculation of questionnaire data that have been distributed in the form of Guttman Scale values from each respondent.

Table 4. 26 Results and Data Processing of Capability Questionnaire APO13 Respondent 2

APO13 – Manage Security					
Level	Process	Activity	Yes	No	Score
		1	-	V	0
		2	-	V	0
		3	-	V	0
	APO13.01	4	-	V	0
1		5	-	V	0
		6	-	V	0
		7	-	V	0
		Total			0
		Capability Level			0%

The result of the Level 2 capability of APO13 in respondent 2 is with the following formula:

$$CC = \frac{\Sigma CLa}{\Sigma Po} \; x \; 100\%$$

$\boldsymbol{CC}$ = 0/7 × **100**%

$\boldsymbol{CC}$ = 0%

Based on the results of the questionnaire data calculation from respondent 2, it was found that the capability in APO13 had a capability level value of 0%.

C. APO13 (Responden 3)

The calculation of the capability level process in the APO13 objective process at XYZ Group is evaluated in stages, or starting from the capability level that has been determined in the COBIT 2019 Framework: Governance and Management Objective module. The following are the results of the calculation of questionnaire data that have been distributed in the form of Guttman Scale values from each respondent.

Table 4. 27 Results and Data Processing of Capability Questionnaire APO13 Respondent 3

APO13 – Manage Security					
Level	Process	Activity	Yes	No	Score
		1	-	V	0
		2	-	V	0
		3	-	V	0
	APO13.01	4	-	V	0
1		5	-	V	0
		6	V	-	1
		7	-	V	0
	Total				1
	Capability Level				14,2%

The result of capability level 2 APO13 in respondent 3 is with the following formula:

$$CC = \frac{\Sigma CLa}{\Sigma Po} \; x \; 100\%$$

$\boldsymbol{CC}$ = 1/7 × **100**%

Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)
Volume 4, Number 10, 2025, DOI 10.58471/esaprom.v4i10
ESSN 2828-9463 (Online)
https://ejournal.seaninstitute.or.id/index.php/esaprom

CC = 14,2%

Based on the results of the questionnaire data calculation from respondent 3, it was found that the capability at level 1 of APO13 had a capability level value of 14,2%.

Capability Calculation Recap – APO13

Based on the results of the evaluation of questionnaire data from each respondent consisting of 3 (Three) respondents, the recapitulation and Result capability of APO13 are as follows:

Table 4. 28 Capability Calculation Recap APO13

Evaluation ID	: EVA-3			
Objective	: APO13 – Manage Security			
Evaluation Date	: Juli, 25 2025			
Capability Level	: 2			
Information	: Partially Achieved			
Proses	Responden	Number of Activity Values	Total Activity	Capability Value
APO13	R1	0	7	0%
	R2	7	7	100%
	R3	1	7	14,2%
Total		8	21	114,2%
Result Capability Level Objective				38%

Result Capability Objective APO13

CLi = R1 + R2 + R3 / ∑R

CLi = 0% + 100% + 14.3% + / 3 x 100%

CLi = 114.2% / 3 x 100%

CLi = 38%

Based on the calculation results above, it shows that the objective process: APO13 – Manage Security on Capability has a capability level of 38%. This shows that the company's capability level is in the category of Partially Achieved level (15% - 49%), Thus, it can be concluded that the capability level objective process APO13 is at level 2, and not continued to level 3.

Work of Product APO13 – Managed Security

The following are the Work of Product results for the APO13 Managed Security process objectives that have been adjusted to the output of COBIT 2019 at XYZ Group:

Table 4. 29 Work of Product APO13

APO13	Work of Product Output	Exist	Proof	%
APO13.01 Establish and maintain an information security management system (ISMS)	ISMS scope statement	V	Pedoman Keamanan. in Appendix B	100%
	ISMS policy	V	Pedoman Keamanan. in Appendix B	100%
APO13.02 Define and manage an information security risk treatment plan	Information security risk treatment plan	-	-	0%
	Information security business cases	-	-	0%
APO13.03 Monitor and review the information security management system (ISMS).	Recommendations for improving the information security	V	Internal Control Self Assesment. in Appendix C	100%

Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)
Volume 4, Number 10, 2025, DOI 10.58471/esaprom.v4i10
ESSN 2828-9463 (Online)
https://ejournal.seaninstitute.or.id/index.php/esaprom

APO13	Work of Product Output	Exist	Proof	%
	management system (ISMS)			
	Information security management system (ISMS) audit reports	V	Surat Hasil Cross Audit ICCA XYZ. in Appendix D	100%
	Summary			400%
	Normalize			67%

It can be seen from the table above, there are 6 outputs or document evidence provided by COBIT 2019, for the APO13 process objective has an average evidence value of 67%, which means that APO13 is at the Largely Achieved level (50% – 84%) and there are 2 from 6 outputs that are not available in the XYZ Group.

Capability Calculation BAI10 Level 2

A. BAI10 (Responden 1)

The calculation of the capability level process in the BAI10 objective process at XYZ Group is evaluated in stages, or starting from the capability level that has been determined in the COBIT 2019 Framework: Governance and Management Objective module. The following are the results of the calculation of questionnaire data that have been distributed in the form of Guttman Scale values from each respondent.

Table 4. 30 Results and Data Processing of Capability Questionnaire BAI10

BAI10 – Managed Configuration					
Level	Process	Activity	Yes	No	Score
	BAI10.02	1	-	V	0
		1	-	V	0
	BAI10.03	2	-	V	0
2		3	-	V	0
	BAI10.04	1	-	V	0
		Total			0
		Capability Level			0%

The result of the Level 2 BAI10 capability in respondent 1 is with the following formula:

$$CC = \frac{\Sigma CLa}{\Sigma Po} \; x \; 100\%$$

CC = 0/5 × 100%

CC = 0%

Based on the results of the questionnaire data calculation from respondent 1, it was found that the capability in BAI10 had a capability level value of 0%.

