

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Saat ini perkembangan Teknologi Informasi begitu pesat dan memiliki peranan yang sangat penting dalam berbagai bidang baik instansi swasta maupun instansi pemerintahan. Peranan Teknologi Informasi bahkan dapat mendukung efektivitas dalam proses bisnis[1]. Seiring dengan penerapan teknologi informasi dengan memberikan segala kemudahan dan manfaat dalam mencapai tujuan bisnis, disamping itu banyak sekali kemungkinan risiko dapat terjadi dalam penerapannya[2]. Kemungkinan risiko yang dapat terjadi menjadi sebuah tantangan tersendiri termasuk bagi instansi pemerintahan. Saat ini instansi pemerintahan di Indonesia telah menerapkan teknologi informasi dalam segala aspek proses bisnis yang berjalan[3]. Penerapan teknologi informasi pada instansi pemerintahan disebut dengan *E-Government*. Wujud penerapan *E-Government* dalam pemerintahan seperti penggunaan sistem informasi, website atau aplikasi untuk memberikan pelayanan kepada publik, *data center* hingga aset teknologi informasi lainnya yang dimiliki sehingga diperlukan manajemen risiko. Implementasi manajemen risiko di sektor publik seperti instansi pemerintahan diharapkan mampu mengendalikan kemungkinan risiko yang ada, sehingga proses bisnis dapat berjalan dengan maksimal dan tujuan organisasi tercapai[4].

Dinas Komunikasi Informatika dan Statistik (DKIS) Kota Cirebon adalah dinas yang memiliki tugas dan kewenangan daerah di bidang Komunikasi, Informatika, Statistika dan persandian, dalam melaksanakan tugas pembantuan bertanggungjawab kepada Walikota[5]. DKIS Kota Cirebon telah menerapkan teknologi informasi dalam segala aspek pelayanan publik. Keberhasilan DKIS Kota Cirebon dalam menerapkan *E-Government* salah satunya layanan *Data Center* sebagai tempat penyimpanan data dan informasi untuk website atau aplikasi milik internal DKIS maupun milik pihak

eksternal seperti Satuan Kerja Perangkat Daerah (SKPD) maupun dinas-dinas lain yang ada di Kota Cirebon.

Pusat data yang dimiliki DKIS Kota Cirebon merupakan salah satu aset TI dimana didalamnya terdiri dari *server*, *router*, *UPS*, hub dan aset pendukung lainnya yang saling terintegrasi. Aset-aset yang ada didalamnya harus dilindungi karena pusat data berfungsi sebagai tempat pengelolaan, penyimpanan, dan layanan untuk berjalannya sebuah layanan sistem informasi serta pendistribusiannya, baik eksternal maupun internal sehingga keamanan data dan informasi yang terdapat didalamnya sangat *crusial* [6], [7]. Keamanan *data center* diperlukan tidak hanya untuk keamanan pada data dan informasi yang ada di dalam *server* maupun *database*-nya saja, tetapi juga keamanan terhadap pemeliharaan aset fisik TI diperlukan untuk menghindari risiko kerusakan, kehilangan, dan kerugian lainnya, sehingga tidak menghambat pengelolaan *data center* secara keseluruhan. Pengelolaan *Data Center* untuk bagian data dan informasi milik DKIS maupun beberapa SKPD lainnya di Kota Cirebon seperti database saat ini berada dibawah pengelolaan Bidang Layanan *E-Government* dan untuk aset fisik *data center* menjadi bagian dari Bidang Infrastruktur TIK dalam memberikan pelayanan sistem jaringan internet.

Berdasarkan hasil pra-penelitian (lihat Bab 3.2) berupa wawancara langsung kepada beberapa *staff* pada Bidang infrastruktur TIK terdapat permasalahan yang terjadi pada layanan *Data Center* bahwa salah satu aset TI berupa UPS (*Uninterruptible Power Supply*) pernah terbakar dan mengalami kerusakan sehingga hal ini akan mempengaruhi proses bisnis pada DKIS Kota Cirebon. Permasalahan lain yang terjadi yaitu belum adanya anggaran untuk pembelian unit aset yang baru atas kerusakan yang terjadi, untuk pengelolaan *data center* pada DKIS Kota Cirebon tidak memiliki standar pusat data nasional maupun ISO sehingga pusat data yang dimiliki saat ini belum ideal dan masih sebatas ruangan *server*. Selain itu, risiko yang terjadi pada *data center* sangat tinggi menurut staf bidang terkait. Dapat disimpulkan dari hasil wawancara tersebut aset-aset TI yang terdapat pada *data center* memiliki banyak kemungkinan risiko yang dapat terjadi sehingga perlu dilakukan analisis manajemen risiko untuk menangani

risiko atau ancaman tersebut terulang kembali dan mencegah kemungkinan risiko TI lainnya. Pada proses analisis risiko dapat dilakukan dengan 3 metode yaitu *Qualitative Analysis Method* (analisis kualitatif), *Quantitative Analysis Method* (analisis kuantitatif) dan *Hybrid Method* (metode hybrid)[8].

Penelitian yang dilakukan ini bertujuan untuk melakukan analisis manajemen risiko terhadap aset TI pada layanan *Data Center* DKIS Kota Cirebon dengan menggunakan metode *Hybrid QRA*. *Hybrid QRA* merupakan kombinasi *Quantitative Risk Analysis* dan *Qualitative Risk Analysis*. Penggunaan *Quantitative Risk Analysis* (QRA) untuk melakukan perhitungan dengan angka sehingga dapat diketahui aset yang memerlukan perhatian khusus. Sedangkan metode *Qualitative Risk Analysis* digunakan untuk memberikan rekomendasi kontrol sebagai tindakan preventif dalam menangani ancaman/risiko berdasarkan hasil ranking dari metode QRA, dengan berpedoman pada NIST SP 800-53.

