

CHAPTER 4 – RESULTS AND DISCUSSIONS

This chapter presents the results and discussion of the research conducted. The findings that are included within this chapter are the outcomes of applying the research framework described in Chapter 3. This chapter begins by outlining the formulation of the research instrument, which establishes the basis for the gap identification. It then presents the results of that analysis, the proposed design improvement to address the identified gaps, and the evaluation and validation of the proposed solution

4.1. Requirement Formulation

In accordance with the discussion in Chapter 3.3 Requirement Formulation, the research instrument is prepared based on the COBIT 2019 framework and tailored by considering the specific regulatory requirements of the banking industry. This approach ensures that the gap identification is based on the mandatory obligations of XYZ Bank.

4.1.1 Regulation Mapping to COBIT Process

The scope of the regulations is limited to the provisions governing the implementation of information technology, which include:

1. POJK No. 11/POJK.03/2022 on The Implementation of Information Technology by Commercial Banks;
2. SEOJK No. 11/POJK.03/2017 on The Application of Risk Management in The Use of Information Technology by Commercial Banks;
3. SEOJK No. 24/SEOJK.03/2023 on Digital Maturity Assessment of Bank; and
4. SEOJK No. 29/SEOJK.03/2022 on Cyber Resilience and Security of Commercial Banks.

The following subchapters explain the mapping analysis conducted between the COBIT 2019 governance and management objectives and each of the defined regulations. This process serves to translate these regulatory mandates into a structured assessment tool for the gap identification phase of the research.

4.1.1.1 Mapping POJK No 11/POJK.03/2022 on The Implementation of Information Technology by Commercial Bank to COBIT

In order to ensure the research instrument aligns with regulatory requirements, a detailed analysis was conducted based on POJK No. 11/POJK.03/2022 concerning the Implementation of Information Technology by Commercial Banks. This process involved mapping the specific articles within the regulation to the corresponding governance and management objectives in the COBIT 2019 framework. The results of this mapping analysis are presented in the table below.

Table 4.1. POJK No.11/POJK.03/2022 to COBIT Mapping

No	POJK No.11/POJK.03/2022 relevancy	COBIT 2019 Processes
1	Relevant	EDM01, EDM02, EDM03, EDM04, EDM05, APO01, APO02, APO03, APO07, APO10, APO12, APO13, APO14, DSS04, DSS05, MEA02, MEA04
2	Irrelevant	APO04, APO05, APO06, APO08, APO09, APO11, BAI01, BAI02, BAI03, BAI04, BAI05, BAI06, BAI07, BAI08, BAI09, BAI10, BAI11, DSS01, DSS02, DSS03, DSS06, MEA01, MEA03

According to the mapping analysis within Table 4.1., out of the 40 COBIT 2019 processes, 17 were identified as relevant to the aforementioned regulation. These processes are primarily focused on the overarching governance and strategic aspects of IT. On the other hand, 23 processes were deemed irrelevant in the context of this high-level regulatory mapping. Thus, the relevant process will be prioritized for gap identification according to POJK No.11/POJK.03/2022. Details of the mapping between POJK No.11/POJK.03/2022 and COBIT 2019 process could be seen further on Appendix 1.1.

4.1.1.2 Mapping SEOJK No 11/POJK.03/2017 on The Application of Risk Management in The Use of Information Technology by Commercial Banks to COBIT

In order to ensure the research instrument aligns with regulatory requirements, a detailed analysis was conducted based on SEOJK No. 11/POJK.03/2017 concerning The Application of Risk Management in The Use of Information Technology by Commercial Banks. This process involved mapping the specific articles within the regulation to the corresponding governance and management objectives in the COBIT 2019 framework. The results of this mapping analysis are presented in the table below.

Table 4.2. SEOJK No.11/POJK.03/2017 to COBIT Mapping

No	SEOJK No.11/POJK.03/2017 relevancy	COBIT 2019 Processes
1	Relevant	EDM01, EDM02, EDM03, EDM04, EDM05, APO01, APO02, APO03, APO07, APO10, APO12, APO13, APO14, DSS04, DSS05, MEA02, MEA04
2	Irrelevant	APO04, APO05, APO06, APO08, APO09, APO11, BAI01, BAI02, BAI03, BAI04, BAI05, BAI06, BAI07, BAI08, BAI09, BAI10, BAI11, DSS01, DSS02, DSS03, DSS06, MEA01, MEA03

According to the mapping analysis within Table 4.2., out of the 40 COBIT 2019 processes, 17 were identified as relevant to the aforementioned regulation. These processes are primarily focused on the overarching governance and strategic aspects of IT. On the other hand, 23 processes were deemed irrelevant in the context of this high-level regulatory mapping. Thus, the relevant process will be prioritized for gap identification according to SEOJK No.11/POJK.03/2017. Details of the mapping between SEOJK No.11/POJK.03/2017 and COBIT 2019 process could be seen further on Appendix 1.2.

4.1.1.3 Mapping SEOJK No. 24/SEOJK.03/2023 on Digital Maturity Assessment of Bank to COBIT

In order to ensure the research instrument aligns with regulatory requirements, a detailed analysis was conducted based on SEOJK No. 24/SEOJK.03/2023 concerning Digital Maturity Assessment of Banks. This process involved mapping the specific articles within the regulation to the corresponding governance and management objectives in the COBIT 2019 framework. The results of this mapping analysis are presented in the table below.

Table 4.3. SEOJK No.24/SEOJK.03/2023 to COBIT Mapping

No	SEOJK No.24/POJK.03/2023 relevancy	COBIT 2019 Processes
1	Relevant	EDM01, EDM02, EDM03, EDM04, EDM05, APO01, APO02, APO03, APO05, APO06, APO07, APO08, APO09, APO10, APO11, APO12, APO13, APO14, BAI02, BAI03, DSS01, DSS02, DSS04, DSS05, MEA01, MEA02
2	Irrelevant	APO04, BAI01, BAI04, BAI05, BAI06, BAI07, BAI08, BAI09, BAI10, BAI11, DSS03, DSS06, MEA03, MEA04

According to the mapping analysis within Table 4.3., out of the 40 COBIT 2019 processes, 26 were identified as relevant to the aforementioned regulation. These processes are primarily focused on the overarching governance and strategic aspects of IT. On the other hand, 14 processes were deemed irrelevant in the context of this high-level regulatory mapping. Thus, the relevant process will be prioritized for gap identification according to SEOJK No.24/POJK.03/2023. Details of the mapping between SEOJK No.24/POJK.03/2023 and COBIT 2019 process could be seen further on Appendix 1.3.

4.1.1.4 Mapping SEOJK No. 29/SEOJK.03/2022 on Cyber Resilience and Security of Commercial Banks to COBIT

In order to ensure the research instrument aligns with regulatory requirements, a detailed analysis was conducted based on SEOJK No. 29/SEOJK.03/2022 concerning Cyber Resilience and Security of Commercial Banks. This process involved mapping the specific articles within the regulation to the corresponding governance and management objectives in the COBIT 2019 framework. The results of this mapping analysis are presented in the table below.

