ABSTRAK

Industri telekomunikasi di Indonesia telah mengalami perkembangan pesat sejak tahun 1980-an, dengan peningkatan signifikan dalam penggunaan internet dan telepon seluler. Namun, industri ini juga menghadapi tantangan besar terkait keamanan data, dengan banyaknya kasus kebocoran data yang menimbulkan kekhawatiran terhadap perlindungan informasi pribadi pengguna. PT XYZ, sebagai penyedia layanan internet, perlu mengadopsi langkah-langkah keamanan yang efektif untuk melindungi aset informasinya dari ancaman yang semakin kompleks.

Penelitian ini bertujuan untuk mengidentifikasi kerentanan dan ancaman terhadap aset-aset perusahaan, menganalisis dampaknya, melakukan penilaian risiko, serta memberikan rekomendasi kontrol untuk mengatasi tingkat risiko. Fokus utama penelitian ini adalah pada aspek keamanan informasi perusahaan, dengan menggunakan standar internasional ISO 27001:2022 sebagai kerangka kerja untuk memastikan pendekatan yang lebih komprehensif terhadap keamanan informasi.

Metode penelitian yang digunakan meliputi evaluasi risiko, mitigasi risiko, serta evaluasi dan penilaian risiko. Proses ini mencakup pengenalan kerentanan dan ancaman, analisis dampak risiko, serta penentuan langkah-langkah pengendalian yang tepat untuk meminimalkan kemungkinan terjadinya risiko. Data yang digunakan dalam penelitian ini diperoleh dari kuesioner, wawancara, serta dokumentasi perusahaan.

Hasil penelitian menunjukkan bahwa tingkat kematangan keamanan informasi di PT XYZ secara keseluruhan adalah 91%, dengan beberapa area yang memerlukan perbaikan, seperti parameter keamanan fisik dan akses fisik. Penelitian ini mengidentifikasi 19 jenis kerentanan dan 11 jenis ancaman yang berpotensi menyasar aset perusahaan. Berdasarkan analisis risiko, disarankan agar PT XYZ meningkatkan kontrol pengendalian fisik dan melakukan tindakan manajemen risiko jangka menengah dan panjang untuk aset dengan prioritas risiko tertinggi.

Penelitian ini berfokus pada analisis risiko aset di PT XYZ, sebuah perusahaan ISP, dengan menggunakan standar Annex A7 ISO 27001:2022, sehingga hasilnya mungkin tidak dapat digeneralisasi ke perusahaan telekomunikasi lain. Data yang digunakan sebagian besar berasal dari kuesioner dan wawancara yang berpotensi bias. Penelitian ini dapat menjadi referensi bagi penelitian selanjutnya di ISP lain, dengan penekanan pada pentingnya analisis pengendalian teknologi untuk memastikan keamanan informasi sesuai kerangka ISO/IEC 27001 dalam memitigasi pembobolan data.

Kata Kunci: Penilaian risiko, manajemen risiko aset, ISO 27001, kontrol keamanan fisik