BAB I

PENDAHULUAN

1.1. Latar Belakang

Kemajuan teknologi yang semakin pesat telah mendorong organisasi untuk memanfaatkan Teknologi Informasi (TI) guna meningkatkan kualitas, akurasi, dan efesiensi operasional. TI tidak hanya menjadi pendorong utama dalam transformasi digital tetapi juga menjadi elemen penting untuk meningkatkan kepuasan pelanggan serta daya saing organisasi. Dalam implementasinya, manajemen risiko menjadi aspek krusial yang tidak dapat diabaikan untuk melindungi aset informasi organisasi. Manajemen risiko yang efektif membantu organisasi mengindentifikasi, menganalisis, dan mengelola risiko yang mungkin terjadi (Whitman & Mattord, 2021).

Manajemen risiko dibidang keamanan siber memiliki peran yang sangat penting, terutama dalam menjaga kerahasiaan, integritas, dan ketersediaan informasi. Keamanan siber bertujuan untuk melindungi sistem informasi dari ancaman serangan siber, kebocoran data, *malware*, dan ancaman lainnnya yang dapat merusak insfrastruktur digital perusahaan (Pfleeger, pfleeger, & Margulies, 2015). Risiko siber semakin meningkat seiring dengan digitalisasi layanan, termasuk dalam layanan perbankan seperti mobile banking. Risiko siber ini tidak hanya berdampak pada

kerugian finansial tetapi juga dapat merusak reputasi organisasi dan kepercayaan pelanggan (Aliyu & Tasmin, 2018).

Mobile banking sebagai salah satu inovasi dalam layanan perbankan digital, memberikan kemudahan bagi pelanggan untuk melakukan transaksi kapan saja dan dimana saja. Namun, peningkatan adopsi layanan ini juga membawa risiko signifikan terkait keamanan siber, seperti pencurian data, eksploitasi kerentanan, dan akses tidak sah ke informasi pelanggan. Kerentanan tersebut menjadi ancaman serius mengingat sifat sensitif dari data yang disimpan dan diolah dalam sistem mobile banking (Alaya, 2016). Manajemen risiko siber diperlukan untuk mengidentifikasi potensi ancaman, mengevaluasi dampaknya, dan merancang langkah mitigasi yang efektif.

Framework NIST SP 800-30 telah 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 (NIST, 2012). Framework ini memiliki keunggulan karena menawarkan detail pelaksanaan yang konprehensif dan memberikan panduan rekomendasi kontrol yang lebih luas dibandingkan framework lainnya.

Penerapan framework NIST SP 800-30 dalam penilaian risiko keamanan siber pada sistem mobile banking saat relevan, mengingat pentingnya pengelolaan risiko dalam mencapai sasaran organisasi. Dengan analisis ini, diharapkan dapat diidentifikasi sumber ancaman, kerentanan, serta risiko yang berpotensi mengganggu operasional layanan mobile banking (Kharraz & Kirda, 2017). Selain itu, penelitian ini bertujuan untuk memberikan rekomendasi kontrol guna meningkatkan keamanan informasi dan meminimalkan risiko siber dalam layanan mobile banking di Indonesia.

Hal tersebut mendorong penulis untuk melakukan analisis yang lebih mendalam mengenai penilaian risiko keamanan siber pada sistem mobile banking. Penilaian ini menjadi penting untuk memastikan keamanan, keandala, serta perlindungan data pelanggan yang sensitif.

1.2. Tujuan

Tujuan penulis dalam membuat laporan yang berjudul "Penilaian Risiko Keamanan Siber pada Mobile Banking menggunakan Framework NIST SP 800-30 adalah sebagai berikut:

1. Mengidentifikasi Risiko Keamanan siber
   Menjelaskan ancaman, kerentanan, dan risiko yang dapat memengaruhi keamanan mobile banking.

2. Mengevaluasi Dampak Risiko

   Menganalisis dampak dari setiap risiko terhadap keandalan, keamanan, dan keberlanjutan sistem mobile banking.

3. Menganalisis Risiko dengan Framework NIST SP 800-30

   Mengkaji ancaman dan kerentanan dalam mobile banking serta menilai risikonya menggunakan pendekatan dari framework NIST SP 800-30.

4. Memberikan Rekomendasi Mitigasi Risiko

   Menyediakan langkah-langkah untuk mengurangi risiko siber, meningkatkan keamanan, dan menjaga kepercayaan pelanggan terhadap mobile banking.

1.3. Manfaat Kerja Praktik

Manfaat yang diharapkan dari laporan berjudul " Penilaian Risiko Keamanan Siber pada Mobile Banking dengan menggunakan Framework NIST SP 800-30 adalah sebagai berikut:

1. Bagi Industri Perbankan

   Laporan ini bertujuan untuk memberikan pemahaman yang komprehensif mengenai risiko keamanan siber yang mengancam sistem mobile banking. Melalui analisis risiko ini, diharapkan industri perbankan dapat mengidentifikasi potensi ancaman, mengembangkan langkah mitigasi yang efektif, dan memperkuat strategi keamanan siber guna

melindungi data nasabah serta menjaga kepercayaan pengguna layanan mobile banking

2. Bagi Pengguna Mobile Banking

   Laporan ini meningkatan kepercayaan pelanggan dengan memastikan bahwa layanan mobile banking yang digunakan memiliki keamanan yang andal dan memadai.

3. Bagi Masyarakat Umum

   Membantu meningkatkan kesadaran masyarakat akan pentingnya keamanan siber dalam penggunakan layanan perbankan digital, sehingga mereka dapat lebih bijak dalam menjaga keamanan data pribadi mereka.

1.4. Waktu dan Tempat Pelaksanaan Kerja Praktik

Adapun proses kerja praktik ini dilakukan pada:

Waktu Pelaksanaa	: 10 September 2024 – 10 Januari 2025
Waktu Kerja	: Senin s.d Jumat, pukul 08.00 sd. 17.00
Tempat	: PT. Bank Sumut
Alamat	: Jl. Imam Bonjol No.18, Madras Hulu, Sumatera Utara.
Bagian	: Divisi Manajemen Risiko

1.5. Metode Pengumpulan Data

Pengumpulan data dilakukan untuk mendukung analisis dan penelitian risiko keamanan siber pada sistem mobile banking. Data yang digunakan meliputi :

a) Data Primer

   Data primer diperoleh langsung melalui wawancara dengan pihak terkait, observasi operasional sistem, serta penggunaan *assessment tools* berbasis framework *NIST SP* 800-30.

b) Data Sekunder

   Data sekunder diperoleh dari dokumen organisasi, seperti kebijakan keamanan informasi, laporan insiden keamanan, dan dokumentasi teknis sistem mobile banking

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, Struktur Organisasi, Lokasi perusahaan serta produk-produk yang ada di perusahaan.

BAB III LANDASAN TEORI

Bab ini menguraikan tentang mobile banking, risiko keamanan pada mobile banking dan menjelaskan tetang 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.