

ABSTRAK

Seiring dengan meningkatnya kebutuhan organisasi terhadap sistem informasi, ancaman terhadap keamanan informasi juga akan semakin beragam. Penelitian ini bertujuan untuk menganalisis dan merancang pengelolaan risiko keamanan informasi pada PT. Dago Endah divisi *accounting* menggunakan framework ISO/IEC 27005:2022. Framework ISO/IEC 27005:2022 merupakan standar internasional yang memberikan panduan sistematis untuk manajemen risiko keamanan informasi. Hasil identifikasi risiko berdasarkan ISO/IEC 27002:2022 menunjukkan adanya kontrol yang belum terpenuhi pada empat aspek *Organizational Control*, *People Control*, *Physical Control*, dan *Technology Control*. Dari analisis risiko, ditemukan beberapa ancaman dengan tingkat risiko tinggi dan sangat tinggi. Ancaman-ancaman ini meliputi keputusan yang tidak tepat akibat penilaian insiden yang salah, karyawan atau vendor membocorkan informasi sensitif, organisasi lambat merespons serangan DoS, karyawan tidak melaporkan insiden keamanan, serta karyawan sembarangan menekan tautan malware atau mengakses situs phishing.

Kata kunci: **ISO/IEC 27005:2022, Manajemen Risiko Keamanan Informasi, Penilaian Risiko, Rekomendasi Kontrol Keamanan Informasi**