ABSTRAK

Perusahaan *financial technology* (fintech) seperti PT XYZ menghadapi tantangan kompleks dalam pengelolaan keamanan informasi, terutama karena tingginya ketergantungan terhadap sistem digital dan tekanan regulasi dari otoritas seperti seperti UU ITE, PP PSTE, serta peraturan OJK dan Bank Indonesia. Permasalahan utama yang teridentifikasi adalah belum optimalnya proses pencatatan dan klasifikasi aset informasi, lemahnya dokumentasi kontrol keamanan, serta tidak tersedianya *Statement of Applicability (SoA)* sebagai acuan pengendalian berbasis ISO 27001:2022. Penelitian ini bertujuan untuk mengimplementasikan kerangka Sistem Manajemen Keamanan Informasi berdasarkan ISO 27001:2022, dengan pendekatan siklus manajemen *Plan–Do–Check–Act* (PDCA). Metode penelitian menggunakan pendekatan kualitatif pada divisi *IT Security & Operation, IT & Network,* serta *IT Planning & Development*. Hasil penelitian menunjukkan bahwa dari total 93 kontrol yang terdapat dalam Annex A ISO/IEC 27001:2022, sebanyak 76 kontrol telah diimplementasikan dan 17 kontrol lainnya belum diterapkan, menghasilkan tingkat kesiapan implementasi sebesar 82%. Penelitian ini berhasil menyusun dokumen SoA yang memuat daftar kontrol keamanan, status penerapan, dan justifikasi pengendalian, serta menghasilkan rekomendasi perbaikan strategis yang memperkuat ketahanan sistem, integritas data, dan kepatuhan regulasi. Dengan demikian, implementasi ISO/IEC 27001:2022 tidak hanya mendukung keamanan informasi di PT XYZ secara menyeluruh, tetapi juga meningkatkan kepercayaan pengguna terhadap layanan digital perusahaan.

Kata Kunci: Fintech, ISO 27001:2022, Kepatuhan Regulasi, Manajemen Risiko, Sistem Manajemen Keamanan Informasi.