BAB I

PENDAHULUAN

1.1 Latar Belakang

Ketika manusia dihadapkan dengan berbagai permasalahan, akal manusia memiliki beragam solusi untuk menyelesaikan permasalahan tersebut yang melahirkan berbagai ide baru sehingga manusia dapat berkembang pada akhirnya. Salah satu bukti perkembangan tersebut adalah kemunculan Teknologi Informasi dan Komunikasi (TIK). Istilah ini mengacu pada dua hal, yaitu Teknologi Informasi dan Teknologi Komunikasi. Teknologi Informasi mencakup segala aspek yang berkaitan dengan pengolahan, penggunaan, manipulasi, dan manajemen informasi. Sementara itu, teknologi komunikasi mencakup segala hal yang terkait dengan penggunaan alat untuk memproses dan mengirim data dari satu perangkat ke perangkat lainnya [1]. Teknologi Informasi dan Komunikasi adalah usaha menyampaikan informasi dengan memanfaatkan perangkat komputer, baik perangkat keras maupun perangkat lunak [2]. Dengan berkembangnya teknologi dan sistem, pekerjaan pengguna dapat diselesaikan secara efisien. Pengolahan ribuan data menjadi informasi dapat dilakukan dalam waktu yang singkat. Informasi yang didapatkan dari pengolahan sekelompok data ini nantinya akan memiliki pengaruh besar dalam proses pengambilan kebijakan. Melalui sebuah artikel yang diterbitkan di website Direktorat Jenderal Kekayaan Negara (DJKN), data dan informasi dianggap penting untuk menunjukkan kondisi yang terjadi saat ini, menentukan arah kebijakan, meningkatkan efisiensi biaya, memunculkan inovasi, dan sebagai materi evaluasi [3]. Oleh sebab itu, data dan informasi menjadi aset penting bagi sebuah lembaga, organisasi, dan perusahaan sehingga sistem keamanan informasi diperlukan. Keamanan informasi secara umum didefinisikan dalam sifat atau karakteristik yang seharusnya dimiliki oleh informasi yang aman [4]. Aspek-aspek ini mencakup kerahasiaan, keutuhan, dan ketersediaan informasi. Akan tetapi, beragam risiko dapat menjadi ancaman terhadap keamanan informasi. Hal ini bisa saja disebabkan oleh masalah pada

perangkat, kesalahan pengguna, hingga faktor dari luar. Perangkat keras meliputi komponen-komponen yang dapat disentuh dan dioperasikan secara fisik [5]. Kerusakan pada perangkat keras yang disengaja maupun tidak disengaja dapat menghilangkan keutuhan dan ketersediaan data. Selanjutnya, risiko lainnya adalah kesalahan pengguna yang bisa mengakibatkan informasi yang didapat menjadi tidak akurat. Selain dua risiko tersebut, terdapat satu faktor eksternal yang mungkin terjadi, yaitu tindak kejahatan. Pencurian perangkat keras mengakibatkan kehilangan data dan sangat memungkinkan terjadinya kebocoran data. Data statistik menunjukkan bahwa jumlah kasus pencurian yang terjadi selama tahun 2022 adalah 91.892 kejadian [6]. Nilai ini meningkat drastis dari jumlah kejadian yang terjadi di 2021. Terlebih lagi, tindak kejahatan siber meningkat pada era digital ini. Dalam Laporan Keamanan Siber Bulan Agustus 2023, jumlah aduan siber mencapai 186 dimana 161 di antaranya adalah kejahatan siber atau cybercrime [7].

Sebagai upaya menjaga keamanan informasi, salah satu langkah yang bisa dilakukan adalah melakukan audit sistem keamanan informasi. Audit sistem informasi adalah proses sistematik dalam mengumpulkan dan menilai bukti untuk menentukan apakah sistem informasi berbasis komputer yang digunakan oleh suatu organisasi telah memenuhi tujuan keamanan, seperti melindungi perangkat komputer, program, komunikasi, dan data dari akses, perubahan, atau kerusakan yang tidak sah [8]. Audit dilakukan dengan tujuan mengetahui bagian yang rentan dari sebuah sistem agar bisa diperbaiki. Akan tetapi, tidak jarang organisasi maupun perusahaan berskala kecil melewatkannya. Padahal, hal ini penting dilakukan untuk meninimalkan risiko-risiko yang tidak diinginkan. Audit Sistem Keamanan Informasi dilakukan dengan bantuan *framework*. Indeks KAMI merupakan *framework* yang digunakan sebagai alat bantu untuk melakukan asesmen dan evaluasi tingkat kesiapan (Kelengkapan dan Kematangan) penerapan keamanan informasi berdasarkan kriteria ISO/IEC 27001 [9]. Penggunaan Indeks KAMI dalam evaluasi keamanan informasi sangat penting karena alat ini menyediakan kerangka kerja yang komprehensif dan terstandarisasi untuk menilai sejauh mana organisasi telah

mengimplementasikan praktik-praktik keamanan informasi yang efektif. Dari berbagai versi yang tersedia, Indeks KAMI 4.2 menjadi pilihan karena cakupan kategori yang dievaluasi cukup luas, yaitu kategori sistem elektronik yang digunakan, tata kelola keamanan informasi, pengelolaan risiko keamanan informasi, kerangka kerja keamanan informasi, serta pengelolaan aset, teknologi dan keamanan informasi.

