

CHAPTER 3 – RESEARCH METHODS

3.1. Research Framework

According to Recker (2021), research that is more focused on understanding a particular phenomenon within a specific context to uncover a condition with a complex and comprehensive view is considered as qualitative research. This qualitative research will be conducted using the following research framework:

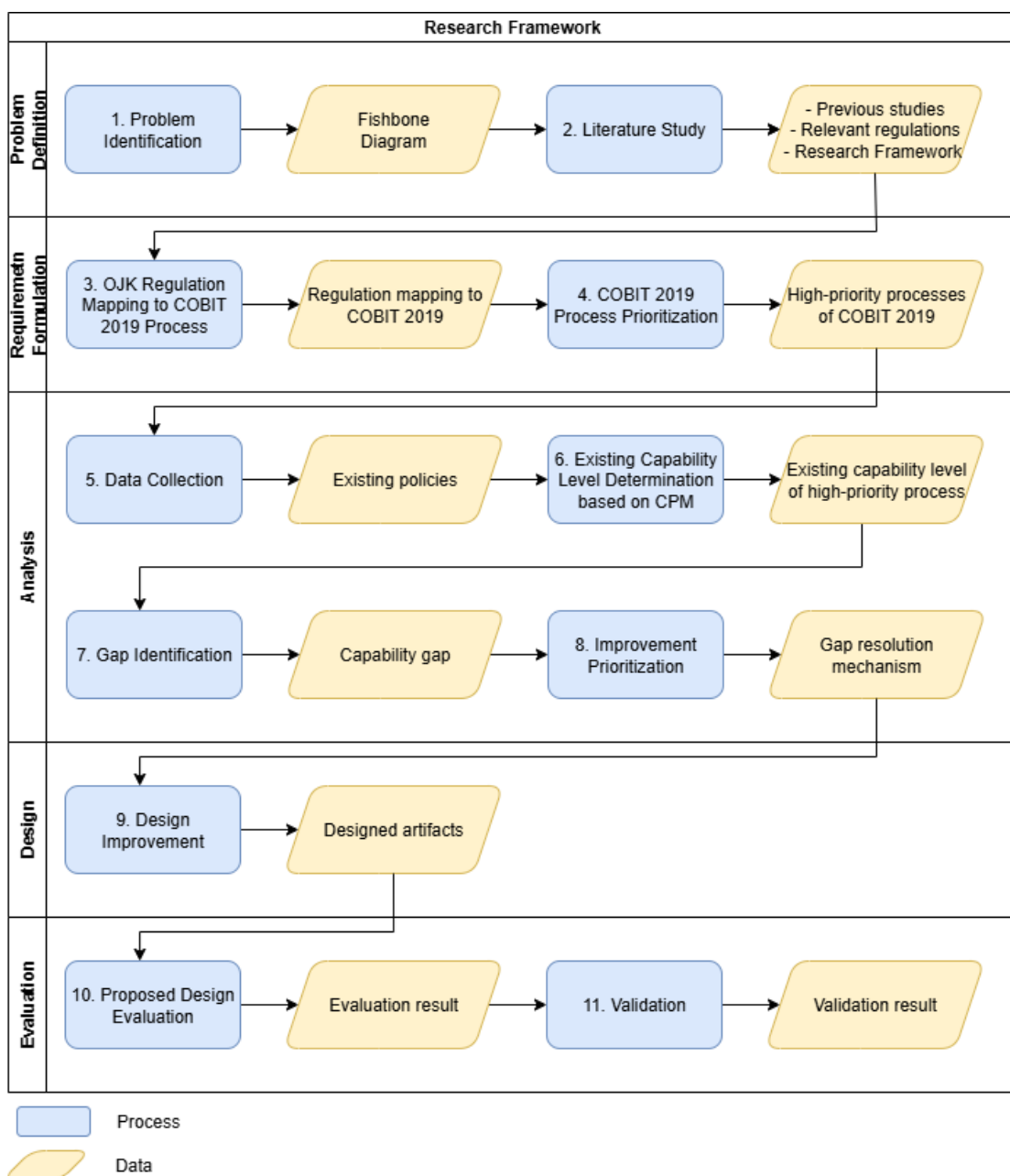


Figure 3.1. Research Framework

As can be seen in Figure 3.1, there are five phases within this research such as Problem Definition phase, Requirement Formulation phase, Analysis phase, Design phase, and Evaluation phase. The Problem Definition phase consists of problem identification and literature study activities. It will be followed by Requirement Formulation phase which focuses on mapping related regulations to COBIT process and prioritization of COBIT processes that are going to be assessed. Then, Analysis phase consists of data collection activity, existing capability level determination activity, gap analysis activity, and improvement prioritization activity. Next phase would be Design phase that is meant to design improvement within the research. The last phase would be Evaluation phase that includes proposed design evaluation and validation. Details of each phase and activity would be explained further in the following subchapters.

3.2. Problem Definition

The first phase in this research is to identify and define the problem at XYZ Bank. This is done by identifying problem and literature study to ground the research in existing theory.

3.2.1 Problem Identification

The first activity of this research is to identify problem within XYZ Bank. To identify problem, it is required to conduct documentation study and interviews to understand the issues occurring within XYZ Bank. The activity conducted within this stage involves root cause analysis using a fishbone diagram. The results of the problem identification are then formulated into relevant research questions.

3.2.2 Literature Study

The next activity is the literature study. This activity is conducted based on previously formulated research questions. The activity begins with searching for relevant past studies through research databases such as IEEE, ScienceDirect, Elsevier, and Google Scholar, covering the period from 2019 to 2024 using keywords like “Digital Banking,” “IT Governance,” “IS Governance,” “COBIT,” “ISO 38500,” and others. Relevant studies are then analyzed using the strength and weakness method. The summary or findings from the literature review serve as a reference in conducting the research, including research framework and methodology.

