BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi sangat pesat mempengaruhi sistem dalam melakukan aktivitas keseharian, baik fungsi dan tugas selalu berkembang mengikuti kemajuan ilmu pengetahuan. Perkembangan teknologi informasi dimulai pada pertengahan tahun 1960-an ketika komputasi menyebar ke negara-negara industri jasa dengan ditandai sebagai munculnya fenomena masyarakat informasi. Era perkembangan komputerisasi terus belanjut pada tahun 1990-an sehingga melahirkan teknologi internet (Setiawan 2018). Berkembangnya teknologi informasi sampai saat ini yang semakin pesat membuat setiap perusahaan maupun organisasi bergerak mengikutinya sebagai atribut yang sangat penting dalam mendukung proses bisnis sehingga penggunaan komputer dan internet sangat mendominasi pekerjaaan manusia hampir disegala bidang baik industri maupun bidang pendidikan.

Bagi dunia pendidikan kebutuhan akan teknologi informasi merupakan sebuah aset dan kebutuhan dalam melakukan operasinya. Hal ini dilakukan untuk memudahkan pekerjaan seperti pelayanan pembelajaran, pelayanan administrasi maupun penyebaran informasi publik. Sebagian besar aktivitas dilakukan memanfaatkan teknologi informasi Akibatnya, semakin banyak pengguna infrastuktur teknologi informasi sehingga dampak resiko semakin meningkat. Resiko terjadi baik berhubungan dengan infrastruktur, hardware, software, internet maupun brainware.

Selanjutnya, Perguruan Tinggi seperti Universitas, Institut dan lainnya yang menerapkan komputerisasi disemua aktivitas baik belajar secara online maupun pengurusan administrasi mata kuliah dan nilai sehingga perlu pengawasan dalam mengetahui status keamanan diantaranya adalah hilangnya data, redundancy, data rusak, infeksi data oleh malware dan virus, personil yang menyalah gunakan hak akses yang dimiliki. Hal tersebut menghambat proses bisnis dan merugikan baik itu dari segi waktu maupun biaya bagi pihak perguruan tinggi dan mahasiswa (Husaini, Ambarwati et al. 2019).

Peruruan tinggi juga diwajibkan oleh pihak regulator (pemerintah) untuk dapat memanfaatkan IT. Sebagai contoh, pelaporan data akademik yang meliputi peserta didik, dosen dan hasil proses akademik dilaporkan berkala melalui sistem yang terstruktur sehingga mengharuskan penggunaan teknologi informasi dalam menunjang proses kerja baik internal maupun untuk eksternal. Penguatan keamanan jaringan dan sistem dalam pembangunan manajemen resiko harus diterapkan bagi Perguruan Tinggi. Sebagai penunjang aktivitas pengolahan data pada bidang teknologi informasi seperti Institut Ilmu Kesehatan dan Teknologi Muhammadiyah Palembang (IKesT MP). Oleh karenanya, peningkatan resiko ini menuntut strategi manajemen yang memadai untuk mencegah resiko buruk terhadap operasional Perguruan Tinggi tersebut.

(IKesT MP) adalah perubahan bentuk Sekolah Tinggi Ilmu Kesehatan Muhamamdiyah Palembang yang bergerak dibidang pelayanan pendidikan kesehatan yang kemudian pada tanggal 05 Agustus 2020 STIKes Muhammadiyah Palembang berubah bentuk menjadi Institut Ilmu Kesehatan dan Teknologi Muhammadiyah Palembang dengan menambah pelayanan pendidikan dibidang

teknologi yang juga merupakan brand baru institusi. Perubahan bentuk berdampak pada penambahan struktur organisasi, adminsirtasi dan SDM sehingga penggunaan teknologi informasi semakin bertambah.

Seiring proses perubahan bentuk dan proses perkembangan infrastruktur di IKesT MP belum adanya manajemen risiko dalam penilaian analisis risiko yang jelas berkaitan dengan ancaman, kelemahan dan keamanan TI. Untuk mengetahui sampai sejauh mana kesiapan untuk menghadapi ancaman-ancaman yang ada. Tindakan untuk meminimalisir kemungkinan terjadinya risiko aset TI pada IKesT MP, yaitu dengan analisis manajamen risiko TI dan penyusunan dokumen operasioanl kebijakan dalam infrastruktur TI. Banyak framework yang telah disediakan untuk menghadapi risiko- risiko ancaman yang kemungkinan terjadi. Salah satunya yaitu *Octave – s.*

Risk assessment memegang peranan penting dalam penerapan sistem manajemen keamanan informasi. Ada banyak metode yang dapat digunakan untuk melaksanakan risk assessment, karena banyaknya konsultan keamanan informasi yang mengembangkan berbagai pendekatan untuk melakukannya. Banyak framework manajemen risiko dapat digunakan dalam membangun *risk manaagmen*t baik dari fungsi maupun struktur dokumen yang sesuai dengan kebutuhan dan misi dari penelitian. Satu yang terkenal diantaranya adalah metode *octave* yang dikembangkan oleh Carnegie Mellon Software Engineering Institute, Pittsburg.

