

CHAPTER 2 – LITERATURE REVIEW

This chapter explains the literature review of this research proposal. It includes references of concepts, related frameworks, and previous studies regarding this topic.

2.1. Digital Banking

Up until now, the Information and Communication Technology field has advanced significantly. This advancement could take form such as improvement of electronics, computers, and communication technology (Har et al., 2022). The improvement of these technologies provides convenience on the level that it could shift people's behavior and lifestyle (Widjaja et al., 2024). One of the shifts in behavior and lifestyle is the way business is conducted (Ma & Gu, 2024).

Digital transformation in the banking industry has allowed banks to provide services to their customers through numerous channels, such as mobile banking and internet banking, to conduct financial activities without having to directly access the bank. This change in the nature of business allows banks to provide services closer to customers, communicate better, and build a closer relationship with their customers (Bankuoru Egala et al., 2021).

Investment in technology is required in order for an organization to have a digital transformation. Some of the technologies are sophisticated such as Internet of Things (IoT) to connect set of devices into an integrated system, Artificial Intelligence (AI) and Machine Learning (ML) to mimic human intelligence, advanced robotics to use semi-autonomous system, cloud technology to remodel and provide platform as a service, blockchain to share data between users, and big data analytics to provide insight and assist in decision making (Sardjono et al., 2024).

According to Shrivastava et al. (2023), these technologies could have its own use cases in the context of digital banking, such as improvement of customer service operations through electronic and mobile banking, enabling Artificial Intelligence (AI) and Machine Learning (ML) to analyze and develop personalized products related to banking and investment, improvement of the legacy system to increase agility, and

enhancement of the fraud analysis and detection system using AI and ML. Through properly managed digital transformation, banks could benefit from improved customer experience, save time and cost which ultimately leads to increased operational efficiency, improve the organization to take decisions based on insights, facilitate innovation, and assist the organization to comply with regulatory requirements.

The advantages of digital banking are not only experienced by the bank but by their customers as well. Through ubiquitous platforms such as mobile banking and internet banking, customers may access their money deposits, conduct withdrawals, transfer money, check their savings, manage their account, apply for financial product, pay bills, and access other additional features (Goumeh & Barforoush, 2021). These services, which are provided with 24/7 availability, provide benefits to customers such as ease of use, accessibility, cost-efficiency, and availability, along with promoting financial inclusion (Bt Shafee et al., 2022; Goumeh & Barforoush, 2021; Harjanti et al., 2019).

2.1.1 XYZ Bank

XYZ Bank is a bank that began as a conventional bank founded in Indonesia back in 1957. In order to expand its line of business, XYZ Bank conducted a share sale and was acquired by a financial technology company in 2021. After this transition, XYZ Bank underwent a digital transformation that enabled it to shift its prior conventional business model into a digital business model. To support this shift, XYZ Bank launched its mobile banking in 2023 (XYZ Bank, 2023).

As a bank, XYZ Bank conducts several activities such as collecting funds from public in the form of deposits, savings, or equivalents forms, provide loans or credits, issuing debts acknowledgement, transferring money, providing financing based on profit sharing, and digital savings.

In 2024, XYZ Bank experienced an IT incident that disturbs the business. The incident itself has been identified, mitigated, and resolved promptly, which could minimize the losses. However, mitigating the issue itself is not enough. According to the regulation of OJK, there are steps of communication, reporting, and escalation that are supposed to be done in due time. Failure to do so will lead to formal reprimand or other sanctions. Unfortunately, XYZ Bank failed to report to communicate, report, and escalate to

relevant stakeholders and received formal reprimand from OJK that highlighted XYZ Bank's weakness in incident management and compliance processes.

This incident reflected the exiting condition of XYZ Bank's IT governance which is underdeveloped. Also, emphasizing the need for improvement on IT governance to mitigate future risks by considering organizations' needs and conditions.

Considering XYZ Bank's needs and conditions requires a structured and comprehensive IT governance documentation framework. At XYZ Bank, this framework is organized into a clear three level such as: (1) Policy; (2) Guidelines; and (3) Procedure.

At the highest level, there is Policy. This serves as the highest internal regulation. It outlines the fundamental principles and commitments of the Bank on a particular subject. A Policy sets the strategic direction for the entire organization. Its authority is highlighted by the requirement for approval from both the Board of Directors and the Board of Commissioners. This approval mechanism highlights the highest level of XYZ Bank's commitment by making the policy binding and its enforcement a top priority across the Bank. Consequently, a Policy scope is universal, with company-wide applicability to all employees, units, and functions without exception.

The more detailed level of policy would be Guidelines. This document provides more detailed guidance on how to implement the principles established in a policy. Although a Guidelines is more detailed than a policy, it is not as granular as a step-by-step procedure. Its applicability is therefore more focused, typically limited to certain functions or a group of related departments, providing a consistent framework for implementation within those defined boundaries.

The most technical level of policy is the Procedure. This document provides detailed, sequential, and action-oriented instructions that dictate exactly how a specific task must be performed. A Procedure is specifically focus with its scope is narrowly defined, with applicability focused on a specific unit, team, or department responsible for carrying out the task. Since it is focused on operational level, a Procedure only requires approval from the relevant Head of Department.

Furthermore, an analysis of XYZ Bank's internal documents reveals a standardized format for creating these regulations, ensuring consistency and clarity. Regardless of the hierarchical level, a typical governance document at the Bank includes the following structural components:

- a. Chapter I – Introduction: This chapter contains sub-sections for background of the policy, objective of the policy, scope of the policy, reference both regarding regulations and framework that are referred to for related documents, and definitions.
- b. Chapter II – Roles and Responsibilities: This chapter highlight relevant roles that are involved within the policy along with each role and responsibilities within that policy.
- c. Chapter III - Content: This chapter consists of the detail of the substance of the policy.
- d. Closing Chapter: This chapter concludes the policy and mentions the applicability of the policy, supersedes of another policy (if any), and the review cycle of the policy.
- e. Appendices: Contains supplementary materials like forms or templates.

2.2. Indonesia Banking Regulations

Banking industry requires special attention and consideration due to its potential impact on a country's economy. Therefore, banking industry is generally regulated by a set of regulations established by each country's regulatory body (Osei et al., 2023). In Indonesia, there are two regulatory bodies that oversee and regulates banking industry. They are Bank Indonesia and the Otoritas Jasa Keuangan (Indonesia's Financial Services Authority).

