BAB 1 PENDAHULUAN

1.1. Latar Belakang

Proses perkembangan teknologi informasi yang cepat dan pesat tentu membawa manfaat yang signifikan dalam berbagai sektor industri, termasuk sektor industri keuangan[9]. Penerapan teknologi informasi dalam operasional bisnis selain meningkatkan efisiensi dan aksesibilitas layanan, tetapi juga mengubah cara suatu organisasi mengelola informasi dan data yang sensitif[9]. Semakin banyak perusahaan yang mengandalkan teknologi informasi dan komunikasi (TIK) di berbagai aspek operasional, telah menyebabkan meningkatnya ancaman dan risiko keamanan informasi [3]. Hal ini menjadikan manajemen keamanan informasi sebagai elemen yang sangat penting bagi setiap organisasi di semua sektor industri[3].

Sistem Manajemen Keamanan Informasi (SMKI) adalah sebuah kerangka kerja yang bertujuan untuk melindungi aset informasi dan menyediakan pendekatan sistematis dalam mengelola risiko, SMKI membantu organisasi untuk mecapai tujuan keamanan informasi mereka sendiri dan mematuhi persyaratan hukum terkait informasi[4]. SMKI mencakup kebijakan, prosedur, dan langkah-langkah yang dirancang untuk menjaga kerahasiaan, integritas, dan ketersediaan data[4]. Sistem manajemen keamanan informasi (SMKI) memiliki tujuan untuk memberikan perlindungan aset informasi dan menyediakan pendekatan sistematis untuk mengelola risiko[4]. Oleh karena itu, SMKI dapat membantu perusahaan untuk mencapai tujuan keamanan informasi dan mematuhi persyaratan hukum terkait keamanan informasi [4]. Dengan adanya SMKI, organisasi dapat mengidentifikasi dan menilai risiko keamanan informasi, menerapkan kontrol yang tepat, serta melakukan pemantauan dan evaluasi secara berkala untuk memastikan keamanan data[4]. Keberadaan SMKI menjadi esensial dalam menghadapi ancaman

siber yang semakin kompleks, terutama di industri yang bergantung pada data sensitif[4].

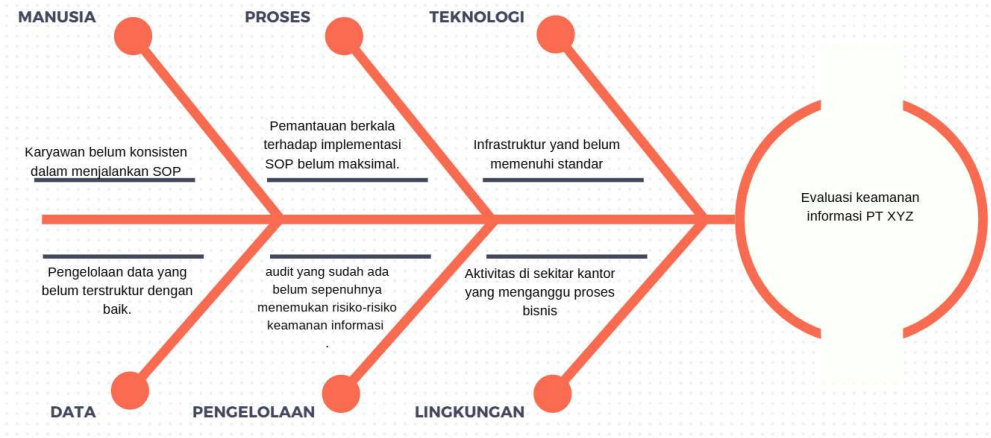
Dalam upaya untuk melindungi informasi, PT XYZ telah melakukan langkah-langkah awal dalam mengimplementasikan Sistem Manajemen Keamanan Informasi (SMKI) secara menyeluruh. Meskipun perusahaan belum mengadopsi standar ISO 27001, perusahaan saat ini mengacu pada standar internal yang ditetapkan oleh perusahaan induk sebagai dasar pengelolaan keamanan informasi. Mereka telah merumuskan kebijakan dan prosedur keamanan informasi yang jelas sebagai pedoman bagi seluruh karyawan dalam mengelola dan melindungi data. Perusahaan juga telah menyusun standar prosedur operasional yang mendetail untuk memastikan bahwa setiap aspek pengelolaan informasi mengikuti praktik keamanan yang ditetapkan. Namun, masih ditemukan kasus karyawan belum konsisten dalam menjalankan standar prosedur operasional yang sudah ditetapkan, serta infrastruktur teknologi yang belum memenuhi standar karena belum adanya perencanaan Disaster Recovery Plan (DRP) yang memadai. Hal ini menyebabkan organisasi belum memiliki prosedur yang jelas untuk memulihkan sistem dan data apabila terjadi gangguan atau kerusakan pada server utama. Oleh karena itu, evaluasi berkala diperlukan untuk memastikan tingkat kepatuhan serta peningkatan efektivitas penerapan prosedur yang telah ditetapkan.

