ABSTRACT

Information security is a crucial aspect in ensuring operational continuity and maintaining trust in information systems, especially with the growing complexity of cyber threats. XYZ Institution, as an institution managing sensitive data, has an urgent need to ensure its information security readiness in alignment with international standards. However, several issues were identified in practice, including the lack of documentation for key policies and the incomplete structuring of information security activities. This study aims to analyze the readiness of documentation and implementation of information security practices at XYZ Institution based on the ISO/IEC 27001:2022 standard. A qualitative approach was used, employing gap analysis techniques and ISO-based checklist assessments to evaluate the existing security framework against the standard's relevant clauses and controls. The assessment was conducted through three iterative evaluation cycles to ensure accuracy and validation of findings. The final assessment results revealed that XYZ Institution has not fulfilled 3 out of the 10 core clauses of ISO/IEC 27001:2022, specifically those related to Organizational Strategic Direction, Performance Evaluation, and Continual Improvement. These gaps were primarily due to the absence of adequate documentation and the lack of structured evaluation and follow-up mechanisms. In conclusion, XYZ Institution needs to improve its policy documentation, implementation of security controls, and the cycle of evaluation and continual improvement to achieve full compliance with ISO/IEC 27001:2022. Strategic recommendations are provided to address these gaps and strengthen the institution's readiness for information security certification and comprehensive risk management.

Keywords: ***Information Security, ISO 27001:2022, LEMBAGA XYZ, Gap Analysis, Compliance Assessment***