According to Pikahulan (2020), Bank Indonesia has the following responsibilities: (1) establishing and implementing monetary policy; (2) regulating and ensuring the smooth operation of the payment system; and (3) regulating and supervising banks. In this

regard, Bank Indonesia conducts regulation and supervision from a macroprudential perspective, as explained in the Article 7 of the UU No. 21 Tahun 2011 about OJK regarding the duties and authorities of Bank Indonesia.

On the other hand, Otoritas Jasa Keuangan is established and defined as an independent institution to carry out its responsibility to supervise the performance of financial institutions, including banks (Pikahulan, 2020). Regulation and supervision of banking institutions include: (1) licensing for bank establishment, branch office openings, articles of association, business plans, ownership, management and human resources, mergers, consolidations, bank acquisitions, and revocation of bank business licenses; and (2) bank business activities. Regulation and supervision of bank soundness cover: (1) liquidity, profitability, solvency, asset quality, minimum capital adequacy ratio, maximum credit exposure, loan-to-deposit ratio, and bank reserves; (2) bank reports related to financial performance; (3) debtor information systems; (4) credit testing; and (5) bank accounting standards. Regulation and supervision of banking prudential aspects include: (1) risk management; (2) bank governance; (3) Customer due diligence and anti-money laundering principles; and (4) prevention of terrorism financing and banking crimes.

Based on the regulatory and supervisory responsibilities of each regulatory body, it can be concluded that Otoritas Jasa Keuangan is the regulator responsible for overseeing governance and risk management in banks. In exercising this authority, the Otoritas Jasa Keuangan has issued various regulations to ensure the implementation of prudential principles by banks. These regulations include POJK No. 11/POJK.03/2022 on The Implementation of Information Technology by Commercial Banks, 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.

2.2.1 POJK No. 11/POJK.03/2022 on The Implementation of Information Technology by Commercial Bank

This regulation was issued by the OJK to support the digital transformation of Indonesia's banking sector by refining regulations that cover data, technology, risk management, collaboration, and institutional structure. Through the existence of POJK about The Implementation of Information Technology by Commercial Banks, it is expected that the resilience and operational maturity of commercial banks could be enhanced in all aspects of information technology management and operations.

This regulation consists of 14 Chapters, with the following substantive content: (1) Chapter I – General Provisions; (2) Chapter II – Bank IT Governance; (3) Chapter III – Bank IT Architecture; (4) Chapter IV – Application of Risk Management in Bank IT Operations; (5) Chapter V – Bank Cyber Resilience and Security; (6) Chapter VI – The Use of IT Service Providers in Bank IT Operations; (7) Chapter VII – Electronic System Placement and IT-Based Transaction Processing; (8) Chapter VIII – Data Management and Personal Data Protection in Bank IT Operations; (9) Chapter IX – Provision of IT Services by Banks; (10) Chapter X – Control and Internal Audit in Bank IT Operations; (11) Chapter XI – Reporting; (12) Chapter XII – Digital Maturity Assessment of Bank; (13) Chapter XIII – Transitional Provisions; and (14) Chapter XIV – Closing Provisions (Otoritas Jasa Keuangan (OJK), 2022a).

This regulation acts as an update to the previous regulations, that are POJK 38/POJK.03/2016 and POJK 13/POJK.03/2020, which governed The Application of Risk Management in The Use of Information Technology by Commercial Banks. Both regulations were revoked upon the enactment of this regulation.

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

Surat Edaran Otoritas Jasa Keuangan (SEOJK) No. 11/POJK.03/2017 is a derivative regulation of POJK 38/POJK.03/2016, providing more technical implementation guidelines for its parent regulation. Although POJK 38 has been revoked and declared no longer in effect, this circular letter remains a technical reference for implementing

IT risk management, as it is still relevant to the latest regulation, POJK 11/POJK.03/2022.

The key topics that are covered in SEOJK 11 include: (1) General provisions; (2) Guidelines for risk management in the use of information technology; (3) Reporting; (4) Approval requests; and (5) Closing provisions. In point (b), Guidelines for Risk Management in the Use of Information Technology, the regulation establishes the minimum requirements for policies, standards, and procedures related to the use of information technology that banks must have. These aspects include management (including IT risk management processes), development and procurement, IT operational activities, communication networks, information security, disaster recovery planning, electronic banking services, the use of IT service providers, and the provision of IT services by banks (Otoritas Jasa Keuangan (OJK), 2017).

2.2.3 SEOJK No. 24/SEOJK.03/2023 on Digital Maturity Assessment of Bank

SEOJK No. 24/SEOJK.03/2023 is a derivative regulation of POJK 11/POJK.03/2022 on The Implementation of Information Technology by Commercial Banks. This SEOJK sets out the implementation provisions for assessing the digital maturity level of banks, as defined in Chapter XII of POJK 11 of 2022.

The key topics covered in this SEOJK include: (1) General provisions; (2) Self-assessment of the bank's digital maturity level; (3) Reporting; and (4) Closing provisions. There are seven aspects/domains assessed in a bank's digital maturity evaluation such as: (1) governance; (2) architecture; (3) risk management; (4) technology; (5) data; (6) collaboration, and (7) consumer protection. Each aspect/domain is further divided into subdomains, which are then broken down into several controls with predefined fulfillment criteria as stipulated in the SEOJK. Additionally, this SEOJK provides a working paper for assessing the quality of digital maturity implementation in banks, along with guidelines on how to use the working paper (Otoritas Jasa Keuangan (OJK), 2023).

Furthermore, the matrix for determining the quality of digital maturity implementation is also regulated in this SEOJK. The maturity matrix is divided into five levels: Level 1, Level 2, Level 3, Level 4, and Level 5. These levels could be explained further as follows:

1. Level 1: Strong

This level of achievement depicts that related aspects or domain have very adequate quality. Although there might be some minor weaknesses or issues, those issues are insignificant and could be ignored.

2. Level 2: Satisfactory

This level of achievement depicts that related aspect or domain have adequate quality. Although there might be minor weaknesses or issues, those issues could be resolved within normal business process.

3. Level 3: Fair

This level of achievement depicts that related aspect or domain have fairly adequate quality. Although the minimum requirements are fulfilled, there are some weaknesses or issues that need attention and consideration of management.

4. Level 4: Marginal

This level of achievement depicts that related aspects or domain have lacking quality. There are significant weaknesses or issues that require immediate attention and corrective control.

5. Level 5: Unsatisfactory

This level of achievement depicts that related aspects or domain have inadequate quality. There are significant weaknesses or issues that require immediate attention and corrective control, however these issues are beyond the capability of management.

Bank are required to conduct the assessment annually, as defined within this SEOJK.

