ABSTRACT

The issue addressed in this research concerns how information security risk management at PT XYZ has not yet fully complied with the established standards, particularly in several controls listed in Annex A of ISO/IEC 27001:2022. This topic is important due to the increasing reliance of companies on information systems, which demands adequate protection of information assets. However, gaps still exist in practice, such as the lack of backup device availability and inconsistent data deletion processes. The solution implemented involved conducting an evaluation and risk analysis based on ISO/IEC 27001:2022 using observation, interviews, and document review methods, as well as comparing current conditions against the standard controls. Based on the gap analysis, a risk assessment was developed, followed by relevant technical recommendations referring to the ISO/IEC 27002:2022 guidelines. The main findings of this research indicate that several controls require improved implementation, and enhancement recommendations have been proposed to support a more comprehensive strengthening of information security within the organization.

Keywords: information security, risk management, evaluation, ISO/IEC 27001:2022, ISO/IEC 27002:2022, audit.