Table 4.4. SEOJK No.29/SEOJK.03/2022 to COBIT Mapping

No	SEOJK No.29/SEOJK.03/2022 relevancy	COBIT 2019 Processes
1	Relevant	EDM01, EDM03, APO01, APO02, APO07, APO10, APO12, APO13, APO14, BAI03, BAI09, DSS02, DSS04, DSS05, MEA02
2	Irrelevant	EDM02, EDM04, EDM05, APO0, APO04, APO05, APO06, APO08, APO09, APO10, APO14, BAI01, BAI02, BAI04, BAI05, BAI06, BAI07, BAI08, BAI09, BAI10, BAI11, DSS01, DSS03, DSS06, MEA01, MEA03, MEA04

According to the mapping analysis within Table 4.3., out of the 40 COBIT 2019 processes, 15 were identified as relevant to the aforementioned regulation. These processes are primarily focused on the overarching governance and strategic aspects of IT. On the other hand, 25 processes were deemed irrelevant in the context of this high-level regulatory mapping. Thus, the relevant process will be prioritized for gap identification according to SEOJK No.29/SEOJK.03/2022. Details of the mapping between SEOJK No.29/SEOJK.03/2022 and COBIT 2019 process could be seen further on Appendix 1.4.

4.1.2 COBIT Process Prioritization

After mapping each individual regulation, the mapping is consolidated altogether to identify a final and relevant processes of COBIT 2019 that will be used for assessment. A process is considered a priority for this research if it was deemed relevant by one or more of related OJK regulations. The logic is that processes that is required by multiple regulations are considered as higher criticality to XYZ Bank's from the perspective of compliance requirement.

Table 4.5 below presents the consolidated mapping, which shows relevant processes across the four regulations that has been analyzed. The "Total" column indicates the number of regulations a single COBIT process is relevant to. A process is marked as relevant ("R") for the final assessment if it was mapped to at least one regulation.

Table 4.5. COBIT Process Prioritization Mapping

COBIT 2019 Process	Regulations				Total	Relevancy
	POJK PTI	SEOJK DMAB	SEOJK KKS	SEOJK MRTI		
EDM01	R	R	R	R	4	R
EDM02	R	R	NR	NR	2	R
EDM03	R	R	R	R	4	R
EDM04	R	R	NR	NR	2	R
EDM05	R	R	NR	NR	2	R
APO01	R	R	R	R	4	R
APO02	R	R	R	R	4	R
APO03	R	R	NR	NR	2	R
APO04	NR	NR	NR	NR	0	NR

COBIT 2019 Process	Regulations				Total	Relevancy
	POJK PTI	SEOJK DMAB	SEOJK KKS	SEOJK MRTI		
APO05	NR	R	NR	NR	1	R
APO06	NR	R	NR	NR	1	R
APO07	R	R	R	NR	3	R
APO08	NR	R	NR	NR	1	R
APO09	NR	R	NR	NR	1	R
APO10	R	R	R	R	4	R
APO11	NR	R	NR	NR	1	R
APO12	R	R	R	R	4	R
APO13	R	R	R	NR	3	R
APO14	R	R	NR	NR	2	R
BAI01	NR	NR	NR	NR	0	NR
BAI02	NR	R	NR	R	2	R
BAI03	NR	R	R	R	3	R
BAI04	NR	NR	NR	NR	0	NR
BAI05	NR	NR	NR	NR	0	NR
BAI06	NR	NR	NR	NR	0	NR
BAI07	NR	NR	NR	R	1	R
BAI08	NR	NR	NR	NR	0	NR
BAI09	NR	NR	R	R	2	R

COBIT 2019 Process	Regulations				Total	Relevancy
	POJK PTI	SEOJK DMAB	SEOJK KKS	SEOJK MRTI		
BAI10	NR	NR	NR	NR	0	NR
BAI11	NR	NR	NR	R	1	R
DSS01	NR	R	NR	R	2	R
DSS02	NR	R	R	R	3	R
DSS03	NR	NR	NR	NR	0	NR
DSS04	R	R	R	R	4	R
DSS05	R	R	R	R	4	R
DSS06	NR	NR	NR	NR	0	NR
MEA01	NR	R	NR	NR	1	R
MEA02	R	R	R	NR	3	R
MEA03	NR	NR	NR	R	1	R
MEA04	R	NR	NR	R	2	R

Based on the consolidation in Table 4.5, a total of 31 processes were identified as having relevance to at least one of the OJK regulations. In order to look into more important processes between these 31 processes, a further prioritization was applied. As established in the literature review in Chapter 2, organizations could prioritize controls that address their most stringent compliance requirements or requirements that are addressed repeatedly between regulations to highlight its importances. Following this approach, this research will focus on the processes that are relevant to all four OJK regulations that has been analyzed. Those high-priority processes are indicated by a "Total" score of 4 in Table 4.5. The high-prioritized processes for analysis are: EDM01 – Ensured Governance Framework Setting and Maintenance, EDM03 – Ensured Risk

Optimization, APO01 – Managed I&T Management Framework, APO02 – Managed Strategy, APO10 – Managed Vendors, APO12 – Managed Risk, DSS04 – Managed Continuity, and DSS05 – Managed Security Services. These 8 high-priority processes would be used analyzed and assessed further in the analysis phase to evaluate the existing state of IT governance at XYZ Bank.

4.2. Analysis

This phase assesses the current state of IT governance at XYZ Bank against the prioritized COBIT 2019 processes. This phase consists of data collection, determining the existing capability levels, identifying gaps against the target state, and prioritizing these gaps for improvement.

4.2.1 Data Collection

As mentioned within Chapter 3.4.1, this activity meant to collect data related to prioritized processes to understand existing IT governance condition of XYZ Bank through documentation study and interviews. Through this activity, following documents are identified and collected for analysis regarding prioritized processes:

1. Information Technology Policy
2. Information Security Policy
3. IT Risk Management Policy
4. IT Risk Management Guidelines
5. IT Steering Committee Charter
6. Internal Audit Charter
7. Risk Appetite and Risk Threshold Statement
8. Digital Maturity Assessment for Bank's Procedure
9. Procurement Procedure
10. Vendor Management Procedure

11. Third Party Security Assessment Procedure

12. Business Continuity Guidelines

13. Disaster Recovery Procedure

14. Asset Protection Procedure

15. Access Management Procedure

16. Vulnerability Management Procedure

17. Incident Handling Procedure

18. Organization structure

19. Job description document

20. Training plan

21. IT risk management socialization and awareness record

22. IT Strategic Plan

23. Bank's Business Plan

24. Vendor catalogue

25. IT risk register

The content and implementation of these documents would be used as basis for the capability assessment activity in the next part.

4.2.2 Existing Capability Level Determination Based on CPM

The collected data then analyzed to determine the existing capability level of each prioritized COBIT process. Each process then assessed using the previously identified documentations and then assigned with capability level that correspond with CMMI within COBIT 2019. Each level will be assigned with rating (Fully achieved, Largely achieved, Partially achieved, or Not achieved). The result then aggregated to determine

the overall capability level for the process. Following Table 4.6 are the result of existing capability level assessment within XYZ Bank.

Table 4.6. Existing Capability Level

Process ID	Process Name	Capability Level
EDM01	Ensured Governance Framework Setting and Maintenance	1 (Initial)
EDM03	Ensure Risk Optimization	2 (Managed)
APO01	Managed I&T Management Framework	2 (Managed)
APO02	Managed Strategy	2 (Managed)
APO10	Managed Vendors	3 (Defined) 
APO12	Managed Risk	3 (Defined)
DSS04	Managed Continuity	2 (Managed)
DSS05	Managed Security Services	2 (Managed)

As can be seen within Table 4.6, from 8 prioritized process it has been found that there are two processes that achieved Level 3 (Defined) capability. Those are APO10 which focus to manage vendor and APO 12 which focus to manage risk. Also, there are 5 processes that achieved capability of Level 2 (Managed). Those processes are EDM03 which mainly focus to optimize risk, APO01 which manage I&T management framework, APO02 which focus on strategy management, DSS04 which focus to manage continuity, and DSS05 which mainly focus on security services management. The last but not least, there is one process that still on Level 1 (Initial) which is EDM01 which mainly focus to ensure I&T governance framework setting.