The results of the digital maturity assessment must be reported to the OJK.

2.2.4 SEOJK No. 29/SEOJK.03/2022 on Cyber Resilience and Security of Commercial Banks

SEOJK No. 29/SEOJK.03/2022 is a derivative regulation of POJK 11/POJK.03/2022 on The Implementation of Information Technology by Commercial Banks. This SEOJK sets out the implementation provisions for cyber resilience and security for commercial banks, as stipulated in Chapter V of POJK 11 of 2022.

The key topics covered in this SEOJK include: (1) General provisions; (2) Inherent risk assessment related to cybersecurity; (3) Implementation of risk management related to cybersecurity; (4) Implementation of cyber resilience processes for commercial banks; (5) Cybersecurity maturity level assessment; (6) Cybersecurity-related risk levels; (7) Cybersecurity testing; (8) Unit or function responsible for bank cyber resilience and security; (9) Bank cyber incident reporting; and (10) Closing provisions (Otoritas Jasa Keuangan (OJK), 2022b).

2.3. IT Governance

The terminology became known in the academic world in the 1990s, with research on the subject initiated by Loh and Venkatraman in 1992 (De Haes et al., 2020). IT Governance is a framework designed to align IT with business strategy, aiming to ensure that IT investments enhance business value (Dutta et al., 2022). On the other hand, Legowo & Christian (2019) on their research argues that IT Governance is a structure of relationships and processes that guide an organization in achieving its objectives by adding value to the use of information technology while managing its associated risks.

Expanding on this, IT Governance is also considered an important part of corporate governance. It consists of the leadership, organizational structures, and processes that ensure an organization's IT sustains and achieve its strategies and objectives (De Haes et al., 2020).

In order to implement IT Governance effectively, organizations employ a combination of mechanisms, which can be categorized into three main types: structures, processes, and relational mechanisms (Van Grembergen et al., 2004).

The first mechanism is Structures. This mechanism refers to formal organization and roles responsible for making IT decisions and ensuring accountability (Borja et al., 2022). This includes the existence of dedicated functions and committees, such as an IT steering committee at the executive level to oversee major projects and manage priorities. The formal definition of roles, such as the Chief Information Officer (CIO) being part of the senior executive team is also important (Van Grembergen et al., 2004). These structures provide the formal authority to ensure that IT decisions are made in a transparent and controlled manner, along with the involvement of the right stakeholders from both business and IT.

The second mechanism is Processes. This mechanism focuses on formal procedures for strategic IT decision-making, execution, and monitoring, which involve creating policies and all necessary documentation to manage IT (Borja et al., 2022). These mechanisms ensure that IT activities are managed consistently and in alignment with business objectives. This includes strategic information systems planning, IT portfolio and investment management, performance measurement, and risk management. To guide these activities, organizations often adopt established frameworks such as COBIT and ITIL. COBIT could be used since it provides a comprehensive framework that outlines what needs to be done by defining key IT processes and control objectives. On the other hand, ITIL framework could complement COBIT by providing detailed guidance on how to implement specific processes, particularly in the area of IT service management (Van Grembergen et al., 2004). The use of such frameworks helps standardise processes and ensures they are repeatable and measurable.

The last mechanism of IT Governance is Relational mechanisms. This mechanism is the less formal, but still important. Relational mechanisms facilitate collaboration, communication, and shared understanding between business and IT stakeholders (Van Grembergen et al., 2004). The goal is to bridge the gap between business and IT, fostering a true partnership and creating a proper environment to reach common objectives (Borja et al., 2022). This is achieved through active participation from

stakeholders in various committees, strategic dialogue, shared learning through cross-training or job rotation, and fostering a culture where IT is viewed as a business enabler (Buchwald et al., 2014). Effective relational mechanisms are essential for building trust and ensuring that IT solutions are well-aligned with actual business needs.

The primary focus of IT Governance is to deliver value from IT investments while managing the associated risks. This is typically addressed across five key IT governance domains. The first domain is Strategic Alignment domain that focuses on ensuring a strong link between the business strategy and the IT strategy, so that IT plans directly support business goals. The second domain would be Value Delivery, which is concerned with making sure that IT delivers the promised benefits and optimizes the return on IT investments. The third domain is Risk Management domain. This domain addresses the identification and mitigation of IT-related risks, safeguarding assets and ensuring business continuity to preserve value. The next domain is Resource Management domain that involves optimal investment in and proper management of critical IT resources, including infrastructure, applications, and people. Finally, Performance Measurement domain which tracks and monitors the performance of IT through metrics to ensure accountability and demonstrate success (Borja et al., 2022; Van Grembergen et al., 2004).

The adoption of IT governance mechanisms has a direct and positive influence on these core domains (Borja et al., 2022). For example, establishing a formal IT steering committee (a structure) and implementing a portfolio management system (a process) would improve Strategic Alignment and Value Delivery domain by ensuring that IT projects are selected based on business priorities and their potential to create value. Similarly, strong relational mechanisms, such as regular meetings between IT and business team would enhance Strategic Alignment by fostering a shared understanding of goals and challenges.

Ultimately, improving performance within these domains leads to higher IT governance effectiveness and delivers benefits to the organization. When IT is strategically aligned with the business, investments are more likely to support growth and asset utilization. Effective Value Delivery ensures that these investments yield a positive return, while robust Risk Management protects the organization from IT-related threats, preserving

business value. This improved governance leads to a more efficient and effective IT organization that is better able to support business needs, which can translate into significant competitive advantages, such as a higher return on assets compared to competitors with less mature IT governance (Buchwald et al., 2014).

2.3.1 COBIT 2019

COBIT is a framework for the governance and management of information and technology across the entire enterprise. Thus, this framework is not intended only to manage the IT department, but instead it is intended to cover the entire IT process within the company, including all departments or division that is related to IT (Legowo & Christian, 2019).

COBIT gives a clear separation between governance and management, both of which are necessary for organizations to achieve different activities and objectives (ISACA, 2018b). Governance ensures that stakeholder needs are met, that direction is set through prioritization and decision-making, and that performance and compliance are monitored according to established guidelines and objectives. Generally, governance is the responsibility of the board of directors. Meanwhile, management plans, builds, executes, and monitors activities according to the direction established by governance to achieve the company's objectives. Generally, management is the responsibility of the executive team under the leadership of the CEO.

