

BAB I

PENDAHULUAN

1.1 Latar Belakang

Teknologi Informasi dan Komunikasi (TIK) telah berkembang dengan pesat hingga saat ini dan tentunya akan terus mengalami inovasi. Seiring dengan berkembangnya TIK, hal tersebut juga melibatkan pengguna yang semakin banyak dan meluas ke seluruh penjuru dunia dengan cepat sehingga memungkinkan pertukaran informasi dapat dilakukan dengan sangat cepat yang tidak terbatas oleh jarak maupun waktu. Perkembangan teknologi mengharuskan individu atau organisasi untuk beradaptasi sesuai dengan perubahan yang terjadi. Oleh karena itu, saat ini TIK merupakan aset yang berharga bagi tiap individu, swasta, dan instansi pemerintah.

Penerapan tata kelola TIK saat ini merupakan kebutuhan dan juga merupakan tuntutan bagi setiap instansi penyelenggara pelayanan publik, dikarenakan peran TIK menjadi semakin penting bagi upaya peningkatan kualitas layanan sebagai salah satu perwujudan dari tata kelola pemerintahan yang baik (*Good Corporate Governance*). Dalam penyelenggaraan tata kelola TIK, penerapan keamanan informasi sangatlah penting karena kinerja tata kelola TIK akan terganggu jika informasi yang merupakan salah satu objek utama tata kelola TIK mengalami masalah keamanan. Masalah keamanan informasi tersebut menyangkut kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*) [1].

Keamanan informasi merupakan salah satu cara untuk mengamankan aset informasi dari ancaman yang ada. Keamanan informasi dapat menjamin keberlangsungan bisnis, mengurangi risiko yang dapat terjadi, dan mengoptimalkan pengembalian investasi secara tidak langsung. Ketika informasi yang disimpan, dikelola, dan dibagikan suatu organisasi semakin banyak, maka risiko terjadinya kerusakan data, kehilangan data, maupun tereksposnya data ke pihak yang tidak berwenang akan semakin besar [2]. Dengan diadopsinya teknologi informasi dan komunikasi ke dalam sistem pemerintahan, maka akan

bermunculan juga masalah baru yang lebih kompleks. Berkaca dari hal ini maka tugas penyelenggaraan persandian dan keamanan informasi sangatlah berat karena harus menangkal segala bentuk ancaman dan kerawanan terhadap pencurian informasi daerah.

Salah satu upaya yang telah dilakukan oleh Kementerian Komunikasi dan Informatika untuk meningkatkan tingkat keamanan informasi dari instansi pemerintahan yaitu dengan menciptakan alat yang digunakan untuk menilai tingkat kematangan serta kelengkapan dalam penerapan keamanan informasi yang disebut Indeks Keamanan Informasi (KAMI) [3]. Indeks KAMI merujuk pada ISO 27001 yang berisi mengenai standar keamanan informasi. dan mengelola aset sehingga organisasi dapat memastikan bahwa keamanan informasi yang diimplementasikan oleh mereka telah berjalan dengan efektif [2].

Dinas Komunikasi, Informatika dan Persandian Kabupaten XYZ yang selanjutnya akan disebut sebagai "Diskominfosandi Kabupaten XYZ" sebelumnya sudah melakukan pengevaluasian mandiri pada tahun 2019. Berdasarkan evaluasi sebelumnya, nilai Indeks KAMI dari Diskominfosandi Kabupaten XYZ adalah II. Dikarenakan pada hasil pengevaluasian mandiri sebelumnya kategori sistem elektronik dari Dinas Komunikasi, Informatika dan Persandian Kabupaten XYZ ternilai strategis, maka pihak Diskominfosandi Kabupaten XYZ wajib mempunyai sertifikat Sistem Manajemen Pengamanan Informasi (SMPI). Hal tersebut diatur di dalam Peraturan Menteri Komunikasi dan Informatika Republik Indonesia nomor 4 tahun 2016 Pasal 7 ayat (1) tentang Sistem Manajemen Pengamanan Informasi, yang berbunyi

"Penyelenggara Sistem Elektronik yang menyelenggarakan Sistem Elektronik strategis harus menerapkan standar SNI ISO/IEC 27001 dan ketentuan pengamanan yang ditetapkan oleh Instansi Pengawas dan Pengatur Sektornya" [4].

Serta pada pasal 21 juga disebutkan bahwa

"Penyelenggara Sistem Elektronik strategis dan Penyelenggara Sistem Elektronik tinggi dapat melakukan Penilaian Mandiri berdasarkan standar SNI/ISO IEC 27001." [4].

