Bab I Pendahuluan

Pada bab ini menjelaskan latar belakang penulis melakukan penelitian, rumusan masalah, tujuan penelitian, ruang lingkup atau batasan masalah yang ada pada penelitian ini, serta sistematika penulisan dari penelitian yang telah dilakukan

I.1 Latar Belakang

Seiring berkembangannya teknologi, banyak kalangan yang menfaatkannya , baik perorangan, kelompok, ataupun organisasi pemanfaatan teknologi salah satunya yaitu dengan menggunakan sistem informasi, penggunaan sistem informasi harus diikuti dengan adanya manajemen keamanan informasi yang bertujuan untuk menjaga, memelihara, keamanan informasinya, karena semakin berkembangnya teknologi akan semakin banyak ancaman-ancaman yang menyerang informasi tersebut. Badan Siber dan Sandi Negara (BSSN) mencatat adanya 225,9 juta serangan siber ke Indonesia pada 2018 dan pusat operasi mencatat 40 persen di antaranya merupakan serangan malware yang menyebabkan terganggunya keamanan informasi (CNN Indonesia, 2019). Sehingga setiap informasi perlu untuk dijaga keamanannya dengan tahapan awal yaitu menganalisis risiko yang akan terjadi lalu dilakukan perancangan manajemen keamanan informasinya, untuk menangani risiko-risiko yang sebelumnya telah dianalisis. Perancangan manajemen keamanan sistem informasi merupakan bagian dari pengendalian internal suatu sistem yang digunakan, yang meliputi pemanfaatan teknologi, dokumen, prosedur untuk melindungi dan memecahkan masalah.

Pada penelitian ini berfokus merancangan manajemen keamanan informasi di suatu instansi pemerintahan yaitu Dinas Komunikasi dan Informatika Provinsi Jawa Barat, merupakan salah satu Instansi Pemerintahan di Indonesia yang memanfaatkan keberadaan teknologi dengan membuat sistem informasi berdasarkan instruksi presiden no 3 tahun 2003 tentang Kebijakan dan Strategi Nasional Pengembangan E-Government dan Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Regulasi SPBE).

Dinas Komunikasi dan Informatika Provinsi Jawa Barat adalah instansi pemerintahan yang memiliki tanggung jawab atas pengolahan informasi dalam lingkungan Pemerintahan Jawa Barat. Instansi ini mencakup penyediaan sistem informasi daerah dan pemberian solusi untuk pengolahan data Pemerintahan Jawa Barat. Sistem Informasi yang dibangun Dinas Komunikasi dan Informatika digunakan oleh instansi-instansi daerah yang berada di Provinsi Jawa Barat. Salah satunya adalah aplikasi Service Desk yang menjadi fokus penelitian ini, aplikasi service desk merupakan aplikasi milik Dinas Komunikasi dan Informatika Jawa Barat yaitu aplikasi berbasis website yang digunakan untuk memfasilitasi perangkat daerah dalam melakukan permintaan atau keluhan terhadap penerapan layanan teknologi informasi dilingkungan Pemerintah Provinsi Jawa Barat. Sehingga keamanan informasi di instansi ini harus dijaga dikelola dengan baik.

Peran sistem informasi di Dinas Komunkasi dan Informatika sangat penting, khususnya aplikasi service desk begitu juga data yang dimiliki oleh Dinas Komunikasi dan Informatika menyangkut data instansi-instansi daerah yang berada di Jawa Barat. Oleh karena itu ancaman terganggunya keamanan informasi sangat rentan, seperti munculnya risiko-risiko yang dapat menyebabkan terganggungnya keamanan informasi. Ancaman terganggunya keamanan informasi dapat diselesaikan dengan menganalisis risiko terlebih dahulu yang merupakan suatu usaha untuk mengetahui, menganalisis serta mengendalikan risiko dalam setiap kegiatan dengan memperoleh efektifitas dan efisiensi yang lebih tinggi. Manajemen risiko sangat dibutuhkan karena berkaitan dengan kemanan informasi dapat mengidentifikasi ancaman yang menyerang sumber daya informasi perusahaan, jika risiko dapat diminimalisir maka Dinas Komunkasi dan Informatika dapat melindungi data dan informasi yang dimiliki

Konsep yang akan diterapkan dalam hal ini yaitu menggunakan metode ISO 27005 sebagai basis untuk menganalisis risiko tentang keamanan informasi yang mengatur tentang manajemen risiko dalam keamanan informasi. ISO 27005 menyediakan pedoman untuk manajemen risiko keamanan informasi, sehingga dapat membantu merancang manajemen keamanan informasi dengan mengetahui

terlebih dahulu risikonya. Setelah mengetahui risikonya maka dilakukan analisis dengan metode ini, dengan tujuan dapat mengendalikan risiko yang telah diketahui.

