ABSTRACT

The government system has now implemented electronics in its process or commonly called the Electronic-Based Government System (E-goverment), with this SPBE making confidential / sensitive assets stored in the electronic system very vulnerable to attack according to data from the BSSN report in 2022 the government administration sector is the field with the most cyber attacks and complaints. This makes assets must be properly guarded, XYZ institution has a task focused on designing and running E-goverment, XYZ institution requires a good information security management system (ISMS) so that assets remain safe. This research aims to improve the information security management system in a qualitative way, namely interviewing and observing related parties and determining the maturity level of the ISMS which is standard SNI ISO / IEC 27001: 2022 using the COBIT 2019 maturity level then analyzed to provide recommendations for improvement based on SNI ISO / IEC 27002: 2022 as a reference for security controls on ISMS SNI ISO / IEC 27001: 2022. The results of this study found that the maturity level of the XYZ institution ISMS is level 2 of COBIT 2019 maturity, where at this point the security controls have successfully achieved the objectives through basic, yet detailed, activities, which can be referred to as a deliverable but there is still no documentation regarding the application to the organization's assets and it was found that there was one unfulfilled control related to web filtering. The level of maturity expected by the leadership of the XYZ institution is level 4, where the results of the implementation on assets are audited to measure whether the implementation is in accordance with the procedure. From the maturity level gap, this research provides recommendations, namely making documentation of the application of procedures on assets that refer to SNI ISO / IEC 27002: 2022 and then auditing its application.

Keywords: Information Security, ISO 27001, ISO 27002, Maturity Level, E-Goverment, ISMS, COBIT.