BAB I PENDAHULUAN

I.1 Latar Belakang

Dalam era digital yang terus berkembang pesat saat ini, teknologi informasi (TI) telah menjadi elemen fundamental bagi keberlangsungan dan pertumbuhan operasional bisnis (Prihandono & Amir, 2024). TI tidak hanya menjadi alat pendukung, tetapi juga faktor strategis yang mempengaruhi berbagai keputusan penting dalam perusahaan. Seiring dengan meningkatnya penggunaan TI, organisasi modern menghadapi tantangan signifikan terkait dengan manajemen risiko, terutama yang berkaitan dengan keamanan dan integritas *data*. Di tengah kompleksitas ini, manajemen risiko TI menjadi semakin krusial karena sistem informasi kini menjadi jantung dari operasional perusahaan, dengan berbagai ancaman yang terus berkembang, seperti serangan siber, pencurian *data*, dan gangguan operasional. Sebagaimana yang dijelaskan oleh Paul Hopkin dalam bukunya *Fundamentals of Risk Management*, risiko adalah elemen yang tidak terpisahkan dari setiap kegiatan bisnis, dan pengelolaan yang baik terhadap risiko tersebut merupakan faktor kunci untuk menjaga efektivitas dan keberlanjutan organisasi (Paul, 2017) .

Keberhasilan sebuah organisasi tidak hanya bergantung pada inovasi teknologinya, tetapi juga pada bagaimana risiko-risiko yang terkait dengan teknologi tersebut dapat dikelola secara efektif. Dalam konteks manajemen risiko TI, ancaman yang paling umum mencakup kebocoran *data*, kegagalan sistem, hingga ketidakmampuan untuk menjaga keandalan sistem secara keseluruhan. Kondisi ini membuat perusahaan yang tidak siap untuk menghadapi risiko-risiko tersebut rentan terhadap gangguan operasional dan penurunan performa bisni (Hoshmand & Ratnawati, 2023). Di dunia bisnis modern, hal ini dapat mengganggu reputasi perusahaan, mengurangi kepercayaan pelanggan, dan pada akhirnya berdampak negatif pada pendapatan perusahaan. Oleh karena itu, penting bagi perusahaan untuk mengadopsi strategi manajemen risiko yang sistematis guna menghadapi tantangan di era digital ini .

Manajemen Risiko Teknologi Informasi (IT *Risk Management*) adalah suatu proses identifikasi kerentanan dan ancaman terhadap sumber daya informasi yang

digunakan oleh sebuah organisasi dan dilakukan oleh manajer TI untuk mencapai tujuan bisnis, mengurangi dampak risiko, serta menyeimbangkan proses bisnis agar dapat berjalan sesuai standar yang diterapkan perusahaan (Rini, 2018)

PT. XYZ merupakan sebuah perusahaan yang bergerak di bidang kontraktor, konsultan properti, perdagangan, serta layanan konstruksi lainnya di Indonesia. Perusahaan ini tidak luput dari tantangan dalam manajemen risiko TI. Sebagai perusahaan yang memanfaatkan TI untuk mendukung operasional harian dan menjaga kelangsungan layanan kepada pelanggan, PT. XYZ menyadari pentingnya pengelolaan risiko TI yang baik. Namun, berdasarkan evaluasi internal, teridentifikasi adanya gap yang signifikan antara sistem manajemen risiko TI yang ada dengan standar terbaik yang diakui secara internasional, seperti ISO 27005:2022. Gap ini menunjukkan bahwa perusahaan belum sepenuhnya mengadopsi langkah-langkah yang diperlukan untuk memastikan keamanan, keandalan, dan kontinuitas operasional TI mereka .

ISO 27005:2022 adalah standar internasional yang dirancang untuk memberikan panduan dalam manajemen risiko keamanan informasi. Standar ini memfokuskan pada metode yang sistematis untuk mengidentifikasi, menilai, dan mengelola risiko yang berkaitan dengan sistem informasi, termasuk perlindungan terhadap kerahasiaan, keutuhan, dan ketersediaan *data* (ISO 27005, 2022) . Dalam standar ini, risiko TI didefinisikan sebagai segala potensi ancaman yang dapat memengaruhi kinerja atau integritas sistem informasi perusahaan. Penerapan ISO 27005:2022 memungkinkan perusahaan untuk menerapkan pendekatan berbasis risiko yang efektif dalam menjaga keamanan informasi dan aset digital mereka. Namun, di PT. XYZ, implementasi standar ini masih berada dalam tahap awal, yang berarti banyak potensi risiko yang belum dikelola dengan baik, termasuk risiko terkait insiden siber, kegagalan sistem TI, dan pengamanan terhadap *data* sensitif perusahaan.

