BAB I PENDAHULUAN

I.1 Latar Belakang

Keamanan informasi telah menjadi perhatian penting bagi organisasi modern yang mengelola data sensitif, termasuk Lembaga XYZ, yang bertanggung jawab atas perlindungan data sensitif terkait fungsinya di Indonesia. Dengan meningkatnya jumlah ancaman keamanan siber, seperti *malware* dan serangan *phishing*, perlindungan data dalam organisasi ini sangat krusial untuk menjaga integritas dan keandalan informasi (Clarissa & Wang, 2023). Lembaga XYZ saat ini menggunakan standar keamanan informasi *International Organization for Standardization* atau ISO versi 27001:2013 yang telah memberikan kerangka kerja untuk mengidentifikasi, mengelola, dan mengurangi risiko keamanan informasi.

Namun pada tahun 2022, ISO 27001 mengalami pembaruan yang signifikan. Pembaruan signifikan tersebut, seperti pengurangan jumlah kontrol dari 114 menjadi 93, pengelompokan ulang dalam empat domain utama (Organizational, People, Physical, Technological), serta penambahan kontrol baru yang mencakup isu ancaman keamanan informasi masa kini seperti penghapusan data, pengamanan layanan cloud, dan pengkodean aman (Nurmi, 2024). ISO 27001:2022 juga memperkenalkan peningkatan dalam pengelolaan risiko yang lebih terintegrasi serta kontrol baru yang relevan dengan lingkungan digital saat ini. Standar baru ini memiliki lebih sedikit kontrol dibanding versi 2013, tetapi lebih fokus pada efektivitas dan pemantauan yang berkelanjutan terhadap keamanan informasi (Lullah dkk., 2024). Pembaruan ini mendorong perlunya evaluasi kesiapan terhadap sistem ISMS yang telah berjalan. Penelitian ini menggunakan pendekatan ilmiah melalui metode kualitatif berbasis studi kasus, didukung oleh model konseptual Design Science Research (DSR) untuk memandu tahapan pengembangan dan evaluasi solusi. Selain itu, kerangka kerja Plan-Do-Check-Act (PDCA) juga digunakan sebagai prinsip siklus hidup manajemen yang selaras dengan struktur ISO 27001, khususnya dalam proses perencanaan, implementasi, monitoring, dan perbaikan berkelanjutan terhadap sistem keamanan informasi.

Penelitian ini bertujuan untuk menganalisis gap antara penerapan ISO 27001:2013 yang saat ini diterapkan di Lembaga XYZ dengan persyaratan dalam ISO 27001:2022. Analisis ini akan memberikan panduan mengenai area yang perlu diperbarui atau disesuaikan agar standar keamanan informasi di Lembaga XYZ tetap relevan dan efektif dalam menghadapi risiko yang berkembang (Fadli, 2024). Dengan memahami kesenjangan antara kedua standar ini, Lembaga XYZ diharapkan dapat melakukan transisi secara strategis, yang pada akhirnya dapat meningkatkan perlindungan terhadap data sensitif serta keandalan layanan yang diberikan.

I.2 Perumusan Masalah

Berdasarkan latar belakang di atas, maka rumusan permasalahan untuk penelitian ini adalah:

1) Bagaimana kesesuaian dokumen Lembaga XYZ terhadap perbedaan ISO 27001:2013 dengan ISO 27001:2022 dalam hal Sistem Manajemen Keamanan Informasi?
2) Apa saja rekomendasi yang dapat diberikan untuk mengatasi kesenjangan yang ada agar penerapan ISO 27001:2022 di Lembaga XYZ dapat berjalan optimal dan sesuai standar terbaru?

I.3 Tujuan Penelitian

Penelitian ini bertujuan untuk:

1) Mengidentifikasi perbedaan utama antara ISO 27001:2013 dan ISO 27001:2022 serta dampaknya pada penerapan Sistem Manajemen Keamanan Informasi di Lembaga XYZ.
2) Memberikan rekomendasi dan strategi kepada Lembaga XYZ dalam menghadapi tantangan transisi dan peningkatan sistem keamanan informasi sesuai dengan standar ISO 27001:2022.