A. BAI10 (Responden 2)

The calculation of the capability level process in the BAI10 objective process at XYZ Group is evaluated in stages, or starting from the capability level that has been determined in the COBIT 2019 Framework: Governance and Management Objective module. The following are the results of the calculation of questionnaire data that have been distributed in the form of Guttman Scale values from each respondent.

Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)
Volume 4, Number 10, 2025, DOI 10.58471/esaprom.v4i10
ESSN 2828-9463 (Online)
https://ejournal.seaninstitute.or.id/index.php/esaprom

Table 4. 31 Results and Data Processing of Capability Questionnaire BAI10

BAI10 – Managed Configuration					
Level	Process	Activity	Yes	No	Score
	BAI10.02	1	-	V	0
		1	-	V	0
	BAI10.03	2	-	V	0
2		3	-	V	0
	BAI10.04	1	-	V	0
		Total			0
		Capability Level			0%

The result of capability level 2 BAI10 in respondent 2 is with the following formula:

$$CC = \frac{\Sigma CLa}{\Sigma Po} \; x \; 100\%$$

$\boldsymbol{CC}$ = 0/5 × **100**%

$\boldsymbol{CC}$ = **0**%

Based on the results of the questionnaire data calculation from respondent 2, it was found that the capability at level 2 BAI10 had a capability level value of 0%.

Capability Calculation Recap – BAI10

Based on the results of the evaluation of questionnaire data from each respondent consisting of 2 (Two) respondents, the recapitulation and Result capability of BAI10 are as follows:

Table 4. 32 Capability Calculation Recap BAI10

Evaluation ID	: EVA-4
Objective	: BAI10 – Managed Configuration
Evaluation Date	: Juli, 25 2025
Capability Level	: 2
Information	: Not Achieved

Proses	Responden	Number of Activity Values	Total Activity	Capability Value
BAI10	R1	0	5	0%
	R2	0	5	0%
Total		0	10	0%
Result Capability Level Objective				0%

Result Capability Level 2 BAI10

CLi = R1 + R2 / σr

CLi = 0% + 0% / 2 x 100%

CLi = 0/2 x 100%

CLi = 0%

Based on the calculation results above, it shows that the objective process: BAI10 – Manage Configuration at Capability Level 2 has a capability level of 0%. This shows that the company's capability level is in the category of Not Achieved level (0-15%), Thus, it can be concluded that the capability level objective process BAI10 at level 2 was not achieved, and was not continued to level 3.

Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)
Volume 4, Number 10, 2025, DOI 10.58471/esaprom.v4i10
ESSN 2828-9463 (Online)
https://ejournal.seaninstitute.or.id/index.php/esaprom

Work of Product BAI10 – Managed Configuration

The following are the work results (Work of Product) for the objectives of the BAI10 Managed Configuration process which has been adjusted to the output of COBIT 2019 at XYZ Group:

Table 4. 33 Work of Product BAI10

BAI10	Work of Product Output	Exist	Proof	%
BAI10.01 Establish and maintain a configuration model	Logical configuration model	-	-	0%
	Scope of configuration management model	-	-	0%
BAI10.02 Establish and maintain a configuration repository and baseline	Configuration baseline	V	SOP Pengembangan Aplikasi. in Appendix E	100%
	Configuration repository	-	-	0%
BAI10.03 Maintain and control configuration items	Approved changes to baseline	-	-	0%
	Updated repository with CIs	-	-	0%
BAI10.04 Produce status and configuration reports	Configuration status reports	-	-	0%
BAI10.05 Verify and review integrity of the configuration repository	Results of repository completeness reviews	-	-	0%
	Results of physical verification of CIs	-	-	0%
	License deviations	-	-	0%
	Summary			100%
	Normalize			10%

It can be seen from the table above, there are 10 outputs or document evidence provided by COBIT 2019, for the BAI10 process objective has an average evidence value of 10%, which means that BAI10 is at the Not Achieved level (0% – 14%) and there are 9 from 10 outputs that are not available in the XYZ Group.

Capability Calculation DSS04 Level 2

A. DSS04 (Responden 1)

The calculation of the capability level process in the DSS04 objective process at XYZ Group is evaluated in stages, or starting from the capability level that has been determined in the COBIT 2019 Framework: Governance and Management Objective module. The following are the results of the calculation of questionnaire data that have been distributed in the form of Guttman Scale values from each respondent.

Table 4. 34 Results and Data Processing of Capability Questionnaire DSS04

DSS04 – Manage Continuity					
Level	Process	Activity	Yes	No	Score
2	DSS04.01	1	V	-	1
		2	V	-	1
		3	V	-	1
		4	V	-	1
	DSS04.02	1	V	-	1
		2	-	V	0
		3	V	-	1
		4	V	-	1
	DSS04.03	1	V	-	1
		2	V	-	1
		3	V	-	1

Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)
Volume 4, Number 10, 2025, DOI 10.58471/esaprom.v4i10
ESSN 2828-9463 (Online)
https://ejournal.seaninstitute.or.id/index.php/esaprom

DSS04 – Manage Continuity					
Level	Process	Activity	Yes	No	Score
		4	V	-	1
		5	-	V	0
		6	V	-	1
		7	V	-	1
		1	V	-	1
	DSS04.04	2	V	-	1
		3	V	-	1
	DSS04.06	1	V	-	1
		1	V	-	1
	DSS04.07	2	V	-	1
		3	V	-	1
		4	V	-	1
		Total			21
		Capability Level			91,3%

The result of the Level 2 capability of DSS04 in respondent 1 is with the following formula:

$$CC = \frac{\Sigma CLa}{\Sigma Po} \; x \; 100\%$$

CC = 21/23 × 100%

CC = 91.3%

Based on the results of the questionnaire data calculation from respondent 1, it was found that the capability at Level 2 DSS04 had a capability level value of 91.3%.