In order for information and technology to be utilized optimally to achieve the company's objectives, a series of governance and management objectives must be met. The governance objectives relate to the Evaluate, Direct, and Monitor (EDM) process. Within EDM process, the governing body evaluates strategic options, directs senior management on the chosen strategies, and monitors the achievement of these strategies. In addition, the management objectives are grouped into four domains: (1) Align, Plan, and Organize (APO), which addresses the overall organization, strategy, and supporting IT activities; (2) Build, Acquire, and Implement (BAI), which manage the definition, acquisition, and implementation of IT solutions as well as their integration with business processes; (3) Deliver, Service, and Support, which focuses on IT operations

and service support, including security; and (4) Monitor, Evaluate, and Assess (MEA), which involves performance monitoring and ensuring that IT aligns with internal performance targets, internal controls, and external requirements (ISACA, 2018b).

These governance and management objectives are then incorporated into 40 processes that must be fulfilled that are grouped into 5 domains. Those processes could be breakdown into this: (1) EDM domain has 5 processes; (2) APO domain has 14 processes; (3) BAI domain has 11 processes; (4) DSS domain has 6 processes; and (5) MEA domain has 4 processes. Together, these objectives and processes constitute the COBIT Core Model, as depicted in Figure 2.1.



Figure 2.1. COBIT Core Model (ISACA, 2018a)

COBIT 2019 emphasize flexibility and tailoring in its use. Since it acknowledges that there is no defined and exact approach to IT governance, COBIT 2019 provides tailoring mechanism named as Design Factors. This approach could be used to customize the design of an organization's IT governance system to its specific context (ISACA, 2018b). These design factors allow an organization to prioritize the most relevant governance and management objectives based on its unique characteristics and needs. Some of the design factors that could be considered when tailoring COBIT 2019

includes Enterprise Strategy, Enterprise Goals, Risk Profile, and Compliance Requirements (Standards, Framework, Regulations) as depicted in Figure 2.2.

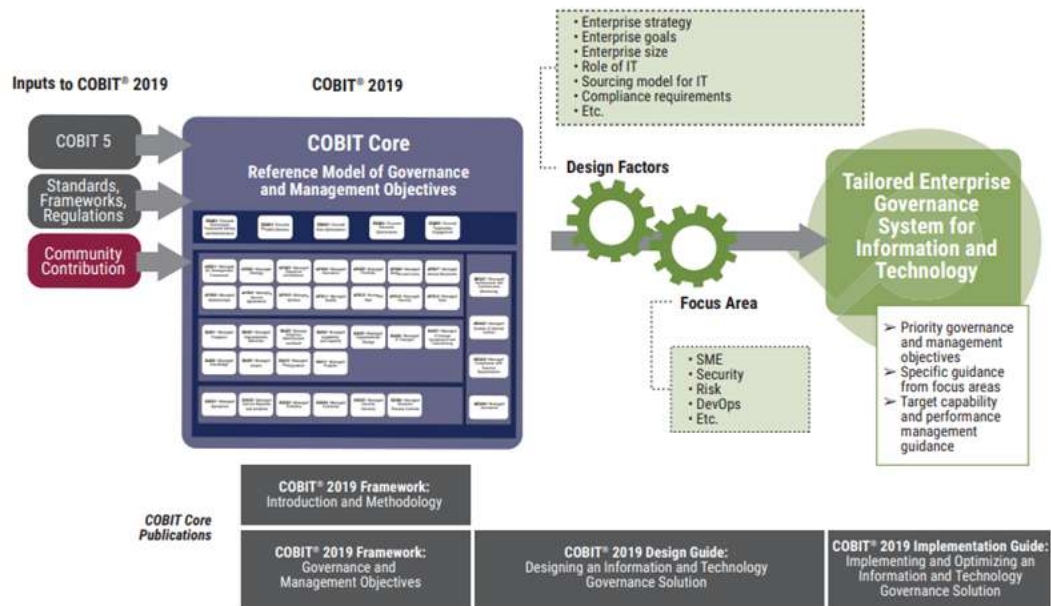


Figure 2.2. COBIT 2019 Tailoring (ISACA, 2018a)

For this research, there are a lot of compliance requirements since XYZ Bank operates in the banking industry. Compliance to OJK's regulations is not optional but a mandatory. As established in the research problem, failures in compliance have led to direct regulatory reprimands and have impeded business agility. Therefore, using compliance requirements as the primary driver for selecting and prioritizing COBIT 2019 processes provides a direct approach to design an IT governance system that addresses the specific issues of XYZ Bank.

This approach involves a systematic process of regulatory mapping, where specific articles, clauses, and stipulations within relevant regulations are analyzed and mapped to the corresponding COBIT 2019 governance and management objectives. This method of translating legal and regulatory text into actionable IT controls is a recognized practice in the field of IT governance (Breux et al., 2013). The result of this mapping would be prioritization of the COBIT 2019 processes. Objectives that are linked to numerous or particularly critical regulatory requirements are identified as the highest priority for assessment and improvement.

In addition to compliance requirements, this research will also leverage the Risk Profile design factor to further refine the prioritization of COBIT processes. A risk-based approach could be used to address the core issue by focusing improvement efforts on the areas of greatest vulnerability and potential business impact (ISACA, 2018a). This approach is consistent with studies that utilize COBIT's design factors, including the enterprise's risk profile and specific IT-related issues, to identify and prioritize the most critical governance and management objectives for improvement (Enrique & Fianty, 2023; Febriyani et al., 2022). This dual focus on both compliance and risk ensures that the designed IT governance system is not only compliant but also resilient and aligned with the bank's specific operational challenges.

Finally, to measure the effectiveness of its processes, COBIT 2019 provides a performance management model based on the Capability Maturity Model Integration (CMMI). This model which is named as COBIT Performance Management (CPM) allows processes to be assessed at different capability levels, ranging from 0 (Incomplete) to 5 (Optimizing), enabling an organization to benchmark its current capabilities, identify gaps against its targets, and plan for incremental improvement. The detailed capability level scheme is shown in Figure 2.3.

