BAB I

PENDAHULUAN

1.1. Latar Belakang

Berkembangnya teknologi dan transformasi digital telah membawa perubahan signifikan dalam berbagai sektor, termasuk sektor perbankan. Peningkatan penggunaan teknologi informasi dan sistem digital telah mengubah cara operasional dilakukan, tetapi hal tersebut juga meningkatkan tantangan dalam pengelolaan risiko, terutama terkait dengan keamanan data dan integritas sistem. Dalam implementasinya, manajemen risiko menjadi aspek penting yang tidak dapat diabaikan untuk melindungi aset informasi organisasi. Pengelolaan risiko yang baik memungkinkan organisasi untuk mendeteksi, mengevaluasi, dan mengendalikan potensi ancaman, sehingga operasional dapat berjalan lancar dan bisnis tetap berkelanjutan.

Dalam konteks perbankan, risiko keamanan menjadi salah satu fokus utama, terutama dengan ketergantungan yang tinggi terhadap berbagai sistem informasi yang semakin kompleks dan saling terhubung. Risiko ini mencakup berbagai sektor dalam sistem manajemen risiko, seperti jaringan komunikasi, audit it, manajemen it, pengembangan dan pengadaan, pengamanan informasi, serta rencana pemulihan bencana.

Salah satu standar yang banyak digunakan dalam analisis risiko keamanan informasi adalah *National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30*. *Framework* ini dikenal luas sebagai standar dalam melakukan analisis risiko keamanan informasi dan siber. *Framework* ini menyediakan pendekatan sistematis melalui sembilan langkah analisis risiko, mulai dari karakteristik sistem, identifikasi ancaman, identifikasi kerentanan, analisis kontrol, analisis dampak, hingga dokumentasi dan rekomendasi kontrol. Framework ini memiliki keunggulan karena menawarkan detail pelaksanaan yang komprehensif dan memberikan panduan rekomendasi kontrol yang lebih luas dibandingkan framework lainnya.

NIST SP 800-30 dapat membantu organisasi dalam memahami potensi/penilaian risiko yang dapat timbul dari berbagai ancaman yang mempengaruhi sistem informasi secara keseluruhan, bukan hanya sektor tertentu. Dengan pendekatan analisis risiko ini, organisasi dapat mengidentifikasi ancaman seperti kebocoran data, kesalahan sistem, serta mengevaluasi kerentanannya terhadap ancaman tersebut.

1.2. Tujuan Kerja Praktik

Adapun tujuan umum dari pelaksanaan kerja praktik ini adalah sebagai berikut:

1). Memenuhi ketentuan syarat kelulusan mata kuliah Kerja Praktik program studi Sistem Informasi Politeknik Caltex Riau.

2). Mengembangkan kemampuan inovatif dan analisis dalam pemecahan masalah sekaligus membangun kerja sama.

3). Mengaplikasikan keterampilan dan pengetahuan yang diperoleh selama perkuliahan melalui pengalaman kerja praktik secara langsung di dunia kerja.

1.3. Manfaat Kerja Praktik

Manfaat yang di peroleh dari diadakannya kerja praktik ini adalah sebagai berikut :

1.3.1 Bagi Mahasiswa

Adapun manfaat kerja praktik bagi mahasiswa adalah sebagai berikut :

1) Mendapatkan pengalaman dalam bekerja, bersosialisasi, serta berinteraksi langsung dengan orang-orang yang berada di instansi.
2) Memperoleh kemampuan untuk bekerja sama dalam tim serta dapat bersosialisasi dengan baik sesama rekan kerja.

1.3.2 Bagi Perguruan Tinggi

Adapun manfaat kerja praktik bagi perguruan tinggi, yaitu sebagai sarana untuk menjalin kerja sama dan riset yang saling menguntungkan dengan instansi.

1.3.3 Bagi Instansi

Adapun manfaat kerja praktik bagi instansi adalah membantu instansi dalam menganalisis dan memitigasi risiko pada setiap sektor IT sehingga dapat meningkatkan keamanan sistem.

1.4. Waktu dan Tempat Pelaksanaan Kerja Praktik

Adapun proses kerja praktik ini dilakukan pada:

Waktu Pelaksanaan : 9 September 2024 – 9 Januari 2025

Waktu Kerja : Senin s.d Jumat, pukul 08.00 sd. 17.00

Tempat : PT. Bank Riau Kepri Syariah (Perseroda)

Alamat : Jl. Jend. Sudirman No. 462, Pekanbaru, Riau 28116

Bagian : Divisi Teknologi & Sistem Informasi, Bagian *Planning*

1.5. Metode Pengumpulan Data

Pengumpulan data dilakukan untuk mendukung analisis dan penilaian risiko keamanan sistem manajemen risiko. Data diperoleh dari dokumen organisasi, seperti kebijakan keamanan informasi dan laporan insiden keamanan.

1.6. Sistematika Penulisan

Sistematika penulisan laporan kerja praktik ini secara keseluruhan terdiri dari lima bab, masing-masing terdiri dari beberapa sub-bab. Adapun pokok pembahasan dari masing-masing bab tersebut secara garis besar sebagai berikut:

BAB I PENDAHULUAN

Bab ini menguraikan tentang latar belakang, tujuan kerja praktik, manfaat kerja praktik, waktu dan tempat pelaksanaan kerja praktik, metode pengumpulan data serta sistematika penulisan laporan kerja praktik.

BAB II PROFIL PERUSAHAAN

Bab ini menguraikan tentang sejarah singkat perusahaan, visi dan misi, logo dan filosofi perusahaan, struktur organisasi, serta lokasi perusahaan.

BAB III LANDASAN TEORI

Bab ini menguraikan tentang konsep dasar keamanan informasi, risiko keamanan, dan menjelaskan tentang framework NIST SP 800-30.

BAB IV HASIL DAN PEMBAHASAN

Bab ini menguraikan tentang landasan teori yang mendukung penyusunan dan pembahasan laporan kerja praktik ini, terutama menjelaskan tentang kegiatan kerja praktik, penilaian risiko dan

evaluasi kerja praktik.

BAB V PENUTUP

Bab ini berisikan kesimpulan dari penelitian yang dilakukan dan saran untuk pengembangan bagi instansi.