The result of this assessment would be the basis of next activity which is to conduct gap identification by considering the existing capability level with the target capability level.

4.2.3 Gap Identification

The gap identification was conducted by comparing the existing capability levels with the target capability level which is Level 3 (Defined) for the prioritized processes as mentioned within Chapter 3.4.3. The analysis shows that there are gaps for prioritized processes which has been identified within Chapter 4.1.2 and has been assessed within Chapter 4.2.2. The gap signifies the absence of standardized, documented, and institutionalized processes that are required to achieve a "Defined" state. Figure 4.1 illustrates the gap between the existing level capability and the target level capability.

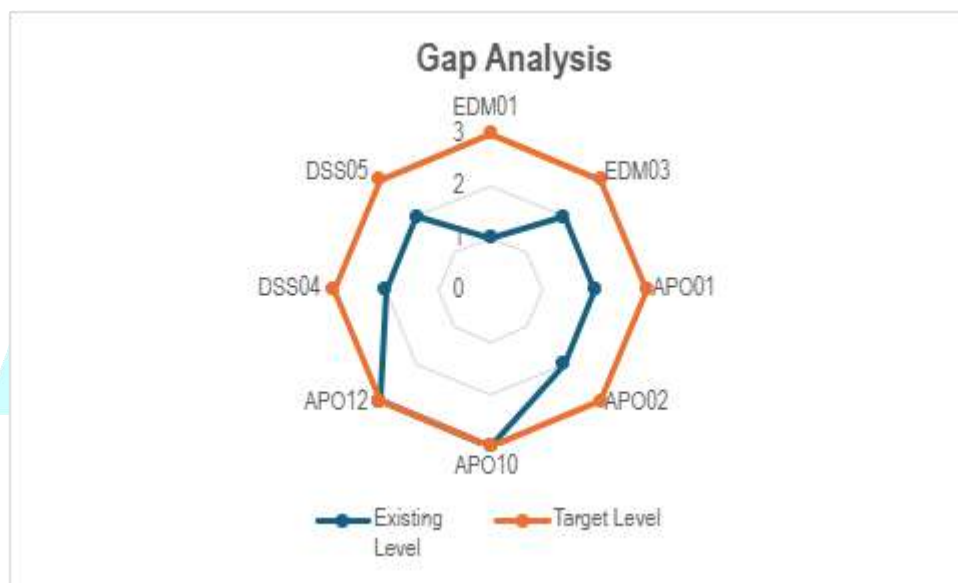


Figure 4.1. Gap Identification Result

As depicted in Figure 4.1, there are two processes that have reached capability level three. Meanwhile, there are five processes with capability level two and one process identified as being at capability level one. Details of the gap results along with the capability gap towards the target level are explained in Table 4.7 Gap Identification Result.

Table 4.7. Gap Identification Result

Process ID	Process Name	Existing Level	Target Level	Capability Gap
	Ensured Governance			
EDM01	Framework Setting and Maintenance	1 (Initial)	3 (Defined)	2
EDM03	Ensure Risk Optimization	2 (Managed)	3 (Defined)	1
APO01	Managed I&T Management Framework	2 (Managed)	3 (Defined)	1
APO02	Managed Strategy	2 (Managed)	3 (Defined)	1
APO10	Managed Vendors	3 (Defined)	3 (Defined)	0
APO12	Managed Risk	3 (Defined)	3 (Defined)	0
DSS04	Managed Continuity	2 (Managed)	3 (Defined)	1
DSS05	Managed Security Services	2 (Managed)	3 (Defined)	1

As shown in Table 4.7, there are several capability gaps of XYZ Bank's IT governance processes since six of the eight high-priority processes does not achieve the target capability level. The processes APO10 – Managed Vendors and APO12 – Managed Risk are the only two that currently meet the target of Level 3, indicating that XYZ Bank has already established relatively mature and standardized processes for vendor and risk management.

Meanwhile, the most significant gap is in EDM01 with a gap of two levels. Its current capability level is on Level 1 (Initial). It means that governance activities are performed in an ad-hoc and disorganized manner. There is a lack of formally documented governance principles, communication and reporting mechanisms, and activities especially regarding evaluate and monitor activities.

For EDM03, a one-level gap exists as the process is currently at a Level 2 (Managed). While IT risks are being identified and addressed, the process is not yet fully defined. This is caused by the lack of several activities such as evaluating IT risk factors regarding strategic enterprise decision, evaluation of risk management activities, and directing implementation of risk treatment. These gaps would cause risk optimization process to be suboptimal, not aligned with strategic business objectives, and the process for defining and monitoring Key Risk Indicators (KRIs) is not standardized across the organization.

More or less, the same issue also happening in APO01 which also achieved Level 2 (Managed). This process has some gaps especially regarding considering and choosing best practices for appropriate governance, communication and reporting mechanism, and defining required target process model.

There are also gaps within APO02 which currently operates at a Level 2 (Managed). This process currently does not yet to identify relevant stakeholders and their requirements in defined manner. Thus, leading to lack of detailed analysis on what is the target digital capabilities, gap identification of digital capabilities, and thorough activities to set a strategic plan. Although this process has been conducted within XYZ Bank, there is no defined approach for strategy development, communication, and performance tracking.

As for DSS04, this process also has one-level gap since it is still on Level 2 (Managed). This is caused by some lacking activities such as identification and mapping of detailed business process and its supporting IT services, distributions of related information regarding this process, and conducting thorough Business Continuity Plan (BCP) testing.

The last process that contains gaps in activity is DSS05. This process also managed to achieve Level 2 (Managed) with several gaps. The gap is specifically about managing sensitive documents and output devices, encrypting information according to its classification, and the lack of overarching policy regarding security services.

These gaps confirm the hypothesis that XYZ Bank's IT governance requires improvement, particularly in establishing a defined and documented process.

4.2.4 Improvement Prioritization

Considering the gap that has been identified from previous chapter, the improvement of XYZ Bank's IT governance process is required. However, attempting to address all of these gaps altogether would be impractical given resource constraints. Therefore, a Focus Group Discussion (FGD) was conducted with the same stakeholders related to data collection activity which is Head of IT and the IT GRC Officer. This FGD meant to prioritize the improvement initiatives. Each gap was treated as a risk to the organization, and the response was determined based on urgency, impact, and feasibility. The results of this prioritization are summarized in Table 4.8.

Table 4.8. Process Improvement Prioritization

Process ID	Process Name	Capability Gap	Response
EDM01	Ensured Governance Framework Setting and Maintenance	2	Mitigate
EDM03	Ensure Risk Optimization	1	Mitigate
APO01	Managed I&T Management Framework	1	Mitigate
APO02	Managed Strategy	1	Mitigate
DSS04	Managed Continuity	1	Accept
DSS05	Managed Security Services	1	Mitigate

As can be seen on Table 4.8, from six processes that has gaps there are five processes that would be mitigated and improved within this research and one process that is accepted and would not be mitigated and improved through this research. The rationale of this comes because DSS04 which mainly focus to manage continuity is currently being mitigated through existing project to enhance business continuity within XYZ Bank. Meanwhile, all the other process are not yet planned or under any project to be

mitigated or improved. Thus, considering this condition, this research will focus on designing artifacts to mitigate gaps related to five processes such as EDM01, EDM03, APO01, APO02, and DSS05.

