BAB I
PENDAHULUAN

1.1. Latar Belakang

Dalam era digitalisasi dan interkoneksi global saat ini, perkembangan bisnis sangat terkait dengan peran pentingnya teknologi informasi. Dengan terus majunya teknologi informasi, kekuatan ini dianggap sebagai sarana utama dalam meraih keunggulan dan mengatasi persaingan di dunia bisnis[1]. Teknologi informasi mencakup semua aspek yang terkait dengan proses operasional, pemanfaatan sebagai alat bantu, manipulasi, dan pengelolaan informasi[2]. Teknologi informasi di sebuah perusahaan biasanya berperan sebagai pusat biaya (cost center), yang berarti bahwa penggunaannya bertujuan untuk menggantikan proses manual dengan otomatisasi guna meningkatkan efisiensi dan efektivitas[3]. Perkembangan teknologi yang terus berinovasi mendorong setiap perusahaan untuk bersaing dan tumbuh dengan pesat. Agar dapat bersaing dan tumbuh, sebuah perusahaan baik di sektor manufaktur maupun jasa perlu menjaga kualitas produk dan layanannya[1]. Kunci keberhasilan suatu perusahaan adalah dengan mempertahankan kualitas layanan tinggi, terus berinovasi dalam produk, dan selalu memprioritaskan kepuasan dan kepercayaan para pesertanya. Namun, kepuasan dan kepercayaan para peserta dapat terancam apabila tidak dilakukan upaya perlindungan dan pemeliharaan yang baik. Sebagai contoh, ketidakperhatian sebuah perusahaan terhadap potensi risiko di masa depan dapat mengakibatkan kerusakan dan kerugian pada perusahaan itu sendiri dan lebih parah mengakibatkan kerusakan pada tingkat kepuasan dan kepercayaan para pesertanya. Oleh karena itu, perlu dilakukan pertimbangan serius terhadap aspek-aspek yang dapat berdampak negatif terhadap hubungan ini guna memastikan kelangsungan dan keberlanjutan kepuasan dan kepercayaan peserta.

Studi kasus peneliti adalah PT. XYZ, BUMN yang bergerak di bidang asuransi sosial. PT. XYZ bertujuan menjadi penyedia solusi terdepan di sektor asuransi sosial, dengan visi keunggulan, kepercayaan, dan keberlanjutan. Transformasi digital yang diadopsi PT. XYZ meningkatkan efisiensi operasional

dan keamanan sistem, meskipun terdapat risiko dalam pengelolaan data. Dalam konteks ini, penting untuk menghindari kerentanan (vulnerabilities) dan ancaman (threats)[4]. Oleh karena itu, implementasi sistem keamanan yang terstandarisasi dan kebijakan manajemen risiko yang cermat menjadi langkah penting guna memastikan integritas, kerahasiaan, dan ketersediaan data. PT. XYZ tentunya memiliki beragam sistem yang berperan dalam mendukung operasional perusahaan. Pada penelitian ini akan difokuskan pada salah satu sistem layanan khusus, yaitu website layanan online terintegrasi untuk peserta PT. XYZ. Website ini menyajikan berbagai layanan yang esensial atau dibutuhkan. Dilihat dari ragam layanan yang ditawarkan oleh sistem ini, terlihat jelas bahwa sistem tersebut menyimpan sejumlah besar data dan informasi yang krusial bagi perusahaan dan pesertanya[5][6]. Manajemen risiko diharapkan dapat menjadi landasan kokoh dalam melindungi integritas data dan informasi penting perusahaan, sehingga meminimalkan potensi dampak negatif. Pengelolaan risiko juga dianggap sebagai tantangan strategis bagi perusahaan, di mana mereka akan menghadapi berbagai ancaman yang kompleks[1]. Maka dari itu, penelitian ini akan melakukan manajemen risiko dengan menerapkan ISO 31000:2018 dan menggunakan metode FMEA (Failure Mode and Effect Analysis) dari ISO 31010:2009. Pendekatan ini bertujuan untuk mendapatkan prioritas risiko yang tepat dan tervalidasi, sehingga dapat menjadi dasar pertimbangan dalam mengambil tindakan respons terhadap risiko yang dihadapi[7].

ISO (International Organization for Standardization) sebagai salah satu badan yang mengeluarkan standarisasi internasional, merilis suatu standar untuk Manajemen Risiko, yaitu ISO 31000:2018[1][4][7]. Tujuan dari penerapan manajemen risiko dengan menggunakan ISO 31000:2018 dalam penelitian ini adalah untuk mengevaluasi sejauh mana ancaman dan risiko yang terkait dengan sistem layanan online terintegrasi PT. XYZ. Penelitian ini akan mengikuti pedoman dan prinsip yang terdapat dalam ISO 31000:2018 untuk menyediakan pemahaman yang komprehensif tentang tingkat risiko yang dihadapi oleh sistem tersebut. Proses manajemen risiko melibatkan penerapan sistematis kebijakan, prosedur, dan praktik dalam kegiatan komunikasi dan konsultasi, penetapan konteks, serta penilaian, peninjauan, hingga pelaporan risiko[8]. Dalam konteks ini, langkah-langkah

tersebut secara holistik membentuk landasan yang kuat untuk mengidentifikasi, menilai, dan mengelola risiko dengan efektif dalam suatu organisasi[4]. Maka dengan adanya standar ISO ini, setidaknya memberikan konfirmasi bahwa standar yang terdefinisi dengan jelas diperlukan dalam pengelolaan risiko karena berkaitan dengan proses pengamanan atau manajemen keamanan informasi, dengan tujuan memberikan prinsip dan panduan umum untuk menerapkan manajemen risiko[4].

