ABSTRACT

XYZ Government Agency utilizes information technology assets to support business processes. The use of IT assets at XYZ agencies cannot be separated from the risk of information security. One of the efforts to secure information is to make a risk-based information security evaluation step. This research will focus on evaluating security risk and information security principles and the mitigation measures taken. The evaluation step using Failure Mode and Effect Analysis method for risk assessment and utilizing ISO 27001:2013 and ISO 27005:2013 standards as a reference for risk management and risk assessment. In this research, mitigation measures are needed as an effort to reduce the impact of the risks that exist in XYZ Agencies with ISO 27002:2013. This research process at XYZ Agency will provide an overview related to the risks. Based on this, a list of risks and assessment results will be obtained as well as a list of risk mitigation that can be used by the organization for handling documents.

Keywords: Information Security, Risk Management, Failure Mode and Effect Analysis, ISO 27001:2013, ISO 27002:2013, ISO 27005:2013