Selain itu, di Indonesia, implementasi standar internasional seperti ISO 27005:2022 semakin didorong oleh regulasi khusus yang berlaku untuk instansi pemerintahan dan organisasi yang bekerja sama dengan lembaga pemerintah. Salah satu regulasi penting adalah Peraturan Badan Siber dan Sandi Negara (BSSN) Nomor 8 Tahun

2020 tentang Pedoman Keamanan Informasi untuk Penyelenggara Sistem Elektronik (PSE). Regulasi ini mewajibkan instansi dan perusahaan yang terlibat dalam pengelolaan *data* sensitif pemerintah untuk menerapkan sistem manajemen keamanan informasi berbasis standar internasional seperti ISO 27001 dan standar pendukung seperti ISO 27005 (Giyanto, 2020).

Kurangnya implementasi terhadap ISO 27005:2022 di PT. XYZ telah menyebabkan beberapa permasalahan yang berdampak langsung pada operasional perusahaan. Sebagai contoh, keterlambatan dalam merespons insiden yang melibatkan teknologi informasi, lemahnya pengawasan terhadap *data* sensitif perusahaan, serta ketidakmampuan untuk memitigasi risiko teknologi yang muncul secara cepat dan efisien (ISO 27005, 2022). Masalah-masalah ini tidak hanya menimbulkan potensi kerugian finansial, tetapi juga dapat merusak reputasi perusahaan di mata klien dan mitra bisnis.

Secara praktis, konsekuensi dari lemahnya keamanan informasi di PT. XYZ dapat berdampak langsung pada operasional inti perusahaan. Sebagai contoh, Data Proyek & Gambar Teknis (D03) seperti Rencana Anggaran Biaya (RAB) dan denah AutoCAD merupakan aset intelektual yang sangat vital. Jika data ini bocor ke tangan kompetitor, PT. XYZ dapat kehilangan keunggulan dalam proses tender proyek. Di sisi lain, insiden keamanan seperti serangan *ransomware* yang menargetkan Server Internal (A01) dapat mengenkripsi seluruh data progres proyek, menyebabkan penundaan pekerjaan konstruksi di lapangan. Penundaan semacam ini tidak hanya berakibat pada kerugian finansial akibat pinalti kontrak, tetapi juga secara langsung merusak reputasi perusahaan di mata klien dan mitra strategis.

Akar permasalahan dari gap ini dapat ditelusuri ke beberapa faktor kunci. Pertama, kurangnya sumber daya manusia yang terlatih dan memiliki kompetensi khusus dalam manajemen risiko TI menjadi salah satu hambatan utama. Pengelolaan risiko TI membutuhkan keahlian khusus, yang mencakup pemahaman mendalam tentang ancaman siber, teknologi perlindungan *data*, serta mekanisme mitigasi risiko. Kedua, terbatasnya pemahaman manajemen perusahaan mengenai pentingnya penerapan standar internasional seperti ISO 27005:2022 mengakibatkan kurangnya

dukungan strategis dalam transformasi digital yang aman dan berkelanjutan. Ketiga, belum adanya proses yang terstruktur dan terpadu untuk menangani risiko TI secara proaktif, yang membuat perusahaan lebih bersifat reaktif dalam menghadapi masalah yang muncul (Prihandono & Amir, 2024).

Melalui identifikasi masalah ini, dapat disimpulkan bahwa perusahaan perlu mengambil langkah strategis untuk memperbaiki manajemen risiko TI mereka. Dengan mengimplementasikan transformasi digital berbasis ISO 27005:2022 secara menyeluruh, PT. XYZ tidak hanya akan meningkatkan pengelolaan risiko teknologi informasi, tetapi juga akan memastikan kesinambungan operasional perusahaan dalam jangka panjang. Penerapan standar ini diharapkan mampu memberikan kerangka kerja yang jelas dan terukur untuk mengelola risiko TI, mengurangi potensi kerugian akibat insiden siber, dan meningkatkan kepercayaan mitra bisnis serta pelanggan terhadap keamanan dan reliabilitas sistem TI perusahaan.

