ABSTRAK

Dalam era transformasi digital, instansi pemerintah semakin bergantung pada teknologi informasi untuk menjalankan tugas-tugasnya. Namun, ketergantungan ini menimbulkan risiko terhadap keamanan informasi yang harus dikelola secara sistematis. Penelitian ini bertujuan untuk menganalisis risiko keamanan informasi pada Diskominfo Provinsi Jawa Barat, khususnya pada Divisi XYZ, menggunakan standar internasional ISO/IEC 27005:2022. Metode penelitian yang digunakan adalah pendekatan kualitatif dengan pengumpulan data primer melalui wawancara, kuesioner dan observasi, serta data sekunder berupa visi dan misi instansi, profil instansi dan struktur organisasi. Proses manajemen risiko dilakukan melalui tahapan penetapan konteks, identifikasi risiko, analisis risiko, evaluasi risiko, hingga perlakuan risiko. Hasil penelitian mengidentifikasi 15 risiko utama terkait keamanan informasi, dengan tingkat risiko bervariasi dari rendah hingga tinggi. Sebagian besar risiko berasal dari kelemahan kontrol akses, kurangnya pembaruan sistem, serta minimnya pelatihan kesadaran keamanan. Sebanyak tujuh risiko memerlukan tindakan mitigasi, sementara delapan lainnya masih dapat diterima. Penelitian ini menghasilkan rekomendasi strategis perlakuan risiko untuk meningkatkan ketahanan keamanan informasi divisi terkait. Penerapan ISO/IEC 27005:2022 terbukti efektif dalam membantu instansi pemerintah melakukan analisis risiko secara terstruktur dan dapat menjadi rujukan untuk perbaikan tata kelola keamanan informasi yang berkelanjutan.

Kata kunci: ISO/IEC 27005:2022, manajemen risiko, keamanan informasi, Diskominfo, risiko TI, sektor publik