BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan zaman membuat banyak perubahan-perubahan yang signifikan secara global, salah satu perkembangan yang sangat pesat dapat kita rasakan seiring berjalannya waktu [1]. Awalnya manusia bertahan hidup dengan mengelola bahan mentah atau bahan baku untuk dijadikan suatu kebutuhan pokok, namun seiring perjalanan waktu manusia mengembangkan banyak inovasi baru untuk dapat bertahan hidup. Hingga pada abad ke-18, merupakan awal dari revolusi industri 4.0, dimana hal tersebut berdampak bagi kehidupan manusia dikarenakan adanya era baru yang tercipta yaitu era teknologi [1]. Pada era ini, manusia semakin melibatkan perkembangan teknologi dalam kehidupannya. Berkembangnya teknologi memberikan dampak baik bagi kehidupan manusia, dimana adanya teknologi membantu manusia dalam melakukan aktivitas sehari-hari agar lebih efektif dan efisien. Selain teknologi yang berkembang dalam kehidupan sehari-hari manusia, teknologi banyak dimanfaatkan dalam pengembangan industri, dimana di zaman sekarang sudah banyak sekali perusahaan yang memanfaatkan teknologi untuk menciptakan lahan bisnis berbasis internet dan digital [2]. Dimana perusahaan di zaman sekarang berusaha untuk dapat mengikuti perkembangan zaman dengan mengimplementasi serta memanfaatkan teknologi yang berkembang. Perusahaan yang memanfaatkan teknologi dalam bisnisnya, tentunya menghasilkan dampak yang positif bagi perusahaan. Salah satu dampak positif yang dihasilkan yaitu terciptanya informasi, dimana informasi tersebut dapat diolah menjadi data, yang nantinya dapat digunakan untuk pengambilan keputusan dalam tercapainya tujuan suatu perusahaan [3]. Namun, adapun risiko yang perlu diperhatikan oleh perusahaan, agar suatu perusahaan dapat terus stabil dalam menghasilkan data-data untuk dapat bersaing serta mengembangkan perusahaan di era teknologi. Risiko tersebut adalah adanya ancaman risiko terhadap Informasi [4].

Ancaman risiko terhadap Informasi perlu diperhatikan karena informasi merupakan *asset* berharga suatu perusahaan dalam membantu pengambilan keputusan [5]. Terdapat banyak ancaman risiko yang perlu diwaspadai oleh perusahaan, salah satunya adalah *cyber-crime*. *Cyber-crime* sendiri adalah kejahatan *illegal* yang dilakukan di dunia maya, yang memanfaatkan celah pada suatu sistem agar dapat menyerang sistem tersebut yang dapat berdampak kerusakan dan dapat merugikan perusahaan [6]. *Cyber-crime* sendiri sudah menjadi kekhawatiran dari tahun 1999, terdapat penelitian yang mengatakan bahwa di era yang berkembang memanfaatkan teknologi, teknologi justru dapat menjadi celah atau salah satu unsur untuk mendukung kejahatan, sehingga diperlukan tindakan untuk menjaga keamanan [7]. Apabila suatu perusahaan mengalami ancaman *cyber-crime*, maka terdapat dampak yang dapat terjadi pada perusahaan dan sifatnya merugikan perusahaan, seperti informasi perusahaan yang disalahgunakan atau lainnya. Adapun upaya atau tindakan yang dapat dilakukan untuk menjaga informasi serta aset perusahaan, apabila perusahaan menghadapi *cyber-crime* atau kejahatan *illegal* yaitu dengan *cyber-security* [8].

Cyber-security sendiri merupakan tindakan pencegahan terhadap kejahatan siber yang telah dikembangkan dari tahun ke tahun. Menurut Ben Densham suatu perusahaan perlu mengubah pola pikir dalam dunia digital, dimana perusahaan jangan menunggu adanya serangan namun perusahaan perlu berpikir mengharapkan adanya serangan atau ancaman siber [8]. Dengan pola pikir tersebut, maka perusahaan harus menyusun rencana untuk menghadapi hal tersebut [9]. Adapun riset yang pernah dilakukan pada perusahaan-perusahaan *small business* di Australia, dimana pada riset tersebut diketahui bahwa perusahaan-perusahaan di Australia masih kurang dalam menghadapi *cyber-security* yang terjadi karena kurangnya arsitektur TI atau ukuran *cohort* yang besar, sehingga diperlukan kebijakan yang dapat membantu perusahaan dalam menghadapi serangan atau ancaman [10]. Tidak hanya dunia industri saja yang perlu memahami pentingnya *cyber-security* dalam instansinya, pada masa pandemi pun organisasi dibidang kesehatan perlu untuk memahami rangkaian kontrol keamanan informasi, hal ini