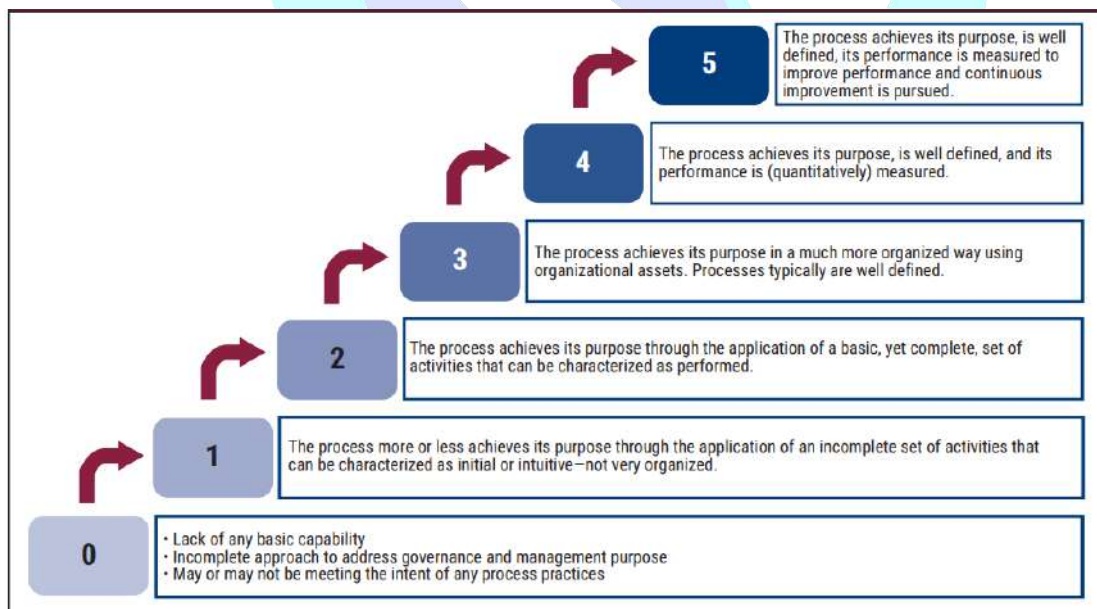


Figure 2.3. CMMI Capability Level for Processes (ISACA, 2018b)

There are 6 levels of process capability. Assessment of each process will reveal the capability levels that have been achieved by each process based on their capability to

achieve the intended outcomes according to the CMMI which could be broken down further as follows (ISACA, 2018b):

1. Fully

This capability level means that the process has achieved the capability level since the required process or components has been fulfilled by more than 85 percents.

2. Largely

This capability level means that the process has achieved about 50 to 85 percents of the process or components.

3. Partially

This capability level means that the process has achieved about 15 to 50 percents of the process or components.

4. Not

This capability level means that the process has achieved below 15 percents of the process or components.

2.3.2 ISO 38500:2024

ISO 38500 is an IT governance framework that is issued by International Organization for Standardization. The framework itself defines governance as the system which allows direction and controls the use of IT to support the organization achieve its plan and objective (Putri & Surendro, 2015).

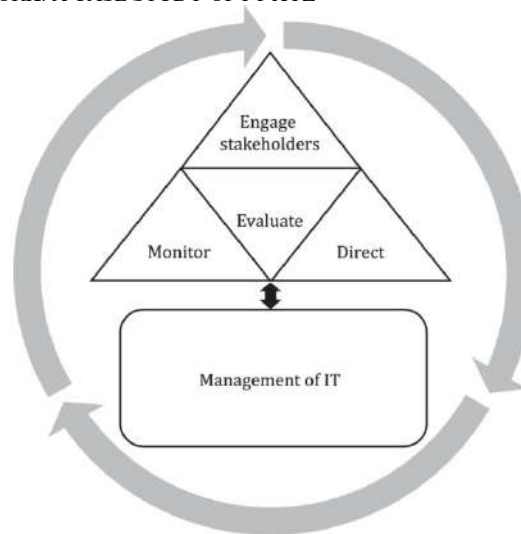


Figure 2.4. Model for IT Governance (International Organization for Standardization, 2024)

The latest version of the framework, ISO 38500:2024 depicts model for IT governance as can be seen on Figure 2.4. The models include governance and management of IT. There are 4 practices in the governance part including (1) engage stakeholders to understand their expectations, (2) evaluate the current and future use of IT; (3) direct preparation and implementation of strategies and policies, and (4) monitor performance of IT through appropriate measurement system to ensure that performance is in accordance with defined strategies and compliant with regulatory requirements (International Organization for Standardization, 2024).

2.3.3 ISO 27001:2022

ISO/IEC 27001:2022 is an international standard published by International Organization for Standardization in 2022. This standard defines the requirements and provides guidance for establishing a Information Security Management System (ISMS) (International Organization for Standardization, 2019).

Establishment of Information Security Management System according to ISO/IEC 27001:2022 requires a systematic approach named as Plan-Do-Check-Act (PDCA) cycle. PDCA cycle itself is referred from ISO/IEC 9001:2015 – Quality Management System which then adopted widely into other version of ISO standards, including ISO/IEC 27001:2022. There are seven requirements that would be grouped into that

PDCA cycle. Those requirements are (1) Context of the organization; (2) Leadership; (3) Planning; (4) Support; (5) Operation; (6) Performance evaluation; and (7) Improvement.

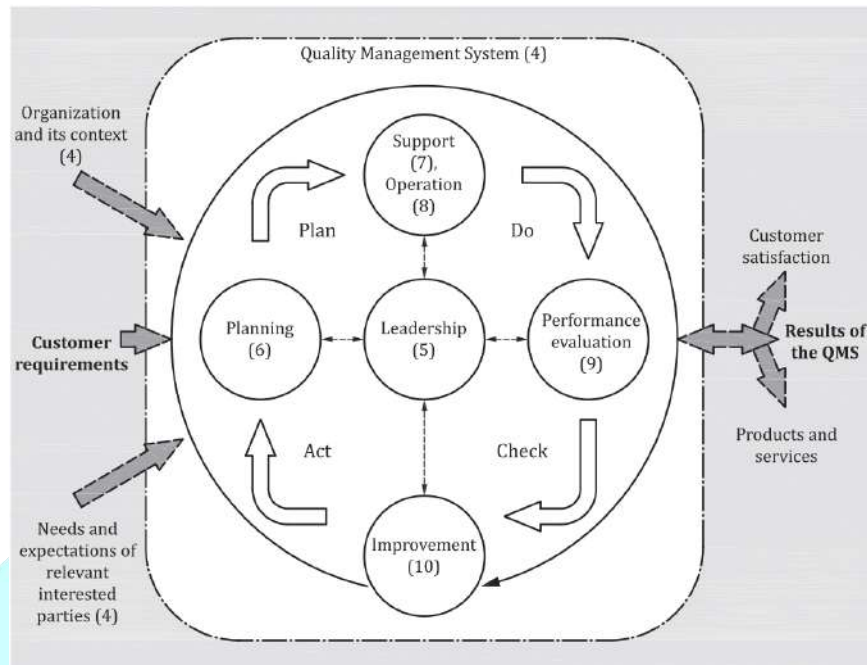


Figure 2.5. PDCA Cycle of Quality Management Cycle (International Organization for Standardization, 2015)

As pictured in Figure 2.5, PDCA cycle is a complete cycle in establishing a management system. The cycle starts with Planning phase which considers the context of an organization, relevant issues of organization, and the needs and expectations coming from related stakeholders. Anything captured from this activity then will act as driver and guidelines in executing any controls that are required from ISO/IEC 27001:2022 and relevant regulations. This execution then will be validated and monitored by performance evaluation activity and will in turn drive an Improvement phase that will give input to another cycle of planning activity. All of these processes are centralized around the leadership that comes from the leaders of the organization by considering all factors and to achieve organization's target of Information Security Management System.

