BAB I
PENDAHULUAN

1.1. Latar Belakang

Teknologi informasi merupakan sumber daya yang dapat menyediakan informasi penting untuk membantu dalam sebuah organisasi (Galbraith, 2012)[1]. Teknologi informasi telah mengalami perkembangan yang pesat saat ini. Perkembangan ini mampu mengubah gaya hidup dan budaya kehidupan manusia. Dengan berkembangnya Teknologi Informasi banyak organisasi menerapkan Teknologi Informasi untuk mempermudah sebuah pekerjaan. Banyak organisasi yang saat ini sudah menggunakan Teknologi informasi untuk menunjang efisiensi pekerjaan salah satunya adalah penggunaan website.

PT XYZ adalah perusahaan integrator sistem independen terkemuka di Indonesia dengan keahlian Teknik lengkap dalam Otomasi Industri, Integrasi Perusahaan, dan Solusi Manufaktur Strategis. Salah satu bagian keamanan informasi yang mempengaruhi keamanan teknologi informasi adalah keamanan informasi (Bernard, 2011)[2]. Adapun kendala yang dihadapi dalam pengelolaan Sistem Informasi yang dimiliki oleh perusahaan yaitu serangan *Virus* dan ancaman terhadap Aset TI lainnya. Dengan demikian, isu keamanan menjadi permasalahan yang penting untuk organisasi tersebut.

Kekuatan keamanan informasi dapat dikontrol menggunakan sistem keamanan informasi, berfungsi untuk mengatur dan mengoperasikan keamanan sistem informasi agar dapat digunakan sesuai dengan prosedur (Sheikhpour & Modiri, 2012)[3]. Tujuan dari Sistem Manajemen Keamanan Informasi (SMKI) adalah menjamin kerahasiaan, keutuhan, dan ketersediaan dari data dan informasi (Sheikhpour & Modiri, 2012).

Ada beberapa standar maupun framework yang biasa digunakan sebagai best practice dalam implementasi SMKI, seperti COBIT 5 for Information Security, NIST Cybersecurity Framework, NIST 800-53, CIS Control (CSC) dan ISO/IEC 27001. Pada penelitian ini, akan menggunakan Standar ISO/IEC 27001, karena standar tersebut ISO/IEC merupakan standar yang dapat digunakan untuk

membantu menetapkan keamanan informasi sesuai aturan dan memiliki fokus untuk menetapkan kebijakan berdasarkan analisis risiko dan kebutuhan pengguna[4].

Berdasarkan hasil observasi dan wawancara yang sudah penulis lakukan bahwa pengelolaan TI pada PT.XYZ ditemukan beberapa control pada klausul *annex* yang masih belum terpenuhi sesuai ISO 27001:2013 yang berdampak pada manajemen keamanan informasi PT.XYZ dan dapat mempengaruhi kinerja dari perusahaan.

Analisis Manajemen Keamanan Informasi menggunakan control ISO 27001:2013 akan dilakukan untuk mengatasi permasalahan terhadap pentingnya kerahasiaan data di PT. XYZ dan sebagai kontrol dalam proses pengelolaan manajemen keamanan. Penerapan ISO 27001:2013 dapat mendeteksi dini bagian-bagian yang berpotensi menyebabkan terjadinya kebocoran data atau hilangnya informasi dan data. Penelitian ini bertujuan untuk menganalisis Sistem Manajemen Keamanan Informasi yang dapat digunakan sebagai pedoman kebijakan keamanan informasi pada PT.XYZ.

1.2. Perumusan Masalah

Berdasarkan latar belakang yang dijabarkan diatas bahwa penelitian ini berfokus pada sistem informasi pada PT.XYZ, maka penulis membuat rumusan masalah dalam penelitian ini yaitu:

1. Bagaimana melakukan analisis manajemen keamanan informasi menggunakan standar ISO 27001:2013 dengan kontrol *annex* (A.8 Manajemen Aset), (A.9 Kontrol Akses), (A.10 Kriptografi), (A.11 Pengamanan Fisik dan Lingkungan), (A.12 Keamanan Operasional), (A.13 Keamanan Komunikasi), (A.14 Akuisisi, Pengembangan, dan Pemeliharaan Sistem) pada PT.XYZ?
2. Apa saja rekomendasi berdasarkan komtrol *annex* (A.8 Manajemen Aset), (A.9 Kontrol Akses), (A.10 Kriptografi), (A.11 Pengamanan Fisik dan Lingkungan), (A.12 Keamanan Operasional), (A.13 Keamanan Komunikasi), (A.14 Akuisisi, Pengembangan, dan Pemeliharaan Sistem)

untuk meningkatkan keamanan informasi di PT. XYZ?

1.3. Batasan Masalah

Tugas Akhir ini hanya berfokus dalam beberapa hal. Batasan masalah tersebut meliputi:

1. Penelitian Analisis Manajemen Keamanan Informasi Menggunakan Kontrol ISO 27001:2013 dilakukan sampai tahap assessment saja dikarenakan batasan resource.
2. Batasan masalah penelitian ini hanya menggunakan control *Annex* (A.8 Manajemen Aset), (A.9 Kontrol Akses), (A.10 Kriptografi), (A.11 Pengamanan Fisik dan Lingkungan), (A.12 Keamanan Operasional), (A.13 Keamanan Komunikasi), (A.14 Akuisisi, Pengembangan, dan Pemeliharaan Sistem)
3. Penelitian ini tidak melakukan identifikasi dan penaksiran dampak finansial pada *risk assessment*.
4. Penelitian ini hanya sampai tahap rekomendasi, tidak sampai tahap perancangan.

1.4. Tujuan

Berdasarkan rumusan masalah, maka terdapat beberapa tujuan penelitian, antara lain:

1. Menganalisis implementasi keamanan informasi pada PT. XYZ menggunakan standar ISO 27001:2013 dengan Kontrol *Annex* (A.8 Manajemen Aset), (A.9 Kontrol Akses), (A.10 Kriptografi), (A.11 Pengamanan Fisik dan Lingkungan), (A.12 Keamanan Operasional), (A.13 Keamanan Komunikasi), (A.14 Akuisisi, Pengembangan, dan Pemeliharaan Sistem)
2. Menghasilkan rekomendasi berdasarkan analisis dari hasil Kontrol *Annex* (A.8 Manajemen Aset), (A.9 Kontrol Akses), (A.10 Kriptografi), (A.11 Pengamanan Fisik dan Lingkungan), (A.12 Keamanan Operasional), (A.13 Keamanan Komunikasi), (A.14 Akuisisi, Pengembangan, dan Pemeliharaan Sistem) untuk meningkatkan keamanan informasi di PT.XYZ.

1.5. Rencana Kegiatan

Penelitian ini akan menjelaskan mengenai analisis manajemen keamanan informasi pada PT. XYZ. Metode pengumpulan data sendiri menggunakan wawancara dan kuesioner dimana peneliti mendapatkan informasi dan memberikan pertanyaan kepada pegawai di Divisi IT PT.XYZ. Penelitian ini juga menggunakan standar manajemen keamanan informasi berdasarkan ISO 27001:2013 untuk melakukan analisisnya.