Dengan demikian, penelitian ini berfokus pada analisis kebutuhan transformasi digital berbasis ISO 27005:2022 di PT. XYZ. Tujuan utama dari penelitian ini adalah untuk memberikan rekomendasi yang tepat dalam meningkatkan pengelolaan risiko TI, sehingga perusahaan dapat menjalankan operasionalnya dengan lebih aman, efisien, dan berkelanjutan. Dengan adopsi penuh terhadap ISO 27005:2022, PT. XYZ diharapkan mampu meningkatkan daya saingnya di industri properti dan konstruksi, serta memperkuat posisi perusahaan sebagai entitas yang berkomitmen pada keamanan dan keandalan sistem informasi.

I.2 Perumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan, PT. XYZ sebagai perusahaan yang bergerak di bidang properti belum memiliki sistem manajemen risiko keamanan informasi yang terdokumentasi ataupun terstruktur. Hal ini menimbulkan kebutuhan mendesak untuk membangun perancangan awal manajemen risiko berdasarkan standar internasional ISO/IEC 27005:2022.

Oleh karena itu, permasalahan yang diangkat dalam penelitian ini adalah:

1. Bagaimana kondisi pengelolaan risiko keamanan sistem informasi pada Aset IT PT. XYZ berdasarkan pedoman ISO 27005:2022
2. Bagaimana perusahaan menentukan bentuk rekomendasi terhadap pengelolaan risiko keamanan sistem informasi pada Aset IT PT. XYZ berdasarkan ISO 27005:2022

I.3 Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk merancang dan mengelola risiko keamanan informasi di PT. XYZ, sebuah perusahaan yang belum memiliki sistem manajemen risiko sebelumnya, dengan mengacu pada standar ISO/IEC 27005:2022. Secara rinci, tujuan penelitian ini adalah:

1. Melakukan analisis pengelolaan risiko keamanan sistem informasi pada aset IT PT. XYZ berdasarkan pedoman ISO 27005:2022
2. Membentuk evaluasi risiko dan merancang rekomendasi terhadap pengelolaan risiko keamanan sistem informasi pada Aset IT PT XYZ berdasarkan ISO 27005:2022.

I.4 Batasan Penelitian

Keluaran dari penelitian ini terbatas pada artefak perancangan dan rekomendasi strategis, sehingga tidak mencakup tahap implementasi teknis dari kontrol yang diusulkan, analisis biaya-manfaat, maupun evaluasi efektivitas pasca-implementasi. Selain itu, analisis risiko hanya mencakup aset-aset teknologi informasi yang berada di bawah pengelolaan langsung Divisi IT PT. XYZ. Dengan demikian, temuan dan rekomendasi yang dihasilkan didasarkan pada data dan kondisi internal perusahaan yang diperoleh selama periode penelitian berlangsung dan tidak memperhitungkan perubahan organisasi atau teknologi di masa mendatang.

I.5 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat sebagai berikut:

1. **Manfaat Teoretis**

   Memberikan kontribusi pada pengembangan literatur tentang manajemen risiko keamanan informasi, khususnya dalam implementasi awal ISO/IEC 27005:2022 pada perusahaan yang belum memiliki sistem manajemen risiko.
2. **Manfaat Praktis untuk PT. XYZ**

   Memberikan gambaran kondisi manajemen risiko TI saat ini dan menyusun rekomendasi langkah awal untuk membangun sistem manajemen risiko keamanan informasi yang sesuai dengan standar internasional. Hasil penelitian ini diharapkan menjadi fondasi awal yang dapat dikembangkan menuju implementasi standar keamanan informasi lebih lanjut, seperti ISO/IEC 27001.
3. **Manfaat bagi Industri**

   Memberikan contoh implementasi praktis penerapan manajemen risiko keamanan informasi di sektor properti, yang dapat menjadi referensi bagi perusahaan lain dalam industri serupa.
4. **Manfaat bagi Pihak Regulator atau Pemerintah**

   Memberikan tambahan referensi untuk pemerintah atau lembaga regulator dalam memahami penerapan manajemen risiko keamanan informasi pada perusahaan swasta di Indonesia.

