ABSTRACT

The rapid development of information technology requires companies to have effective IT governance to support operational continuity and achieve business goals. This study aims to analyze and design IT governance at PT XYZ using the COBIT 2019 framework, focusing on the APO12 (Manage Risk) and DSS05 (Managed Security Services) domains. The research method used is a qualitative case study approach, through data collection in the form of interviews, observations, internal documents, and questionnaires. The results of the capability level assessment indicate that the DSS05 domain has approached the expected capability target, while the APO12 domain is still below the desired level. Gap analysis revealed several gaps, such as the absence of a formal and comprehensive IT risk policy, lack of risk mitigation documentation, and monitoring mechanisms that are not yet optimal. Based on these findings, recommendations are formulated in the form of policy improvements, increasing HR competencies, and utilizing technology for real-time risk monitoring. It is hoped that the results of this study can help PT XYZ in improving its IT risk and security governance capabilities sustainably, in accordance with COBIT 2019 best practices.

Keyword: *COBIT 2019, IT Governance, APO12, DSS05*