ABSTRAK

Instansi XYZ adalah salah satu instansi pemerintahan yang memanfaatkan aset tekonologi informasi sebagai pendukung berjalannya proses bisnis. Penggunaan aset TI pada Instansi XYZ dapat memicu adanya risiko akan keamanan informasi. Salah satu upaya untuk melakukan pengamanan informasi adalah dengan membuat langkah evaluasi keamanan informasi berbasis risiko. Penelitian ini akan berfokus pada evaluasi keamanan informasi dan langkah manajemen risiko yang dilakukan oleh Instansi XYZ serta langkah mitigasi yang dilakukan. Langkah evaluasi keamanan informasi pada penelitian ini dilakukan dengan menggunakan metode *Failure Mode and Effect Analysis* sebagai alat untuk melakukan penilaian terhadap risiko serta memanfaatkan standar ISO 27001:2013 dan 27005:2013 sebagai acuan untuk melakukan *Risk Assessment*. Pada penelitian ini langkah mitigasi diperlukan sebagai upaya untuk mengurangi dampak dari risiko yang ada pada Instansi XYZ sesuai dengan ISO 27002:2013. Proses penelitian yang akan dilakukan pada Instansi XYZ akan memberikan gambaran terkait dengan risiko-risiko yang terjadi. Berdasarkan hal tersebut maka akan didapatkan daftar risiko dan hasil penilaian serta daftar mitigasi risiko yang dapat digunakan oleh organisasi untuk dokumen penanganan.

Kata kunci : Keamanan informasi, Manajemen risiko, *Failure Mode and Effect Analysis*, ISO 27001:2013, ISO 27002:2013, ISO 27005:2013