BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan teknologi berdampak besar pada perubahan tatanan dunia. Kebutuhan layanan teknologi semakin tinggi diseluruh bidang. Perkembangan teknologi informasi menjadi sebuah kebutuhan utama terhadap proses bisnis sebuah organisasi, perusahaan, maupun instansi sehingga diharuskan untuk selalu beradaptasi terhadap pembaharuan teknologi informasi. Hal ini dikarenakan bahwa teknologi informasi memberikan berbagai manfaat bagi organisasi seperti efisiensi, efektivitas, dan keunggulan kompetitif yang menjadi prioritas utama bagi organisasi yang harus ditingkatkan dengan terus berinovasi dan melakukan evaluasi terhadap proses bisnis organisasi[1]. Pemanfaatan teknologi informasi bagi organisasi perlu melakukan pengolahan data dengan baik karena terdapat sebuah aset yang bernilai dan menyimpan data privasi. Keamanan informasi merupakan hasil dari peningkatan kebutuhan informasi aset yang digunakan untuk mencegah adanya penipuan, pencurian, *plagiarisme*, atau sabotase pada sistem suatu organisasi yang berbasis informasi. Aspek yang dapat menjamin keamanan dari sistem yaitu kelengkapan informasi yang diberikan, kewenangan menyampaikan informasi oleh orang yang tepat, kemudahan dalam mengakses dan menggunakan informasi sesuai dengan kebutuhan, dan format informasi disusun secara tepat dan mudah dipahami. Selain itu, sebuah informasi dapat dinilai aman apabila memenuhi aspek seperti kerahasiaan terjaga dengan baik *(Confidentiality*), informasi secara utuh (*Integrity*), dan ketersediaan sumber informasi *(Availibitiy*)[2].

Penerapan teknologi yang mendukung proses bisnis organisasi memiliki risiko yang dapat terjadi dan harus dapat dikendalikan dengan baik. Apabila risiko yang ditimbulkan tersebut tidak dapat diminimalisir maka akan berdampak pada terganggunya efektivitas bahkan dapat menggangu

berjalannya proses bisnis organisasi[3]. Pengendalian risiko terhadap teknologi informasi akibat perkembangan teknologi yang cepat dapat dilakukan dengan *maintenance* dan *backup* oleh departemen teknologi informasi organisasi. Risiko yang dapat terjadi memiliki tingkatan intensitas yang berbeda seperti bencana alam, sistem yang gagal, *human error*, dan kriminalitas[4]. Risiko yang terjadi tersebut akan selalu ada seiring dengan berjalannya pengimplementasian teknologi informasi pada organisasi tersebut. Usaha meminimalisir dampak dari risiko tersebut maka sebuah organisasi membutuhkan adanya manajemen risiko yang baik[5].

Salah satu organisasi yang memanfaatkan teknologi informasi dalam setiap proses bisnisnya adalah Lembaga Perguruan Tinggi Institut Teknologi Telkom Purwokerto yang terletak di kota Purwokerto Jawa Tengah yang merupakan kampus pertama yang menyediakan layanan Pendidikan *Information and Communications Technologies (ICT)* di Provinsi Jawa Tengah. Institut Teknologi Telkom Purwokerto ini mengedepankan pemanfaatan layanan berbasis teknologi terkait data aktivitas akademik, data mahasiswa, dan data penting lainnya yang dikelola oleh unit Sistem Teknologi Informasi (STI)[6]. STI dimonitori oleh unit *IT Support* dibawah naungan bidang II sumber daya yang bertugas melakukan perombakan dan transformasi terhadap proses bisnis dari konvensional menjadi digital terhadap seluruh layanan yang dibutuhkan oleh mahasiswa, dosen, atau unit lainnya. Data dan informasi yang digunakan yang diberikan sebagai layanan informasi di ITTP masih membutuhkan standarisasi layanan digital dan memastikan keamanan informasinya untuk meminimalisir risiko yang akan terjadi.

Berdasarkan hasil wawancara pra penelitian bersama Yudha Saintika, S.T.,M.T.I selaku Kepala Bidang Unit STI ITTP bahwa pengelolaan manajemen risiko keamanan informasi di ITTP belum memiliki standarisasi yang baku pada layanan sistem informasi seperti data center dan belum mempunyai *site backup* pada sistem yang digunakan. Berdasarkan dokumen TI *Masterplan* ITTP tahun 2019 – 2023 bahwa layanan sistem informasi ITTP belum terstandarisasi ISO 22301. Standarisasi ISO 22301 merupakan sebuah

standar penyusunan manajemen risiko terhadap keamanan informasi pada perguruan tinggi di bidang teknologi informasi (TI). Sistem manajemen kelangsungan bisnis berdasarkan standar internasional ISO 22301 berfungsi untuk meminimalkan risiko kegagalan akibat kejadian serius yang dapat mengancam keberadaan organisasi Anda. Berbeda dengan manajemen risiko konvensional, BCP berfokus pada proses kunci penting untuk memastikan kelangsungan organisasi jika terjadi keadaan darurat. Standarisasi ISO 22301 merupakan metode yang efektif untuk memperkuat ketahanan, meningkatkan stabilitas proses, mempersingkat waktu henti dan waktu pemulihan, mengurangi tingkat kerusakan, dan memungkinkan manajemen risiko holistik. Standar ini didasarkan pada siklus PDCA (*Plan-Do-Check-Act*) dan struktur tingkat tinggi/*High Level Structure* (HLS)[7]. Perbedaan dari standar ISO 22301 dengan ISO 27001:2013 yaitu ISO 27001:2013 tujuannya untuk memberikan kerangka perlindungan *Information Security Management Systems (ISMS)* pada proses bisnis untuk meminimalisir adanya risiko yang dapat merugikan perusahaan[8].

