BAB I
PENDAHULUAN

1.1. Latar Belakang

Informasi adalah aset yang tidak terukur lantaran merupakan salah satu sumber daya penting yang meningkatkan nilai bisnis dan kepercayaan publik. Seiring berkembangnya informasi, keamanan informasi juga patut untuk diawasi. Keamanan informasi merupakan dengan cara apa kita menghalangi penyamaran (cheating) atau paling tidak mengetahui penipuan dalam sistem berbasis informasi, dimana informasi itu sendiri tidak memiliki arti fisik. Dalam ISO 27001, keamanan informasi ini mencakup 3 aspek penting yang disebut sebagai aspek C.I.A, yang berarti kerahasiaannya (confidentiality), dapat dipastikan keasliannya (integrity), serta dapat selalu tersedia ketika dibutuhkan (availability) [1]. Akan tetapi pada kenyataannya dalam upaya yang dilangsungkan oleh organisasi untuk menjalankan C.I.A tentu tidak selalu berjalan dengan mulus dan pastinya ada beberapa hal atau peristiwa yang dapat menghalangi keberlangsungannya. Hal tersebut akan berakibatkan jika suatu organisasi gagal dalam memenuhi dan menjalankan salah satu dari aspek C.I.A, yaitu akan berdampak pada akurasi dan ketersediaan informasi pada organisasi serta kepercayaan para pengguna informasi tersebut akan berkurang sehingga dapat menimbulkan risiko bagi perusahaan tersebut [1].

Risiko harus dikendalikan untuk meminimalkan imbas dan kemungkinan terjadi. Pengelolaan risiko ini didukung harus oleh program keamanan informasi. Organisasi harus dapat menentukan dan mengimplementasikan proses penanganan risiko keamanan informasi. Dalam ISO 27001:2013, hal ini dapat dicapai melalui penanganan risiko, yang dilakukan dalam beberapa tahap, yaitu: menetapkan dan memelihara kriteria risiko keamanan informasi, memastikan bahwa penilaian risiko keamanan informasi yang diulang akan memberikan hasil yang konsisten, valid dan sebanding, mengidentifikasi risiko keamanan informasi, menganalisis risiko keamanan informasi, dan mengevaluasi risiko keamanan informasi [2]. Selain itu, kebijakan pengamanan informasi serta implementasi kontrol juga dibutuhkan [3]. Jika kontrol termasuk bagian dari aspek pengamanan informasi dan sistem informasi perusahaan, maka pemasangan proteksi seperti firewall dan enkripsi merupakan kontrol teknis

terkait yang biasanya muncul dalam pikiran [3]. Tentu saja, dari hal semua ini memerlukan pengaturan, dan penyusunan yang dimulai dengan memiliki kebijakan keamanan informasi yang sesuai. Oleh karena itu, risiko terhadap sumber daya informasi perusahaan harus dikelola untuk meminimalkan kemungkinan dan dampak risiko tersebut ketika terjadi.

Namun, tidak banyak organisasi yang menyadari akan pentingnya keamanan informasi. Dimana dari kehilangan, kerusakan, ketidaktersediaan, atau gangguan lainnya terhadap informasi masih umum terjadi di suatu organisasi. PT. Telkom Akses Makassar merupakan anak perusahan dari PT Telekomunikasi Indonesia, Tbk (Telkom) yang bergerak dalam jasa penggelaran dan pengelolaan infrastruktur jaringan akses fixed-broadband, dengan bisnis inti jasa konstruksi penggelaran jaringan akses fixed broadband, managed service & operation maintenance jaringan akses fixed broadband. Kebocoran PT. Telkom Akses Makassar yang merupakan bagian dari perusahaan di Indonesia diminta untuk memberikan pelayanan yang baik bagi pihak yang memerlukan informasi, seperti karyawan dari perusahaan itu sendiri maupun pihak lainnya. Maka dari itu perlu dibentuknya suatu divisi terkhusus yang dapat melayani suatu sistem manajemen informasi dan layanan terkoneksi. Untuk itu suatu informasi tentunya menjadi sebuah aset yang bernilai sebab informasi bersifat rahasia dan mempunyai banyak risiko yang terjadi, seperti adanya pencurian data, *human error*, penyalahgunaan hak akses, kerusakan *hardware* dan *software*, hingga adanya risiko berupa bencana alam.

