ABSTRACT

This research aims to analyze and design information security risk management at PT. Dago Endah accounting division using the ISO/IEC 27005:2022 framework. The ISO/IEC 27005:2022 framework is an international standard that provides systematic guidance for information security risk management. The risk identification results based on ISO/IEC 27002:2022 reveal unmet controls in four aspects: Organizational Control, People Control, Physical Control, and Technology Control. From the risk analysis, several threats with high and very high risk levels were found. These threats include incorrect decisions due to misjudgment of incidents, employees or vendors leaking sensitive information, slow organizational response to DoS attacks, employees failing to report security incidents, and employees carelessly clicking malware links or accessing phishing sites.

Keywords: ***Information Security Risk Management, ISO/IEC 27005:2022, Information Security Control Recommendations, Risk Assessment***