BAB I

PENDAHULUAN

1.1 Latar Belakang

Teknologi informasi saat ini telah menjadi sarana yang paling penting dan berpengaruh besar terhadap berlangsungnya proses bisnis sebuah organisasi untuk menjalankan dan mencapai sebuah tujuan tertentu. Tingginya penggunaan teknologi di berbagai aspek organisasi baik bidang ekonomi, informasi, bisnis, kesehatan dan lain sebagainya mengakibatkan ancaman keamanan data juga meningkat. Dengan seiring beralihnya seluruh kegiatan proses bisnis yang memanfaatkan perkembangan teknologi maka dapat memberikan peluang bagi beberapa pihak melakukan kejahatan di bidang teknologi dan tindak kriminalitas atas pencurian data untuk tujuan tertentu yang dapat merugikan banyak pihak dengan terhambatnya proses operasional teknologi informasi. Pada tahun 2017 diketahui terdapat banyak kejadian terkait dengan penyerangan keamanan tekniologi informasi pada perangkat lunak dengan memanfaatkan media *email* untuk menyerang badan pemerintahan dan sektor public (Symantec, 2018). Pada pertengahan tahun 2022 juga kerap terjadi kejahatan pencurian data dari berbagai aplikasi dan serangan *hacker* atas beberapa website instansi pemerintah dengan domain go.id. Berdasarkan adanya kejadian tersebut mengharuskan organisasi yang mayoritas proses bisnisnya memanfaatkan teknologi informasi untuk meningkatkan keamanan informasinya.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur merupakan lembaga pemerintahan yang memiliki fungsi sebagai penyelenggaraan urusan pemerintah bidang komunikasi dan informatika untuk wilayah Provinsi Jawa Timur. Lembaga pemerintahan yang berkedudukan dibawah naungan Gubernur terebut berwenang untuk

memberikan izin merumuskan layanan dan website sesuai kebijakan dan undang-undang yang berlaku. Dalam proses pelaksaan tugas dan wewenangnya lembaga pemerintahan tersebut sangat memanfaatkan penggunaan teknologi informasi yang mengharuskan untuk terjamin keamanan datanya. Badan pemerintahan dinilai wajib untuk melakukan pengendalian dan manajemen keamanan informasi untuk mengamankan data dan informasi yang bersifat rahasia agar mencegah terjadinya pencurian data (Candra dkk, 2019). Seiring berkembangnya teknologi informasi mengakibatkan kurang maksimalnya penerapan manajemen keamanan informasi. Oleh sebab itu diperlukan adanya pengukuran tingkat manajemen keamanan informasi yang ada pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur serta mengetahui kendala apa saja yang menghambat proses teknologi informasi agar mendapat solusi dari permasalahan tersebut.

Manajemen keamanan informasi pada dasarnya ditujukan untuk menjamin pengamanan kerahasiaan data, integritas informasi, dan ketersediaan informasi. Manajemen keamanan informasi juga dilakukan untuk melakukan pengecekan atas ketaatan sebuah organisasi terhadap aturan yang berlaku, serta telah mengacu pada standar yang konkrit (Fauzi, 2018). Penelitian terkait audit teknologi informasi yang dilakukan pada rentang tahun 2014 hinga tahun 2018 diketahui banyak menggunakan *framework* COBIT (Rochmania dkk, 2020). Kerangka kerja COBIT sendiri membahas tentang keseluruhan proses bisnis perusahaan dan cenderung banyak digunakan untuk melakukan audit tata kelola teknologi informasi. Sedangkan ISO 27002:2013 merupakan *framework* yang banyak digunakan untuk melakukan audit Sistem Keamanan Manajemen Informasi (SKMI) yang berstandar internasional mengenai panduan implementasi keamanan informasi yang terdiri dari 14 divisi utama, 37 subdivisi dan 114 kontrol.

Kerangka kerja lain yang dapat digunakan untuk melakukan analisis manajemen keamanan adalah dengan menggunakan Indeks Keamanan Informasi (KAMI). Indeks KAMI merupakan kerangka kerja berstandar nasional yang dibuat dengan berdasar Peraturan Menteri Komunikasi dan Informatika untuk melakukan evaluasi dan analisis tingkat kesiapan keamanan informasi sebuah perusahaan sebelum dinyatakan layak untuk melakukan sertifikasi ISO 27001:2013 (Septanto, 2020). Dinas Komunikasi dan Informatika Provinsi Jawa Timur sejauh ini telah menerapkan standar keamanan informasi ISO 27001, sehingga dinilai telah memenuhi tingkat kesiapan keamanan informasi pada Indeks KAMI dan memerlukan analisis keamanan informasi lebih lanjut dengan mengikuti perkembangan teknologi dan panduan standar audit yang telah diperbarui.