A. DSS04 (Responden 2)

The calculation of the capability level process in the DSS04 objective process at XYZ Group is evaluated in stages, or starting from the capability level that has been determined in the COBIT 2019 Framework: Governance and Management Objective module. The following are the results of the calculation of questionnaire data that have been distributed in the form of Guttman Scale values from each respondent.

Table 4. 35 Results and Data Processing of Capability Questionnaire DSS04

DSS04 – Manage Continuity					
Level	Process	Activity	Yes	No	Score
		1	-	V	0
	DSS04.01	2	-	V	0
		3	-	V	0
		4	-	V	0
		1	V	-	1
	DSS04.02	2	-	V	0
		3	-	V	0
		4	-	V	0
		1	V	-	1
2		2	-	V	0
		3	-	V	0
	DSS04.03	4	-	V	0
		5	-	V	0
		6	-	V	0
		7	-	V	0
		1	-	V	0
	DSS04.04	2	-	V	0
		3	-	V	0
	DSS04.06	1	-	V	0

Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)
Volume 4, Number 10, 2025, DOI 10.58471/esaprom.v4i10
ESSN 2828-9463 (Online)
https://ejournal.seaninstitute.or.id/index.php/esaprom

DSS04 – Manage Continuity					
Level	Process	Activity	Yes	No	Score
	DSS04.07	1	V	-	1
		2	-	V	0
		3	-	V	0
		4	-	V	0
		Total			3
		Capability Level			13%

The result of the Level 2 capability DSS04 in respondent 2 is with the following formula:

$$CC = \frac{\Sigma CLa}{\Sigma Po} \; x \; 100\%$$

CC = 3/23 × 100%

CC = 13%

Based on the results of the questionnaire data calculation from respondent 2, it was found that the capability at Level 2 DSS04 had a capability level value of 13%.

A. DSS04 (Responden 3)

The calculation of the capability level process in the DSS04 objective process at XYZ Group is evaluated in stages, or starting from the capability level that has been determined in the COBIT 2019 Framework: Governance and Management Objective module. The following are the results of the calculation of questionnaire data that have been distributed in the form of Guttman Scale values from each respondent.

Table 4. 36 Results and Data Processing of Capability Questionnaire DSS04

DSS04 – Manage Continuity					
Level	Process	Activity	Yes	No	Score
2	DSS04.01	1	-	V	0
		2	-	V	0
		3	-	V	0
		4	-	V	0
	DSS04.02	1	V	-	1
		2	-	V	0
		3	-	V	0
		4	-	V	0
	DSS04.03	1	V	-	1
		2	-	V	0
		3	-	V	0
		4	-	V	0
		5	-	V	0
		6	-	V	0
		7	-	V	0
	DSS04.04	1	-	V	0
		2	-	V	0
		3	-	V	0
	DSS04.06	1	-	V	0
	DSS04.07	1	V	-	1
		2	-	V	0
		3	-	V	0
		4	-	V	0
		Total			3
		Capability Level			13%

Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)
Volume 4, Number 10, 2025, DOI 10.58471/esaprom.v4i10
ESSN 2828-9463 (Online)
https://ejournal.seaninstitute.or.id/index.php/esaprom

The result of the Level 2 capability DSS04 in respondent 3 is with the following formula:

$$CC = \frac{\Sigma CLa}{\Sigma Po} \; x \; 100\%$$

$\boldsymbol{CC}$ = 3/23 × $\mathbf{100}$%

$\boldsymbol{CC}$ = 13%

Based on the results of the questionnaire data calculation from respondent 3, it was found that the capability at Level 2 DSS04 has a capability level value of 13%.

Capability Calculation Recap – DSS04

Based on the results of the evaluation of questionnaire data from each respondent consisting of 3 (Three) respondents, the recapitulation and Result capability of DSS04 are as follows:

Table 4. 37 Capability Calculation Recap DSS04

Evaluation ID	: EVA-5
Objective	: DSS04 – Managed Continuity
Evaluation Date	: Juli, 25 2025
Capability Level	: 2
Information	: Partially Achieved

Proses	Responden	Number of Activity Values	Total Activity	Capability Value
DSS04	R1	21	23	91,3%
	R2	3	23	13%
	R3	3	23	13%
Total		27	69	500%
Result Capability Level Objective				39,1%

DSS04 Objective Capability Results

CLi = R1 + R2 + *R3* / SR x 100%

CLi = 91.3% + 13% + 13% / 3 x 100%

CLi = 117,3 / 3 %

CLi = 39,1%

Based on the results of the calculation above, it shows that the objective process: DSS04 – Manage Continuity in Capability has a capability level of 39.1%. This shows that the company's capability level is in the category of Partially Achieved (15% - 49%), Thus, it can be concluded that the capability level objective process DSS04 is at level 2, and not continued to level 3.