Didukung juga oleh Peraturan Badan Siber dan Sandi Negara Nomor 8 tahun 2020 tentang Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik Pasal 12 ayat 1 yang berbunyi

“Untuk mempersiapkan penerapan SNI ISO/IEC 27001 sebagaimana dimaksud dalam Pasal 9, Penyelenggara Sistem Elektronik dapat melakukan penilaian berdasarkan Indeks KAMI.” [5].

Oleh karena itu, pihak Diskominfo Kabupaten XYZ harus melakukan penilaian mandiri lagi untuk menilai kecukupan sistem manajemen pengamanan informasinya dalam rangka memenuhi standar SNI/ISO IEC 27001.

1.2 Rumusan Masalah

Dalam rangka mendapatkan sertifikasi SNI/ ISO IEC 27001 pihak Diskominfo Kabupaten XYZ harus memenuhi standar SNI/ ISO IEC 27001, sehingga perlu dilakukan penilaian sistem manajemen pengamanan informasi menggunakan Indeks Keamanan Informasi (KAMI) 4.2.

1.3 Pertanyaan Penelitian

Berdasarkan latar belakang yang sudah dijelaskan sebelumnya, maka diperoleh pertanyaan penelitian sebagai berikut:

1. Berapa nilai hasil evaluasi yang diperoleh Manajemen Keamanan Informasi Dinas Komunikasi, Informatika dan Persandian Kabupaten XYZ berdasarkan Indeks KAMI versi 4.2?
2. Apa saja rekomendasi yang dapat diberikan kepada Dinas Komunikasi, Informatika dan Persandian Kabupaten XYZ untuk meningkatkan Keamanan Informasi mereka?

1.4 Tujuan Penelitian

Tujuan dilakukannya evaluasi Manajemen Risiko Keamanan Informasi ini adalah sebagai berikut:

1. Untuk mengetahui nilai hasil evaluasi Keamanan Informasi Dinas Komunikasi, Informatika dan Persandian Kabupaten XYZ berdasarkan Indeks KAMI versi 4.2

2. Untuk memberikan rekomendasi yang dapat meningkatkan Keamanan Informasi pada Dinas Komunikasi, Informatika dan Persandian Kabupaten XYZ.

1.5 Batasan Masalah

Adapun Batasan masalah pada penelitian ini adalah:

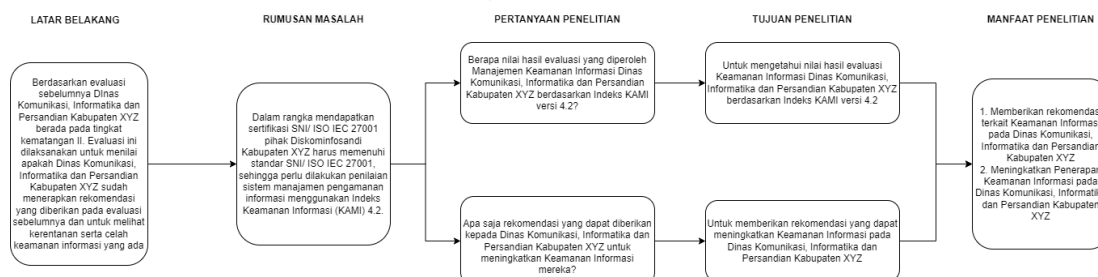
1. Sampel dalam penelitian berdasarkan seluruh dokumen Keamanan Informasi pihak Dinas Komunikasi, Informatika dan Persandian Kabupaten XYZ.
2. Penelitian ini hanya menilai terkait Keamanan Informasi di Dinas Komunikasi, Informatika dan Persandian Kabupaten XYZ sesuai dengan pertanyaan yang ada dalam Indeks KAMI 4.2.
3. Keamanan Informasi yang dinilai menggunakan Indeks KAMI hanya terbatas pada Tata Kelola Keamanan Informasi, Pengelolaan Risiko Keamanan Informasi, Kerangka Kerja Pengelolaan Keamanan Informasi, Pengelolaan Aset Informasi, dan Teknologi dan Keamanan Informasi.

1.6 Manfaat Penelitian

Adapun manfaat dari penelitian ini adalah sebagai berikut:

1. Memberikan rekomendasi terkait Keamanan Informasi pada Dinas Komunikasi, Informatika dan Persandian Kabupaten XYZ.
2. Meningkatkan Penerapan Keamanan Informasi pada Dinas Komunikasi, Informatika dan Persandian Kabupaten XYZ.

1.7 Bagan Keterkaitan



Gambar 1.1 Bagan Penelitian