ABSTRACT

Financial technology (fintech) companies such as PT XYZ face complex challenges in managing information security, particularly due to high dependence on digital systems and regulatory pressure from authorities such as the ITE Law, PSTE Regulation, and regulations from the Financial Services Authority (OJK) and Bank Indonesia. The main problems identified include the suboptimal process of recording and classifying information assets, weak documentation of security controls, and the absence of a Statement of Applicability (SoA) as a reference for control implementation based on ISO 27001:2022. This study aims to implement an Information Security Management System (ISMS) framework based on ISO 27001:2022 using the Plan–Do–Check–Act (PDCA) management cycle approach. The research employs a qualitative method focusing on three key divisions: IT Security & Operation, IT & Network, and IT Planning & Development. The results show that out of the 93 controls listed in Annex A of ISO/IEC 27001:2022, 76 controls have been implemented while 17 controls have not yet been applied, resulting in an implementation readiness level of 82%. This research successfully produced a SoA document that outlines the list of security controls, their implementation status, and justification, along with strategic improvement recommendations that strengthen system resilience, data integrity, and regulatory compliance. Thus, the implementation of ISO/IEC 27001:2022 not only enhances information security at PT XYZ comprehensively, but also builds greater user trust in the company's digital services.

***Keywords**: Fintech, ISO 27001:2022, Information Security Management System, Regulatory Compliance, Risk Management.*