Work of Product DSS04 – Managed Continuity

The following are the results of the work (Work of Product) for the DSS04 Managed Continuity process objectives which have been adjusted to the output of COBIT 2019 at XYZ Group:

Table 4. 38 Work of Product DSS04

Work of Product				
DSS04	Output	Exist	Proof	%
DSS04.01 Define the business continuity policy, objectives and scope	Policy and objectives for business continuity	-	-	0%
	Assessments of current continuity capabilities and gaps	-	-	0%
	Disruptive incident scenarios	-	-	0%

Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)
Volume 4, Number 10, 2025, DOI 10.58471/esaprom.v4i10
ESSN 2828-9463 (Online)
https://ejournal.seaninstitute.or.id/index.php/esaprom

Work of Product				
DSS04	Output	Exist	Proof	%
DSS04.02 Maintain business resilience	Approved strategic options	-	-	0%
	BIAs	-	-	0%
	Continuity requirements	-	-	0%
	Updated repository with CIs	-	-	0%
DSS04.03 Develop and implement a business continuity response	Incident response actions and communications	-	-	0%
	BCP	-	-	0%
Exercise, test and review the business continuity plan (BCP) and disaster response plan (DRP)	Test results and recommendations	-	-	0%
	Test exercises	-	-	0%
	Test objectives	-	-	0%
DSS04.05 Review, maintain and improve the continuity plans	Recommended changes to plans	-	-	0%
	Results of reviews of plans	-	-	0%
DSS04.06 Conduct continuity plan training.	Monitoring results of skills and competencies	-	-	0%
	Training requirements	-	-	0%
DSS04.07 Manage backup arrangements	Test results of backup data	-	-	0%
	Backup data	-	-	0%
DSS04.08 Conduct post-resumption review	Approved changes to the plans	-	-	0%
	Post-resumption review report	-	-	0%
Summary				0%
Normalize				0%

It can be seen from the table above, there are 20 outputs or document evidence provided by COBIT 2019, for the DSS04 process objective has an average evidence value of 0%, which means that DSS04 is at the Not Achieved level (0% – 14%) and there are 20 from 20 outputs that are not available in the XYZ Group.

Capability Calculation DSS05 Level 2

A. DSS05 (Responden 1)

The calculation of the capability level process in the DSS05 objective process at XYZ Group is evaluated in stages, or starting from the capability level that has been determined in the COBIT 2019 Framework: Governance and Management Objective module. The following are the results of the calculation of questionnaire data that has been distributed in the form of the Guttman Scale value of each respondent.

Table 4. 39 Results and Data Processing of Capability Questionnaire DSS05

DSS05 – Managed Security Services					
Level	Process	Activity	Yes	No	Score
2	DSS05.01	1	V	-	1
		2	V	-	1
	DSS05.02	1	V	-	1
		2	V	-	1
		3	V	-	1
		4	V	-	1
	DSS05.03	1	V	-	1
		2	-	V	0
		3	V	-	1
		4	V	-	1
		5	V	-	1
		6	V	-	1
		7	V	-	1
		8	V	-	1
		9	-	V	0

Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)
Volume 4, Number 10, 2025, DOI 10.58471/esaprom.v4i10
ESSN 2828-9463 (Online)
https://ejournal.seaninstitute.or.id/index.php/esaprom

DSS05 – Managed Security Services					
Level	Process	Activity	Yes	No	Score
	DSS05.04	1	V	-	1
	DSS05.05	1	V	-	1
		2	V	-	1
		3	V	-	1
		4	V	-	1
	DSS05.06	1	V	-	1
		2	V	-	1
	Total				21
	Capability Level				91,3%

The results of the Level 2 capability DSS05 in respondent 1 are as follows:

$$CC = \frac{\Sigma CLa}{\Sigma Po} \; x \; 100\%$$

$\boldsymbol{CC}$ = 21/23 × $\mathbf{100}$%

$\boldsymbol{CC}$ = 91,3%

Based on the results of the calculation of questionnaire data from respondent 1, it was found that the capability at Level 2 DSS05 had a capability level value of 91.3%.

A. DSS05 (Responden 2)

The calculation of the capability level process in the DSS05 objective process at XYZ Group is evaluated in stages, or starting from the capability level that has been determined in the COBIT 2019 Framework: Governance and Management Objective module. The following are the results of the calculation of questionnaire data that has been distributed in the form of the Guttman Scale value of each respondent.

Table 4. 40 Results and Data Processing of Capability Questionnaire DSS05

DSS05 – Managed Security Services					
Level	Process	Activity	Yes	No	Score
2	DSS05.01	1	V	-	1
		2	-	V	0
	DSS05.02	1	V	-	1
		2	V	-	1
		3	V	-	1
		4	V	-	1
	DSS05.03	1	V	-	1
		2	V	-	1
		3	-	V	0
		4	V	-	1
		5	-	V	0
		6	-	V	0
		7	V	-	1
		8	V	-	1
		9	-	V	0
	DSS05.04	1	V	-	1
	DSS05.05	1	-	V	0
		2	V	-	1
		3	V	-	1
		4	V	-	1
	DSS05.06	1	V	-	1
		2	-	V	0
	Total				16
	Capability Level				69,5%

Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)
Volume 4, Number 10, 2025, DOI 10.58471/esaprom.v4i10
ESSN 2828-9463 (Online)
https://ejournal.seaninstitute.or.id/index.php/esaprom

The results of capability level 2 DSS05 in respondent 2 are as follows:

$$CC = \frac{\Sigma CLa}{\Sigma Po} \; x \; 100\%$$

CC = 16/23 × 100%

CC = 69.5%

Based on the results of the calculation of questionnaire data from respondent 2, it was found that the capability at level 2 of DSS05 had a capability level value of 69.5%.

A. DSS05 (Responden 3)

The calculation of the capability level process in the DSS05 objective process at XYZ Group is evaluated in stages, or starting from the capability level that has been determined in the COBIT 2019 Framework: Governance and Management Objective module. The following are the results of the calculation of questionnaire data that has been distributed in the form of the Guttman Scale value of each respondent.