Penelitian ini juga merekomendasikan penggunaan metode FMEA dalam proses analisisnya. FMEA adalah sebuah metodologi untuk mengevaluasi potensi kegagalan dalam suatu sistem, desain, proses, atau layanan. Penilaian kegagalan potensial dilakukan dengan memberikan nilai atau skor untuk setiap mode kegagalan berdasarkan tingkat kejadian (occurrence), tingkat keparahan (severity), dan tingkat deteksi (detection)[7]. Secara umum, terdapat dua kategori FMEA, yaitu FMEA desain dan FMEA proses. FMEA desain memusatkan evaluasinya pada desain produk, sementara FMEA proses lebih berorientasi pada kegiatan produksi. Dalam konteks penelitian ini, metode yang diterapkan adalah FMEA proses karena penelitian difokuskan pada pengamatan kegiatan proses dalam suatu sistem yang sedang berlangsung[7]. Tujuan utama penerapan metode ini adalah untuk secara efektif mengurangi risiko kemungkinan terjadinya cacat dalam jalannya proses. FMEA ini menekankan pada pengutamaan mode kegagalan yang sudah diidentifikasi sebelumnya melalui nilai Risk Priority Number (RPN)[1]. RPN sendiri dihitung dengan mengalikan nilai Severity (S) yang menunjukkan tingkat keparahan kegagalan, Occurrence (O) yang mencerminkan kemungkinan terjadinya kegagalan, dan Detection (D) yang mengindikasikan kemungkinan terdeteksinya kegagalan. Nilai untuk Severity, Occurrence, dan Detection masing-masing dinilai pada skala 1 hingga 10[1]. Dengan demikian, penelitian ini mengajukan penerapan ISO 31000:2018 dan FMEA untuk menentukan risiko mana yang menjadi fokus utama.

Pemilihan NIST 800-53 sebagai rekomendasi dan kontrol dalam penelitian ini didasarkan pada framework ini yang menyediakan kontrol keamanan yang mencakup berbagai aspek, seperti manajemen akses, perlindungan informasi, dan keberlanjutan operasional. Framework ini mudah diadaptasi untuk berbagai jenis sistem atau organisasi, termasuk sistem layanan online terintegrasi di PT. XYZ.

Pendekatan berbasis risiko yang digunakan dalam NIST 800-53 memungkinkan organisasi atau sistem menyesuaikan kontrol keamanan sesuai dengan profil risiko mereka. Studi oleh *Rosenthal* dan *FitzGerald (2018)* menunjukkan bahwa pendekatan berbasis risiko dalam NIST 800-53 efektif dalam membantu organisasi dan sistem untuk mengidentifikasi dan mengurangi ancaman. Oleh karena itu, NIST 800-53 dipilih untuk memberikan rekomendasi kontrol yang dapat diterapkan pada pada sistem layanan online terintegrasi PT. XYZ.

1.2. Perumusan Masalah

Berdasarkan pemaparan latar belakang penelitian ini, terdapat sejumplah perumusan masalah yang dapat dijadikan fokus utama penelitian. Beberapa aspek permasalahan yang tercakup meliputi:

1. Bagaimana implementasi manajemen risiko pada sistem layanan online terintegrasi menggunakan panduan ISO 31000:2018 dan metode FMEA?
2. Apa saja prioritas risiko yang diidentifikasi dari hasil penerapan ISO 31000:2018 dan FMEA?
3. Apa saja rekomendasi dan kontrol NIST 800-53 yang disarankan dalam penanganan risiko berdasarkan prioritasnya?

Perumusan masalah ini akan menjadi landasan untuk melakukan analisis mendalam dalam penelitian ini dan mencapai tujuan penelitian yang telah ditetapkan.

1.3. Batasan Masalah

Dalam lingkup penelitian ini, batasan masalahnya adalah sebagai berikut:z

1. Penelitian ini dilakukan di PT. XYZ, sebuah Badan Usaha Milik Negara (BUMN) yang bergerak di bidang asuransi sosial, dengan fokus pada website layanan dalam satu tahun terakhir.
2. Penelitian ini akan menggunakan standar ISO 31000:2018 dan metode FMEA sebagai pedoman dalam analisis manajemen risiko.
3. Rekomendasi dan kontrol yang diusulkan dalam penelitian ini akan berdasarkan pada NIST 800-53.

1.4. Tujuan

Berdasarkan perumusan masalah di atas, tujuan penelitian ini adalah:

1. Memahami bagaimana manajemen risiko diterapkan pada sistem layanan online terintegrasi dengan menggunakan pedoman ISO 31000:2018 serta metode Failure Mode and Effects Analysis (FMEA).
2. Mengidentifikasi dan menetapkan prioritas risiko berdasarkan hasil penerapan ISO 31000:2018 dan metode FMEA.
3. Menyusun rekomendasi dan kontrol yang sesuai dengan standar NIST 800-53 untuk penanganan risiko berdasarkan prioritas yang telah ditetapkan.

Dengan mencapai tujuan-tujuan ini, penelitian diharapkan dapat meningkatkan pemahaman tentang manajemen risiko, metode FMEA dan prioritas risiko dalam konteks sistem layanan online terintegrasi PT. XYZ