ABSTRACT

The importance of information and the possible risk of disruption, therefore the universities need to designed and implemented of the information security. One of the standards that can be used to analyze the level of information security in the organization is ISO/IEC 27001 : 2013 and this standard has been prepared to provide requirements for establishing, implementing, maintaining and continually improving an information security management system.

The objective of this research is to measure the level of information security related Information Security Policy, Asset Management, Access Control, Physical and Environmental Security, Operational Security and Communications Security based on standard ISO/IEC 27001: 2013 and modeling systems for information security management.

This research uses descriptive qualitative approach, data collection and validation techniques with tringulasi (interview, observation and documentation). Data was analyzed using gap analysis and to measure the level of maturity this research uses SSE-CMM (Systems Security Engineering Capability Maturity Model).

Based on the research results, Maturity level clause Information Security Policy reaches level 1 (Performed-Informally), clause Asset Management reaches level 3 (Well-Defined), clause Access Control reaches level 3 (Well-Defined), clause Physical and Environmental Security reaches level 3 (Well-Defined), clause Operational Security reaches level 3 (Well-Defined), Communication Security clause reaches the level 2 (Planned and Tracked).

Based on the results of maturity level discovery of some weakness in asset management in implementing the policy. Therefore, the modeling system using the flow map and CD / DFD focused on Asset Management System.

Keywords : *Analysis Information Security,* ISO/IEC 27001 : 2013, *Maturity Level,* SSE-CMM, CD/DFD