Besides the mandated PDCA area, ISO 27001:2022 also has additional set of controls that is named as Annex A which act as reference for controls to manage information security-related risks (International Organization for Standardization, 2022). Annex A of ISO 27001:2022 is grouped into 4 types of controls. Respectively they are

Organizational controls, People controls, Physical controls, and Technological controls. Added together, all of reference controls that are mentioned within Annex A of ISO 27001:2022 amount to 93 controls.

2.4. Use of Framework

After analysing several frameworks related to IT governance, it is imperative to compare these frameworks in order to find out the most suitable framework to be used within this research. Following table is the comparison between IT governance frameworks:

Table 2.1. IT Governance Framework Comparison

No	Aspect	COBIT 2019	ISO 38500:2024
1	Comprehensiveness	Provides detailed governance and management objectives specific processes	High-level principles without detailed guidelines on how to implement
2	Level of Detail	Provides clear direction for IT governance and management functions	Provides broad guidance but require further interpretation for practical application
3	Measurability	Provides structured assessment model using CMMI (Level 0-5)	Does not provide any measurement model
4	Alignment with Requirements	Provide tailoring mechanism to align enterprise's requirement to relevant governance and management objectives	Does not provide any detail alignment model

As can be seen on Table 2.1, there are multiple factors that could differentiate COBIT 2019 and ISO 38500:2024 even though both are IT governance framework. COBIT 2019 is more comprehensive than ISO 38500:2024 since it provides more specific process and more detailed approach on the application of each process. COBIT 2019 also defines the measurement method through the use of CMMI model. In order to ensure alignment with requirements, COBIT 2019 also provide clear and applicable Goals Cascade model to map enterprise goals and alignment goals to governance and management objectives. Considering all of this, the framework that will be used on this research would be COBIT 2019 as the main framework.

However, COBIT 2019 is not the only framework. To complement and to fulfil the need of regulatory requirements, there are other framework that need to be combined with COBIT 2019 that specifically discuss regarding IT risk management and information security. Thus, ISO 27001:2022 as Information Security Management System standard will be added on top of COBIT 2019 to fulfil this requirement along with related regulatory requirements such as POJK No. 11/POJK.03/2022, SEOJK 11/POJK.03/2017, SEOJK No.24/POJK.03/2023, and SEOJK No.29/SEOJK.03/2022.

2.5. Design Science Research

Design Science Research (DSR) is a research approach focused on problem-solving through the creation of new and purposeful artifacts, such as tools, models, or methods, to address specific, real-world challenges (Hevner et al., 2004). It serves as a bridge between theoretical research and practical application. It seeks to develop innovative solutions that are not only effective in practice but are also grounded in rigorous academic principles which ultimately contribute new knowledge to the field (Gregor & Hevner, 2013).

Within the Information Systems field, research often follows one of two main paths: behavioural science or design science. Behavioural science aims to develop and test theories to explain or predict phenomena. On the other hand, DSR aims to build and evaluate effective solution to achieve desired outcomes (Hevner et al., 2004). The idea behind DSR is "knowing through building" (Delpont et al., 2024). This means that the

act of designing, constructing, and evaluating an artifact provides a deeper understanding of the problem itself and the principles that lead to a successful solution.

In order to conduct DSR properly, Hevner et al. (2004) proposed a conceptual framework that operates in three interconnected cycles: (1) The Relevance Cycle connects the research to the real-world environment, ensuring the problem being addressed is significant and important and the provided solution is practical to practitioners; (2) The Rigor Cycle connects the research to the existing scientific knowledge base of theories, frameworks, and methods and ensures the work is grounded in scientific bases; and (3) The Design Cycle is the essential of the research, where the artifact is build, tested, evaluated, and refined until it effectively addresses the problem.

There is a structured methodology to guide DSR's practical application. A widely recognized process model for conducting DSR was proposed by (Peppers et al., 2007). This model, the Design Science Research Methodology (DSRM), outlines a sequence of six key activities that guide a researcher from the initial problem definition to the final communication of the results. The DSRM process is iterative and provides a clear pathway for executing a DSR project, which can be summarized into six key activities.

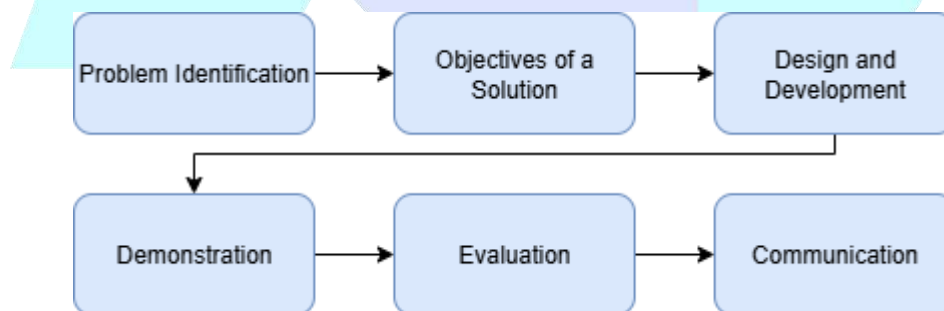


Figure 2.6. Design Science Research Process

As can be seen in Figure 2.6, DSR process begins with problem identification, where the specific research problem is defined. The second activity is to define objectives of a solution which could be qualitative or quantitative goals that will serve as the basis for evaluation. The third and core activity of DSR is the design and development of the artifact itself. This is followed by a demonstration of the artifact's use in solving the problem which could use several methods such as case study, simulation, or

experiment. The fifth activity is evaluation. This activity focus on measuring the artifact's effectiveness compared to the objectives. Finally, the process concludes with communication. This process focuses on communicating the result of artifact and evaluation to relevant stakeholders (vom Brocke et al., 2020).

