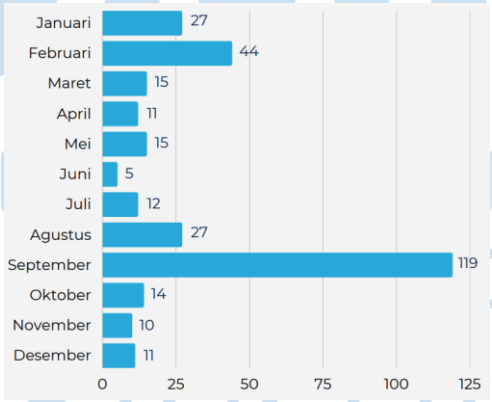
BAB I

PENDAHULUAN

1.1 Latar Belakang

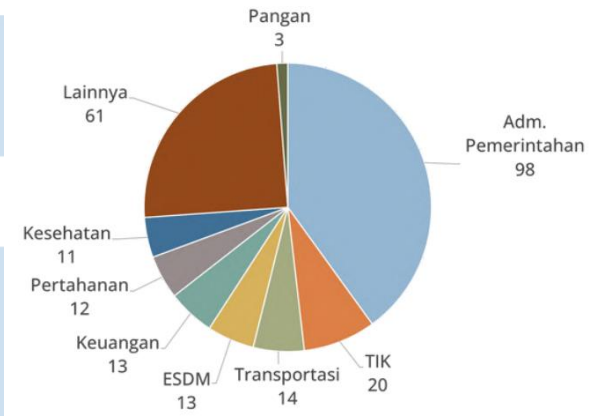
Sejalan dengan berkembangnya zaman, teknologi informasi juga akan mengalami perkembangan yang semakin pesat [1]. Saat ini, teknologi informasi telah banyak dimanfaatkan oleh masyarakat untuk memperoleh informasi. Selain masyarakat, perusahaan-perusahaan juga menggunakan teknologi informasi untuk mengolah data yang diterima dalam jumlah besar. Data tersebut akan diolah menjadi informasi yang berharga bagi perusahaan dalam proses pengambilan keputusan [2]. Data atau informasi adalah aset penting yang harus diperhatikan dan dijaga dengan baik oleh perusahaan. Hal ini dikarenakan data atau informasi dapat membantu perusahaan dalam pengambilan keputusan sesuai dengan kondisi yang sedang dialami oleh perusahaan. Pentingnya data atau informasi perusahaan tersebut menyebabkan munculnya berbagai ancaman. Ancaman-ancaman yang dapat terjadi, seperti informasi atau data dirusak atau dihapus, informasi atau data diakses atau diubah oleh orang yang tidak berhak, dan pemalsuan informasi oleh orang yang tidak berhak [3].

Salah satu insiden terkait dengan data adalah *data breach* (kebocoran data). Berdasarkan laporan tahunan monitoring keamanan siber BSSN (Badan Siber dan Sandi Negara), terdapat 311 dugaan insiden kebocoran data yang terdeteksi di Indonesia.



Gambar 1.1 Grafik Jumlah Insiden Kebocoran Data 2022
Sumber: BSSN (Badan Siber dan Sandi Negara)

Berdasarkan Gambar 1.1 di atas, dugaan insiden kebocoran data terbanyak terjadi di bulan September dengan dugaan jumlah insiden sebanyak 119 insiden [4]. Insiden kebocoran data dapat terjadi kepada individu maupun organisasi. Beberapa sektor yang terdampak insiden kebocoran data, antara lain:



Gambar 1.2 Sektor Terdampak Insiden Kebocoran Data 2022
Sumber: BSSN (Badan Siber dan Sandi Negara)

Berdasarkan Gambar 1.2 di atas, sektor yang paling banyak terjadi dugaan insiden kebocoran data adalah Administrasi Pemerintahan, kemudian diikuti oleh Sektor Lainnya, dan Sektor Teknologi Informasi dan Komunikasi (TIK). Dampak dari insiden ini adalah peretas mengetahui informasi *user* sehingga dapat menjadi target terjadinya serangan *phising.* Selain itu, peretas juga dapat memanfaatkan informasi yang telah didapatkan untuk masuk ke sistem dan mengakses *database* atau dokumen penting perusahaan, seperti dokumen yang berkaitan dengan keuangan, *customer,* dan lain-lain [4].

