ABSTRACT

Information security is a crucial aspect in ensuring business continuity, particularly for PT. XYZ, a company engaged in contracting and construction services. In an effort to enhance information security governance in accordance with the regulations of the National Cyber and Crypto Agency (BSSN), this study aims to design an information security risk management framework based on the ISO/IEC 27005:2022 standard. This standard provides a systematic approach through the stages of context establishment, risk assessment, and risk treatment. This study adopts a qualitative method with a case study approach focused on the IT Division of PT. XYZ. Data collection techniques include in-depth interviews with internal stakeholders, document analysis, and literature review to support the theoretical foundation. The results indicate that out of all the information assets owned by PT. XYZ, a total of 87 potential risks were identified. These risks are classified into five severity levels: very high, high, medium, low, and very low. Based on the risk evaluation aligned with the company's risk acceptance criteria, 18 risks require further treatment through the implementation of appropriate control measures tailored to the types of assets and threats involved.

***Keywords**: risk management, information security, ISO/IEC 27005:2022*