ABSTRAK

Keamanan informasi merupakan aspek krusial dalam menjaga kelangsungan bisnis, khususnya bagi PT. XYZ yang bergerak di bidang kontraktor dan layanan konstruksi. Dalam rangka meningkatkan tata kelola keamanan informasi yang sesuai dengan regulasi Badan Siber dan Sandi Negara (BSSN), penelitian ini bertujuan untuk merancang pengelolaan risiko keamanan informasi dengan mengacu pada standar ISO/IEC 27005:2022. Standar ini menyediakan pendekatan sistematis melalui tahapan *context establishment, risk assessment*, dan *risk treatment.* Penelitian dilakukan menggunakan metode kualitatif dengan pendekatan studi kasus pada Divisi IT PT. XYZ. Teknik pengumpulan *data* meliputi wawancara mendalam dengan pihak internal perusahaan, analisis terhadap dokumen-dokumen terkait, serta studi literatur untuk memperkuat landasan teoritis. Hasil penelitian menunjukkan bahwa dari total aset yang dimiliki PT. XYZ, teridentifikasi 87 risiko yang berpotensi mengancam keamanan informasi. Risiko-risiko tersebut diklasifikasikan ke dalam lima tingkat risiko, yaitu sangat tinggi, tinggi, sedang, rendah, dan sangat rendah. Berdasarkan hasil evaluasi risiko yang mengacu pada kriteria penerimaan risiko perusahaan, sebanyak 18 risiko memerlukan penanganan lebih lanjut berupa implementasi kontrol pengendalian yang disesuaikan dengan jenis aset dan jenis ancaman yang dihadapi.

Kata Kunci: manajemen risiko, keamanan informasi, SNI ISO/IEC 27005:2022