Business Continuity Plan (BCP) merupakan cara yang dapat dilakukan untuk identifikasi terhadap risiko yang belum atau sedang terjadi pada organisasi sehingga organisasi dapat melakukan antisipasi dan minimalisir terjadinya pemberhentian proses bisnis organisasi yang dapat merugikan organisasi baik secara fisik maupun non fisik[9]. Metode BCP berkaitan dengan proses identifikasi, validasi, pengembangan, dokumentasi, dan pengujian terhadap sumber daya yang mendukung proses bisnis suatu organisasi yang dapat terus berjalan secara kondusif pada saat terjadi bencana atau insiden[3]. Fokus utama dari BCP yaitu jaminan atas kontinuitas bisnis ketika terjadi masalah terhadap *people, facilitation, information system,* dan *resources*[10]. BCP memiliki standar yang menjadi panduan analisis yaitu ISO 22301:2012 dengan PDCA *Life Cycle* dan 10 klausul diantaranya adalah *scope, normative references, terms and definitions, context of the organization, leadership, planning, support, operation, performance evaluation,* dan *improvement*[9]. Berdasarkan permasalahan yang disudah

dijelaskan diatas, maka penelitian ini disusun dengan judul **"Perencanaan *Business Continuity Plan* Sesuai Standar ISO 22301 Pada Unit STI Institut Teknologi Telkom Purwokerto".**

1.3 Perumusan Masalah

Berdasarkan uraian latarbelakang diatas dapat dirumuskan sebuah permasalahan pada penelitan ini adalah pengelolaan manajemen risiko keamanan informasi di Institut Teknologi Telkom Purwokerto belum memiliki standarisasi yang baku pada layanan sistem informasi seperti data center dan belum mempunyai *site backup* pada sistem yang digunakan.

1.3 Pertanyaan Penelitian

Berdasarkan rumusan masalah yang diuraikan diatas, maka pertanyaan yang dapat diajukan adalah :

1. Apa standarisasi yang dipergunakan dalam penyusunan kerangka dokumen BCP pada layanan sistem informasi di Institut Teknologi Telkom Purwokerto?
2. Apa hasil dari penyusunan dokumen BCP berdasarkan kondisi saat ini organisasi?

1.4 Tujuan Penelitian

Tujuan penulisan penelitian ini adalah :

1. Menghasilkan dokumen BCP pada unit STI Institut Teknologi Telkom Purwokerto sesuai standarisasi ISO 22301.
2. Menghasilkan penilaian dampak bisnis pada TI unit STI Institut Teknologi Telkom Purwokerto.

1.5 Batasan Masalah

Batasan masalah dalam penelitian ini sebagai berikut :

1. Objek penelitian berupa aset data di unit STI Institut Teknologi Telkom Purwokerto
2. Data didapat dari wawancara dengan unit bagian *IT Support* Institut Teknologi Telkom Purwokerto
3. Penelitian ini mengidentifikasi klausul berdasarkan standari ISO 22301

4. Penelitian ini memiliki fokus analisis pada risiko dan strategi mitigasi risiko pada layanan teknologi informasi di bagian bagian *IT Support* Institut Teknologi Telkom Purwokerto

1.6 Manfaat Penelitian

Hasil penelitian ini diharapkan dapat memberikan manfaat sebagai berikut :

1. Bagi Akademisi

   Dengan adanya penelitian ini, diharapkan dapat memberikan informasi dan referensi tambahan bagi yang membutuhkan untuk penelitian lanjutan terkait dengan penelitian perencanaan BCP dan sebagai bentuk upaya menambah variasi judul penelitian pada Program Studi Sistem Informasi, Fakultas Informatika, Institut Teknologi Telkom Purwokerto.
2. Bagi Objek Penelitian

   Penelitian ini akan menghasilkan testing, evaluasi, dan dokumen BCP yang sesuai dengan kebutuhan unit STI Institut Teknologi Telkom Purwokerto yang diharapkan dapat melakukan pembaruan pada sistem sehingga dapat lebih efektif dalam penggunnya.
3. Bagi Penulis
   a. Mempelajari dan mengidentifikasi risiko teknologi informasi yang diterapkan dalam sebuah organisasi
   b. Meningkatkan keilmuan mengenai penyusunan kerangka dokumen keamanan informasi sesuai ISO 22301
   c. Menyelesaikan syarat tugas mata kuliah Tugas Akhir di Program Studi Sistem Informasi, Fakultas Informatika, Institut Teknologi Telkom Purwokerto,