4.3. Design

This phase focuses on creating the IT artifacts required to close the prioritized gaps and elevate XYZ Bank's IT governance to the target capability level of 3 (Defined). The artifacts designed are primarily Method artifacts, as defined by Design Science Research, consisting of policies that provide formal guidance for consistent and repeatable execution.

4.3.1 Design Improvement

Based on the prioritized gaps, a set of integrated IT governance documents were designed. These artifacts incorporate best practices from COBIT 2019 and ISO 27001:2022, tailored to the specific context and needs of XYZ Bank.

There is a consideration upon designing the following artifacts, especially related to target capability level. The analysis from previous section showed that there are different capability gaps across the prioritized processes. Some processes have one-level gap and the other have two-level gap. The consideration in mitigating this difference was the need for all prioritized processes to achieve a consistent, stable, and defined approach or mechanism. Therefore, the decision was made to target Level 3 (Defined) capability for all processes, rather than pursuing incremental, one-level improvements.

This approach was chosen to address the issues at XYZ Bank, such as its unestablished processes. Improving a Level 1 process to Level 2 would be an insufficient since Level 2 process remains largely reactive and person-dependent since the process was not defined properly in an agreed mechanism. Thus, it is necessary to achieve to Level 3 for all processes, as it meant to target a process that is institutionalized and defined across XYZ Bank. Consequently, the design does not differentiate between processes with large or small gaps in terms of priority. Instead, it aims for the comprehensive implementation of all practices required to achieve Defined capability level (Level 3).

A larger capability gap only shows that more foundational practices were missing and needed to be incorporated into the policy design.

The creation of the policy artifacts was guided by a systematic, gap-driven methodology. The selection of each policy item was a direct response to the gap identified during the analysis phase, addressing both practices that were not yet conducted within XYZ Bank and the processes and activities that already existed but conducted in ad-hoc approach. The primary input was the detailed gap analysis from Chapter 4.2.3. For every COBIT process practice required for Level 3 that was identified as "Not achieved" or "Partially achieved," a corresponding policy statement, procedure, or defined role was created. While the gaps dictated what needed to be included, the COBIT 2019 and ISO 27001:2022 frameworks dictated how the content should be structured.

The designed artifacts are the IT Governance Policy and the Cyber Resilience and Security Policy. The first of these, the IT Governance Policy, focuses on creating an IT governance and management framework that aligns with business strategy, optimizes risk, and complies with relevant regulations. The summary of the policy can be mapped as shown in the following Table 4.9.

Table 4.9. IT Governance Policy Fulfilment Mapping with Related Framework

No.	Policy Content	SEOJK No. 24 / 2023 (DMAB)	COBIT 2019 Process	ISO 27001:2022 Clause/Control
	Organizational			
1	Structure, Roles, and Responsibilities (Chapter II)	1.a.4, 1.a.5, 1.a.6 (Institutional Arrangement)	EDM01, APO01	N/A
2	IT Governance: Governance	1.b.1 (IT Governance)	EDM01	N/A

No.	Policy Content	SEOJK No. 24 / 2023 (DMAB)	COBIT 2019 Process	ISO 27001:2022 Clause/Control
	Framework (Chapter III.A)			
2.1	IT Governance System Evaluation	1.b.1 (IT Governance)	EDM01.01	N/A
2.2	IT Governance System Direction	1.b.1 (IT Governance)	EDM01.02	N/A
2.3	IT Governance System Monitoring	1.b.1 (IT Governance)	EDM01.03	N/A
3	IT Governance: Risk Optimization (Chapter III.B)	1.b.3 (IT Risk)	EDM03	N/A
3.1	Risk Management Evaluation	1.b.3 (IT Risk)	EDM03.01	N/A
3.2	Risk Management Direction	1.b.3 (IT Risk)	EDM03.02	N/A
3.3	Risk Management Monitoring	1.b.3 (IT Risk)	EDM03.03	N/A
4	IT Management: Management Framework (Chapter IV.A)	1.a.5, 1.a.6 (Organizational Design & Digital Culture)	APO01	Clause 7.5, A.5.1

No.	Policy Content	SEOJK No. 24 / 2023 (DMAB)	COBIT	ISO
			2019 Process	27001:2022 Clause/Control
4.1	IT Management System Design	1.a.5 (Organizational Design)	APO01.01	N/A
4.2	IT Management Process Implementation	1.a.5 (Organizational Design)	APO01.02 APO01.03	N/A
4.3	Organization Structure and Digital Culture Definition	1.a.5, 1.a.6 (Organizational Design & Digital Culture)	APO01.04 APO01.05	Clause 7.5, A.5.1
4.4	Policy and Procedure Definition	1.a.5 (Organizational Design)	APO01.09	N/A
4.5	Framework Continuous Improvement	1.a.5 (Organizational Design)	APO01.11	N/A
5	IT Management: Strategy Management (Chapter IV.B)	1.b.7 (ITSP Alignment), 5.a.1, 5.a.2, 5.a.3, 5.a.4 (IT Adoption)	APO02	N/A
5.1	Context and Vision Understanding	1.b.7 (ITSP Alignment)	APO02.01	N/A
5.2	Digital Capability, Performance, and	1.b.7 (ITSP Alignment)	APO02.02	N/A

No.	Policy Content	SEOJK No. 24 / 2023 (DMAB)	COBIT	ISO
			2019 Process	27001:2022 Clause/Control
	Maturity Assessment			
5.3	Digital Maturity Target Definition	1.b.7 (ITSP Alignment)	APO02.03	N/A
5.4	Gap Analysis and Feasibility Study	1.b.7 (ITSP Alignment), 5.a.1, 5.a.2, 5.a.3, 5.a.4 (IT Adoption)	APO02.04	N/A
5.5	IT Strategic Plan and Road Map Definition	1.b.7 (ITSP Alignment), 5.a.1, 5.a.2, 5.a.3, 5.a.4 (IT Adoption)	APO02.05	N/A
5.6	ITSP Communication and Evaluation	1.b.7 (ITSP Alignment), 5.a.1, 5.a.2, 5.a.3, 5.a.4 (IT Adoption)	APO02.06	N/A
6	IT Management: Risk Management (Chapter IV.C)	3.a.1, 3.a.2, 3.a.3, 3.a.4, 3.a.5 (IT Risk Management)	N/A	N/A
7	Monitoring, Evaluation, and Assessment (Chapter V)	N/A	N/A	Clause 9.1, 9.2, 9.3 Clause 10.1, 10.2

As can be seen in Table 4.9, the design of the policy is not only derived from a single COBIT 2019 process but is a consolidated artifact that integrates requirements from multiple frameworks, including ISO 27001:2022 and the OJK's DMAB framework. This IT Governance Policy is designed to address the gaps in COBIT processes EDM01, EDM03, APO01, and APO02. This approach was chosen because these processes are highly interrelated.

To provide a more detailed view of how this policy resolve the specific gap identified in the analysis phase, Table 4.10 details the previous condition and the improvement for each COBIT 2019 process practice.

