ABSTRACT

Information security is a crucial aspect in the digital era, particularly for government institutions such as the Communication and Information Office (Diskominfo) of Bogor Regency. According to the report by the National Cyber and Crypto Agency (BSSN), cyberattacks in Indonesia have increased significantly, with the government sector being one of the main targets. This study aims to design information security risk management at Diskominfo Bogor Regency using the ISO/IEC 27005:2022 standard. A qualitative method with a Design Science Research (DSR) approach is employed. Data were collected through interviews, document analysis, and literature review. The risk management process follows the ISO/IEC 27005:2022 framework, which includes context establishment, risk assessment, and risk treatment. The results identify 119 risks, consisting of 3 very high risks, 2 high risks, 18 medium risks, 16 low risks, and 80 very low risks. A total of 23 risks categorized as very high to medium are then provided with control recommendations based on ISO/IEC 27001:2022.

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