As a design research, DSR produces output named artifact. (Venable et al., 2016a) defined four distinct types of DSR artifacts: (1) Constructs, which could be described as concepts to define a problem and describe a solution; (2) Models, which is abstractions and representations (e.g., diagrams, frameworks) that illustrate the problem domain, the solution, along with their relationship; (3) Methods, which is guidelines, algorithms, or systematic processes that guide how to solve a class of problems; and (4) Instantiations, that could be described as implemented prototypes or fully operational systems that demonstrate the feasibility, utility, and principles of the other artifacts in a real-world context.

Designed artifact needs to go through an evaluation activity. This evaluation is an important step in conducting DSR since it provides empirical evidence that an artifact works and meets its intended goals. There are multiple approaches that could be used within evaluation activity. In terms of evaluation purpose, there are formative evaluation and summative evaluation (Venable et al., 2016a). Formative evaluation is conducted iteratively during the design process to identify weakness and provide feedback for improvement. Meanwhile, summative evaluation is conducted at the end to assess the final artifact's overall success and impact. In terms of evaluation timing, there are ex-ante evaluation and ex-post evaluation. Ex-ante evaluation is predictive and occurs before full-scale implementation. This evaluation was meant to assess an artifact's potential impact and behaviour. Meanwhile ex-post evaluation happens after artifact's implementation to measure its actual performance and effects in a real context (Venable et al., 2016).

In order to conduct evaluation, there are variety of methods that could be used including observational techniques like case studies where an artifact is applied directly to the real world. The next one would be expert evaluations, where subject matter experts assess an artifact. Also, there is technical experiment to test performance. The last one would be the use of prototypes to demonstrate functionality (Müller et al., 2024).

Evaluation of artifact must be judged against a clear set of criteria. A review by Müller et al. (2024) identifies that there are ten criteria that commonly used within DSR such as:

1. Usefulness: How well an artifact could improve the work performance of its users.
2. Ease of Use: How well an artifact could be used without much effort both in usage and in learning on how to use it.
3. Effectiveness: How well an artifact could achieve its intended goals and provide the expected results.
4. Appropriateness: How well an artifact is designed to fulfil specific requirements that is intended to be solved.
5. Applicability: How well an artifact could be used beyond its original design should the original context of the problem evolve.
6. Correctness: How well an artifact produces result that is aligned with the expectation.
7. Feasibility: How viable an artifact is designed and operated from operational, technical, and economical perspective.
8. Functionality: How well an artifact is functioning that meets the defined requirements.
9. Understandability: How well an artifact could be comprehended by its users.
10. Validity: How well an artifact could achieve its purpose using the intended approach.

However, not all of these criteria are used for all method. The use of criteria would be based on the evaluation method that are going to be used (Müller et al., 2024). For example, a Method artifact could not be evaluated using functionality criteria, but an Instantiation artifact could be evaluated using criteria. Another example is

Appropriateness of a Method could not be assessed if the evaluation is conducted by case study or literature review, but an Appropriateness of a Method could be assessed if it is evaluated using technical experiment.

Within this research, the IT artifact that is going to be produced is a Method artifact of proposed policies regarding IT governance processes based on COBIT 2019. It would be evaluated using formative evaluation with ex-ante timing. The evaluation would be conducted by expert evaluation. Thus, the applicable DSR criteria for this research would be Correctness, Ease of Use, Effectiveness, Feasibility, Understandability, Usefulness, and Validity.

2.6. Previous Studies

A review of existing literature reveals that to improve IT governance of an organization, COBIT is a renowned framework to be used. Its applicability is demonstrated across a wide range of industries including banking (Legowo & Christian, 2019), manufacturing (Kwak & Desanti, 2023a), telecommunications (Lubis et al., 2023; Rama et al., 2020), education (Abdelilah et al., 2024; Febriyani et al., 2022; Ishlahuddin et al., 2020), IT services (Enrique & Fianty, 2023), and government institutions (Komang Lusinta et al., 2024). This allows COBIT to be used for various purposes, including conducting audits, performing evaluations of existing IT processes, and designing improvement of IT governance and management.

According to the previous studies, the first step is to identify and prioritize the most relevant governance and management objectives for the specific organizational context. There are several methods for this prioritization. The first approach is to use COBIT 2019 Design Factor toolkit. This approach is done by considering relevant factors such as enterprise strategy, risk profile, and current IT-related issues (Febriyani et al., 2022; Komang Lusinta et al., 2024; Lubis et al., 2023). The second approach is the Goals Cascade. This approach systematically maps an organization's vision and strategy to Enterprise Goals, then to Alignment Goals, and finally to specific COBIT processes (Ishlahuddin et al., 2020; Kwak & Desanti, 2023a; Legowo & Christian, 2019). The third approach is to select processes based on external compliance requirements. This may come from such as a government-mandated IT regulations (da Silva et al., 2019).

The fourth approach is predefined scope based on specific problems that are going to be investigated (Abdelilah et al., 2024; Rama et al., 2020).

An extensive empirical study by Huygh et al. (2022) shows significant correlation between the level of compliance requirements an organization faces and the maturity of its IT governance implementation. The study showed that as compliance pressures increase, organizations demonstrate higher capability levels across all COBIT domains. Furthermore, an organization need to conduct thorough systematic regulations mapping to IT control catalogues to ensure compliance with related requirements (Breaux et al., 2013).

In order to conduct assessment and improve IT governance using COBIT, there are methodologies that could be used which is organized into distinct phases (Abdelilah et al., 2024; Enrique & Fianty, 2023; Viamianni et al., 2023). Within those phases there are activities such as process prioritization through mapping regulations to IT controls (da Silva et al., 2019), using Goals Cascade (Ishlahuddin et al., 2020; Kwak & Desanti, 2023a), or Design Factor (Lubis et al., 2023).

After that, the next activity would be data collection (Abdelilah et al., 2024; Enrique & Fianty, 2023; Rama et al., 2020; Viamianni et al., 2023) and continued by capability level assessment and gap analysis (Ishlahuddin et al., 2020; Komang Lusinta et al., 2024; Legowo & Christian, 2019). When the gap is already identified, the next step would be to provide recommendations or the design of recommended controls based on the gap (Febriyani et al., 2022; Kwak & Desanti, 2023a) The recommendation then would be evaluated by relevant stakeholders to ensure that it answer the problem (Viamianni et al., 2023).

To summary previous study, it could be seen within the next table about each research, strengths, and weakness.

