ABSTRAK

Pentingnya informasi dan adanya kemungkinan risiko terjadi gangguan, oleh karena itu perguruan tinggi perlu untuk merancang dan mengimplementasikan keamanan informasi. Salah satu standar yang dapat digunakan untuk menganalisa tingkat keamanan informasi di organisasi adalah ISO/IEC 27001 dan standar ini telah disiapkan untuk menyediakan persyaratan untuk membuat, mengimplemetasikan dan meningkatkan secara berkelanjutan sistem manajemen keamanan informasi.

Tujuan dari penelitian ini adalah untuk mengukur tingkat keamanan informasi terkait Kebijakan Keamanan Informasi, Manajemen Aset, Kontrol Akses, Keamanan Fisik dan Lingkungan, Keamanan Operasional dan Keamanan Komunikasi berdasarkan standar ISO/IEC 27001 : 2013 dan pemodelan sistem manajemen keamanan informasi.

Penelitian ini menggunakan jenis pendekatan kualitatif deskriptif, teknik pengumpulan dan validasi data dengan teknik tringulasi (wawancara, observasi dan dokumentasi). Analisis data dilakukan dengan *gap analysis* dan untuk mengukur tingkat kematangan penelitian ini mengunakan SSE-CMM *(Systems Security Engineering Capability Maturity Model*).

Berdasarkan hasil penelitian, *Maturity level* pada klausul Kebijakan Keamanan Informasi mencapai level 1 (*Performed-Informally*), klausul Manajemen Aset mencapai level 3 (*Well-Defined*), klausul Kontrol Akses mencapai level 3 (*Well-Defined*), klausul Keamanan Fisik dan Lingkungan mencapai level 3 (*Well-Defined*), klausul Keamanan Operasional mencapai level 3 (*Well-Defined*), klausul Keamanan Komunikasi mencapai level 2 (*Planned and Tracked*).

Berdasarkan hasil penilaian *maturity level* ditemukan beberapa kekurangan pada manajemen aset dalam mengimplementasikan kebijakan. Oleh karena itu, pemodelan sistem dengan menggunakan *flow map* dan CD/DFD difokuskan pada Sistem Manajemen Aset.

Kata Kunci : Analisis keamanan informasi, ISO/IEC 27001 : 2013, *Maturity Level*, SSE-CMM, CD/DFD