Table 4.10. IT Governance Policy Detail on COBIT 2019 Process

No.	COBIT 2019 Process	Previous Condition	Improvement
1	EDM01: Ensured Governance Framework Setting and Maintenance	• There is no identification on internal and external factors regarding IT governance	• Enforcement to conduct identification on internal and external factors that could impact IT governance
1.1	EDM01.01	• There is no explicit consideration of regulations and laws regarding IT governance • No defined principles for IT decision making	• Enforcement on considering IT regulations and laws • Provide principles that could be used for IT decision making

COBIT 2019		Previous Condition	Improvement
No.	Process		
1.2	EDM01.02	• No explicit definition delegation mechanism • No explicit definition on IT Governance Board should direct the IT governance of XYZ Bank • No direction for communication and directing mechanism	• Enforcement for delegation mechanism • Enforce IT Governance Board to direct the IT governance • Enforcement to communicate and direct IT governance
1.3	EDM01.03	• No periodical assessment on IT governance's effectiveness or performance	• Enforce periodical assessment regarding IT governance's effectiveness and performance
2	EDM03 Ensured Risk Optimization		
2.1	EDM03.01	• No proactive evaluation on IT risk • No alignment on IT Risk with Enterprise Risk Management	• Provide enforcement and mechanism for proactive evaluation on IT risk • Enforcement on alignment on IT Risk with ERM

COBIT 2019		Previous Condition	Improvement
No.	Process		
2.2	EDM03.02	• No mechanism on changing risk and reporting • No identification and management of key goals and metrics for IT Risk	• Provide enforcement to report any changing risk • Enforce identification and management of key IT Risk
2.3	EDM03.03	• No routine mechanism to report IT risk to board • No periodical monitoring for IT Risk	• Enforcement for routing monitoring of board regarding IT risk
3	APO01 Managed I&T Management Framework		
3.1	APO01.01	• No analysis and consideration of internal and external factors that could impact IT framework	• Enforcement of analysis and consideration of internal and external factors that could impact IT framework
3.2	APO01.02	• No defined communication rules	• Enforcement to have communication rules within company
3.3	APO01.03	• No defined mechanism for IT	• Enforcement to conduct assessment

COBIT 2019		Previous Condition	Improvement
No.	Process		
		management processes both for assessing the existing condition and target condition	for IT management processes including existing and target condition on periodical basis
3.4	APO01.04	No defined requirement about the need to define organizational structure along with related responsibilities	Enforcement to define organizational structure along with related responsibilities
3.5	APO01.05	No defined requirement about the need to define organizational structure along with related responsibilities	Enforcement to define organizational structure along with related responsibilities
3.6	APO01.06	There is no gap for this subprocess	There is no improvement for this subprocess
3.7	APO01.07	There is no gap for this subprocess	There is no improvement for this subprocess
3.8	APO01.08	There is no gap for this subprocess	There is no improvement for this subprocess
3.9	APO01.09	No defined mechanism to manage policies	Enforcement and mechanism for policies lifecycle including creation,

No.	COBIT 2019 Process	Previous Condition	Improvement
			review, update, and communication of policies
3.10	APO01.10	There is no gap for this subprocess	There is no improvement for this subprocess
3.11	APO01.11	• No enforcement to conduct periodical assessment for IT management system	• Enforcement to conduct assessment for IT management processes including existing and target condition on periodical basis
4	APO02 Managed Strategy		
4.1	APO02.01	• No defined mechanism to understand internal and external factor regarding IT strategy	• Enforcement to consider internal and external factor that could impact IT strategy
4.2	APO02.02	• No defined mechanism for assessment on existing capability	• Enforcement to conduct assessment on existing digital capability of XYZ Bank
4.3	APO02.03	• No defined mechanism to define	• Enforcement to define target capability along

COBIT 2019		Previous Condition	Improvement
No.	Process		
4.4	APO02.04	target capability along with relevant products • No enforcement on gap analysis for capabilities	with relevant product that supports it • Enforcement to conduct gap analysis to identify what capabilities are required to achieve the target
4.5	APO02.05	• No enforcement to conduct strategic planning and roadmap definition • No enforcement to formalize ITSP and roadmap	• Enforcement to conduct IT strategic planning and to conduct periodical review to ensure the achievement of the strategic planning • Enforcement to formalize ITSP
4.6	APO02.06	• No defined mechanism to communicate IT strategy and roadmap	• Enforcement to communicate ITSP and roadmap to relevant stakeholders within XYZ Bank

The improvements detailed in Table 4.10 shows what is lacking on previous condition and what is the improved condition by IT Governance Policy. This policy meant to address the root cause of unestablished governance processes by providing the outline and responsibilities of each party.

Meanwhile, the Cyber Resilience and Security Policy are designed to protect assets from cybersecurity attacks, covering asset identification, protection, and incident handling. The summary of its alignment with relevant frameworks is mapped in Table 4.11.

Table 4.11. Cyber Resilience and Security Policy Fulfilment Mapping with Related Framework

No.	Policy Content	SEOJK 29 / 2022 (KKS)	COBIT 2019 Process	ISO 27001:2022 Clause/Control
Organizational				
1	Structure, Authorities, and Responsibilities (Chapter II.A)	Appendix I.b	EDM01,	A.5.2
		(1.1.a, 1.1.b, 2.2.c)	APO01	A.5.3
2	Risk Appetite and Tolerance Statement (Chapter II.B)	Appendix I.b (1.2.a, 1.2.b)	EDM03	Clause 6.1.2
3	Cybersecurity Risk Culture and Awareness (Chapter II.C)	Appendix I.b (1.3.a, 1.3.b, 1.3.c)	N/A	Clause 7.3, A.6.3
4	Risk Management Framework (Chapter III.A)	Appendix I.b (2.1, 2.2, 2.3)	N/A	Clause 6.1
5	Process, HR, Information System, Control & Review (Chapter III.B)	Appendix I.b (3.1, 3.2, 3.3, 4.1, 4.2)	N/A	Clause 8, Clause 9

No.	Policy Content	SEOJK 29 / 2022 (KKS)	COBIT 2019 Process	ISO 27001:2022 Clause/Control
6	Identification of Assets, Threats, and Vulnerabilities (Chapter IV.A)	Appendix I.c (1.a, 1.b)	DSS05.07	A.5.9, A.5.7, A.8.8
7	Asset Protection (Chapter IV.B)	Appendix I.c (2.a, 2.b, 2.c, 2.d, 2.e, 2.f, 2.g, 2.h, 2.i, 2.j)	DSS05.01 DSS05.02 DSS05.03 DSS05.04 DSS05.06	A.5, A.8
8	Cyber Incident Detection (Chapter IV.C)	Appendix I.c (3.a - 3.e)	DSS05.07	A.8.16
9	Cyber Incident Response and Recovery (Chapter IV.D)	Appendix I.c (4.a - 4.f)	N/A	A.5.24, A.5.25, A.5.26, A.5.27, A.5.28, A.5.29, A.5.30
10	Inherent Risk Assessment (Chapter V.A)	Appendix I.a	N/A	Clause 9.1
11	Cybersecurity Maturity Level	Appendix I.b, I.c	N/A	Clause 9.1

No.	Policy Content	SEOJK 29 / 2022 (KKS)	COBIT 2019 Process	ISO 27001:2022 Clause/Control
	Assessment (Chapter V.B)			

As can be seen in Table 4.11, the Cyber Resilience and Security Policy refer more to ISO 27001:2022 controls and the specific requirements of SEOJK No. 29/2022. This policy was designed as a artifact to address the specific gaps in COBIT process DSS05 and to ensure clear alignment with its corresponding regulation. The following table details how the policy addresses the specific gaps within DSS05.