No	Paper	Strength	Weakness
1	(Lubis et al., 2023)	• The research clearly explain the use of Goals Cascade to ensure the alignment between Enterprise Goals, Alignment Goals, and other factors to achieve relevant governance and management objectives. • The research provides specific set of process as the result of process prioritization.	• Limited scope of research which only focus on process prioritization to produce relevant governance and management objectives. • Does not assess the existing condition and provide any actionable recommendation that could be used to improve IT governance.
2	(Abdelilah et al., 2024)	• Conduct thorough end-to-end analysis using COBIT framework by using a clear research framework. • Using predefined approach to define domain and process to be assessed and improved. • Provide clear and detailed recommendations for each process derived from the gap.	• The research jumps directly to the capability level result after providing the methodology without explaining in detail about the questionnaire and audience. • Capability target level that had been used for gap analysis is not explained or justified where it is derived from.

No	Paper	Strength	Weakness
3	(Kwak & Desanti, 2023)	• The research covers end-to-end analysis from Goals Cascade, prioritization of governance and management objective, and gap analysis. • This research delivers results of gap analysis for specific processes and provides granular actionable findings.	• The research is mainly focused on audit using COBIT. However, there's no clear justification and reasoning why Capability Level 3 is chosen as the base of audit.
4	(Ishlahuddin et al., 2020)	• The research shows the approach of Goals Cascade which was conducted thoroughly to produce prioritized governance and management objectives. • Data collection method uses combination of multiple data source to ensure validity of data: interviews, analysis of formal documents, and structured questionnaires	• Gap analysis of governance and management objectives is broad and cover a lot of process but are not detailed enough. Instead, it only shows the result and highlight more of the result and what needs to be improved by the institution rather the calculation and analysis. • The research does not provide clear justification on why the organization need to achieve Capability Level 2.

No	Paper	Strength	Weakness
5	(Legowo & Christian, 2019)	• This research is conducted in similar industry of banking company. This research also had been done with thorough analysis from Goals Cascade until gap analysis and recommendation.	• The research has been done using older version of COBIT 2019 (COBIT 5) which has some different processes and enterprise goals and alignment goals. • Provided recommendations are not detailed and specific enough in the context of organization and COBIT.
6	(Enrique & Fianty, 2023)	• The research framework that is used is structured, specific, and grouped within phases to conduct audit. • The research is based on specific business problem to be solved. • The research provides specific findings based on the audit.	• The research does not provide specific and tailored recommendations. • No strong justification on why the audit criteria needs to be defined at Level 3. • The research does not specify on how data is collected
7	(Viamianni et al., 2023)	• The research was conducted using comprehensive research	• Although the research framework mention that it conducted process prioritization, the

No	Paper	Strength	Weakness
		framework that grouped activities accordingly. • The research was conducted by referring Design Science Research (DSR) to develop related artifact. • The research conducted proper prioritization for processes and provide roadmap for improvement.	methodology or justification is not explained. • The research focuses on providing recommendation and improvement but does not provide justification on why those recommendations are required. • The artifact provided by the research was limited to recommendation and does not provide any design.
8	(da Silva et al., 2019)	• The research was based on process prioritization using compliance requirements approach that is based on regulations. • The research provides clear actionable items and roadmap to be prioritized by related organization to improve its IT governance.	• The research was conducted based on older version of COBIT (COBIT 5). • The research does not specifically mention on how the process improvement roadmap was designed along with the considerations.

No	Paper	Strength	Weakness
			• The research is limited on the prioritization for improvement without specifically mentioning what needs to be improved for each process.
9	(Febriyani et al., 2022)	• The research properly followed good practices of COBIT Design Factors that considers related factors of an organization to prioritize processes. • The research is based on specific issue that was faced by the organization.	• The research only focus on prioritization of processes based on COBIT Design Factor approach and does not provide any specific artifact. • The target Capability Level (Level 1 and Level 2) that had been defined as the objective for each process is not based on clear justification.
10	(Komang Lusinta et al., 2024)	• The research was conducted comprehensively to all of COBIT process which prioritized using COBIT Design Factor approach. • The research produces detailed actionable items in	• The research does not specify on why the existing condition was correlated to the identified problem especially when the process already achieved Level 4 Capability.

No	Paper	Strength	Weakness
		order to improve the IT governance.	The defined target capability of Level 5 was not derived with proper justification.
11	(Huygh et al., 2022)	- The research was based on large number of datasets which increase the validity of the research. - The research used rigorous research framework to achieve the conclusion that higher compliance requirements correlated with higher IT governance performance.	- The research was based on perception of the users that was surveyed. Thus, there was no direct assessment to the object. This may lead to bias. - The sampling size is not balanced between Low, Medium, and High level of compliance requirements. This also may lead to bias to the result.
12	(Rama et al., 2020)	- The research was trying to combine the use of COBIT 2019 and ISO 38500 altogether in conducting assessment within EDM and DSS domain. - The research provided detailed analysis on the existing condition and also	- Although the objective was to combine the two frameworks, the results was more focused on COBIT 2019 rather than the combinations of both - The target Capability Level to be achieved within the research was set at Level 5. This target

No	Paper	Strength	Weakness
		recommendation to improve.	was not based on sound justification. Although the research provide improvement, there's no mention why the improvement was needed to be done.
13	(Breaux et al., 2013)	The research was focusing on the specific issue that compliance requirement that come up from regulatory could be mapped directly to IT controls.	- The research was not specifically discussing the use of any framework like COBIT 2019 or ISO 38500. - The detailed process of mapping may lead to bias between professional since professional may use their own ad-hoc method.

After considering previous studies that could be seen in Table 2.2, this research will be started by problem identification within XYZ Bank's to fully understand the issue and the context of XYZ Bank's existing condition related to IT governance. The next step would be to conduct literature review from previous study to gain understanding theoretical basis and state-of-the-art condition related to IT governance research. These activities would be grouped as Problem Definition phase.

The next phase would be Requirement Formulation phase that includes identifying XYZ Bank's requirements related to IT governance. This identification would be

conducted using mapping from related regulations to COBIT processes thus would lead to process prioritization both by using the related regulations and the frequencies of the process mentioned within those regulations.

Following phase would be Analysis phase. Within this phase, there are activities such as data collection, determining existing capability level, conducting gap analysis, and improvement prioritization. This phase would be directly followed by Design phase that is specifically meant to design artifact in the form of design improvement.

The last phase would be Evaluation phase. This phase consists of two activities, evaluation activity which is going to be conducted to stakeholders that directly conduct the process and validation activity which is going to be conducted with the head or lead from related stakeholders to validate the result of evaluation.