Insiden kebocoran data ini sangat merugikan pihak-pihak yang bersangkutan sehingga perlu adanya tindakan pencegahan agar dapat terhindar dari insiden kebocoran data. Terdapat beberapa tindakan atau upaya pencegahan yang disarankan oleh BSSN agar dapat terhindar dari insiden kebocoran data [4]:

1. Melakukan penilaian keamanan IT pada sistem informasi yang dimiliki.
2. Menerapkan kebijakan penggunaan *password* yang kompleks serta melakukan penggantian *password* secara berkala.
3. Memberikan edukasi terhadap sesama pengguna sistem.

4. Melakukan *review* terhadap akun sistem dan aplikasi.
5. Menonaktifkan *port* layanan yang tidak digunakan.
6. Melakukan validasi data.
7. Menyampaikan kepada pemilik data atau masyarakat.
8. Melakukan *hardening* dan *patching* terhadap sistem yang terdampak.

Setiap individu ataupun organisasi tentunya ingin terhindar dari insiden kebocoran data, begitu pula dengan PT XYZ yang merupakan perusahaan swasta yang bergerak dibidang kontraktor dan *developer*. Dalam kegiatan operasionalnya, PT XYZ memiliki data keuangan, *supplier*, *customer*, karyawan, dan lain-lain. Data-data tersebut merupakan aset penting perusahaan terutama data keuangan karena pada data tersebut terdapat arus kas sehingga perlu untuk dilindungi dan disimpan dengan aman dan baik. Apabila data-data tersebut mengalami kebocoran data, maka dapat berdampak pada reputasi perusahaan sehingga menyebabkan hilangnya kepercayaan masyarakat terhadap perusahaan. Banyaknya data dan informasi penting pada perusahaan menyebabkan perusahaan ingin melakukan sertifikasi ISO 27001 agar dapat terhindar dari ancaman-ancaman keamanan informasi, seperti kebocoran data. Perlu untuk melakukan evaluasi terhadap sistem manajemen keamanan informasi terlebih dahulu sebelum melakukan sertifikasi ISO 27001 guna mengetahui kelayakan dan kesiapan perusahaan dalam melakukan sertifikasi. Standar yang digunakan dalam evaluasi tersebut adalah ISO 27001:2013. Adapun *tools* yang dapat digunakan adalah indeks KAMI (Keamanan Informasi). ISO 27001:2013 berfungsi sebagai panduan atau standar dalam melakukan evaluasi, sedangkan indeks KAMI (Keamanan Informasi) berfungsi sebagai alat bantu dalam melakukan pengukuran tingkat kematangan keamanan informasi serta kepatuhan penerapan standar ISO 27001:2013. Standar ISO 27001:2013 dan indeks KAMI (Keamanan Informasi) memiliki korelasi atau hubungan, dimana lima area pada indeks KAMI (Keamanan Informasi) berhubungan dengan *Annex A* yang ada dalam standar ISO 27001:2013.

Terdapat penelitian sebelumnya mengenai evaluasi sistem manajemen keamanan informasi yang mengacu kepada standar ISO 27001:2013 serta

menggunakan alat bantu indeks KAMI (Keamanan Informasi) untuk membantu proses evaluasi tersebut [5][6][7][8][9][10][11]. Adapun penelitian lainnya yang menunjukkan bahwa ISO 27001 digunakan untuk mengukur pemenuhan standar ISO 27001 pada berbagai sektor bisnis [12], untuk melindungi kerahasiaan, integritas, dan ketersediaan informasi, serta mengendalikan risiko yang ada [13]. Selain itu, ISO 27001 juga dapat mengatasi pelanggaran keamanan informasi yang terjadi [14].

Oleh karena itu, penelitian ini akan berfokus pada evaluasi sistem manajemen keamanan informasi menggunakan standar ISO 27001:2013 dan *tools* indeks KAMI (Keamanan Informasi) dengan kebaruan pada objek yang digunakan, yaitu perusahaan swasta yang bergerak dibidang konstruksi dan *developer* serta versi indeks KAMI (Keamanan Informasi) yang digunakan merupakan versi terbaru, yaitu versi 4.2.