Dengan menerapkan manajemen risiko maka dapat menjaga keamanan informasi, dalam sebuah informasi pasti akan terdapat beberapa risiko yang akan terjadi dan perlu dikendalikan. ISO 27005 merupakan salah satu metode manajeman risiko yang dapat mengetahui *Asset Vulnerability* (Kerentanan), *Threath* (Ancaman) dari segi manajemen, teknikal dan operasional yaitu: *Threath* (Ancaman) yang terjadi serangan dari luar meliputi: *Hacker* yaitu dengan penyusupan ke sistem d`engan menggunakan akses yang illegal, serangan *virus ransomeware* yang dapat menimbulakan kehilagan data. *Vulnerability* (Kerentanan) yang terjadi yaitu kesalahan sumber daya manusia, kesalahan dalam *Hardware*. Untuk pemilihan kontrol keamanan informasi mengacu pada kerangka kerja standar internasional yaitu ISO 27001 yang menyediakan kerangka kerja dalam ruang lingkup penggunakan teknologi informasi dan pengelolaan asset sehingga dapat membantu organisasi dalam memastikan keamanan informasi yang diterapkan sudah efektif. (Jurnal Teknik ITS Vol. 6, No. 1, 2017).

Keamanan informasi begitu penting dalam mendukung kesuksesan Teknologi Informasi pada suatu organisasi atau instansi pemerintahan, oleh karena terdapat beberapa tahapan untuk mengelola keamanan informasi dengan cara mengidentifikasi, menganalisis, memberikan solusi dan melaporkan risiko. Maka dari itu Dinas Komunikasi dan Informatika sebagai instansi pemerintahan memerlukan pedoman atau acuan dalam menjalankan keamananan informasi yang efisien dan efektif sehingga dapat menjaga dan melindungi informasi yang dimiliki. Penelitian ini dilakukan bermaksud untuk membantu dan memberikan solusi dalam penilaian risiko dan memberikan solusi dengan melakukan perancangan kontrol informasi di Dinas Komunikasi dan Informatika Jawa Barat. Dengan demikian bentuk dukungan dalam pengendalian sistem manajemen keamanan informasi, dengan membuat kontrol keamanan sesuai dengan hasil dari analisis risiko sebelumnya.

I.2 Rumusan Masalah

Di bagian latar belakang peneliti telah mengulas mengenai manajemen risiko dan kontrol keamanan informasi maka rumusan Masalah yang akan diteliti pada tugaas akhir ini yaitu :

1. Bagaimana cara mengetahui profil risiko pada aplikasi Service Desk yang dikelola oleh Dinas Komunikasi dan Informatika Jawa Barat
2. Bagaimana rancangan manajemen keamanan informasi dengan menggunakan referensi framework ISO 27005 sebagai metode analisis risiko dan referensi ISO 27001 untuk pemilihan kontrol keamanan informasi

I.3 Tujuan

Penelitian ini memiliki beberapa tujuan, sebagai berikut :

1. Mengetahui profil risiko aplikasi Service Desk yang dikelola oleh Dinas Komunikasi dan Informatika Jawa Barat
2. Membuat rancangan manajemen keamanan informasi dengan menggunakan referensi framework ISO 27005 sebagai metode analisis risiko dan referensi ISO 27001 untuk pemilihan kontrol keamanan informasi

I.4 Batasan Masalah

Batasan masalah dari penelitian ini yaitu sebagai berikut :

1. Batasan yang menjadi objek penelitian adalah aplikasi Service Desk Dinas Komunikasi dan Informatika Jawa Barat
2. Penelitian menggunakan ISO 27005 sebagai metode analisis risiko
3. Penelitian menggunakan ISO 27001 untuk pemilihan kontrol keamanan informasi
4. Kontrol risiko yang direkomendasikan tidak sampai kepada tahap pengujian

I.5 Manfaat Penelitian

Manfaat yang diperoleh dari penelitian ini adalah :

1. Mengetahui ancaman dan kerentanan pada aplikasi service desk

2. Membantu Dinas Komunikais dan Informatika Jawa Barat untuk mengetahui apakah keamanan informasi untuk aplikais service desk telah sesuai dengan standar
3. Dapat memberikan rancangan solusi terhadap perancangan keamanan informasi pada aplikasi service desk

I.6 Sistematika Penulisan

Bab I Pendahuluan

Dalam bab ini terdiri dari latar belakang masalah tentang alasan dilakukannya penelitian, identifikasi masalah, perumusan masalah,tujuan dan manfaat penelitian, ruang lingkup dan batasan masalah, metode yang akan digunakan dalam penelitian, dan sistematika penulisan

Bab II Landasan Teori

Dalam bab ini berisi teori yang mendukung penulisan tugas akhir sesuai dengan tema yang diambil dan latar belakang dari penelitian

Bab III Metodologi Penelitian

Pada bab ini akan dijelaskan bagaimana metode yang digunakan dapat diimplementasikan terhadap data-data yang didapatkan.

Bab IV Data dan Analisis Penelitian

Dalam bab ini menjelaskan bagaimana data yang didapat akan dianalisa, serta hasil apa yang diperoleh dari pengumpulan dan pengelolaan data yang dilakukan

Bab V Perancangan Kontrol Keamanan Informasi

Dalam bab ini merupakan langkah selanjutnya setelah membahas hasil yang didapatkan pada bab sebelumnya, yaitu untuk mengusulkan rancangan manajemen risiko teknologi informasi yang sesuai dengan analisis.

Bab VI Kesimpulan dan Saran

Dalam bab ini menjelaskan kesimpulan dari hasil penelitian dan saran-sarang atas hasil penelitian bagi objek observasi peneliti berikutnya