3.3. Requirement Formulation

The focus of this phase is to translate the compliance requirement of XYZ Bank to map to COBIT 2019 processes. This mapping would result in process prioritization that will be used as basis for the next phase.

3.3.1 Regulation Mapping to COBIT Process

The first activity within Requirement Formulation phase is regulation mapping to COBIT process. The mapping formulation will be based on the COBIT 2019 framework. However, not all of the process within COBIT 2019 will be used within the research. There will be prioritization of the processes to ensure alignment between framework with bank requirements by mapping compliance requirements from related regulations with COBIT governance and management objectives.

All of the identified regulations within Chapter 2 including OJK No. 11/POJK.03/2022 on The Implementation of Information Technology by Commercial Bank, SEOJK No.11/POJK.03/2017 on The Application of Risk Management in The Use of Information Technology by Commercial Banks, SEOJK No. 24/SEOJK.03/2023 on Digital Maturity Assessment of Bank, and SEOJK No. 29/SEOJK.03/2022 on Cyber Resilience and Security of Commercial Banks will be analyzed thoroughly. Each of the regulations would be analyzed thoroughly for each chapter, verse, or part and will be mapped to COBIT process to find out whether there is any relevancy.

3.3.2 COBIT Process Prioritization

Following the mapping of regulatory requirements to COBIT 2019 processes, the next activity is to prioritize the processes that will be the focus of the assessment. Since the mapping for each regulatory requirement could produces different mapping of COBIT 2019 process, a comprehensive mapping that considers all of the regulation mapping is needed. This will be done by compiling and consolidating all the relevant COBIT 2019 processes from each regulation mapping. The result of the compilation across mapping will be taken as the relevant COBIT 2019 processes.

However, not all of the relevant processes would be taken within this step. The relevant process then would be prioritized further by considering how often or how frequent the related process is required and highlighted by related regulations. The more the process

is mentioned means that the process is becoming more important from compliance requirement point of view. Thus, the process that is required by all of the process would be taken as the prioritized COBIT 2019 processes. These prioritized processes then will be used in later activity for analysis phase.

