BAB V
KESIMPULAN

5.1 Kesimpulan

Hasil penelitian tentang Analisis Kesesuaian PT XYZ terhadap Standar ISO 27001:2022 dalam Mengatasi Ancaman Pencurian Data dengan Metode Decision Tree berikut adalah beberapa kesimpulan yang dapat diambil dari penelitian tersebut:

1. PT XYZ memperoleh nilai persentase sebesar 96%, berada pada tingkat Optimisasi, berdasarkan hasil pengukuran tingkat kematangan (maturity level) seluruh unit atau departemen terhadap standar ISO 27001:2022. Hal ini menunjukkan bahwa PT XYZ telah menerapkan praktik terbaik untuk setiap kontrol Annex pada ISO 27001:2022, dan bahwa mereka telah mendokumentasikan pelaksanaan tersebut dalam kebijakan dan prosedur yang sesuai. Oleh karena itu, dapat disimpulkan bahwa PT XYZ sangat siap untuk mencegah pencurian data dan aset perusahaan.

2. Siklus Plan-Do-Check-Act (PDCA) pada PT XYZ beroperasi dengan baik dan konsisten sesuai dengan standar ISO 27001:2022. Organisasi harus menetapkan ruang lingkup, konteks, dan perencanaan manajemen risiko pada tahap Plan. Pada tahap Do, mereka harus memastikan implementasi kontrol keamanan secara menyeluruh dan terdokumentasi. Pada tahap Check, mereka melakukan audit internal untuk menilai efektivitas, dan pada tahap Act, mereka melakukan perbaikan terus menerus berdasarkan temuan audit dan evaluasi. Ini akan memperkuat kesiapan perusahaan untuk menghadapi ancaman pencurian data.

3. Dengan menggunakan algoritma Decision Tree ID3, analisis menunjukkan bahwa pengendalian organisasi (pengendalian organisasi) memiliki pengaruh terbesar terhadap tingkat kesiapan PT XYZ, dengan nilai kontribusi 0,342, diikuti oleh pengendalian teknologi (pengendalian teknologi) dengan nilai kontribusi 0,235, dan faktor lain seperti konteks organisasi (0,124), dukungan (0,111), perencanaan (0,094), dan evaluasi kinerja (0,094) juga berpengaruh, tetapi hanya dengan tingkat kesiapan Sementara itu, karena variasi data yang

kurang signifikan, fitur seperti manajemen, operasional, pengendalian manusia, pengendalian fisik, dan peningkatan tidak terlihat sebagai penentu. Secara keseluruhan, hasil ini menunjukkan bahwa peningkatan tata kelola organisasi dan pengendalian teknologi merupakan komponen utama dalam membangun sistem keamanan informasi yang berfungsi dengan baik, dan bahwa komponen lainnya berfungsi sebagai pendukung keberlanjutan sistem.

5.2 Saran

Berdasarkan hasil analisis dan kesimpulan yang diperoleh, penulis memberikan saran sebagai berikut:

1. Meningkatkan Tata Kelola Organisasi dan Kontrol Teknologi

PT XYZ harus terus memperkuat sistem keamanan informasi melalui kebijakan yang lebih ketat, prosedur yang terdokumentasi, dan pengawasan terus menerus. Untuk mengantisipasi ancaman siber yang berkembang, pengendalian teknologi juga harus diperkuat dengan menerapkan teknologi keamanan terbaru.

2. Pemeliharaan Audit Internal dan Evaluasi Berkala

Meskipun tingkat kematangan perusahaan berada pada kategori optimisasi, perusahaan masih harus melakukan audit internal secara berkala sesuai siklus PDCA. Ini dilakukan untuk memastikan bahwa penerapan ISMS berjalan dengan baik serta untuk menemukan potensi celah keamanan yang mungkin muncul sebagai akibat dari perubahan bisnis dan teknologi.

3. Meningkatkan Perencanaan, Dukungan, dan Evaluasi

Meskipun dua faktor utama tidak memberikan kontribusi yang signifikan, elemen perencanaan, dukungan sumber daya, dan evaluasi harus diperkuat untuk memastikan implementasi jangka panjang ISMS dan kemampuan untuk menyesuaikannya dengan perubahan kebutuhan organisasi.
4. Meningkatkan Kesadaran Keamanan Informasi

Untuk mengurangi risiko yang disebabkan oleh faktor manusia, program pelatihan dan sosialisasi keamanan informasi bagi seluruh karyawan harus

ditingkatkan, terutama yang berkaitan dengan kebijakan akses, penggunaan teknologi, dan pengelolaan data sensitif.