dikarenakan sistem layanan di masa pandemi menjadi target utama serangan siber [11]. Oleh sebab itu, *cyber-security* merupakan tindakan yang perlu dilakukan oleh suatu perusahaan, agar dapat menghadapi serangan atau ancaman dari kejahatan siber. Selain itu, adanya *cyber-security* dalam suatu perusahaan tentunya dapat membantu perusahaan dalam mencegah adanya ancaman risiko terhadap informasi perusahaan. Salah satu tindakan *cyber-security* untuk mengamankan informasi dalam perusahaan adalah keamanan informasi [8]. Keamanan informasi sendiri merupakan hal penting yang perlu diterapkan oleh suatu perusahaan. Penerapan keamanan informasi dalam suatu perusahaan berguna untuk mencapai 3 tujuan utama yaitu aspek kerahasian, ketersedian, dan integritas informasi [5]. Salah satu penerapan keamanan informasi yang dapat diterapkan oleh perusahaan adalah dengan melakukan evaluasi Sistem Manajemen Keamanan Informasi pada perusahaan. Evaluasi Sistem Manajemen Keamanan Informasi merupakan acuan bagi perusahaan dalam memastikan keamanan informasi di perusahaannya [12]. Dalam mengevaluasi Sistem Manajemen Keamanan Informasi suatu perusahaan, maka diperlukan *framework* atau standar pendukung untuk menjadi pedoman atau acuan dalam melakukan evaluasi Sistem Manajemen Keamanan Informasi [13].

Ada banyak *framework* untuk tata kelola keamanan informasi seperti COBIT dan ISO 17799 (ISO 17799 merupakan adopsi dari BS7799), dimana kedua *framework* tersebut merupakan pedoman atau acuan dalam tata kelola keamanan informasi. Akan tetapi, setelah dilakukan pemetaan terhadap kedua *framework* tersebut, diketahui bahwa konten ISO 17799 lebih bermanfaat dalam menerapkan lingkungan tata kelola keamanan informasi yang komprehensif dan terstandarisasi [14]. Seiring berjalannya waktu, pada tahun 2005 *framework* ISO 17799 pun direvisi untuk menyelaraskan dengan praktik dan kemajuan yang berlaku pada saat itu, sehingga muncul ISO 27001:2005 sebagai hasil revisi dari ISO 17799 [15]. ISO 27001 sendiri merupakan *framework* yang berfokus kepada Sistem Manajemen Keamanan Informasi. Dengan suatu perusahaan menggunakan ISO 27001, maka perusahaan memiliki acuan dalam menjaga keamanan informasi yang sesuai dengan

standar internasional. Terbitnya standarisasi ISO 27001 ini tentunya bermanfaat bagi perusahaan yaitu sebagai acuan dalam menjaga keamanan informasi yang disesuaikan standar internasional. Adapun sertifikasi untuk ISO 27001, dimana sertifikasi ISO 27001 dapat memberikan manfaat bagi perusahaan, seperti diakuinya kredibilitas perusahaan, meningkatnya kepercayaan konsumen, serta menjamin kualitas perusahaan sesuai dengan standar internasional [16]. ISO 27001 sendiri tentunya terus berkembang dan memperbaharui konten didalamnya, untuk menyelaraskan kebutuhan di masa tersebut [17]. Dari ISO 27001:2005 hingga akhirnya sekarang ISO 27001 sudah mencapai versi 2022 (ISO 27001:2022). Namun, salah satu standarisasi ISO 27001 versi 2013 merupakan versi yang sering dijumpai di Indonesia. Hal ini dikarenakan di Indonesia sendiri terdapat *tools* dalam melakukan evaluasi terhadap tingkat kematangan dan kesiapan keamanan informasi yang telah disesuaikan dengan standar ISO 27001 versi 2013 dan standar yang berlaku di negara Indonesia, *tools* tersebut yakni Indeks KAMI (Keamanan Informasi) [18]. Salah satu perusahaan di Indonesia yaitu PT XYZ, merupakan perusahaan yang menyadari akan pentingnya penerapan Keamanan Informasi beserta dengan manfaat yang bisa didapatkan dengan melakukan sertifikasi ISO 27001.

