ABSTRACT

This study assesses the level of information security risk in the information system of EDUCATIONAL INSTITUTIONS X using the ISO/IEC 27005: 2022 framework and NIST SP 800-30 Revision 1. This assessment aims to identify, analyze, and evaluate risks that can affect data security and school information system operations.

This research is motivated by the importance of managing information security in the digital era, especially in the education sector which is vulnerable to cyber-attacks. EDUCATIONAL INSTITUTIONS X has never conducted a risk assessment on its information system, even though there have been several problems, such as disruption of access to the database that hampers the work process. This shows the need for a risk assessment to ensure data protection and reliability of school information systems.

The research method includes several main stages, namely risk identification, risk analysis, and risk evaluation based on ISO/IEC 27005:2022 and NIST SP 800-30 standards. Data was collected through interviews, observations, and document analysis. The results of each stage are used to design mitigation strategies that are relevant and appropriate to the needs of the organization.

This study concludes that the implementation of the combined framework of ISO/IEC 27005:2022 and NIST SP 800-30 Revision 1 on the ZZZ information system at government institution X is effective in comprehensively identifying, analyzing, and evaluating information security risks. From the identification results, 15 information assets were found (4 main assets and 11 supporting assets) with 25 threat scenarios originating from 20 threat entities, both adversarial and non-adversarial.

Therefore, it can be concluded that educational institution X needs to implement information security risk management, at least for internal stakeholders, in order to maintain confidentiality, availability, and integrity (CIA). The data from this research can be used as a basis for future studies to determine risk treatment for each asset using other documents such as ISO 27002 and so on.