PT Mitra Cipta Sarana merupakan sebuah perusahaan yang berdiri sejak tahun 1996. Jumlah karyawan yang dimiliki kurang dari 1000 orang sehingga perusahaan ini bisa dikategorikan sebagai perusahaan berskala kecil. Pada awalnya, perusahaan berfokus sebagai perusahaan umum dan kontraktor. Kemudian, sejak tahun 2013, PT Mitra Cipta Sarana mulai melayani bidang jasa telekomunikasi. Perusahaan juga sedang bergerak di bidang distribusi penerangan saat ini. Dengan banyaknya data yang dimiliki, sistem keamanan informasi perusahaan sudah menggunakan server. Namun, selama 28 tahun berdiri, perusahaan ini belum pernah melaksanakan evaluasi sistem, terutama dalam bidang Information Technology (IT). Hingga saat ini, metode yang digunakan PT Mitra Cipta Sarana dalam menghadapi kehilangan data hanya recovery data. Akan tetapi, sistem yang belum pernah dievaluasi tentunya lebih rentan terhadap serangan siber, pencurian data, penyalahgunaan informasi, dan risiko-risiko lainnya. Kehilangan data-data penting, seperti data finansial dan data vital perusahaan, akan menghambat kelancaran operasional serta hilangnya kepercayaan dari pelanggan. Ditambah lagi, minimnya kesadaran dan pengetahuan tentang keamanan sistem informasi meningkatkan berbagai risiko bagi perusahaan.

Berdasarkan uraian di atas, disusunlah penelitian yang berjudul "Evaluasi Tingkat Keamanan Informasi Menggunakan Standar ISO/IEC 27001 dengan Framework Indeks KAMI 4.2 pada PT Mitra Cipta Sarana".

1.2 Rumusan Masalah

1. Bagaimana hasil penilaian keamanan informasi di PT Mitra Cipta Sarana menggunakan Indeks KAMI 4.2?

2. Bagaimana tingkat kematangan sistem keamanan informasi di PT Mitra Cipta Sarana dalam memenuhi standar Keamanan Informasi ISO 27001:2013?
3. Bagaimana rekomendasi yang dihasilkan dari evaluasi dengan Indeks KAMI 4.2 untuk meningkatkan keamanan informasi di PT Mitra Cipta Sarana?

1.3 Batasan Masalah

1. Asesmen dilakukan pada PT. Mitra Cipta Sarana secara keseluruhan pada pengelolaan keamanan informasinya.
2. Asesmen dilakukan dengan menggunakan Indeks Keamanan Informasi KAMI 4.2 sebagai media untuk membantu evaluasi sesuai dengan tingkat ketergantungan sistem elektronik dan juga lima area tingkat kematangan: Tata Kelola Keamanan Informasi, Pengelolaan Risiko Keamanan Informasi, Kerangka Kerja Keamanan Informasi, Pengelolaan Asset Informasi, Teknologi dan Keamanan Informasi.

1.4 Tujuan dan Manfaat Penelitian

1.4.1 Tujuan Penelitian

Tujuan yang dilaksanakannya penelitian ini adalah:

1. Menggunakan Indeks KAMI 4.2 untuk mengevaluasi Sistem Manajemen Keamanan Informasi di PT Mitra Cipta Sarana.
2. Menilai tingkat kematangan dan kesiapan PT Mitra Cipta Sarana dalam memenuhi persyaratan Keamanan Informasi berdasarkan standar internasional ISO 27001 versi 2013.
3. Membuat rekomendasi terkait keamanan informasi untuk PT Mitra Cipta Sarana guna membantu perusahaan memenuhi standar keamanan informasi.

1.4.2 Manfaat Penelitian

1. Bagi PT. Mitra Cipta Sarana, evaluasi kematangan manajemen keamanan informasi ini diharapakan menjadi acuan untuk perusahaan dalam meningkatkan sistem, serta mengetahui kesiapan sistem yang sedang dipakai saat ini.

1.5 Sistematika Penulisan

Bab I Pendahuluan

Bab ini terdiri dari latar belakang, rumusan masalah, batasan masalah, tujuan dan manfaat penelitian, serta sistematika penulisan skripsi.

Bab II Landasan Teori

Bab ini berisikan penelitian terdahulu yang sebelumnya pernah dilakukan. Selain itu, bab ini juga berisi landasan teori tentang Keamanan Informasi, *International Organization for Standardization* (ISO), ISO 27001:2013, dan *Framework* Indeks KAMI.

Bab III Metodologi Penelitian

Bab ini berisi tentang gambaran umum objek penelitian berupa profil perusahaan, Visi & Misi perusahaan, struktur organisasi. Bab ini juga berisi metode penelitian, teknik pengumpulan data, dan kerangka kerja penelitian.

Bab IV Analisis dan Hasil Penelitian

Bab ini berisi pembahasan hasil evaluasi Sistem Manajemen Keamanan Informasi menggunakan Indeks KAMI 4.2 yang telah dilakukan di perusahaan, serta rekomendasi yang didasarkan pada standar ISO 27001:2013.

Bab V Simpulan dan Saran

Bab ini membahas kesimpulan yang didapatkan selama proses penelitian dan saran terhadap perusahaan, serta rekomendasi untuk penelitian selanjutnya.