BAB I
PENDAHULUAN

1.1. Latar Belakang

Langkah pengamanan informasi bagi organisasi atau perusahaan perlu dilakukan sebagai upaya untuk melindungi data dan informasi dari ancaman. Instansi pemerintahan biasanya memiliki pedoman untuk melakukan langkah pengamanan yang wajib untuk dilakukan karena jika tidak dilakukan bisa menimbulkan ancaman yang dapat memicu adanya risiko pada organisasi. Risiko yang mungkin terjadi dapat mengakibatkan dampak negatif bagi organisasi, contohnya seperti terhambatnya proses bisnis serta dapat membuat adanya penurunan reputasi pemerintah atau bahkan bisa mengurangi kepercayaan masyarakat [1].

Penggunaan aset teknologi informasi di organisasi perlu diimbangi juga dengan upaya pengamanan, hal ini dilakukan untuk tetap menjaga aset perusahaan atau organisasi sesuai dengan prinsip keamanan informasi. Organisasi akan menerapkan beberapa hal untuk melindungi aset seperti mengatur *control access*, pemasangan proteksi seperti firewall dan yang pasti adalah membuat kebijakan dan evaluasi terkait dengan keamanan informasi berbasis risiko. Pembuatan kebijakan dan evaluasi keamanan harus berbasis risiko dan dilakukan sesuai dengan standar yang ditetapkan seperti SNI ISO/IEC 27001.

Instansi XYZ merupakan salah satu organisasi pemerintahan yang bertanggung jawab untuk melaksanakan tugas pada bidang komunikasi dan informatika daerah kota atau kabupaten. Ancaman terhadap keamanan informasi yang terjadi pada organisasi XYZ salah satunya disebabkan oleh semakin banyaknya penggunaan teknologi informasi serta kurang terkelolanya evaluasi terhadap keamanan informasi. Instansi XYZ memiliki kewajiban untuk melakukan evaluasi keamanan dan manajemen risiko sesuai dengan Perpres No.95 Th. 2018 yang menyatakan bahwa semua Sistem Pemerintahan Berbasis Elektronik (SPBE) diharapkan dapat meminimalkan risiko untuk menjaga agar pelayanan publik tetap maksimal [2]. Aturan lain yang bisa dijadikan dasar akan pentingnya evaluasi keamanan berbasis risiko adalah Peraturan Badan Siber dan Sandi Negara atau BSSN No. 10 tahun 2019 [3]. Proses evaluasi keamanan dan manajemen risiko bisa dilakukan dengan acuan ISO 27005:2013.

Pada ISO 27005:2013, *risk assessment* dimulai dengan melakukan proses *risk identification, risk analysis* dan *risk evaluation*. Setiap fase yang dilakukan akan saling terkait hingga mendapatkan informasi berupa potensi risiko dari aset maupun *potential cause* dari risiko yang terjadi. Mengingat potensi akan adanya risiko yang terjadi pada Instansi XYZ maka dibutuhkan langkah solusi untuk menjaga keamanan informasi pada organisasi. Berdasarkan hal tersebut akan dilakukan proses evaluasi keamanan informasi berbasis risiko dimana hal ini akan dilakukan dengan menggunakan metode *Failure Mode and Effect Analysis* sebagai alat penilaian dan standar ISO 27001:2013 serta 27002:2013 sebagai penentuan kontrol terhadap risiko.

1.2. Perumusan Masalah

Berdasarkan pemaparan latar belakang di atas, rumusan masalah yang ada dapat difokuskan menjadi beberapa hal untuk dibahas pada tugas akhir. Permasalah yang ada meliputi :

1. Bagaimana hasil identifikasi risiko aset TI pada Instansi XYZ?
2. Bagaimana hasil dari penilaian risiko dengan menggunakan metode *Failure Mode and Effects Analysis* (FMEA)?
3. Apa langkah mitigasi terkait dengan risiko yang terjadi pada Instansi XYZ?

1.3. Batasan Masalah

Berdasarkan pemaparan latar belakang di atas, rumusan masalah yang ada dapat difokuskan menjadi beberapa hal untuk dibahas pada tugas akhir. Permasalahan yang ada meliputi :

1. Studi Kasus pada penelitian ini adalah Instansi XYZ.
2. Penelitian ini menganalisis aset teknologi informasi yang digunakan di Instansi XYZ.

1.4. Tujuan

Pada proses penelitian dan pengerjaan tugas akhir ada beberapa tujuan yang ingin dicapai, diantaranya adalah sebagai berikut :

1. Mengidentifikasi aset TI serta risiko dari aset yang ada pada Instansi XYZ.
2. Melakukan penilaian risiko menggunakan metode FMEA untuk mengetahui prioritas risiko dari yang tertinggi hingga terendah.

3. Membuat saran mitigasi risiko yang tepat sesuai dengan hasil penilaian risiko yang digunakan sebagai acuan dalam membuat langkah penanganan yang ada pada Instansi XYZ.

1.5. Rencana Kegiatan

Kegiatan penelitian ini akan dilakukan dalam masa waktu kurang lebih 5-6 bulan. Pengerjaan tugas akhir ini dimulai dengan melakukan studi literatur dengan topik yang sesuai dan berasal dari jurnal atau referensi terpercaya. Pengumpulan data akan dilakukan dengan teknik wawancara dengan narasumber yang bertanggung jawab serta melakukan *review* dokumen pendukung lainnya. Data yang akan diambil berfokus terhadap aset atau infrastruktur teknologi informasi pada lokasi penelitian serta ancaman atau risiko yang pernah terjadi. Setelah mengumpulkan data maka akan dilakukan proses pengolahan data dengan cara mengklasifikasi serta melakukan penilaian. Selanjutnya adalah melakukan pembuatan saran mitigasi risiko berdasarkan hasil penilaian yang didapatkan. Fase terakhir adalah membuat laporan terkait dengan penelitian yang sudah dilakukan dalam bentuk laporan tugas akhir.

1.6. Jadwal Kegiatan

Waktu dan tempat penelitian tugas akhir dilaksanakan pada tahun ajaran 2021/2022. Berikut adalah tabel rancangan atau jadwal kegiatan yang sudah disusun untuk melaksanakan penelitian.

Tabel 1 Jadwal Kegiatan

Nama Kegiatan	**Bulan**								
	Des	Jan	Feb	Mar	Apr	Mei	Jun	Jul	Ags
Studi Literatur									
Penyusunan dan Pengajuan Judul									
Pengajuan Proposal									
Perijinan Penelitian Tugas Akhir									
Pengumpulan Data									
Pengolahan dan Analisis Data									
Penyusunan Laporan									

Sidang									
Revisi Laporan									