Panduan keamanan informasi ISO 27001 banyak digunakan oleh organisasi dan perusahaan karena berisikan *information security management*, dimana khusus membahas terkait informasi umum berbagai persyaratan yang perlu disiapkan untuk mempersiapkan Sistem Manajemen Keamanan Informasi (SMKI) yang baik dengan tujuan mengamankan data dan asset informasi perusahaan. Namun, dengan seiring berjalannya waktu standar ISO 27001 dikembangkan menjadi ISO 27002 untuk menyempurnakan standar keamanan informasi sebelumnya yang hanya sampai sebatas persiapan menjadi standar keamanan informasi yang lebih kompleks. Dalam standar ISO 27002 kemudian dikembangkan lebih detail panduan terkait penerapan, pemeliharaan, dan perbaikan manajemen keamanan informasi untuk meningkatkan kualitas sistem kemanan dan mengurangi resiko terjadinya pencurian data. Sehubungan hal tersebut maka dalam penelitian ini dilakukan audit keamanan informasi menggunakan standar ISO 27002 untuk dilakukan analisis lebih lanjut tetapi dengan

tetap berdasar pada ISO 27001 yang telah diterapkan Dinas Komunikasi dan Informatika Provinsi Jawa Timur sejauh ini.

Standar ISO 27002:2013 berfokus membahas panduan terkait audit di bidang keamanan teknologi informasi, dan dalam penerapannya organisasi dapat memilih atau mengembangkan kontrol sesuai pengelolaan dan pengendalian manajemen keamanan informasi yang dibutuhkan (Purba dkk, 2018). Penelitian ini berfokus pada Klausul 16 yaitu tentang Manajemen Insiden Keamanan Informasi yang didalamnya terdapat 7 kontrol objek yaitu Kontrol 16.1.1 tentang Tanggung Jawab dan Prosedur, Kontrol 16.1.2 tentang Melaporkan Kejadian Keamanan Informasi, Kontrol 16.1.3 Melaporkan Kelemahan Keamanan Informasi, Kontrol 16.1.4 Penilaian dan Keputusan tentang Peristiwa Keamanan Informasi, Kontrol 16.1.5 Menanggapi Insiden Keamanan Informasi, Kontrol 16.1.6 Belajar dari Insiden Keamanan Informasi. Hasil dari pengukuran 6 kontrol objek tersebut selanjutnya akan menghasilkan nilai uji kematangan yang di analisis dampak dari tingkat penerapan Manajemen Kemanan Informasi dan menciptakan rekomendasi perbaikan untuk penerapan kedepannya.

Berdasarkan uraian di atas, maka dilakukan penelitian audit keamanan teknologi informasi dengan judul **"Analisis Manajemen Insiden Keamanan Informasi Menggunakan ISO 27002:2013 (Studi Kasus: Dinas Komunikasi dan Informatika Provinsi Jawa Timur)"**.

1.2. Rumusan Masalah

Rumusan masalah berdasarkan uraian latar belakang diatas adalah sebagai berikut:

1. Bagaimana melakukan analisis Manajemen Insiden Keamanan Informasi menggunakan ISO 27002:2013 pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur?
2. Bagaimana dampak Manajemen Insiden Keamanan Informasi berdasarkan hasil audit menggunakan *framework* ISO 27002:2013?
3. Bagaimana rekomendasi perbaikan Manajemen Insiden Keamanan Informasi yang tepat berdasarkan ISO 27002:2013?

1.3. Batasan Masalah

Batasan masalah dalam penelitian ini sebagai berikut:

1. Sistem yang diaudit adalah teknologi informasi yang digunakan Dinas Komunikasi dan Informatika Provinsi Jawa Timur menggunakan 27002.
2. Studi kasus dilakukan pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur dengan pengguna sistem pada divisi APTIKA sebagai responden.
3. Data-data yang digunakan dalam proses analisis dan pembahasan masalah adalah data yang diperoleh dari hasil observasi, dokumentasi, studi kepustakaan dan wawancara.
4. Klausul ISO 27002:2013 yang digunakan yaitu Klausul 16 (Manajemen Insiden Keamanan Informasi).

1.4. Tujuan Penelitian

Tujuan dari penelitian yang dilakukan Dinas Komunikasi dan Informatika Provinsi Jawa Timur adalah sebagai berikut :

1. Mengetahui hasil analisis Manajemen Insiden Keamanan Informasi menggunakan ISO 27002:2013 pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur.
2. Mengetahui dampak Manajemen Insiden Keamanan Informasi Dinas Komunikasi dan Informatika Provinsi Jawa Timur berdasarkan hasil audit menggunakan *framework* ISO 27002:2013.
3. Membuat rekomendasi berdasarkan hasil audit Manajemen Insiden Keamanan Informasi Dinas Komunikasi dan Informatika Provinsi Jawa Timur.

1.5. Manfaat Penelitian

Adapun manfaat yang dapat diambil dari hasil penelitian ini adalah sebagai berikut:

1. Penelitian ini diharapkan dapat membantu meningkatkan tingkat implementasi sistem Manajemen Insiden Keamanan Informasi yang tepat.
2. Hasil analisis dampak Manajemen Insiden Keamanan Informasi Dinas Komunikasi dapat menjadi pertimbangan untuk meningkatkan implementasi jangka panjang dengan mempertimbangkan resiko.
3. Menghasilkan rekomendasi untuk melakukan perbaikan dan pengembangan Manajemen Insiden Keamanan Informasi pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur.