

ABSTRAK

Perkembangan teknologi memegang peran penting dalam mendapatkan informasi terutama dengan adanya internet, akses untuk mendapatkan informasi akan lebih mudah. Informasi merupakan salah satu kebutuhan penting bagi perusahaan untuk mendukung pengambilan keputusan. Diperlukannya pengelolaan sistem informasi yang baik apabila ingin mengelola suatu informasi. Hasil dari pengelolaan informasi bersifat secara rahasia yang akan membutuhkan kontrol perlindungan untuk meminimalisir risiko yang dapat menimbulkan kerugian pada perusahaan. Penelitian ini bertujuan untuk melakukan *assessment* risiko keamanan informasi pada sistem informasi ZZZ di instansi pemerintah X. Penelitian ini merupakan penelitian kualitatif dengan tujuan deskriptif. Teknik pengolahan data menggunakan kombinasi perhitungan risiko dan matriks dokumen ISO/IEC 27005:2011 dan NIST SP 800-30 Revisi 1 yang didukung dengan teori triangulasi.

Hasil dari penelitian ini menunjukkan bahwa terdapat 24 risiko yang perlu dimitigasi sedangkan terdapat 29 risiko yang diterima oleh instansi pemerintah X. Jumlah risiko dengan nilai *very low* sebanyak tujuh, *low* sebanyak 40, *moderate* sebanyak lima. Diidentifikasi sebanyak 25 jenis ancaman pada masing-masing aset yang berhubungan dengan sistem informasi ZZZ, jenis ancaman tersebut berasal dari 19 sumber ancaman yang telah dipertimbangkan. Kontrol yang terdapat pada masing-masing aset berjumlah 22.

Dengan begitu dapat disimpulkan bahwa instansi pemerintah X perlu untuk menerapkan manajemen risiko keamanan informasi minimal untuk kalangan internal agar dapat menjaga kerahasiaan, ketersediaan dan integritas (CIA). Data dari penelitian ini dapat dijadikan bahan sebagai penelitian selanjutnya untuk mengetahui tindakan terhadap risiko pada masing-masing aset dengan menggunakan dokumen lain seperti ISO 27002 dan lain sebagainya.

Kata Kunci: *Assessment* risiko, keamanan informasi, ISO/IEC 27005:2011, NIST SP 800-30 Revisi 1.