

CHAPTER 5– CONCLUSIONS AND RECOMMENDATIONS

This chapter concludes the entire research process. It presents the conclusions drawn from the analysis, directly addressing the research questions outlined in Chapter 1. This chapter also provides actionable recommendations for XYZ Bank based on the research outcomes and suggests future works for upcoming studies.

5.1. Conclusions

Based on the previous analysis and design which has been conducted in the previous chapters, this research has concluded that:

1. The existing condition of IT governance at XYZ Bank when being measured against the eight high-priority COBIT 2019 processes shows varied result. The analysis showed that from eight processes, two process achieved Level 3 (Defined) which are APO10 – Managed Vendors and APO12 – Managed Risk. Five processes achieved Level 2 (Managed), This includes EDM03 – Ensured Risk Optimization, APO01 – Managed I&T Management Framework, APO02 – Managed Strategy, DSS04 – Managed Continuity, and DSS05 – Managed Security Services. Also, there is one process that achieved Level 1 (Initial) which is EDM01 – Ensured Governance Framework Setting and Maintenance.
2. There is capability gap between the existing condition and the target condition of Level 3 (Defined) for six processes out of the eight prioritized processes. The most gap is a two-level gap capability in EDM01. Meanwhile the other processes such as EDM03, APO01, APO02, DSS04, and DSS05 have a one-level capability gap.
3. This research has designed and evaluated two policies: the IT Governance Policy and the Cyber Resilience and Security Policy. These artifacts were designed by integrating best practices from COBIT 2019 and ISO 27001:2022 and were explicitly mapped to address the identified capability gaps and OJK regulatory requirements. The evaluation and validation conducted with practitioners and management at XYZ Bank confirmed that these policies are understandable, useful, and effective. The feedback indicates that the implementation of these artifacts will close the identified. This will achieve the

objective to improve XYZ Bank's IT governance processes to Level 3 (Defined) capability and improve XYZ Bank's DMAB score of Governance Domain and Risk Management Domain to Level 2.

5.2. Recommendations

Based on the analysis and design of IT governance for XYZ Bank, the recommendations are categorized for two distinct audiences: practical recommendations for XYZ Bank and the broader digital banking industry, and recommendations for future academic research in this field.

These recommendations are action items that XYZ Bank and other institutions in the digital banking sector can take to improve their IT governance posture based on the findings of this study:

1. It is recommended that XYZ Bank implement the proposed governance and management processes in a phased manner. The priority should be given to processes with the lowest current capability levels and the highest impact on business goals and risk mitigation. This approach ensures that the most critical gaps are addressed first, providing immediate value and building momentum for the overall governance program.
2. The role of the IT Steering Committee should be strengthened. This body must be empowered to make binding decisions on IT strategy, investment portfolio, and risk appetite.
3. It is recommended that XYZ Bank invest in training and communication to embed a culture of security and governance awareness across the organization. Every employee should understand their role in protecting information assets and adhering to governance policies, transforming governance from a top-down mandate into a shared responsibility.

This study also opens several potentials for future academical purposes that could be built upon its findings:

1. Future research could conduct study to track the capability maturity of XYZ Bank's IT governance processes over several years following the implementation of these recommendations. This would provide valuable empirical evidence on the effectiveness of the COBIT 2019 framework in a digital banking context over time.
2. While this study qualitatively outlines the business impact, future research could focus on a quantitative analysis. This could involve developing and applying metrics to measure the Return on Investment (ROI) of IT governance improvements, such as cost reduction in IT incidents, increased revenue from stable digital channels, or improved customer satisfaction scores.

5.3. Future Works

On the process of conducting this research, it could be found that there are areas to be researched further. These are the suggestions for future research:

1. Future research could conduct research that is not only limited to design but also the implementation of IT governance period. This summative evaluation meant to measure the impact of the improved process.
2. Future research could expand the analysis to include other relevant COBIT 2019 processes that is not the highest priority according to the compliance mapping.
3. Future research could use quantitative study to statistically measure the correlation between the improved IT governance maturity and its impact to prevent operational losses, improve product-to-market times, improved customer satisfaction scores or other metrics that could be measured quantitatively.