Table 4. 41 Results and Data Processing of Capability Questionnaire DSS05

DSS05 – Managed Security Services					
Level	Process	Activity	Yes	No	Score
2	DSS05.01	1	V	-	1
		2	-	V	0
	DSS05.02	1	V	-	1
		2	V	-	1
		3	V	-	1
		4	V	-	1
	DSS05.03	1	V	-	1
		2	V	-	1
		3	V	-	0
		4	V	-	1
		5	V	-	0
		6	V	-	0
		7	V	-	1
		8	V	-	1
		9	-	V	0
	DSS05.04	1	V	-	1
	DSS05.05	1	V	-	0
		2	V	-	1
		3	V	-	1
		4	V	-	1
	DSS05.06	1	V	-	1
		2	-	V	0
	Total				20
	Capability Level				86,9%

The results of the Level 2 capability DSS05 in respondent 3 are as follows:

$$CC = \frac{\Sigma CLa}{\Sigma Po} \; x \; 100\%$$

$\boldsymbol{CC}$ = 20/23 × $\mathbf{100}$%

$\boldsymbol{CC}$ = 86,9%

Based on the results of the calculation of questionnaire data from respondent 3, it was found that the capability at Level 2 DSS05 had a capability level value of 86.9%.

Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)
Volume 4, Number 10, 2025, DOI 10.58471/esaprom.v4i10
ESSN 2828-9463 (Online)
https://ejournal.seaninstitute.or.id/index.php/esaprom

Capability Calculation Recap – DSS05

Based on the results of the evaluation of questionnaire data from each respondent consisting of 3 (Three) respondents, the recapitulation and results of DSS05 capability are as follows:

Table 4. 42 Capability Calculation Recap DSS05

Evaluation ID	: EVA-6	
Objective	: DSS05 – Managed Security Services	
Evaluation Date	: Juli, 25 2025	
Capability Level	: 2	
Information	: Largely Achieved	

Proses	Responden	Number of Activity Values	Total Activity	Capability Value
DSS05	R1	21	23	91,3%
	R2	16	23	69,5%
	R3	20	23	86,9%
Total		57	69	247,7%
Result Capability Level Objective				82,5%

DSS05 Capability Level 2 Results

CLi = R1 + R2 + R3 / SR x 100%

CLi = 91.3 + 69.5 + 86.9 / 3 x 100%

CLi = 247.7/3 x 100%

CLi = 82.5%

Based on the results of the calculation above, it shows that the objective process: DSS05 – Managed Security Services at Capability Level 2 has a capability level of 82.5%. This shows that the company's capability level is in the category of Largely Achieved level (50% - 84%). Thus, it can be concluded that the capability level of the DSS05 objective process is at level 2, and not continued to level 3.

Work of Product DSS05 – Managed Security Services

The following are the results of the work (Work of Product) for the DSS04 Managed Continuity process objectives which have been adjusted to the output of COBIT 2019 at XYZ Group:

Table 4. 43 Work of Product DSS05

	Work of Product			
DSS05	Output	Exist	Proof	%
DSS05.01 Protect against malicious software	Malicious software prevention policy	V	SOP-ITS-004 Pengelolaan_Software. in Appendix F	100%
	Evaluations of potential threats	-	-	0%
DSS05.02 Manage network and connectivity security	Connectivity security policy	V	Pedoman Keamanan IT. in Appendix B	100%
	Results of penetration tests	V	Ringkasan Hasil Penetration Testing. in Appendix G	100%
DSS05.03 Manage endpoint security	Security policies for endpoint devices	V	Pedoman Keamanan IT. in Appendix B	100%
DSS05.04 Manage user identity and logical access	Results of reviews of user accounts and privileges	V	UAM Document. in Appendix H	100%
	Approved user access rights	V	UAM Document. in Appendix H	100%
	Access logs	V	User Access Log.	100%

Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)
Volume 4, Number 10, 2025, DOI 10.58471/esaprom.v4i10
ESSN 2828-9463 (Online)
https://ejournal.seaninstitute.or.id/index.php/esaprom

DSS05	Work of Product Output	Exist	Proof	%
			in Appendix I	
DSS05.05 Manage physical access to I&T assets	Approved access requests	-	-	0%
DSS05.06 Manage sensitive documents and output devices	Access privileges	-	-	0%
	Inventory of sensitive documents and devices	-	-	0%
DSS05.07 Manage vulnerabilities and monitor the infrastructure for security-related events	Security incident tickets	-	Ticketing System – Document Monitoring Ticket. in Appendix J	100%
	Security incident characteristics	-	-	0%
	Security event logs	-	-	0%
	Summary			800%
	Normalize			57%

It can be seen from the table above, there are 14 outputs or document evidence provided by COBIT 2019, for the DSS05 process objective has an average evidence value of 57%, which means that DSS05 is at the Largely Achieved level (50% – 84%) and there are 6 from 14 outputs that are not available in the XYZ Group.

Final Conclusion Capability Level Objective

After calculating the capability level in each activity in the evaluated objective process, the results of the IT governance capability level are obtained as follows:

Table 4. 44 Final Conclusion Capability Level Objective

Governance and Management Objective	Capability Level	Capability Rating (PA 2.1)	Capability Rating Output (PA 2.2)
EDM03 – Ensured Risk Optimization	2	N (11%)	P (25%)
APO12 – Managed Risk	2	P (16,6%)	N (13%)
APO13 – Managed Security	2	P (38%)	L (67%)
BAI10 – Managed Configuration	2	N (0%)	N (10%)
DSS04 – Managed Continuity	2	P (39,1%)	N (0%)
DSS05 - Managed Security Service	2	L (82,5%)	L (57%)
Capability Level		P (31,2%)	P (28,6%)

The results of the discovery of the level of capability were obtained through the processing of quantitative data on questionnaires filled out by the company's respondents. The activity statement on the questionnaire is assessed according to the company's condition whether it is applied or not, where each activity statement has its own value weight that has been calculated and determined by COBIT 2019.