Table 4.12. Cyber Resilience and Security Policy Detail on COBIT 2019 Process

No.	COBIT 2019 Process	Previous Condition	Improvement
1	DSS05		
1.1	DSS05.01	There is no gap for this subprocess	There is no improvement for this subprocess
		• No high-level enforcement to conduct encryption	• Enforcement and commitment to conduct encryption
1.2	DSS05.02	• No high-level enforcement to conduct vulnerability assessment and penetration testing	• Enforcement and commitment to conduct vulnerability assessment and penetration testing on period basis

COBIT 2019		Previous Condition	Improvement
No.	Process		
1.3	DSS05.03	• No enforcement to protect system integrity • No enforcement to block access through email and prevent phishing	• Commitment to protect system integrity • Enforcement to block malicious access through email and to prevent phishing attack
1.4	DSS05.04	• No high-level enforcement of least-privilege principle • No high-level enforcement to ensure non-repudiation aspects	• Commitment to enable least-privilege principle regarding access management • Commitment and enforcement to manage audit trail in order to ensure non-repudiation aspects
1.5	DSS05.05	There is no gap for this subprocess	There is no improvement for this subprocess
1.6	DSS05.06	• No enforcement to manage and secure document according to its sensitivity level	• Enforcement to manage and secure data and information based on its information classification

No.	COBIT 2019	Previous Condition	Improvement
	Process		
1.7	DSS05.07	There is no gap for this subprocess	There is no improvement for this subprocess

As shown in Table 4.12, the Cyber Resilience and Security Policy directly address the gaps within DSS05 by establishing a comprehensive and defined approach to security services. This artifact was designed not only fulfils the requirements of the COBIT process but also aligns directly with the specific mandates of SEOJK No. 29/2022, ensuring both best practice adoption and regulatory compliance.

These designed documentations are intended to improve XYZ Bank's IT governance process from a reactive state to a defined state. However, these documentations need to be evaluated to check whether the solutions really fit the requirements of XYZ Bank.

4.4. Evaluation

The evaluation phase was conducted to assess the quality, applicability, and potential effectiveness of the designed artifacts before their formal implementation. This was performed through an ex-ante formative evaluation with practitioners, followed by a final validation with senior stakeholders, as outlined in the research methodology.

4.4.1 Proposed Design Evaluation

An ex-ante formative evaluation was conducted through a Focus Group Discussion (FGD) with practitioners from the IT GRC team. The participants were selected based on the criteria mentioned in Chapter 3, ensuring they possessed the necessary expertise and contextual understanding to provide a credible assessment. The profiles of the FGD participants are summarized in Table 4.13.

Table 4.13. Participant of Evaluation FGD

Participants	Role	Educational Background	Relevant Experience
Participant A	Senior IT GRC Officer	Bachelor's Degree	7+ years of experience regarding IT GRC. Mainly responsible for policy management and IT risk management
Participant B	IT GRC Officer	Bachelor's Degree	5+ years of experience regarding IT GRC. Mainly responsible for policy management and regulatory liaison
Participant C	IT GRC Officer	Bachelor's Degree	5+ years of experience regarding IT GRC. Mainly responsible for fulfilment of compliance requirements and regulatory liaison

The designed artifacts were presented to the team, and the discussion was guided by the questions outlined in Chapter 3 to evaluate the artifacts against key DSR criteria with more details regarding related processes and requirements as follows.

Table 4.14. List of Question for Evaluation

ID	Criteria	Questions	SC	Related Framework
Q.01	Understandability	How clear and how easy to understand are the proposed steps, roles, and responsibilities in the proposed	1	DSR

ID	Criteria	Questions	SC	Related Framework
		design? Are there any part that are ambiguous? This includes: a. IT Governance Policy b. Cyber Resilience and Security Policy		
Q.02	Ease of Use	How much effort do you think would be required for the organization to learn and adopt this new policy? This includes: a. IT Governance Policy b. Cyber Resilience and Security Policy	1	DSR
Q.03	Usefulness	How useful will this new policy help you to perform related process in order to manage risk and fulfill compliance requirements? This includes: a. IT Governance Policy b. Cyber Resilience and Security Policy	1 & 2	DSR
Q.04	Usefulness	Are there any parts of this proposed policy that you feel	1 & 2	DSR

ID	Criteria	Questions	SC	Related Framework
		might be too lengthy or add unnecessary steps without adding value? This includes: a. IT Governance Policy b. Cyber Resilience and Security Policy		
Q.05	Feasibility	Considering the bank's current conditions including resources, tools, and culture, how feasible is it to implement and sustain this process as designed? What are the biggest potential barriers? This includes: a. IT Governance Policy b. Cyber Resilience and Security Policy	1 & 2	DSR
Q.06	Correctness & Validity	For IT Governance Policy, does its content and structure correctly align with the best practices outlined in COBIT 2019 especially EDM01, EDM03, APO01, and APO02 processes?	1 & 2	COBIT 2019 – EDM01, EDM03, APO01, and APO02
Q.07	Correctness & Validity	For IT Governance Policy, does its content and structure correctly align with the	1 & 2	DMAB – Governance Domain &

ID	Criteria	Questions	SC	Related Framework
		requirements outlined in SEOJK DMAB especially Governance and Risk Management Domain?		Risk Management Domain
Q.08	Correctness & Validity	For Cyber Resilience and Security Policy, does its content and structure correctly align with the requirements outlined in SEOJK KKS especially regarding Cyber Risk Management and Cyber Resilience Part?	1 & 2	KKS – Appendix 1.b and 1.c
Q.09	Correctness & Validity	For Cyber Resilience and Security Policy, does its content and structure correctly align with the best practices outlined in COBIT 2019 especially regarding DSS05 process?	1 & 2	COBIT 2019 – DSS05
Q.10	Effectiveness	For IT Governance Policy, how effectively does it work to achieve the objective of relevant control within COBIT 2019 especially regarding EDM01, EDM03, APO01, and APO02 processes?	1 & 2	COBIT 2019 – EDM01, EDM03, APO01, and APO02

ID	Criteria	Questions	SC	Related Framework
Q.11	Effectiveness	For IT Governance Policy, how effectively does it work to achieve the objective of relevant control within SEOJK DMAB especially regarding Governance and Risk Management Domain?	1 & 2	DMAB – Governance Domain & Risk Management Domain
Q.12	Effectiveness	For Cyber Resilience and Security Policy, how effectively does it work to achieve the objective of relevant control within COBIT 2019 especially regarding DSS05 process?	1 & 2	COBIT 2019 – DSS05
Q.13	Effectiveness	For Cyber Resilience and Security Policy, how effectively does it work to achieve the objective of relevant control within SEOJK KKS especially regarding Cyber Risk Management and Cyber Resilience Part?	1 & 2	COBIT 2019 – DSS05
Q.14	Effectiveness	For IT Governance Policy, do you think it would help XYZ Bank to achieve Level 3 Capability for EDM01, EDM03, APO01, and APO02?	1	COBIT 2019 – EDM01, EDM03, APO01, APO02

ID	Criteria	Questions	SC	Related Framework
Q.15	Effectiveness	For Cyber Resilience and Security Policy, do you think it would help XYZ Bank to achieve Level 3 Capability for DSS05?	1	COBIT 2019 – DSS05
Q.16	Effectiveness	For IT Governance Policy, do you think it would help XYZ Bank to achieve Level 2 for DMAB process such as Governance Domain and Risk Management Domain?	2	DMAB Requirements
Q.17	Effectiveness	For Cyber Resilience and Security Policy, do you think it would help XYZ Bank to achieve Level 2 for DMAB process such as Governance Domain and Risk Management Domain?	2	DMAB Requirements

As can be seen on Table 4.14, there are 17 questions to be asked for both IT Governance Policy and Cyber Resilience and Security Policy. The questions have several topics that range from the understandability, ease of use, feasibility, correctness and validity, and effectiveness. The questions also includes whether it has been designed correctly according to the related framework and regulations and also asked whether it could be used effectively to achieve its objective.

