ABSTRAK

Permasalahan dalam penelitian ini berkaitan dengan bagaimana pengelolaan risiko keamanan informasi di PT XYZ belum sepenuhnya sesuai dengan standar yang ditetapkan, khususnya pada beberapa kontrol yang terdapat dalam Annex A ISO/IEC 27001:2022. Topik ini penting karena semakin tingginya ketergantungan perusahaan pada sistem informasi menuntut perlindungan yang memadai terhadap aset informasi, namun dalam praktiknya masih ditemukan celah seperti ketersediaan perangkat cadangan dan penghapusan data yang tidak konsisten. Solusi yang dilakukan adalah melakukan evaluasi dan analisis risiko berdasarkan standar ISO/IEC 27001:2022, dengan metode observasi, wawancara, dan studi dokumen, serta membandingkan kondisi eksisting terhadap kontrol standar tersebut. Dari hasil analisis gap, disusun penilaian risiko dan diberikan rekomendasi teknis yang relevan mengacu pada panduan ISO/IEC 27002:2022. Hasil utama dari penelitian ini menunjukkan bahwa terdapat beberapa kontrol yang memerlukan peningkatan implementasi, serta telah disusun rekomendasi perbaikan yang dapat mendukung penguatan keamanan informasi secara menyeluruh di perusahaan.

Kata Kunci: keamanan informasi, manajemen risiko, evaluasi, ISO/IEC 27001:2022, ISO/IEC 27002:2022, audit.