ABSTRACT

XYZ Institution, as an independent entity, holds a significant responsibility in protecting and managing sensitive data. To ensure the security of such information, the institution has adopted ISO 27001:2013 *as the framework for its Information Security Management System* (ISMS). *However, with the release of* ISO 27001:2022*, which introduces several important changes, evaluating the organization's readiness for transitioning to the new standard becomes crucial. This study aims to analyze the gaps between the current* ISMS *implementation and the requirements of the updated* ISO *version. The research employs a qualitative case study approach, supported by the Design Science Research* (DSR) *conceptual model and the Plan-Do-Check-Act* (PDCA) *cycle to strengthen the analytical structure. Data were collected through semi-structured interviews and internal document analysis. The results reveal that* 26 *out of the* 93 *controls in* ISO 27001:2022 *have not been fully implemented, particularly within the technological domain and new controls such as cloud service security and secure coding. Based on these findings, a transition strategy was developed, including human resource training, documentation revisions, and internal audits based on the new control structure. The final conclusion indicates that while* ISO 27001:2022 *offers flexibility and relevance to modern threats, XYZ Institution must strengthen its internal readiness to ensure an effective transition process.*

Keywords— ISO 27001:2013, ISO 27001:2022, *Information Security Management System, information security, standard transition, gap analysis.*