ABSTRACT

In the digital era, information security has become a critical concern for organizations due to the increasing threats posed by cyber incidents. This study aims to mitigate information security risks through the optimization of risk assessment based on ISO 27005:2022 and NIST SP 800-300 Revision 1 standards at Company XYZ. The research employs a qualitative approach, utilizing observation and interviews as primary data collection methods to gain insights into the current practices and challenges faced in managing information security risks.

The findings reveal that Company XYZ has implemented several risk management strategies; however, there are still significant vulnerabilities that need to be addressed. The integration of ISO 27005:2022 and NIST SP 800-30 Revision 1 frameworks provides a comprehensive methodology for assessing and treating risks, enhancing the organization's ability to protect its information assets effectively. This research contributes to the existing body of knowledge by offering a tailored risk assessment framework that can be adapted by other organizations facing similar challenges.

Based on the results, it is recommended that Company XYZ invest in continuous training for employees, enhance communication regarding security policies, and regularly review and update their risk management practices to adapt to evolving threats.

Keywords: *Information Security, Risk Assessment*, ISO 27005:2022, NIST SP 800-30 Revision 1.