I.4 Batasan Penelitian

1) Penelitian hanya akan difokuskan pada penerapan Sistem Manajemen Keamanan Informasi di Lembaga XYZ dengan fokus pada transisi dari ISO 27001:2013 ke ISO 27001:2022.
2) Penelitian ini hanya mencakup perbandingan antara ISO 27001:2013 dan ISO 27001:2022, tanpa membahas standar keamanan informasi lainnya.
3) Data yang digunakan dalam analisis bersumber dari dokumentasi internal Lembaga XYZ berupa wawancara dan analisis dokumen pada penerapan standar ISO.
4) Rekomendasi akan disesuaikan dengan kondisi dan kapasitas Lembaga XYZ dalam mengimplementasikan standar ISO 27001:2022.
5) Analisis yang dilakukan hanya mencakup aspek-aspek utama dari ISO 27001:2022 yang berbeda dari ISO 27001:2013 dan relevan dengan konteks operasional Lembaga XYZ.

I.5 Manfaat Penelitian

Manfaat penelitian ini:

1) Penulis berharap penelitian ini bermanfaat sebagai literatur rujukan tentang analisis gap penerapan standar ISO 27001 khususnya dalam konteks perubahan dari versi 2013 ke versi 2022, yang dapat digunakan sebagai referensi bagi peneliti lain yang memiliki fokus serupa.
2) Bagi Telkom University, penelitian ini dapat meningkatkan reputasi universitas dengan berkontribusi pada pengembangan teknologi yang relevan dengan industri keamanan informasi, khususnya dalam penerapan standar internasional ISO 27001:2022 di institusi pemerintah. Penelitian ini juga membuka peluang kerja sama antara Telkom University dengan lembaga pemerintah dan industri keamanan siber untuk menciptakan solusi yang lebih inovatif dan efektif dalam melindungi data sensitif, sekaligus memperkaya wawasan mahasiswa dan dosen dalam bidang keamanan informasi yang berkembang pesat.

I.6 Sistematika Penulisan

Penelitian ini diuraikan dengan sistematika penulisan sebagai berikut:

Bab I **Pendahuluan**

Konteks permasalahan, latar belakang penelitian, perumusan masalah, tujuan penelitian, batasan penelitian, manfaat penelitian, dan sistematika penulisan diuraikan dalam bab ini.

Bab II **Tinjauan Pustaka**

Teori dan penelitian terdahulu yang relevan dengan topik penelitian disajikan dalam bab ini. Selain itu, dijelaskan beberapa metodologi atau kerangka kerja yang digunakan dalam penelitian sebelumnya untuk mengatasi permasalahan, serta analisis pemilihan metodologi yang akan digunakan dalam penelitian ini.

Bab III **Metodologi Penelitian**

Bab ini menjelaskan pendekatan dan langkah-langkah yang digunakan untuk menyelesaikan penelitian. Metode pengumpulan data diuraikan, termasuk teknik yang digunakan untuk mendapatkan data yang relevan dan valid. Juga menjelaskan bagaimana data yang terkumpul akan dianalisis untuk memberikan hasil yang objektif dan dapat diandalkan. Pada bab ini, peneliti juga memastikan bahwa teknik yang dipilih sesuai dengan tujuan dan pertanyaan penelitian.

Bab IV **Analisis**

Pada bab ini, dilakukan analisa terhadap data yang telah dikumpulkan untuk menjawab rumusan masalah yang telah ditetapkan sebelumnya. Bab ini bertujuan untuk memberikan pemahaman mendalam tentang hasil penelitian, baik secara kualitatif maupun kuantitatif, dengan menghubungkan temuan yang diperoleh terhadap teori atau konsep yang relevan.

Bab V **Hasil dan Evaluasi**

Hasil rancangan, temuan, analisis dan pengolahan data terdapat pada bab ini. Selain itu juga berisi tentang validasi atau verifikasi hasil dari

penelitian, sehingga hasil tersebut apakah telah benar-benar menyelesaikan masalah atau menguraikan gap antara kondisi eksisting dan target yang akan dicapai. Analisis yang digunakan di bab ini untuk lebih mengetahui hasil penelitian dapat diterapkan baik secara khusus di konteks penelitian maupun secara umum di konteks serupa (misal perusahaan di sektor serupa). Selain itu metode-metode evaluasi yang lain dapat di terapkan untuk memvalidasi hasil TA sesuai dengan kebutuhan.

Bab VI Kesimpulan dan Saran

Kesimpulan dari penelitian serta jawaban dari aspek permasalahan terdapat pada bab ini. Saran penelitian dikemukakan pada bab ini untuk memberikan arah bagi penelitian selanjutnya, baik dalam hal pengembangan metodologi, pemilihan topik yang lebih mendalam, atau implementasi hasil pada penelitian selanjutnya.