ABSTRAK

Lembaga XYZ sebagai institusi independen memiliki tanggung jawab besar dalam melindungi dan mengelola data sensitif. Untuk menjamin keamanan informasi tersebut, lembaga ini telah menerapkan ISO 27001:2013 sebagai kerangka kerja *Information Security Management System* (ISMS). Namun, dengan terbitnya ISO 27001:2022 yang membawa sejumlah perubahan penting, evaluasi kesiapan terhadap transisi standar menjadi hal yang krusial. Penelitian ini bertujuan untuk menganalisis kesenjangan antara implementasi ISMS yang telah berjalan dengan persyaratan ISO versi terbaru. Metode penelitian yang digunakan adalah pendekatan kualitatif berbasis studi kasus, dengan dukungan model konseptual *Design Science Research* (DSR) dan siklus *Plan-Do-Check-Act* (PDCA) untuk memperkuat struktur analisis. Teknik pengumpulan data dilakukan melalui wawancara semi-terstruktur dan analisis dokumen internal. Hasil penelitian menunjukkan bahwa terdapat 26 kontrol dari total 93 kontrol dalam ISO 27001:2022 yang belum sepenuhnya diimplementasikan, terutama pada domain teknologi dan kontrol baru seperti keamanan layanan cloud dan pengkodean aman. Berdasarkan temuan tersebut, disusun strategi transisi yang mencakup pelatihan sumber daya manusia, revisi dokumentasi, serta audit internal berbasis struktur kontrol baru. Kesimpulan akhir menunjukkan bahwa meskipun struktur ISO 27001:2022 menawarkan fleksibilitas dan relevansi terhadap ancaman modern, Lembaga XYZ perlu memperkuat kesiapan internal agar proses transisi dapat berjalan optimal.

Kata kunci— **ISO 27001:2013, ISO 27001:2022, ISMS, keamanan informasi, strategi transisi standar, analisis gap.**