ABSTRAK

Di era digital, keamanan informasi telah menjadi perhatian penting bagi organisasi karena meningkatnya ancaman yang ditimbulkan oleh insiden siber. Penelitian ini bertujuan untuk memitigasi risiko keamanan informasi melalui optimalisasi penilaian risiko berdasarkan standar ISO 27005:2022 dan NIST SP 800-300 Revisi 1 di Perusahaan XYZ. Penelitian ini menggunakan pendekatan kualitatif, dengan menggunakan observasi dan wawancara sebagai metode pengumpulan data primer untuk mendapatkan wawasan tentang praktik dan tantangan yang dihadapi dalam mengelola risiko keamanan informasi.

Temuan menunjukkan bahwa Perusahaan XYZ telah menerapkan beberapa strategi manajemen risiko, namun masih terdapat kerentanan yang signifikan yang perlu ditangani. Integrasi kerangka kerja ISO 27005:2022 dan NIST SP 800-30 Revisi 1 menyediakan metodologi yang komprehensif untuk menilai dan menangani risiko, meningkatkan kemampuan organisasi untuk melindungi aset informasinya secara efektif. Penelitian ini berkontribusi pada pengetahuan yang sudah ada dengan menawarkan kerangka kerja penilaian risiko yang disesuaikan yang dapat diadaptasi oleh organisasi lain yang menghadapi tantangan serupa.

Berdasarkan hasil penelitian, disarankan agar Perusahaan XYZ berinvestasi dalam pelatihan berkelanjutan untuk karyawan, meningkatkan komunikasi mengenai kebijakan keamanan, dan secara teratur meninjau dan memperbarui praktik manajemen risiko mereka untuk beradaptasi dengan ancaman yang terus berkembang.

Kata kunci: Keamanan Informasi, Penilaian Risiko, ISO 27005, NIST SP 800-30 Revisi 1.