Berdasarkan hal tersebut, tentu dibutuhkannya sebuah penilaian risiko untuk sebuah perusahaan. Penilaian risiko itu sendiri diperuntukkan sebagai bentuk mengantisipasi semua potensi maupun peluang risiko yang dikemudian hari untuk mungkin terjadi. Dengan demikian, diperlukan tahapan identifikasi, analisis risiko, tahap penilaian, dan mitigasi risiko keamanan informasi di PT. Telkom Akses Makassar. Adapun standar yang digunakan yakni ISO/IEC 27001:2013, yang mana standar ini sangat dibutuhkan dalam pengukuran tingkat keamanan informasi. Kerangka kerja *Failure Mode & Effect Analysis* (FMEA) menjadi salah satu perangkat yang digunakan untuk menilai risiko keamanan informasi di PT. Telkom Akses Makassar. Metode FMEA (Failure Mode & Effect Analysis) adalah mekanisme yang digunakan untuk mengidentifikasi aturan dimana elemen, metode, atau teknik bisa kandas memenuhi arti desainnya [4]. Penerapan metode FMEA ini dipilih karena

metode ini dapat menggambarkan kerusakan yang terjadi secara rinci sehingga memudahkan untuk penentuan tindakan dalam menanganinya. Dimana metode FMEA ini memiliki cara dalam memprioritaskan mode kegagalannya berdasarkan dengan *Risk Priority Number (RPN).*

1.2. Perumusan Masalah

Berdasarkan pemaparan latar belakang penelitian ini, ada beberapa rumusan masalah yang dapat difokuskan menjadi beberapa hal untuk dibahas pada penelitian kali ini. Permasalahan yang ada meliputi :

1. Bagaimana hasil identifikasi aset teknologi informasi perusahaan?
2. Bagaimana hasil penilaian risiko menggunakan metode Failure Mode & Effect Analysis (FMEA)?
3. Bagaimana hasil rekomendasi kontrol keamanan informasi pada perusahaan PT. Telkom Akses Makassar?

1.3. Batasan Masalah

Berikut adalah beberapa dari batasan masalah yang telah ditetapkan dan menjadi perhatian pada pelaksanaan penelitian ini :

1. Studi Kasus pada penelitian ini adalah PT. Telkom Akses Makassar.
2. Penelitian akan menganalisis risiko berdasarkan aset-aset dan informasi yang ada pada PT. Telkom Akses Makassar.
3. Standar yang akan diterapkan dalam penelitian ini adalah ISO/IEC 27001:2013.
4. Metode penilaian risiko yang digunakan adalah metode Failure Mode & Effect Analysis (FMEA).

1.4. Tujuan

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

1. Mengidentifikasi aset teknologi informasi serta risiko dari aset yang ada pada PT. Telkom Akses Makassar.
2. Melakukan penilaian risiko menggunakan metode FMEA untuk mengetahui prioritas risiko dari yang tertinggi hingga terendah.
3. Memberikan rekomendasi kontrol keamanan informasi.

1.5. Rencana Kegiatan

Pada rencana kegiatan penelitian untuk tugas akhir ini akan dilakukan dalam masa waktu kurang lebih 5-6 bulan, yang dimana jadwal kegiatannya sudah disusun untuk melaksanakan penelitian pada tabel jadwal kegiatan. Penyusunan tugas akhir ini akan dimulai dengan melakukan studi literatur mendalam sesuai topik yang akan diangkat dengan mencari referensi sejenis di portal jurnal yang terpercaya dan kredibel. Selanjutnya menentukan tempat penelitian yaitu PT. Telkom Akses Makassar. Kemudian pengumpulan data akan dilakukan dengan menggunakan metode kuantitatif.

Pengumpulan data akan dilakukan dengan teknik membagikan kuesioner kepada 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 rekomendasi perbaikan kontrol berdasarkan hasil penilaian yang didapatkan. Fase terakhir adalah membuat laporan terkait dengan penelitian yang sudah dilakukan dalam bentuk laporan tugas akhir.

Setelah itu akan dilakukan proses pengambilan data kuantitatif terhadap studi kasus. Data Kuantitatif diambil dengan cara membagikan kuesioner untuk mendata aset aset informasi dalam studi kasus kepada pihak-pihak yang berkaitan langsung dengan aset-aset tersebut. Proses selanjutnya dari penelitian adalah melakukan assessment terhadap studi kasus yang didalamnya mencakup identifikasi, penilaian, dan perancangan kontrol keamanan informasi.

1.6. Jadwal Kegiatan

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

Tabel 1.1 Jadwal Kegiatan

No.	Kegiatan	Bulan					
		1	2	3	4	5	6
1	Studi Literatur						
2	Penyusunan dan Pengajuan Judul						
3	Pengumpulan Data Analisis dan Perancangan Sistem						
4	Implementasi Sistem						
5	Analisa Hasil Implementasi						
6	Penulisan Laporan						