PT XYZ sendiri merupakan salah satu perusahaan di Indonesia yang bergerak di bidang pariwisata atau *travel agent*, dimana diketahui PT XYZ telah mengambil sertifikasi ISO 27001:2013 pada lingkup Proses *Payment*. Lingkup tersebut dilakukan sertifikasi dikarenakan lingkup tersebut mengandung banyak informasi terkait dengan *user* seputar data pribadi, informasi kartu kredit, dan lainnya. Adapun, pada saat wawancara dengan pihak perusahaan, diketahui saat pengambilan sertifikasi tersebut masih terdapat aspek dalam sertifikasi ISO 27001 yang masih perlu diperbaiki. Aspek tersebut yaitu Annex 7 yang terdapat pada ISO 27001 versi 2013, yang membahas mengenai *screening* verifikasi latar belakang terhadap calon tenaga kerja. Adanya hal tersebut, PT XYZ berusaha untuk memperbaiki Sistem Manajemen Keamanan Informasi yang terdapat pada perusahaan. Selain itu, untuk mempertahankan kompatibel dalam bersaing dengan industri lain,

mempertahankan konsumen, serta jaminan layanan yang sesuai dengan standar internasional, maka PT XYZ akan melakukan sertifikasi ISO 27001 kembali di tahun yang akan datang. Hal tersebut dikarenakan sertifikasi ISO 27001 yang telah didapatkan suatu perusahaan memiliki masa berlaku yaitu maksimal 3 tahun. Sehingga, untuk mempersiapkan sertifikasi ISO 27001 di tahun yang akan datang, diperlukan evaluasi Sistem Manajemen Keamanan Informasi dengan standar ISO 27001 yang dapat dilakukan secara berkala. Hasil dari evaluasi tersebut dapat digunakan oleh perusahaan dalam mematangkan dan mempersiapkan aspek-aspek untuk dapat memenuhi ISO 27001. Maka dari itu, penelitian ini dilakukan dengan harapan dapat berguna untuk membantu PT XYZ dalam kegiatan evaluasi berkala Sistem Manajemen Keamanan Informasi yang sesuai dengan standar ISO 27001 versi 2013 untuk mempersiapkan sertifikasi ISO 27001 pada tahun yang akan datang. Dalam rangka mengevaluasi Sistem Manajemen Keamanan Informasi pada PT XYZ ini pun dibantu dengan *tools* yaitu Indeks KAMI (Keamanan Informasi).

Berdasarkan latar belakang yang ada, maka penelitian ini mengajukan penelitian dengan judul **"Evaluasi dan Rekomendasi Sistem Manajemen Keamanan Informasi pada PT XYZ Berdasarkan Standar ISO 27001:2013 Menggunakan Indeks KAMI"**.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan, adapun berikut merupakan rumusan masalah dalam penelitian skripsi ini sebagai berikut:

1. Bagaimana hasil evaluasi Sistem Manajemen Keamanan Informasi menggunakan indeks KAMI pada PT XYZ?
2. Berapa tingkat atau *level* kematangan dan kesiapan PT XYZ dalam memenuhi Keamanan Informasi yang sesuai dengan standar ISO 27001:2013?
3. Bagaimana hasil rekomendasi pada temuan evaluasi menggunakan Indeks KAMI, yang dapat diberikan dalam rangka meningkatkan Keamanan Informasi pada PT XYZ?

1.3 Batasan Masalah

Dalam mempermudah penulisan skripsi ini adapun batasan masalah, dimana tujuan adanya batasan masalah ini adalah agar penulisan skripsi dapat lebih terarah, terorganisi, serta jelas. Berikut merupakan batasan masalah pada penelitian skripsi ini:

1. Penelitian dilakukan pada PT XYZ yang merupakan salah satu perusahaan penyedia layanan *travel online* di Indonesia.
2. Penelitian ini menggunakan standar ISO 27001 versi 2013 serta menggunakan *tools* Indeks KAMI sebagai alat yang membantu dalam melakukan evaluasi tingkat kematangan serta kelengkapan Keamanan Informasi pada PT XYZ. Indeks KAMI sendiri telah diselaraskan dengan standar ISO 27001 pada versi 2013.
3. Penelitian ini menggunakan data hasil wawancara dan *Forum Group Discussion* (FGD) pada PT XYZ.
4. Penelitian ini menghasilkan evaluasi serta rekomendasi terkait keamanan informasi pada PT XYZ.