ID	Questions	Answer
Q.01	How clear and how easy to understand are the proposed steps, roles, and responsibilities in the proposed design? Are there any part that are ambiguous? This includes: c. IT Governance Policy d. Cyber Resilience and Security Policy	The practitioners confirmed that both the IT Governance Policy and the Cyber Resilience and Security Policy are clear and easy to understand.
Q.02	How much effort do you think would be required for the organization to learn and adopt this new policy? This includes: c. IT Governance Policy d. Cyber Resilience and Security Policy	The policies are considered straightforward to adopt.  Because they formalize and structure many activities that are already partially in place, the adoption would not be hard.
Q.03	How useful will this new policy help you to perform related process in order to manage risk and fulfill compliance requirements? This includes: c. IT Governance Policy d. Cyber Resilience and Security Policy	The policies are seen as useful. They directly address the identified gaps and provide a clear, documented approach to governance and security.

ID	Questions	Answer
Q.04	Are there any parts of this proposed policy that you feel might be too lengthy or add unnecessary steps without adding value? This includes: c. IT Governance Policy d. Cyber Resilience and Security Policy	The content is considered concise and value-adding.
Q.05	Considering the bank's current conditions including resources, tools, and culture, how feasible is it to implement and sustain this process as designed? What are the biggest potential barriers? This includes: c. IT Governance Policy d. Cyber Resilience and Security Policy	It is feasible with note. While the policies themselves are good, the practitioners raised specific feasibility concerns. For the IT Governance Policy, there is a concern about the lack of manpower in the GRC team to handle the increased load of regular monitoring and evaluation. For the Cyber Resilience and Security Policy, concerns were raised about the lack of 24/7 manpower for SIEM monitoring and the absence of a Data Loss Prevention (DLP) tool, which is mandated in the policy.
Q.06	For IT Governance Policy, does its content and structure correctly align with the best practices outlined in COBIT	The content and structure of the policy are correctly aligned with the best

ID	Questions	Answer
	2019 especially EDM01, EDM03, APO01, and APO02 processes?	practices and specific process activities outlined in the specified COBIT 2019 processes.
Q.07	For IT Governance Policy, does its content and structure correctly align with the requirements outlined in SEOJK DMAB especially Governance and Risk Management Domain?	The policy correctly incorporates and addresses the specific controls and requirements stipulated in the SEOJK DMAB framework for these domains.
Q.08	For Cyber Resilience and Security Policy, does its content and structure correctly align with the requirements outlined in SEOJK KKS especially regarding Cyber Risk Management and Cyber Resilience Part?	The policy's structure and content are correctly aligned with the requirement of SEOJK KKS.
Q.09	For Cyber Resilience and Security Policy, does its content and structure correctly align with the best practices outlined in COBIT 2019 especially regarding DSS05 process?	The policy correctly reflects the best practices and control objectives for the DSS05 process.
Q.10	For IT Governance Policy, how effectively does it work to achieve the objective of relevant control within COBIT 2019 especially regarding EDM01, EDM03, APO01, and APO02 processes?	The policy is deemed effective in achieving the objectives of the specified COBIT processes.

ID	Questions	Answer
Q.11	For IT Governance Policy, how effectively does it work to achieve the objective of relevant control within SEOJK DMAB especially regarding Governance and Risk Management Domain?	The policy is considered effective for meeting the objectives of the DMAB framework.
Q.12	For Cyber Resilience and Security Policy, how effectively does it work to achieve the objective of relevant control within COBIT 2019 especially regarding DSS05 process?	The policy is judged to be effective in meeting the objectives of DSS05.
Q.13	For Cyber Resilience and Security Policy, how effectively does it work to achieve the objective of relevant control within SEOJK KKS especially regarding Cyber Risk Management and Cyber Resilience Part?	The policy is viewed as an effective instrument for achieving the regulatory objectives related to cyber resilience and security as mandated by the OJK.
Q.14	For IT Governance Policy, do you think it would help XYZ Bank to achieve Level 3 Capability for EDM01, EDM03, APO01, and APO02?	The practitioners agreed that the implementation of this policy would provide the necessary documented and standardized processes to elevate the capability of these processes to Level 3 (Defined).
Q.15	For Cyber Resilience and Security Policy, do you think it would help XYZ Bank to achieve Level 3 Capability for DSS05?	Yes, the policy is expected to be effective in raising the

ID	Questions	Answer
		capability of the DSS05 process to Level 3.
Q.16	For IT Governance Policy, do you think it would help XYZ Bank to achieve Level 2 for DMAB process such as Governance Domain and Risk Management Domain?	The practitioners confirmed that the policy would provide the necessary evidence and process maturity to improve the bank's DMAB score to Level 2 for these domains.
Q.17	For Cyber Resilience and Security Policy, do you think it would help XYZ Bank to achieve Level 2 for DMAB process such as Governance Domain and Risk Management Domain?	Yes, by strengthening security controls and formalizing risk management, this policy will contribute effectively to achieving a Level 2 score in the relevant DMAB domains.

As can be seen in Table 4.15, these are the details of the evaluation's questions and correlated answer. As for IT Governance Policy, the practitioners confirmed that the documents could be understood easily and could be use easily. Thus, would be useful for XYZ Bank to adopt the policy which will improve the capability of related processes. The IT Governance Policy also has been designed correctly that aligns with COBIT 2019 framework and compliance requirements. This design also would enable XYZ Bank to achieve the intended objectives for each process. Ultimately, would improve the related processes capability to Level 3 and improve DMAB score for Governance Domain and Risk Management Domain. However, there is a note about feasibility of the policy which is highlighted that the GRC team could not execute the policy especially regarding the regular evaluation and improvement of management

system which would require more manpower from the existing team since the load is already full.

The condition is more or less the same with Cyber Resilience and Security Policy. This policy is confirmed as clear and understandable, easy to use, and would be useful for XYZ Bank to adopt this policy. Especially since the adoption of this policy would improve the fulfilment of compliance requirements. The content of the policy has been correctly designed in alignment with related framework such as COBIT 2019 and ISO 27001:2022. Thus, this policy would improve the capability of related process to Level 3 and improve DMAB score especially within Governance Domain and Risk Management Domain. Although, there is a note from the practitioners about this policy which highlights the technology that is required to be used for SIEM monitoring already existed but not supported with sufficient manpower to monitor it within 24/7 timeframe. Another concern is about the attempt of data protection that requires Data Loss Prevention (DLP) tools that is currently not implemented yet but are mandated within the policy.

From the feedback of the evaluation activity, it could be seen that the designed policy of IT Governance Policy and Cyber Resilience and Security Policy could help XYZ Bank to improve its IT governance process capability since the designed policies are understandable, easy to use, useful, correct, and effective. Although, there are some issues on the feasibility part. This result shows that the designed policy improves IT governance process capability of related COBIT 2019 processes to Level 3 (Defined) and improve the DMAB score of Governance Domain and Risk Management domain to Level 2.

4.4.2 Validation

Following the evaluation with the practitioners, a validation activity was conducted. The IT Governance Policy and the Cyber Resilience and Security Policy were presented to the Head of IT along with the feedback that has been gathered from evaluation activity with related stakeholders. The profile of Head of IT as audience of validation activity is detailed in Table 4.16 as follows.