3.4. Analysis

The analysis phase is designed to assess the exiting condition of IT governance at XYZ Bank especially related to process and activity part of IT governance mechanism and comparing it to the prioritized COBIT 2019 processes. This phase also involves collecting data, determining the existing process capability levels, identifying gaps, and prioritizing these gaps for improvement.

3.4.1 Data Collection

To gain a comprehensive understanding of the existing IT governance process and activities at XYZ Bank, this research will employ a mixed-method approach for data collection. The following two techniques will be used:

- 1. Documentation Study**

An in-depth review of existing internal documents will be performed. Internal documents include current IT policies and procedures. This study will provide objective evidence of the processes and identify whether there is any gap between documentation and practice.

- 2. Interviews**

Semi-structured interviews will be conducted with key stakeholders from XYZ Bank. The interviews will aim to gather qualitative data on current IT governance processes, roles, and responsibilities. Interviews were conducted with the head of the Information Technology Department and three staff members from the department.

3.4.2 Existing Capability Level Determination Based on CPM

Once the data is collected, it will be analyzed to determine the current capability level of each prioritized COBIT process. This research will use the COBIT Performance Management from COBIT 2019, which is based on the CMMI framework. Each

process will be assessed against the activities and goals defined in COBIT 2019 for capability levels 0 through 5 as explained further on Chapter 2.3.1 regarding Capability Maturity Model Integration.

A working paper that has been designed in the form of a structured questionnaire will be used based on the specific practices of each prioritized COBIT process. The collected evidence from documentations and review will be used to answer the questionnaire and assign a rating for each process practice. The rating scale described in the COBIT 2019 (Fully achieved, Largely achieved, Partially achieved, or Not achieved) will be used to determine the capability level of each process that has been achieved by XYZ Bank. The final output of this activity would be a determined capability level (from 0 to 5) for each prioritized process. This output of capability level would represent the existing condition or usually called as "as-is" condition of IT governance at XYZ Bank.

3.4.3 Gap Identification

The next step would be gap identification activity. This activity involves comparing the existing condition of process capability with the targeted capability or usually called as "to-be" state that is required by XYZ Bank.

As mentioned within the research objectives the target capability for the prioritized processes is Level 3 (Defined). This target is selected based on a analysis of the CMMI-based capability model within COBIT 2019 and its correlation to XYZ Bank's problem.

CMMI's concept of capability levels represents process maturity. The current issues at XYZ Bank include but are not limited to unestablished processes, incomplete IT-related policies, and lack of risk oversight. These issues are characteristic of processes at lower capability levels. A Level 1 (Initial) process is ad-hoc and disorganized which means a process may be or may not be conducted and achieve its intended purposes. A Level 2 (Managed) process achieves its purpose. However, in achieving its purpose a Level 2 process is often done reactively and dependent on individual skills and competence rather than on institutionalized practices within an organization. Although a Level 2 process may appear to be functional, the execution of the process is not repeatable and could be vulnerable to human error or changes in personnel.

In order to overcome the challenges that XYZ Bank faces, the organization must advance to Level 3 (Defined). According to the COBIT framework, a Level 3 process means that the process achieves its intended purposes in organized and well-defined way. This means that there's a need to transition from relying on individuals to relying on documented and standardized processes. Therefore, reaching Level 3 is the minimum acceptable state to transform XYZ Bank's governance from a reactive, unstable environment to one that is proactive, controlled, and aligned with enterprise requirements.

The gap will be identified by pinpointing which process practices required to achieve Level 3 are not currently being met or are only partially met. The results of this analysis will be documented. This list of gaps will form the direct input for the design improvement phase.