A process is considered to have reached a certain level of capability if the implementation of process activities at that level has reached > 85% (fully achieved). XYZ Group has not yet reached capability level 2 because all activities are considered not to have achieved a Fully achieved rating at level 2. Based on the results of the assessment, capability level 2 only reached 31,2% with an P rating (Partially Achieved) with evaluation Work Product similar 28,6% status was Partially Achieved, so that the assessment cannot be continued to the next stage. It can be concluded that XYZ Group still reaches capability level 1 (Not Very Organized), meaning that The process more or less achieves its purpose through the application of an incomplete set of activities that can be characterized as initial or intuitive.

Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)
Volume 4, Number 10, 2025, DOI 10.58471/esaprom.v4i10
ESSN 2828-9463 (Online)
https://ejournal.seaninstitute.or.id/index.php/esaprom

After conducting an analysis of activities, conclusions were reached regarding the level of the company's capabilities in implementing the principles of COBIT 2019. The next analysis is the finding of the current level of capability (as-is) conditions in XYZ.

Gap Analysis

A process of evaluation and assessment of current conditions and capabilities (as-is) with the expected best practices (to-be) that exist in managing information technology (IT). This analysis was carried out by collecting data, conducting observations, interviews, and filling out questionnaires that were previously conducted to get a comprehensive picture of the condition of IT governance in the XYZ Group. The results of this analysis can be used as a basis for the development and improvement of IT governance in the future.

Analysis as is condition

The following are the findings for the current condition (as-is) of each objective process that has been evaluated previously, namely:

Table 4. 45 Analysis As Is Condition

Governance and Management Objective	Capability Level	Finding
EDM03 – Ensured Risk Optimization	1	1. The IT risk management process has not been thoroughly and periodically documented. 2. The risk register is available but not updated consistently and there is no policy related to Risk Management.
APO12 – Managed Risk	1	1. Risk management has been partially implemented, but it is not yet fully integrated.
APO13 – Managed Security	1	1. Information security policies exist, but they do not yet cover all assets and applications. 2. Proof of work product is limited to policy documents. 3. There has never been a security audit report.
BAI10 – Managed Configuration	1	1. IT asset configuration management is not yet comprehensive. The configuration database (CMDB) is incomplete, the change control process is inconsistent and there is little documentation evidence.
DSS04 – Managed Continuity	1	1. The Business Continuity Plan (BCP) is available in the form of a Draft. 2. There has never been a simulated simulation or disaster recovery test that is not scheduled.
DSS05 - Managed Security Service	1	1. IT security services are still reactive, focusing on incident handling. 2. Incident reporting has not been structured, and documentation of monitoring results is minimal.

Analysis to be condition

The discovery of the expected level of capability targets is a form of appropriate expectation because it is measured based on the goals and targets that have been set in each goal process in Cobit 2019. By setting the expected capability targets in each goal process, XYZ Group can carry out more effective and efficient IT governance planning and development to achieve the desired success. Information regarding the expected level of capability with step by step level to achieved these in realize, targets is listed in the following table:

Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)
Volume 4, Number 10, 2025, DOI 10.58471/esaprom.v4i10
ESSN 2828-9463 (Online)
https://ejournal.seaninstitute.or.id/index.php/esaprom

Table 4. 46 Analysis To Be Condition

Governance and Management Objective	Capability Level	Expected
EDM03 – Ensured Risk Optimization	2	Scheduled IT risk evaluations, regularly updated risk registers, evaluation results integrated into business.
APO12 – Managed Risk	2	Complete IT risk profile, reviewed at least once a year.
APO13 – Managed Security	2	Comprehensive security policy, periodic security testing, documented monitoring.
BAI10 – Managed Configuration	2	Complete CMDB, standard change control management, up-to-date documentation.
DSS04 – Managed Continuity	2	BCP is routinely tested, simulations involve the entire unit, procedures are updated from test results.
DSS05 - Managed Security Service	2	Proactive security services, 24/7 monitoring, structured security reports with follow-ups.

By conducting these comparisons, organizations can figure out where the gap lies between current and expected capabilities, so they can identify which process objectives need improvement. In conducting a gap analysis, organizations can look at the results of a comparison of the level of as-is and to-be capabilities, and determine where there is a gap between the two. If there are gaps, the organization can provide recommendations based on findings and differences between desires and expectations, so that the organization can achieve the expected level of IT governance capability

Gap

The results of the analysis of the gap that have been obtained through the results of the analysis that have been conduct previously are as follows:

Table 4. 47 Gap Analysis

Governance and Management Objective	Capability Level		
	As-is	To-be	Gap
EDM03 – Ensured Risk Optimization	1	2	1
APO12 – Managed Risk	1	2	1
APO13 – Managed Security	1	2	1
BAI10 – Managed Configuration	1	2	1
DSS05 – Managed Continuity	1	2	1
DSS05 - Managed Security Service	1	2	1

Validation

Overview

This chapter presents the validation process for the proposed IT Governance Framework designed to address the problem of application continuity disruption at XYZ Group.

Validation Methodology

Gathering information from a panel of experts through of structured feedback. This method allows the refinement of the research based on expert insights until agreement is reached.

