ABSTRACT

In the era of digital transformation, government institutions are increasingly dependent on information technology to carry out their duties. However, This dependency introduces risks to information security that must be managed systematically. This study aims to analyze information security risks at the Communication and Information Office (Diskominfo) of West Java Province, specifically in Division XYZ, using the international standard ISO/IEC 27005:2022. The research employs a qualitative approach, collecting primary data through interviews, questionnaires, and observations, as well as secondary data such as the agency's vision and mission, institutional profile, and organizational structure. The risk management process includes context establishment, risk identification, risk analysis, risk evaluation, and risk treatment. The results identify 15 major information security risks, with risk levels ranging from low to high. Most risks stem from weak access control, lack of system updates, and minimal security awareness training. Seven risks require mitigation actions, while the remaining eight are considered acceptable. This study presents strategic risk treatment recommendations to enhance information security resilience in the respective division. The implementation of ISO/IEC 27005:2022 proves effective in supporting government institutions to conduct structured risk analysis and serves as a reference for continuous improvement in information security governance.

***Keywords**: ISO/IEC 27005:2022, risk management, information security, Diskominfo, IT risk, public sector*