Penentuan metode *Quantitative Risk Analysis* (QRA) sebagai metode dalam penelitian ini didasarkan pada permasalahan yang terjadi, dimana fokus masalah yang ada berkaitan dengan pengelolaan aset TI Layanan Data Center DKIS Kota Cirebon, anggaran kebutuhan aset TI, pemeliharaan aset TI dan risiko/ancaman yang terjadi terhadap aset TI tersebut. Dinas Komunikasi Informatika dan Statistik (DKIS) Kota Cirebon sebenarnya telah merencanakan Manajemen Risiko SPBE. Berdasarkan Permenpanrb No. 5 Tahun 2020 tentang pedoman manajemen risiko SPBE, dimana pedoman tersebut diadopsi dari metode COBIT5 for risk dan ISO 31000[9]. Namun, panduan Manajemen Risiko SPBE dirasa masih awam dan masih sangat kompleks untuk dipahami, khususnya bagi DKIS Kota Cirebon walaupun sudah diberikan sosialisasi mengenai Manajemen Risiko SPBE. Selain itu, Manajemen Risiko SPBE hanya menilai risiko secara deskriptif saja, sehingga tidak dapat diketahui nilai potensi risiko secara numerik. Dari kondisi tersebut, peneliti memilih metode *Quantitative Risk Analysis* (QRA) yang digunakan dalam menganalisis nilai risiko, mengetahui nilai aset TI dan nilai potensi kerugian dari risiko/ancaman hanya pada ruang lingkup Layanan Data Center DKIS Kota Cirebon, bukan terhadap DKIS Kota Cirebon secara

keseluruhan. Hasil dari analisis risiko menggunakan QRA dalam penelitian ini dapat mendukung poin-poin yang terdapat dalam Manajemen Risiko SPBE.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dibahas sebelumnya, maka rumusan masalahnya adalah:

Bagaimana penerapan Manajemen Risiko untuk mengetahui nilai risiko, tingkat risiko yang terjadi, dan mitigasi risiko yang dilakukan pada layanan *data center* Dinas Komunikasi Informatika dan Statistik (DKIS) Kota Cirebon?

1.3 Pernyataan Masalah

Berdasarkan latar belakang yang telah dibahas di atas, dapat diidentifikasi terdapat permasalahan pada aset TI beserta risiko yang muncul pada *Data Center* DKIS Kota Cirebon, diantaranya sebagai berikut.

1. Manajemen risiko terhadap aset TI pada *Data Center* DKIS Kota Cirebon belum dilakukan secara optimal.
2. Pengelolaan data center tidak memiliki standar pusat data nasional ataupun ISO hanya sebatas ruangan server saja, sehingga kemungkinan risiko yang terjadi pada layanan *Data Center* tinggi.

1.4 Tujuan

Tujuan dari penelitian ini adalah sebagai berikut.

1. Mengidentifikasi nilai risiko yang muncul terhadap aset TI Layanan *Data Center* DKIS Kota Cirebon
2. Melakukan penilaian risiko berdasarkan nilai risiko yang telah diidentifikasi terhadap aset TI Layanan *Data Center* DKIS Kota Cirebon
3. Memberikan rekomendasi kontrol sebagai mitigasi risiko terhadap aset Layanan *Data Center* DKIS Kota Cirebon

1.5 Batasan Masalah

Batasan masalah yang menjadi lingkup penelitian adalah sebagai berikut.

1. Analisis manajemen risiko aset TI yang dilakukan hanya pada ruang lingkup Layanan *Data Center* DKIS Kota Cirebon.
2. Analisis manajemen risiko terhadap aset TI *Data Center* menggunakan metode *Hybrid QRA* yaitu metode *Quantitative Risk Analysis (QRA)* dan *Qualitative Risk Analysis* dengan berpedoman pada NIST SP 800-53 Revisi 5.

1.6 Hipotesis

1. Metode *Hybrid QRA* yang digunakan dalam penelitian ini memberikan hasil yang lebih lengkap. Dimana metode *QRA (Quantitative Risk Analysis)* akan fokus pada analisis pemeliharaan aset TI dengan perhitungan angka sehingga diperoleh nilai untuk aset yang memerlukan perhatian khusus dan paling utama. Sedangkan metode *Qualitative Risk Analysis* akan menghasilkan rekomendasi kontrol terhadap kemungkinan risiko dan ancaman yang muncul yang berdampak pada aset TI yang ada.
2. Penilaian risiko dan rekomendasi kontrol yang dihasilkan dari penelitian ini dapat dijadikan *output* atau bahan pertimbangan evaluasi untuk pengelolaan aset dan penanganan risiko pada Layanan *Data Center* DKIS Kota Cirebon.

1.7 Jadwal Kegiatan

Berikut ini adalah tabel masa pengerjaan tugas akhir yang penulis susun:

Tabel 1 Jadwal Kegiatan

Kegiatan	Bulan					
	1	2	3	4	5	6
Konsultasi dengan Pembimbing						
Studi Literatur						
Perumusan Masalah						
Pengumpulan Data						
Analisis dan Pengolahan Data						
Penyusunan laporan tugas akhir						
Memaparkan Hasil Penelitian						