ABSTRACT

XYZ Organization is a regional security organization based in East Java that has implemented Information Technology (IT) for data processing and information dissemination through one of its departments, the Department of Information & Data Processing. However, the implementation of IT has encountered various risks that may threaten business operations within the department, particularly in the Smart Integrated Command Center (SICC) service. This is evident from the increasing trend in risk event mapping, with 33 incidents recorded in 2020 and rising to 59 incidents in 2024, based on a preliminary study that mapped IT risk types in the SICC service over the past five years. These risks include natural disasters, human-related issues, and IT infrastructure vulnerabilities.To mitigate these risks, a risk management analysis is necessary using the ISO 31000:2018 framework, which includes the stages of risk identification, analysis, and evaluation. Data collection was conducted through a quantitative approach by distributing questionnaires to those impacted by the risks or users of the SICC service, resulting in 164 respondents. Based on the risk assessment results, a total of 34 risks were identified with risk levels of 9 and 6 (moderate level). Of these, 3 risks had a risk level of 12, 13 risks had a risk level of 9, and 21 risks had a risk level of 6. Meanwhile, 30 risks were identified with a risk level of 4 (low level). Controls were established for each risk based on COBIT 2019 and NIST SP 800-53 Rev.5. The recommended controls include system monitoring, data backup, and personnel training. The results of the risk assessment were documented in a risk register, which includes all identified risks and assigns accountability for each risk.

Keywords**:** *Risk, Risk Management, ISO 31000:2018, Information Technology (IT), Risk Register.*