Valuation (*octave*) merupakan metode yang dapat digunakan untuk mengidentifikasi ancaman yang dapat menimbulkan risiko TI. Dalam praktiknya *octave - s* juga dapat membantu dalam melakukan evaluasi risiko, identifikasi aset

TI yang penting sesuai organisasi, juga melakukan identifikasi kerentanan dan ancaman terhadap aset TI tersebut serta melakukan evaluasi potensi jika ancaman tersebut terjadi (Rohman, Ambarwati et al. 2020).

Indentifikasi resiko ancaman dan kelemahan infrastukrur menjadi prioritas, mengetahui apa saja ancaman yang akan terjadi untuk dapat menerapkan standar operasional dalam menjaga keamanan data. Sehingga pentingnya membangun manajemen risiko sebagai proses pengembangan kedepan sebagai strategi untuk menghindari kesalahan – kesalahan di bidang infrastuktur TI di IKesT Muhammadiyah Palembang

1.2 Identifikasi Masalah

Dari uraian diatas, beberapa permasalahan dapat di indetifikasi sebagai berikut:

1. Pemanfaatan TI dapat menimbulkan beberapa risiko yang dapat merugikan aset
2. Risiko Keamanan dalam TI yang dapat menggangu organisasi
3. Pentingnya memperkuat keamanan IT dalam melakukan pekerjaan
4. Objek (IKesT MP) Belum ada kebijakan dan menerapkan manajemen keamanan dalam pengelolaan TI

1.3 Batasan Masalah

Dari permasalahan yang dapat diidentifikasi, penelitian berfokus pada penguatan fungsi dan keamanan TI dengan menerapkan manajemen resiko penggunaan teknologi informasi. Pada penelitian ini menggunakan framework octave – s dalam melakukan manajemen aset.

1.4 Rumusan Permasalahan

Adapun rumusan penelitian yang diangkat dalam penelitian ini adalah bagaimana mengukur status risiko dan keamanan dalam mencari kelemahan TI menggunakan framework *Octave-S.*

1.5 Tujuan Penelitian

Adapun Penelitian ini bertujuan untuk :

1. Mengindentifikasi sumber risiko dalam pemanfaatan TI
2. Mendapatkah hasil profil ancaman yang mungkin dapat terjadi
3. Menerapkan kebijakan operasional dalam memperkuat keamanan TI
4. Menjadi rujukan dokumentasi pembuatan renstra dalam pegembangan mutu institusi terutama dibidang teknologi informasi

1.6 Manfaat Penelitian

Manfaat dari penelitian diatas diharapakan dapat mengetahui status resiko kesalahan dan kerusakan untuk meningkatkan kualitas layanan khususnya di teknologi informasi, membantu mengetahui ancaman dan kelemahan sehingga dapat melakukan pembenahan dan strategi dalam melakukan perkembangan teknologi informasi.

1.7 Susunan dan Struktur Penelitian

Susunan dan struktur penelitian yang dilakukan dalam membangun manajemen TI sebagai landasan dan teori dalam menyelesaikan laporan penelitian secara sistematik. Berikut susunan dan susunan penelitian :

BAB I PENDAHULUAN

Pada bab ini membahas tentang latar belakang, identifikasi masalah, batasan masalah, rumusan masalah, tujuan dan manfaat penelitian, ruang lingkup penelitian, serta susunan dan struktur dalam melakukan penelitian.

BAB II LANDASAN TEORI

Pada bab ini membahas tentang landasan teori sebagai penunjang penelitian, rivew penelitian terdahulu u, kerangka berfikir, dan hipotesis penelitian yang akan dilakukan.

BAB III METODOLOGI PENELITIAN

Pada bab ini pembahasannya yang terdiri dari desain dan jadwal penelitian, data penelitian meliputi jenis data, populasi dan sampel penelitian, kemudian konsep dan metode penelitian yang digunakan, metode pengumpulan data serta teknik analisis data.

LAMPIRAN

Berisi lampiran pendukung daripada penelitian yang akan dilakukan.