Pemilihan ISO 27001:2022 sebagai dasar evaluasi dalam penelitian ini didasarkan pada fungsinya sebagai standar internasional yang dirancang khusus untuk membangun, menerapkan, dan mengevaluasi Sistem Manajemen Keamanan Informasi (SMKI) secara sistematis[4], Penggunaan standar ISO 27001 diperkuat dengan Peraturan OJK yang mengatur bahwa pengamanan informasi dilakukan terhadap aspek teknologi, sumber daya manusia, dan proses.Implementasi ISO 27001:2022 di PT XYZ dapat memberikan manfaat signifikan dalam pengelolaan keamanan informasi dengan menyediakan kerangka kerja yang sistematis untuk melindungi data

sensitif dan mengurangi risiko ancaman siber yang semakin kompleks[3][4]. implementasi ISO 27001 membantu perusahaan meningkatkan perlindungan terhadap ancaman serta mematuhi persyaratan hukum, yang penting di industri berbasis data [3][4]. Selain keuntungan internal seperti efisiensi proses, penerapan standar ini juga membawa manfaat eksternal berupa peningkatan citra dan kepercayaan dari pemangku kepentingan [3]. Walaupun tingkat adopsi di sektor non-ICT cenderung lebih rendah, keuntungan pencegahan yang ditawarkan menjadikan ISO 27001 sebagai inovasi preventif yang penting untuk menghindari kerugian di masa depan dan membuktikan komitmen perusahaan dalam melindungi data, yang pada akhirnya memperkuat kepercayaan pelanggan dan mitra bisnis [3][4].

1.2. Rumusan Masalah

Berbagai masalah yang dihadapi oleh PT XYZ dalam pengelolaan keamanan informasi telah diidentifikasi dan dirangkum dalam Diagram Ishikawa berikut. Diagram ini menggambarkan faktor-faktor utama yang memengaruhi risiko keamanan informasi, yang kemudian dijelaskan secara rinci untuk memberikan pemahaman yang lebih mendalam.



Gambar 1.1 Ishikawa Diagram

Berikut adalah penjelasan rinci untuk setiap poin dalam Diagram Ishikawa yang menguraikan risiko keamanan informasi :

1. Manusia

Karyawan belum konsisten dalam menjalankan SOP yang telah ditetapkan, sehingga memengaruhi efektivitas penerapan prosedur keamanan informasi di organisasi.

2. Proses

   Pemantauan berkala terhadap implementasi SOP belum maksimal, yang menunjukkan kurangnya pengawasan terhadap pelaksanaan prosedur yang telah dibuat dan ditetapkan.

3. Teknologi

   Infrastruktur teknologi belum memenuhi standar karena belum adanya perencanaan Disaster Recovery Plan (DRP) yang memadai, sehingga organisasi belum memiliki prosedur yang jelas untuk memulihkan sistem dan data apabila terjadi gangguan atau kerusakan pada server utama..

4. Data

   Pengelolaan data yang belum terstruktur dengan baik menjadi salah satu masalah, di mana data-data lama yang sudah tidak digunakan masih disimpan, meskipun seharusnya sudah dihapus. Hal ini meningkatkan risiko penyimpanan data yang tidak diperlukan dan menyulitkan pengelolaan serta perlindungan data yang penting.