I.6 Sistematika Laporan

Sistematika penulisan laporan tugas akhir berguna sebagai panduan bagi mahasiswa dalam penyusunan laporan sebagai bentuk pertanggungjawaban atas kegiatan penelitian yang telah dilaksanakan. Sistematika ini memberikan struktur yang jelas untuk memastikan laporan disusun dengan baik dan mencakup semua aspek penting dari tugas akhir. Berikut adalah sistematika penulisan laporin tugas akhir adalah sebagai berikut;

BAB I PENDAHULUAN

Bab ini menyajikan dasar-dasar awal dari penelitian, mencakup latar belakang, perumusan masalah, tujuan, manfaat, dan batasan studi. Penyajiannya bertujuan untuk memberikan konteks menyeluruh atas alasan pelaksanaan penelitian, arah dan fokus kajian, serta lingkup pembahasan yang dibatasi secara jelas. Dengan demikian, pembaca diharapkan memperoleh pemahaman awal yang komprehensif sebelum memasuki pembahasan teknis pada bab-bab selanjutnya.

BAB II LANDASAN TEORI

Bab ini membahas berbagai teori dan literatur yang berkaitan langsung dengan topik penelitian. Termasuk di dalamnya adalah penguraian konsep-konsep dasar, definisi penting, dan penjelasan mengenai kerangka kerja (*framework*) yang menjadi fondasi pendekatan penelitian. Penelitian-penelitian terdahulu yang relevan juga ditinjau sebagai bahan perbandingan dan pendukung pembentukan kerangka teoritis yang kokoh, sehingga seluruh pendekatan yang digunakan memiliki dasar ilmiah yang valid.

BAB III METODE PENYELESAIAN MASALAH

Bab ini memaparkan metode yang digunakan untuk menyelesaikan permasalahan penelitian berdasarkan rumusan masalah yang telah ditetapkan. Penjelasan disampaikan secara sistematis mengenai langkah-langkah yang diambil, termasuk justifikasi atas pemilihan *framework* sebagai solusi yang tepat. Bab ini juga menyajikan kerangka berpikir yang mendasari metode yang dipilih, sekaligus memperlihatkan alasan mengapa pendekatan tersebut sesuai dengan konteks permasalahan yang dihadapi.

BAB IV PENYELESAIAN MASALAH

Bab ini menjelaskan pelaksanaan metode yang telah dirancang, mencakup proses pengumpulan dan pengolahan *data*. *Data* diperoleh dari berbagai sumber terpercaya, disusun secara sistematis, lalu dianalisis untuk menghasilkan informasi

yang relevan guna mendukung penyusunan solusi atas permasalahan yang diidentifikasi sebelumnya. Tahapan-tahapan ditampilkan secara terstruktur, agar pembaca dapat mengikuti alur penyelesaian masalah dengan jelas dan logis.

BAB V VALIDASI, ANALISIS HASIL, DAN IMPLIKASI

Bab ini menyajikan hasil dari pengolahan *data* yang telah dilakukan serta menganalisis keterkaitannya dengan rumusan masalah. Temuan-temuan utama ditampilkan, termasuk identifikasi gap antara kondisi aktual dan kondisi yang diharapkan. Berdasarkan analisis tersebut, diberikan rekomendasi untuk perbaikan. Bab ini juga memuat proses validasi untuk memastikan bahwa hasil yang diperoleh akurat dan relevan dengan tujuan penelitian.

BAB VI KESIMPULAN DAN SARAN

Bab terakhir ini merangkum temuan utama dari penelitian, menjawab pertanyaan penelitian, serta menyusun kesimpulan berdasarkan hasil analisis yang telah dilakukan. Selain itu, disampaikan saran-saran yang bersifat membangun, baik untuk penerapan hasil dalam konteks nyata, perbaikan proses yang sedang berjalan, maupun sebagai arah pengembangan untuk penelitian lanjutan di masa men*data*ng.