1.4 Tujuan dan Manfaat Penelitian

1.4.1 Tujuan Penelitian

Berdasarkan rumusan masalah yang ada, adapun pada penelitian skripsi ini diharapkan dapat memenuhi tujuan yang ingin diraih oleh peneliti. Tujuan penelitian skripsi ini adalah sebagai berikut:

1. Mendapatkan hasil evaluasi untuk Sistem Manajemen Keamanan Informasi pada PT XYZ dengan menggunakan alat bantu Indeks KAMI.
2. Mengetahui tingkat kematangan serta kesiapan PT XYZ dalam memenuhi Keamanan Informasi sesuai acuan standar internasional yaitu ISO 27001 pada versi 2013.

3. Menghasilkan rekomendasi terkait keamanan informasi pada PT XYZ, yang dapat membantu PT XYZ dalam memenuhi standar keamanan informasi.

1.4.2 Manfaat Penelitian

Manfaat yang dapat diperoleh dari penelitian skripsi ini adalah dengan melakukan penelitian untuk mengukur tingkat kematangan serta kesiapan PT XYZ sesuai dengan standar ISO 27001:2013, peneliti mendapatkan ilmu pengetahuan baru serta pemahaman lebih mendalam terkait audit suatu perusahaan dengan menggunakan standar ISO 27001:2013 dan penggunaan *tools* indeks KAMI sebagai alat bantu dalam melakukan evaluasi. Selain itu, dengan melakukan penelitian ini dalam rangka mempersiapkan sertifikasi di tahun yang akan datang, maka PT XYZ dapat mengetahui tingkat kematangan dan kesiapan keamanan informasi pada perusahaan yang sesuai dengan standar ISO 27001:2013. Selain itu, perusahaan mendapatkan referensi hasil evaluasi serta rekomendasi yang dapat dijadikan sebagai acuan untuk meningkatkan keamanan informasi pada perusahaan.

1.5 Sistematika Penulisan

Untuk menyederhanakan dalam mengetahui serta melihat pembahasan dalam penelitian ini, adapun sistematika penulisan yang merupakan kerangka serta pedoman dalam penulisan penelitian. Berikut merupakan sistematika penulisan pada penelitian ini:

BAB I PENDAHULUAN

Bab ini terdiri dari latar belakang yang berisikan gambaran mengenai Keamanan Informasi, *cyber-security*, ISO 27001, Indeks KAMI sebagai *tools* untuk mengevaluasi Sistem Manajemen Keamanan Informasi, *State of the Art* sebagai penelitian terdahulu mengenai Keamanan Informasi, penjelasan secara singkat mengenai PT XYZ. Selain itu, adapun rumusan masalah, batasan masalah,

tujuan dan manfaat penelitian, serta sistematika penulisan penelitian ini.

BAB II LANDASAN TEORI

Bab ini berisi uraian teori mengenai pengertian Keamanan Informasi, Sistem Manajemen Keamanan Informasi (SMKI), *International Organization for Standardization* (ISO), ISO 27001:2013, Indeks KAMI, serta penelitian terdahulu.

BAB III METODOLOGI PENELITIAN

Bab ini membahas mengenai metodologi penelitian yang digunakan dalam penelitian ini. Bab ini berisi gambaran umum objek penelitian, metode penelitian, teknik pengumpulan data, dan teknik analisa data.

BAB IV ANALISIS DAN HASIL PENELITIAN

Bab ini membahas mengenai hasil evaluasi Sistem Manajemen Keamanan Informasi menggunakan Indeks KAMI yang telah dilakukan pada perusahaan, beserta rekomendasi yang berdasarkan standar ISO 27001:2013.

BAB V SIMPULAN DAN SARAN

Bab ini berisikan kesimpulan serta saran terhadap seluruh penelitian yang telah dilakukan. Kesimpulan menjelaskan secara singkat dan padat mengenai keseluruhan terhadap hasil penelitian yang telah dilakukan. Pada bagian saran berisikan rekomendasi yang dapat diimplementasikan untuk menyempurnakan penelitian serupa dimasa yang akan datang.