ABSTRAK

ANALISIS PENERAPAN MANAJEMEN RISIKO KEAMANAN INFORMASI PADA ISO/IEC/IEC 27001 DAN ISO/IEC/IEC 27002 PADA PT XYZ

Oleh

Fayza Indah Lestari Nasution

NIM: 1721005

Program Studi Administrasi Bisnis Otomotif

PT XYZ membutuhkan kebijakan baru pada sistem keamanan informasi untuk serangan *cyber* yang semakin gencar dan Sistem Manjemen Keamanan Informasi (SMKI) mempunyai standar edisi terbaru yaitu ISO 27001:2022, yang sebelumnya ialah ISO/IEC 27001:2013. Penelitian dilakukan bertujuan untuk melihat aset kritis dan penilaian risiko melalui penerapan manajemen keamanan informasi berdasarkan standar ISO/IEC 27001: 2022 dan kontrol ISO/IEC 27002:2022. Menggunakan 10 klausul kontrol dengan Metode Operationally *Crictical Threat, Asset, and Vulnerability Evaluation (OCTAVE)* untuk menentukan aset kritis perusahaan dan Metode *Failure Mode and Effect Analysis (FMEA)* mengidentifikasi serta menilai risiko dari masing-masing aset kritis. Hasil Analisis dari penelitian ini didapatkan 9 aset kritis perusahaan, dari perhitungan level risiko *extreme* terdapat 2 potensi risiko kebocoran data perusahaan dan *cyber risk* dengan skor 125, serta level risiko *high* terdapat 3 potensi risiko yaitu, penyalahgunaan akses pengguna, kerusakan perangkat server dan penggunaan *illegal software* dengan skor 100, serta *rating scale* tingkat kematangan perusahaan untuk menerapkan ISO/IEC 27001:2022 sebesar 38%. Hasil ini terbukti metode FMEA efektif untuk mengidentifikasi, menganalisis dan memprioritaskan risiko serta metode OCTAVE dapat mengklasifikasikan aset kritis infrastruktur perusahaan dengan menentukan tingkat kesiapan, kematangan dan kemampuan perusahaan dalam menerapkan ISO/IEC 27001 dan ISO/IEC 27002 versi tahun 2022.

Kata Kunci : SMKI, ISO/IEC 27001, ISO/IEC 27002, OCTAVE, FMEA.