Table 4.16. Participant of Validation Activity

Participant	Role	Educational Background	Relevant Experience
Participant D	Head of IT Department	Bachelor's degree	10+ years of experience regarding IT GRC with experience in various industries, ranging from telecommunications, consulting, financial services industry to banking. Mainly responsible providing direction, supervision and developing strategies related to the company's IT governance

The validation activity conducted with the same approach as evaluation activity that use the same list of questions as been listed within Table 4.14 with 17 questions. The overall feedback from this activity is positive for both policies.

Table 4.17. Validation Result

ID	Questions	Answer
Q.01	How clear and how easy to understand are the proposed steps, roles, and responsibilities in the proposed design? Are there any part that are ambiguous? This includes: e. IT Governance Policy f. Cyber Resilience and Security Policy	The Head of IT affirmed the evaluation from the practitioners, agreeing that both policies are well-structured, clear, and easy to understand. The language and format are consistent with the bank's standards.

ID	Questions	Answer
Q.02	How much effort do you think would be required for the organization to learn and adopt this new policy? This includes: e. IT Governance Policy f. Cyber Resilience and Security Policy	The adoption effort is considered manageable. The Head of IT agreed that because the policies formalize and build upon many existing activities, the learning curve for the operational teams would not be steep.
Q.03	How useful will this new policy help you to perform related process in order to manage risk and fulfill compliance requirements? This includes: e. IT Governance Policy f. Cyber Resilience and Security Policy	The policies were validated as being useful. The Head of IT confirmed they provide a necessary and clear framework that directly addresses the identified governance gaps.
Q.04	Are there any parts of this proposed policy that you feel might be too lengthy or add unnecessary steps without adding value? This includes: e. IT Governance Policy f. Cyber Resilience and Security Policy	The content was validated as being concise and focused.
Q.05	Considering the bank's current conditions including resources, tools, and culture, how feasible is it to implement and	It is feasible with notes. The Head of IT confirmed the policies are feasible but

ID	Questions	Answer
	sustain this process as designed? What are the biggest potential barriers? This includes: e. IT Governance Policy f. Cyber Resilience and Security Policy	highlighted two key challenges. For the IT Governance Policy, the main barrier is organizational culture; successful implementation requires commitment not just from IT but from all departments and the Board of Directors, whose awareness of IT governance importance is currently insufficient. For the Cyber Resilience and Security Policy, the concern is resource-related, specifically the cost-benefit of acquiring a Data Loss Prevention (DLP) tool. The bank may need to use compensating controls since it is not feasible yet.
Q.06	For IT Governance Policy, does its content and structure correctly align with the best practices outlined in COBIT 2019 especially EDM01, EDM03, APO01, and APO02 processes?	The alignment with the specified COBIT 2019 processes was validated as correct. The policy's content and structure accurately reflect the best practices for these governance and management objectives.

ID	Questions	Answer
Q.07	For IT Governance Policy, does its content and structure correctly align with the requirements outlined in SEOJK DMAB especially Governance and Risk Management Domain?	The policy's alignment with the OJK's DMAB framework was confirmed as correct.
Q.08	For Cyber Resilience and Security Policy, does its content and structure correctly align with the requirements outlined in SEOJK KKS especially regarding Cyber Risk Management and Cyber Resilience Part?	The Head of IT validated that the policy's content is correctly aligned with the requirements of SEOJK KKS.
Q.09	For Cyber Resilience and Security Policy, does its content and structure correctly align with the best practices outlined in COBIT 2019 especially regarding DSS05 process?	The alignment with the COBIT DSS05 process was validated as correct.
Q.10	For IT Governance Policy, how effectively does it work to achieve the objective of relevant control within COBIT 2019 especially regarding EDM01, EDM03, APO01, and APO02 processes?	The policy was deemed effective for achieving the objectives of the specified COBIT processes.
Q.11	For IT Governance Policy, how effectively does it work to achieve the objective of relevant control within SEOJK DMAB especially regarding Governance and Risk Management Domain?	The policy was validated as an effective tool for meeting the objectives of the DMAB requirements.

ID	Questions	Answer
Q.12	For Cyber Resilience and Security Policy, how effectively does it work to achieve the objective of relevant control within COBIT 2019 especially regarding DSS05 process?	The policy was judged to be effective in meeting the objectives of DSS05.
Q.13	For Cyber Resilience and Security Policy, how effectively does it work to achieve the objective of relevant control within SEOJK KKS especially regarding Cyber Risk Management and Cyber Resilience Part?	The Head of IT confirmed that the policy is an effective instrument for achieving the regulatory objectives.
Q.14	For IT Governance Policy, do you think it would help XYZ Bank to achieve Level 3 Capability for EDM01, EDM03, APO01, and APO02?	The Head of IT agreed with the practitioners' evaluation, confirming that the policy provides the necessary documented and standardized processes to elevate the capability of these processes to Level 3 (Defined).
Q.15	For Cyber Resilience and Security Policy, do you think it would help XYZ Bank to achieve Level 3 Capability for DSS05?	es, the policy was validated as being effective in raising the capability of the DSS05 process to Level 3.
Q.16	For IT Governance Policy, do you think it would help XYZ Bank to achieve Level 2 for DMAB process such as Governance Domain and Risk Management Domain?	The Head of IT confirmed that the policy would provide the necessary evidence and process maturity to improve the bank's DMAB score to

ID	Questions	Answer
		Level 2 (Satisfactory) for these domains.
Q.17	For Cyber Resilience and Security Policy, do you think it would help XYZ Bank to achieve Level 2 for DMAB process such as Governance Domain and Risk Management Domain?	Yes, the Head of IT validated that this policy will contribute effectively to achieving a Level 2 score in the relevant DMAB domains.

Table 4.17 above presents the results of the final validation activity, which was conducted with the Head of the IT Department. This session served to confirm the findings from the earlier practitioner evaluation and to secure senior management's endorsement of the designed artifacts.

From the discussion regarding IT Governance Policy, the audience affirmed the evaluation result regarding all aspect. This includes the understandability, ease of use, and usefulness aspect of the policy. The correctness of the policy regarding related framework such as COBIT 2019 and compliance requirements are affirmed altogether with the effectiveness of the policy. The audience also agrees with the evaluation result that with this policy, XYZ Bank's processes capability would improve to Level 3 and also the score of DMAB especially related to Governance Domain and Risk Management Domain. However, the audience also highlight another concern beside the feasibility of the policy regarding the lack of manpower which is the feasibility of process execution and endorsement within corporate level. It was mentioned that to enact this policy, the IT team could not be the only one who is committed. But rather, it takes the commitment of all department and all Board of Directors to ensure this policy would be executed properly. Meanwhile, the awareness of other department and Board of Directors are deemed insufficient regarding the importance of IT governance.

However, the same concern was not mentioned for Cyber Resilience and Security Policy. The audience also affirmed the evaluation result about the understandability,

ease of use, usefulness aspect of the policy. Along with the correctness of the content and effectiveness of the policy which in turn would improve the capability level of related process to Level 3 along with the fulfilment of compliance requirement. The note of this policy is more focused on the cost-benefit analysis to implement security controls such as DLP tools which currently calculated as not a fit solution considering the analysis and the data protection process would be mitigated with other compensating control. Thus, XYZ Bank could do the related processes, but it will be conducted with best effort approach.

The validation concluded with a formal endorsement from the Head of the IT Department for the adoption of the designed policies. This final approval confirms that the designed artifact is technically feasible with some notes. Thus, it could be concluded that the two success criteria that has been defined within Chapter 2 are achieved through this research. This successfully concludes the design and evaluation cycle of the research.

