BAB 1

PENDAHULUAN

1.1 Latar Belakang

Lembaga Penerbangan dan Antariksa Nasional (LAPAN) adalah Lembaga Pemerintah Non Kementrian Indonesia yang melaksanakan tugas pemerintahan di bidang penelitian dan pengembangan kedirgantaraan dan pemanfaatannya. Dengan visi meningkatkan kualitas litbang penerbangan dan antariksa bertaraf internasional, meningkatkan kualitas produk teknologi dan informasi di bidang penerbangan dan antariksa dalam memecahkan permasalahan nasional, melaksanakan dan mengatur penyelenggaraan keantariksaan untuk kepentingan nasional.

Pengelolaan informasi di LAPAN sudah terkomputerisasi. Implementasi infrastruktur teknologi informasi memiliki risiko yang dapat mengganggu kinerja organisasi maupun operasional. Risiko ini disebabkan oleh manusia atau sistem itu sendiri. Risiko yang timbul sebagai akibat dari implementasi teknologi informasi yang kurang memadai dapat menyebabkan kegiatan organisasi yang tidak optimal, kerugian finansial, atau bahkan menurunnya reputasi organisasi. Karena itu, organisasi dituntut untuk memiliki manajemen risiko, dimana manajemen risiko merupakan suatu pengelolaan yang melihat potensi-potensi atau hal-hal apa saja yang harus dilakukan agar dapat meminimalkan risiko sekecil mungkin yang dapat terjadi sewaktu-waktu pada organisasi. Potensi-potensi risiko tersebut dapat dilihat dari berbagai aspek, baik itu secara sengaja maupun tidak sengaja. Organisasi diharapkan dapat mengelola berbagai risiko teknologi informasi.

Dalam analisis ini, digunakan ISO 27005:2011 untuk menyusun suatu kebijakan mengenai manajemen risiko keamanan, proses dan prosedur dalam peningkatan keamanan informasi sehingga sesuai dengan kebijakan dan tujuan LAPAN.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah di atas, maka dapat dikemukakan identifikasi permasalahan penelitian sebagai berikut:

1. Apa saja aset-aset teknologi informasi yang perlu dilindungi terkait teknologi informasi RDSA?
2. Bagaimana potensi ancaman yang dapat terjadi terhadap aset teknologi informasi RDSA di LAPAN bandung?
3. Bagaimana potensi kerentanan yang dapat terjadi terhadap aset teknologi informasi RDSA di LAPAN bandung?
4. Bagaimana *level* risiko yang mungkin terjadi terhadap aset teknologi informasi RDSA di LAPAN bandung berdasarkan *framework* ISO/IEC 27005:2011?

1.3 Tujuan Pembahasan

Tujuan pembahasan pada pembuatan tugas akhir ini adalah sebagai berikut:

1. Menentukan aset-aset teknologi informasi yang perlu dilindungi terkait teknologi informasi untuk infrastruktur RDSA di LAPAN bandung.
2. Mengetahui potensi ancaman yang dapat terjadi terhadap aset teknologi informasi RDSA di LAPAN bandung.
3. Mengetahui potensi kerentanan yang dapat terjadi terhadap aset teknologi informasi RDSA di LAPAN bandung.
4. Menentukan *level* risiko yang mungkin terjadi terhadap aset teknologi informasi RDSA di LAPAN bandung berdasarkan *framework* ISO/IEC 27005:2011.

1.4 Ruang Lingkup

Berikut ini adalah ruang lingkup kajian dalam pembuatan tugas akhir ini:

1. Penelitian dilakukan pada divisi IT LAPAN bandung.
2. Penilaian risiko teknologi informasi ini terkait aset teknologi informasi untuk infrastuktur RDSA di LAPAN bandung.
3. Pembahasan akan mengacu pada penggunaan ISO 27005:2011.

1.5 Sumber Data

Berikut ini adalah sumber data yang digunakan dalam pembuatan tugas akhir ini :

1. Metode Pengumpulan Data

Pengumpulan data dilakukan dengan dua metode, yaitu :

a. Studi Pustaka

Dalam metode ini, penulis mengumpulkan data-data berupa buku-buku yang berhubungan dengan topik, dimana merupakan panduan dalam penyusunan skripsi ini serta membantu dalam memecahkan masalah dalam skripsi ini.

b. Kunjungan Lapangan

Kunjungan lapangan dilakukan untuk memperoleh data langsung dari organisasi dengan cara :

1. Wawancara (*interview*)

Proses wawancara dilakukan dengan mengadakan tanya jawab secara langsung dengan pihak-pihak yang terkait dan berhubungan dengan topik skripsi.

2. Observasi

Metode ini dilakukan dengan melakukan pengamatan dan peninjauan secara langsung terhadap objek penelitian untuk mendapatkan gambaran umum organisasi serta kondisi sistem jaringan yang diterapkan.

3. Checklist

Metode ini dilakukan untuk menyederhanakan proses identifikasi risiko. Dengan menggunakan *checklist* dapat dilakukan identifikasi awal kemungkinan risiko yang terjadi yang nantinya dapat dikembangkan dengan menggunakan metode identifikasi risiko lainnya untuk mendapat informasi yang lebih mendalam.

2. Teknik Analisis

Dalam melakukan pengukuran risiko infrastruktur teknologi informasi RDSA pada divisi IT LAPAN, penelitian ini menggunakan *framework* ISO 27005:2011, yaitu:

- a. *Risk analysis*
 1. *Risk identification*
 2. *Risk estimation*
- b. *Risk assessment*

1.6 Sistematika Penyajian

Sistematika penyajian diuraikan sebagai berikut:

BAB I PENDAHULUAN, bab ini menjelaskan gambaran singkat mengenai latar belakang, rumusan masalah, tujuan pembahasan, ruang lingkup kajian, sumber data yang digunakan serta sistematika penulisan.

BAB II KAJIAN TEORI, bab ini menjelaskan pembahasan mengenai dasar atau kajian teori yang digunakan dalam penyusunan tugas akhir.

BAB III HASIL ANALISIS, bab ini berisi penjelasan tentang analisis manajemen risiko keamanan informasi terkait infrastruktur teknologi informasi RDSA di LAPAN dengan menggunakan ISO 27005:2011.

BAB IV KESIMPULAN DAN SARAN, merupakan bagian penutup pada laporan yang berisikan penjelasan mengenai simpulan dan saran dari tugas akhir yang dibuat agar berguna bagi lembaga.