3.4.4 Improvement Prioritization

Although the previously identified gaps must be addressed to reach the target capability level, not all gaps present the same level of urgency or importance to the organization. Adopting the philosophy of risk response as mentioned within Chapter 2.3.1, each identified gap can be viewed as a risk. This means that the improvement that is designed to close these gaps are considered as risk responses. This perspective allows that initiatives might not be done altogether at the same time but could be prioritized based on their ability to deliver the greatest value in risk reduction for a given cost and time.

The input of this activity would be gap identification result. The gap then would be prioritized through a Focus Group Discussion (FGD) with related stakeholders. Thus, the output of this activity will be a prioritized roadmap for the design phase.

3.5. Design

The design phase focuses on creating the primary artifact of this research: an improved IT governance framework for XYZ Bank. This artifact will consist of a set of policies, standards, and procedures designed to close the gaps identified in the analysis phase.

3.5.1 Design Improvement

As established in Chapter 2, IT governance is implemented through a combination of structures, processes, and relational mechanisms. Considering that the fact that this research is conducted based on root causes analysis that identified several problems and has defined the research focus to process-related issue such as incomplete IT-related policies and unestablished governance process. This activity of design improvement would focus on improving the process mechanism of IT governance at XYZ Bank.

The design of the improvement artifact will therefore be based on the prioritized gap identification results. For each identified gap, a corresponding solution will be designed by referencing the best practices detailed in the COBIT 2019 framework and the ISO/IEC 27001:2022 standard. The design will be tailored to the specific context of XYZ Bank considering its existing organizational structure, technology stack, and related constraints.

The output of this activity would be a set of proposed documents that meant to improve process mechanism including IT governance policy, standard, or procedures. The proposed design will serve as a comprehensive solution to improve XYZ Bank's IT governance to the target capability level.

3.6. Evaluation

The evaluation phase means to ensure the designed artifact is effective and fit for purpose. This research will use a two-step process involving an initial evaluation of the proposed design followed by a validation with stakeholders.

3.6.1 Proposed Design Evaluation

Evaluation will be conducted to assess whether the proposed design theoretically achieves the research objectives. This research will use an ex-ante formative evaluation method, as mentioned within Chapter 2.4 regarding Design Science Research. This evaluation approach could assess the artifact's potential effectiveness prior to the implementation. The evaluation will be conducted through a Focus Group Discussion (FGD) with practitioners from the IT team regarding the proposed design.

The participants for the FGD will be selected based on a set of criteria designed to ensure they possess the necessary expertise and contextual understanding. The selection criteria are detailed in Table 3.1.

Table 3.1. Participant Criteria for Evaluation

Criteria	Description
Role	IT GRC Executive
Experience	Minimum five years of experience
Domain Expertise	Experience in the fields of IT Governance, Risk Management, and Compliance

These criteria are designed to select a group of experts who are capable and have the capacity to evaluate the proposed artifact within XYZ Bank. As the individuals that match the criteria have the responsibility to create, maintain, and manage the lifecycle of IT-related document such as IT policies, standards, and procedures. Thus, their experience combined with their responsibilities would be a fit to evaluate the design that has been proposed.

The FGD would be conducted by assessing the designed policies and procedures. The qualitative data gathered from audience's responses to the questions in Table 3.2 will then be analyzed. This analysis will determine if the proposed design is likely to be successful. The success of the artifact will be judged by this research using two key indicators:

1. The simulated capability level for the prioritized processes reaches Level 3 (Defined) (SC1).
2. The simulated score for the Governance domain and Risk Management domain in the Digital Maturity Assessment for Banks (DMAB) improves to Level 2 (Satisfactory) (SC2).

These success criteria were chosen to proof that the proposed design could really improve XYZ Bank's IT Governance posture. Furthermore, it could be break down that the first success criteria (SC1) is selected to demonstrate improvement of process maturity. As explained in the gap identification activity, achieving Level 3 means shifting a process that is ad-hoc or dependent on specific personnel to a process that is defined and documented. Thus, achieving Level 3 is addressing the root causes of inconsistent execution and lack of oversight at XYZ Bank.