1.2 Rumusan Masalah

Berdasarkan latar belakang tersebut, maka rumusan masalah yang dihasilkan adalah sebagai berikut:

1. Bagaimana hasil evaluasi sistem manajemen keamanan informasi pada PT XYZ dengan menggunakan alat bantu indeks KAMI (Keamanan Informasi)?
2. Bagaimana hasil tingkat kematangan keamanan informasi dan kepatuhan penerapan ISO 27001:2013 pada PT XYZ?
3. Bagaimana hasil rekomendasi perbaikan untuk meningkatkan keamanan informasi pada PT XYZ dengan berdasarkan standar ISO 27001:2013 dan indeks KAMI (Keamanan Informasi)?

1.3 Batasan Masalah

Terdapat beberapa batasan masalah guna mempermudah penjelasan dan mencapai tujuan yang diharapkan. Berikut adalah batasan masalah dalam penelitian ini:

1. Penelitian ini menggunakan standar ISO 27001:2013 yang berfokus terhadap manajemen keamanan informasi.
2. Penelitian ini menggunakan indeks KAMI (Keamanan Informasi) versi terbaru, yaitu 4.2 untuk mengukur tingkat kematangan serta kepatuhan penerapan standar ISO 27001:2013.
3. Penelitian ini menggunakan metode PDCA (*Plan-Do-Check-Act*).
4. Narasumber dan responden pada penelitian ini merupakan staf IT pada PT XYZ.
5. Rekomendasi perbaikan keamanan informasi dirumuskan dengan mengacu pada standar ISO 27001:2013.

1.4 Tujuan dan Manfaat Penelitian

1.4.1 Tujuan Penelitian

Terdapat beberapa tujuan yang ingin dicapai dalam penelitian ini, antara lain:

1. Mengetahui hasil evaluasi sistem manajemen keamanan informasi pada PT XYZ dengan menggunakan indeks KAMI (Keamanan Informasi).
2. Mengetahui tingkat kematangan keamanan informasi dan kepatuhan penerapan ISO 27001 pada PT XYZ.
3. Menghasilkan rekomendasi perbaikan dengan berdasarkan standar ISO 27001:2013 dan indeks KAMI (Keamanan Informasi) guna meningkatkan keamanan informasi pada PT XYZ.

1.4.2 Manfaat Penelitian

Terdapat beberapa manfaat yang diperoleh dalam penelitian ini, antara lain:

1. PT XYZ mengetahui tingkat kematangan keamanan informasi yang terdapat pada perusahaan.
2. PT XYZ mengetahui kelayakan dan kesiapan perusahaan untuk mengikuti sertifikasi ISO 27001.

3. PT XYZ mengetahui aspek-aspek pada sistem manajemen keamanan informasi yang perlu ditingkatkan agar siap melakukan sertifikasi ISO 27001.

1.5 Sistematika Penulisan

Adapun sistematika penulisan pada Tugas Akhir ini adalah sebagai berikut:

1. BAB I PENDAHULUAN

   Bab ini membahas mengenai latar belakang yang berisikan gambaran umum mengenai penggunaan ISO 27001 dan indeks KAMI (Keamanan Informasi) dalam meningkatkan sistem manajemen keamanan informasi, beserta dengan rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.
2. BAB II LANDASAN TEORI

   Bab ini berisikan teori-teori yang berkaitan dengan topik penelitian, *framework* yang digunakan, dan penelitian terdahulu yang menjadi pedoman atau sumber referensi dalam melakukan penelitian ini.
3. BAB III METODOLOGI PENELITIAN

   Bab ini membahas mengenai gambaran umum objek penelitian, metode penelitian, teknik pengumpulan data, dan variabel penelitian.
4. BAB IV ANALISIS DAN HASIL PENELITIAN

   Bab ini membahas mengenai hasil evaluasi sistem manajemen keamanan informasi berdasarkan langkah-langkah yang telah dibahas pada bab sebelumnya.
5. BAB V SIMPULAN DAN SARAN

   Bab ini berisikan kesimpulan dari hasil evaluasi yang dilakukan dan permasalahan yang terdapat pada rumusan masalah serta saran yang dapat digunakan untuk pengembangan pada penelitian selanjutnya.