ABSTRACT

Information security is a crucial aspect of managing information systems in hospital environments, aimed at protecting patient data and medical operations from evolving threats. This study aims to evaluate the Information Security Management System (ISMS) at RSD Gunung Jati Cirebon based on the ISO/IEC 27001:2022 standard, focusing on gap analysis, risk identification, and the provision of specific improvement recommendations.

The research methodology includes questionnaire surveys, structured interviews, and an analysis of relevant policy documents. The gap analysis revealed that out of 93 evaluated controls, 25.8% fully met the standard, 51.6% were at a medium level of implementation, and 22.6% required significant improvement. The risk analysis also identified major threats in the areas of data access management and software updates, with most risks falling into the medium to high categories.

The findings indicate that RSD Gunung Jati has several areas needing improvement to meet ISO/IEC 27001:2022 requirements, particularly in security policy and information access management. Based on these results, recommendations were formulated to enhance the hospital's ISMS, including staff training, the development of clearer security procedures, and stricter oversight of data access. It is advised that RSD Gunung Jati regularly update its ISMS policies to keep pace with the evolving landscape of cybersecurity threats. This study is expected to serve as a reference for other hospitals planning to implement ISMS based on ISO/IEC 27001:2022.

***Keywords**: Information Security Management System, ISO/IEC 27001:2022, RSD Gunung Jati Cirebon, Cybersecurity, Patient Data Protection, Gap Analysis.*