The second success criteria (SC2) is chosen because it could demonstrate an improvement in IT governance of XYZ Bank from the perspective of regulatory requirements. The OJK has mandated through POJK No. 11/2022 about The Implementation of Information Technology by Commercial Bank and SEOJK No. 24/2023 about Digital Maturity Assessment of Bank, that all commercial banks should conduct an annual self-assessment of their digital maturity using the DMAB framework. This framework is used by OJK to measure the quality and adequacy of a bank's IT governance. Within DMAB, there are several domains to be assessed, including Governance domain and Risk Management domain. Therefore, demonstrating an improved score within this framework would also provide proof of improvement of IT governance and with the same time improving fulfilment of compliance requirements. The target level 2 (Satisfactory) itself derived since the existing score of XYZ Bank within those domains are level 3 (Fair).

To guide the FGD and ensure all DSR evaluation criteria are addressed, the discussion will be structured around the questions detailed in following table.

Table 3.2. Evaluation FGD List of Question

No	Criteria	Questions	SC	Related Framework
1	Understandability	How clear and how easy to understand are the proposed steps, roles, and responsibilities in the proposed design? Are	1	DSR

No	Criteria	Questions	SC	Related Framework
		there any part that are ambiguous?		
2	Ease of Use	How much effort do you think would be required for the organization to learn and adopt this new process?	1	DSR
3	Usefulness	How useful will this new policy help you to perform related process in order to manage risk and fulfilling compliance requirements?	1 & 2	DSR
4	Usefulness	Are there any parts of this proposed policy that you feel might be too lengthy or add unnecessary steps without adding value?	1 & 2	DSR
5	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?	1 & 2	DSR
6	Correctness & Validity	For [related policy document], does its content and structure correctly align with the best practices outlined in [relevant	1 & 2	Related regulations or framework

No	Criteria	Questions	SC	Related Framework
		framework: regulations, COBIT Process ID, and/or ISO 27001:2022 controls]?		
7	Effectiveness	For [related policy document], how effectively does it work to achieve the objective of relevant control [relevant framework: regulations, COBIT Process ID, and/or ISO 27001:2022 controls]?	1 & 2	Related regulations or framework
8	Effectiveness	For [related policy document] and all the process within, do you think it would help this company to achieve Level 3 Capability for [specific COBIT 2019 process]?	1	COBIT 2019
9	Effectiveness	For [related policy document] and all the process within, do you think it would help XYZ Bank to achieve Level 2 for DMAB process such as [specific DMAB requirements]?	2	DMAB Requirements

The question that has been listed within Table 3.2 will be asked and the feedback from the audience would be recorded and assessed as the result of the evaluation regarding the proposed design to evaluate whether the proposed designs work effectively and achieve the defined success criteria or not.

3.6.2 Validation

Following the formative evaluation of the proposed design by the practitioners, there will be validation activity to be conducted. This activity meant to present the designed artifacts and the results from the initial evaluation to management. This validation serves as a final check to confirm that the proposed solution is correct, applicable, feasible, and could be adopted further for formal endorsement.

The validation will be performed through a one-on-one presentation and interview session with related stakeholder. The inputs for this session will be the complete set of designed artifacts (the proposed policies) and concerns that have been gathered within the evaluation activity.

The participant for this validation will be selected based on their strategic oversight and decision-making authority, as detailed in the criteria below.

Table 3.3. Participant Criteria for Validation

Criteria	Description
Role	Head of IT
Experience	Minimum ten years of experience
Domain Expertise	Experience in the fields of IT Governance, Risk Management, and Compliance

As can be seen on Table 3.3., the audience of validation would be Head of IT with relevant expertise and experience. This interview would use the same set of questions as evaluation criteria which has been explained within Table 3.2. The outcome of this validation will be a final decision on the acceptance of the proposed design.