BAB I
PENDAHULUAN

1.1. Latar Belakang Masalah

Penggunaan teknologi yang berkembang pesat pada saat ini, tentu memberi dampak positif yang cukup signifikan terhadap perorangan, organisasi, ataupun perusahaan. Seiring dengan berkembangnya teknologi tersebut pula, perusahaan-perusahaan tertentu mampu bersaing dengan perusahaan lainnya dan memperoleh target serta tujuannya masing-masing. Dengan penggunaan teknologi ini tentunya, dapat mempercepat proses pengerjaan, dapat menjaga kelangsungan dari proses bisnis ataupun memaksimalkan layanan produk/jasa yang ditawarkan pada perusahaan tersebut [1]. Penggunaan teknologi, juga harus disesuaikan dengan kebutuhan perusahaan agar mampu menyesuaikan nilai efektivitas dan efisiensi [2].

Penggunaan teknologi yang efektif harus mampu mencapai tujuan atau sasaran yang telah ditetapkan, yang berupa nilai kuantitas; kualitas; serta waktu untuk mencapai target/tujuan tersebut [3]. Sedangkan efisien berarti, teknologi yang digunakan harus dapat menyelesaikan pekerjaan secara lebih cepat dengan penggunaan sumber daya dan dana yang serendah-rendahnya [4]. Sehingga setiap perusahaan, harus mampu memenuhi nilai efektivitas dan efisiensi agar mampu menyesuaikan dengan dana yang dikeluarkan secara lebih hemat dan dapat menyelesaikan target/sasaran waktu yang telah ditetapkan. Dengan begitu risiko yang mungkin muncul, dapat dihindari dan kerugian pada perusahaan dapat diminimalisir.

Risiko sendiri merupakan suatu kejadian yang tidak pasti dan dapat terjadi dalam selang waktu tertentu yang dimana dapat menyebabkan kerugian dalam skala kecil bahkan besar yang dapat mengganggu keberlangsungan sebuah perusahaan [5]. Risiko ini dapat berupa tindakan pencurian data, peretasan, kebakaran atau kecelakan, pemalsuan hak akses atau pengrusakan yang dilakukan secara sengaja oleh pihak luar maupun perusahaan sendiri yang tentunya dapat mengancam keamanan teknologi informasi tersebut [6]. Dengan begitu, sebuah perusahaan akan mengalami kerugian yang dapat mengganggu kinerja terhadap pelayanan,

menurunkan reputasi, atau berkurangnya kepercayaan dari masyarakat [7]. Oleh karena itu, proses dalam manajemen risiko sangat dibutuhkan agar mampu menghindari kemungkinan risiko yang akan terjadi [8].

Manajemen risiko merupakan sebuah proses pengidentifikasian dalam bentuk pengukuran untuk memastikan risiko dan mengembangkan strategi yang sesuai dalam mengolah risiko tersebut [5]. Dengan adanya manajemen risiko yang efektif, perusahaan mampu mencapai target/tujuannya; mengatasi permasalahan pelaporan keuangan; dan menyelamatkan reputasi [9]. Dalam hal ini, pemerintah mengupayakan aturan serta tindakan berupa bimbingan teknis seperti pembekalan mengenai manajemen risiko keamanan informasi terhadap perusahaan; pemerintah daerah; maupun penyelenggara publik lainnya [10]. Dengan begitu, kegiatan manajemen risiko dapat terealisasi dengan baik dalam upaya pencegahan terjadinya risiko.

Dari tindakan tersebut, tentu diperlukannya peraturan untuk menerapkan dan menetapkan standar manajemen risiko, seperti yang terdapat pada PP No. 60 Tahun 2008 mengenai Pengendalian Intern Pemerintah. Dengan menciptakan pengendalian intern, tentu keandalan dalam pelaporan keuangan; pengamanan aset Negara; dan ketaatan terhadap peraturan perundang-undangan dapat dilaksanakan dengan baik [11]. Aturan lainnya yang dapat dijadikan pedoman dalam pengelolaan manajemen risiko keamanan informasi, terdapat pada PP No. 82 Tahun 2012 mengenai Penyelenggara Sistem dan Transaksi Elektronik, yang berupa pengaturan tentang perangkat lunak (*software*); perangkat keras (*hardware*); pengaturan tentang pengawasan; dan pengaturan mengenai tenaga ahli serta sertifikasi akan kelayakan terhadap penyelenggaraan sistem transaksi elektronik [12]. Ditegaskan pula, setiap instansi pemerintahan harus memenuhi kriteria terhadap Peraturan Menteri Komunikasi dan Informatika No. 4 Tahun 2016, yang berisi pengaturan akan pencegahan; penanggulangan ancaman; dan serangan yang dapat mengakibatkan gangguan berdasarkan analisis risiko sesuai standar ISO/IEC 27001 [13], serta dari pengendalian risiko yang terbaru dapat menggunakan standar ISO 31000 dalam bidang informasi teknologinya.

Berikut merupakan standar yang dapat digunakan sebagai pedoman dalam melaksanakan manajemen risiko, antara lain standar ISO 31000, ISO 27001, *OCTAVE* (*Operationally, Critical, Threat, Asset, Vulnerability Evaluation*), dan *FAIR* (*Factor Analysis of Information Risk*) [11] [14] [15]. Maka setiap organisasi/perusahaan, terutama yang berkaitan dengan pemerintahan serta penyelenggara publik, disarankan menggunakan seri ISO 31000 dalam penerapan manajemen risiko keamanan teknologi informasinya.