Participants

The validation involved two experts, consisting of:

1. 1 academic experts specializing in academician.
2. 1 industry practitioners, specializing IT managers

Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)
Volume 4, Number 10, 2025, DOI 10.58471/esaprom.v4i10
ESSN 2828-9463 (Online)
https://ejournal.seaninstitute.or.id/index.php/esaprom

Participants were selected based on their academic, expertise and experience relevant to IT governance implementation in medium to large organizations.

Table 4. 48 Participant of Validation

Name	Title	Institution/Company	As
Setyo Haryadi., S.Pd., M.T.	Lecturer, Deputy of Director UT School	Politeknik Astra, PT United Tractors Tbk	Academic Expert
Henry Martawidjaja., M.T.	IT General Manager	PT United Tractors Tbk	IT Expert

Validation Instruments

Document for Expert Review

A summary document was provided to all participants. It included:

1. Background and problem statement
2. Objectives of the governance framework
3. Key components of the proposed framework (structure, policy, process, and controls)
4. Implementation Capability model

Actually this is a part of Chapter 1 until Chapter 4

Giving Questionnaire

A structured questionnaire consisting of 12 items was used to evaluate the research based on five dimensions (Lamm et al., 2020):

1. Clarity
2. Relevance
3. Feasibility
4. Strategic Alignment
5. Completeness

Experts responded using a Likert scale (1 = Strongly Disagree to 5 = Strongly Agree), followed by ended questions for qualitative feedback.

List Of Questionare :

Section A – Clarity

1. The framework structure is clearly defined and easy to understand.
2. The roles and responsibilities (RACI) described are unambiguous.
3. The flow of processes is logically presented and traceable.

Section B – Relevance to XYZ

1. The Research addresses the current challenges in XYZ's application management.
2. The governance components are suitable for a multi-application environment.

Section C – Feasibility

1. The Research is practical to implement within existing resource.
2. There are minimal conflicts with current organizational culture/processes.

Section D – Strategic Fit

1. The governance aligns with long-term IT and business strategy.There are minimal conflicts with current organizational culture/processes.
2. The governance supports future scalability and digital transformation.

Section E – Completeness

Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)
Volume 4, Number 10, 2025, DOI 10.58471/esaprom.v4i10
ESSN 2828-9463 (Online)
https://ejournal.seaninstitute.or.id/index.php/esaprom

1. The framework includes essential components (policies, structure, controls, metrics).
2. The Capability/maturity model/phased implementation strategy is helpful.

Section F – Open Feedback

1. What would you recommend to improve the framework/Research?

Validation Results

Quantitative Results

The aggregated results are summarized below:

Table 4. 49 Quantitatif Feedback Result

Evaluation Criteria	Expert 1	Expert 2	Total
Clarity	4,3	4,7	4,5
Relevance	4,0	5,0	4,5
Feasibility	4,0	4,0	4,0
Strategic Alignment	5,0	5,0	5,0
Completeness	4,0	4,5	4,3
Average			4,5

The scores indicate (Strongly Agree) from expert agreement that the proposed framework is valid and suitable for implementation. The validation results show a positive trend towards the proposed framework. However, there are indications of polarity in the response, with some experts giving very high scores and others lower. This can reduce consistency in the generalization of results. Thus, validation conclusions are more appropriately interpreted as an indication of initial acceptance rather than full confirmation.

Qualitative Feedback

Key insights from ended responses include:

From Expert 1 :

“Complete with a COBIT 19 diagram image, so that it will make it easier for readers to understand the flow process in COBIT 19.”

These suggestions were incorporated into the final version of the research.

From Expert 2 :

1. “Provide more specific metrics of KPIs (Key Performance Indicators) to measure the effectiveness of the governance process (example: downtime cost reduction, improvement projections in capability levels), in addition to just measuring capability.
2. Add a clear roadmap to achieve the desired (to-be) capability level. For example, what specific steps XYZ Group must take in the next 6 months, 12 months, and 24 months to move from level 1 to level 2.”

These suggestions were incorporated into the final version of the research.

The validation confirmed that six governance and management objectives from COBIT 2019 are most critical for supporting business application continuity in XYZ: EDM03, APO12, APO13, BAI10, DSS04, and DSS05. The following presents the evidence, expert input, and validation conclusions for each objective:

Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)
Volume 4, Number 10, 2025, DOI 10.58471/esaprom.v4i10
ESSN 2828-9463 (Online)
https://ejournal.seaninstitute.or.id/index.php/esaprom

Table 4. 50 Validation Conclution

COBIT Objective	Evidence (Assessment Findings)	FGD Expert Input	Validation Conclusion
EDM03 – Ensured Risk Optimization	Risk considerations are ad-hoc, fragmented, and not aligned with enterprise risk appetite.	Establish governance-level ownership of IT risks and integrate into enterprise-wide risk policy.	Validated as critical to formalize risk governance and balance IT risk with business value.
APO12 – Managed Risk	Risk registers are incomplete, inconsistent, and not updated regularly; limited linkage to business risks.	Embed IT risk into enterprise risk management (ERM) with clear thresholds and periodic reviews.	Validated as essential to achieve enterprise-wide risk integration and consistency.
APO13 – Managed Security	Security is reactive; policies exist but are not consistently enforced.	Implement proactive monitoring, standardized policies, and regular vulnerability assessments.	Validated as key to strengthen preventive security and support application continuity.
BAI10 – Managed Configuration	Redundant applications, poor documentation, and lack of centralized configuration repository.	Develop CMDB and application architecture inventory to reduce duplication.	Validated as necessary to control configurations and prevent operational inefficiencies.
DSS04 – Managed Continuity	Few systems have BCP/DRP; most lack continuity arrangements or regular testing.	Establish systematic BCP/DRP and conduct regular continuity tests aligned with business needs.	Validated as aligned with EG06 to ensure resilience and service availability.
DSS05 – Managed Security Services	Security operations are siloed; incident handling inconsistent and slow.	Centralize security services (SOC) and standardize incident response procedures.	Validated as essential to unify security management and reduce vulnerabilities.

This table summarizes how the evidence from capability assessment was combined with FGD expert validation. Each COBIT objective has direct evidence of gaps, expert recommendations, and was validated as critical to XYZ's continuity strategy.

Expert Agreement

A formal Expert Validation Statement was signed by participants, confirming that the framework/research.

Conclusion of Validation

The validation phase confirmed that the proposed IT Governance is:

1. Clearly structured and communicable
2. Contextually appropriate for XYZ Group
3. Feasible to implement with minor adjustments
4. Strategically aligned and scalable for future needs

Based on the validation results, the proposed framework met the defined success criteria, proving its applicability for XYZ Group and its contribution to the body of knowledge on IT governance for application continuity.

CONCLUSIONS

This research evaluated the current state of IT governance at XYZ Group with a specific focus on Business Application Continuity, using the COBIT 2019 framework as the primary assessment and improvement reference. The study addressed the identified challenges of lack of standardized governance processes, and insufficient continuity planning against critical systems. The capability assessment revealed that several governance and

management objectives—specifically EDM03 (Ensured Risk Optimization), APO12 (Managed Risk), APO13 (Managed Security), BAI10 (Managed Configuration), DSS04 (Managed Continuity), and DSS05 (Managed Security Services) were at low capability levels. For instance, EDM03 achieved only 11.1%, categorizing it as Not Achieved, while APO12 scored 16.6% (Partially Achieved). These results highlight that current practices are reactive rather than proactive, Waiting until a critical application goes down, then fix it. with limited documentation, formalized processes, and integration between risk management and continuity strategies. The gap analysis confirmed that XYZ Group lacks a structured governance system to ensure application continuity in the long term. This absence poses risks to operational stability, especially given the organization's dependence on over 66 business applications across its diverse business units. A proposed governance improvement model, grounded in COBIT 2019 principles, was validated through the method involving both academic and industry experts. The validation results indicated that the model is feasible, relevant, and aligned with XYZ Group's digital growth objectives, offering a clear and strengthen governance to improve process capability/maturity, and enhance resilience against disruptions.This research concludes that implementing a tailored IT governance framework aligned with COBIT 2019 significantly enhances an organization's ability to manage application continuity, mitigate operational risks, and align IT with strategic business goals.

REFERENCES

Bocken, N. M. P., Short, S. W., Rana, P., & Evans, S. (2014). A literature and practice review to develop sustainable business model archetypes. *Journal of Cleaner Production*, 65, 42-56.

Doherty, N. F., Fulford, H., & McGowan, S. (2016). The role of information systems in the sustainability of organizations. *Journal of Information Technology*, 31(3), 273-288.

Annual Report-United-Tractors-2023-Final.pdf, n.d.

Hsu, P.D., Lander, E.S., Zhang, F., 2014. Development and Applications of CRISPR-Cas9 for Genome Engineering. Cell 157, 1262–1278. https://doi.org/10.1016/j.cell.2014.05.010

Lamm, K., Lamm, A., Edgar, D., 2020. Scale Development and Validation: Methodology and Recommendations. J. Int. Agric. Ext. Educ. 27, 24–35. https://doi.org/10.5191/jiaee.2020.27224

Nachrowi, E., Yani Nurhadryani, Heru Sukoco, 2020. Evaluation of Governance and Management of Information Technology Services Using Cobit 2019 and ITIL 4. J. RESTI Rekayasa Sist. Dan Teknol. Inf. 4, 764–774. https://doi.org/10.29207/resti.v4i4.2265

Brown, A., & Taylor, B. (2021). Applications are a critical aspect of the
Applications Landscapes Model

Tamm, T., Seddigh, A., & Pärssinen, J. (2016). "How Enterprise Architecture Can Support Business Sustainability." *Journal of Enterprise Architecture*, 12(1), 24-36.

Khalifa, M., & Davison, R. (2015). "The Role of Enterprise Architecture in Sustainable Business Practices." *Journal of Information Technology Management*, 26(1), 1-10.

Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID)
Volume 4, Number 10, 2025, DOI 10.58471/esaprom.v4i10
ESSN 2828-9463 (Online)
https://ejournal.seaninstitute.or.id/index.php/esaprom

Hanafi, M., & Al-Bahadili, H. (2018). "The Role of Enterprise Architecture in Achieving Sustainability Goals: A Case Study." *International Journal of Information Systems and Project Management*, 6(2), 5-20.

Bertelsen, P., & Krogstie, J. (2018). "Enterprise Architecture for Sustainable Development: A Framework for Analysis." *Proceedings of the 51st Hawaii International Conference on System Sciences*.

Pérez, M. P., & Pino, J. A. (2019). "Sustainability in Enterprise Architecture: A Systematic Literature Review." *Journal of Cleaner Production*, 210, 1231-1243.

Al-Faifi, S. A., Alharbi, S., & Alshahrani, S. (2022). Long-term sustainability in application portfolios: The role of integrated planning. *International Journal of Information Management*, 62, 102431.

Boehm, B. W. (2006). A view of 20th and 21st century software engineering. *Software Engineering, IEEE Transactions on*, 32(10), 788-799.

De Haes, S., & Van Grembergen, W. (2015). *Enterprise Governance of Information Technology: Achieving Alignment and Value*. Springer.