Standar dan peraturan dalam menjaga keamanan informasi sangatlah penting, agar siklus organisasi/perusahaan tetap utuh. Namun, dalam penerapannya yang disesuaikan dengan peraturan pemerintah mengenai evaluasi keamanan informasi yang dilengkapi dengan bimbingan teknis, masih belum dilaksanakan oleh Diskominfo DIY dalam bentuk manajemen risiko keamanan informasinya. Salah satu bentuk kurang tepatnya dalam penerapan manajemen risiko adalah terjadinya kasus peretasan pada *server* Pemda yang diurus oleh Diskominfo DIY yang berkaitan dengan kegiatan Pemilu. Diskominfo DIY sudah mencatat 30.000 kasus berupa dilakukan penyerangan dan melambatnya *server* pada tahun 2019 [16]. Disisi lain, sistem mengalami insiden berupa *backup failure* (pencadangan gagal), sistem *crash* (web *service* mati secara tiba-tiba), *server down* dan *data corrupt*. Insiden tersebut dapat memberi dampak negatif pada reputasi Diskominfo DIY dan menurunnya kepercayaan masyarakat serta kerugian secara finansial, sehingga kegiatan berupa penanganan serta pencegahan perlu diterapkan [17]. Salah satu tindakan yang perlu diterapkan adalah kegiatan manajemen risiko agar dapat mengurangi; mengatasi; serta memetakan ancaman yang akan muncul [18].

1.2. Perumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan, Diskominfo DIY memiliki permasalahan seperti kurangnya penerapan yang tepat dalam pengelolaan manajemen risiko yang dilakukan secara konkrit. Mengingat bahwa keamanan informasi sangatlah penting pada lingkup pemerintahan agar tidak terjadi penyalahgunaan data. Kurangnya perhatian manajemen risiko dapat mengakibatkan permasalahan akan penanganan risiko yang akan muncul. Masalah ini dapat mengakibatkan dampak seperti menghambat kinerja karyawan, serta meningkatnya kerugian dikarenakan harus mengeluarkan biaya yang lebih, bahkan reputasi terhadap Diskominfo DIY dapat menurun akibat ketidakpercayaan masyarakat.

1.3. Pertanyaan Penelitian

1. Bagaimana membuat pengendalian risiko terhadap manajemen risiko keamanan aset teknologi informasi yang tepat untuk Diskominfo DIY?

1.4. Tujuan Penelitian

1. Membuat pengendalian risiko pada manajemen risiko keamanan aset teknologi informasi dalam penerapannya pada Diskominfo DIY.
2. Memberikan saran atau rekomendasi berdasarkan tingkatan risiko yang dihasilkan.

1.5. Batasan Masalah

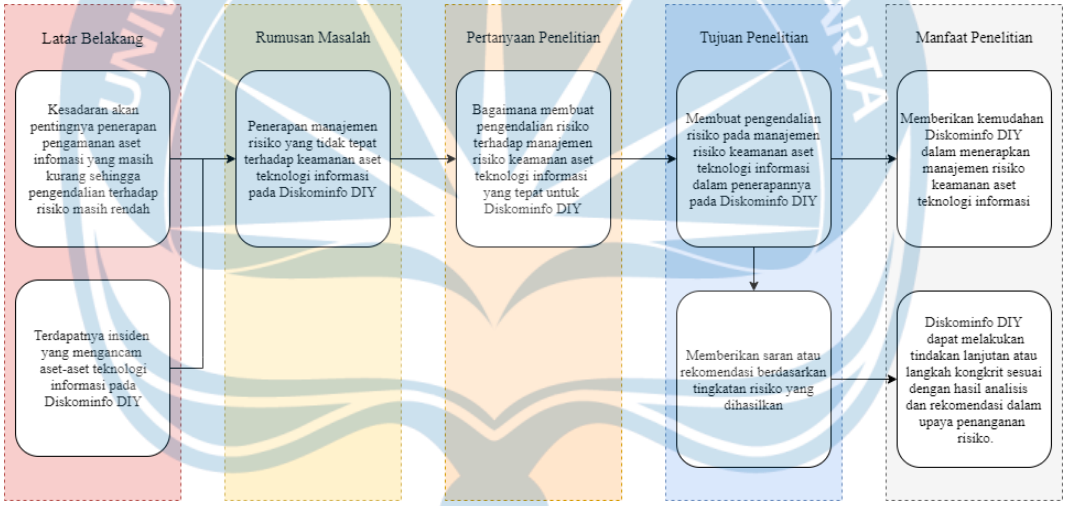
1. Penelitian ini melibatkan karyawan yang berada pada *back office* Diskominfo DIY.
2. Penelitian ini hanya sebatas perangkat lunak saja.
3. Menggunakan metodologi ISO 31000:2018, namun hanya sampai pada tahap pengendalian risiko.

1.6. Manfaat Penelitian

1. Memberikan kemudahan Diskominfo DIY dalam menerapkan manajemen risiko keamanan aset teknologi informasi.
2. Diskominfo DIY dapat melakukan tindakan lanjutan atau langkah kongkrit sesuai dengan hasil analisis dan rekomendasi dalam upaya penanganan risiko.

1.7. Bagan Keterkaitan

Berikut merupakan diagram keterkaitan antara latar belakang, rumusan masalah, pertanyaan penelitian, tujuan penelitian, dan manfaat penelitian pada gambar 1.1.



Gambar 1. 1. Diagram Keterkaitan