5. Pengelolaan

   Audit yang telah dilakukan belum sepenuhnya mampu menemukan semua risiko terkait keamanan informasi yang ada. Ini menunjukkan bahwa audit saat ini masih memiliki kekurangan dalam mengenali ancaman potensial atau titik lemah keamanan yang mungkin muncul. Proses audit yang menyeluruh sangat krusial untuk mengidentifikasi risiko-risiko yang tidak terlihat agar dapat segera ditangani oleh perusahaan.

6. Lingkungan

Aktivitas di sekitar kantor yang mengganggu proses bisnis, seperti demonstrasi di sekitar gedung, pernah terjadi dan menyebabkan seluruh karyawan harus bekerja dari rumah (WFH). Situasi ini menunjukkan bahwa faktor eksternal, seperti gangguan di lingkungan sekitar kantor, dapat memengaruhi kelancaran operasional dan produktivitas perusahaan.

Berdasarkan hal tersebut, permasalahan yang akan dibahas dalam penelitian ini adalah sebagai berikut:

1. Bagaimana kesenjangan keamanan informasi berdasarkan standar ISO 27001:2022 pada PT XYZ?
2. Bagaimana probabilitas dan dampak risiko berdasarkan standar ISO 27001:2022 pada kontrol di PT XYZ?
3. Apa rekomendasi yang bisa diberikan dengan standar ISO 27002:2022 pada PT XYZ?

1.3. Tujuan dan Manfaat

Berdasarkan perumusan masalah yang ada, tujuan penelitian ini adalah

1. Mengidentifikasi dan melakukan analisis kesenjangan keamanan informasi di PT XYZ berdasarkan standar ISO 27001:2022.
2. Mengidentifikasi probabilitas dan dampak risiko pada kontrol keamanan informasi di PT XYZ sesuai dengan standar ISO 27001:2022.
3. Memberikan rekomendasi perbaikan yang sesuai dengan standar ISO 27002:2022 untuk meningkatkan keamanan informasi di PT XYZ.

Manfaat yang didapatkan adalah membantu perusahaan mengenali celah keamanan informasi yang belum teridentifikasi sebelumnya, memberi gambaran sejauh mana perusahaan sudah memenuhi standar ISO 27001:2022 serta rekomendasi area yang perlu ditingkatkan, dan peneliti menambah referensi mengenai implementasi ISO 27001:2022 dalam industri keuangan.

1.4. Batasan Masalah

Berikut adalah batasan masalah atau ruang lingkup yang ada pada penelitian ini :

1. Penelitian hanya berfokus pada tim IT, GRC(Governance Risk Compliance), HR(Human Resource) PT XYZ.
2. Aspek yang diperiksa berfokus pada identifikasi risiko keamanan informasi yang dihadapi oleh tim IT dengan menggunakan standar iso 27001:2022
3. Pertanyaan pada audit *checklist* hanya berdasarkan Annex A ISO 27001:2022.
4. Penelitian ini akan menggunakan pendekatan kualitatif dengan metode wawancara, observasi, dan studi dokumen untuk mengumpulkan data.

1.5. Metode Penelitian

Metode penelitian yang digunakan dalam tugas akhir ini menggabungkan beberapa pendekatan, yaitu studi literatur, observasi, wawancara, studi dokumen, analisis gap, serta evaluasi dan perancangan rekomendasi.

1.6. Sistematika Penulisan

Dalam menyusun karya tulis imiah ini, agar dalam pembahasan terfokus pada pokok permasalahan dan tidak melebar kemasalah yang lain,maka penulis membuat sistematika penulisan karya tulis ilmiah sebagai berikut :

- BAB 1 PENDAHULUAN

Bab ini menjelaskan latar belakang masalah, rumusan masalah, tujuan dan manfaat penelitian, batasan masalah, serta metode penelitian yang digunakan.

- BAB 2 TINJAUAN PUSTAKA

Bab ini memuat teori-teori pendukung yang relevan dengan penelitian, termasuk konsep dasar manajemen keamanan informasi, ISO 27001:2022, risiko keamanan informasi, dan penelitian terdahulu yang relevan.

- BAB 3 METODOLOGI

Bab ini menjelaskan pendekatan penelitian, metode pengumpulan data, alat analisis yang digunakan, serta langkah-langkah dalam mengevaluasi dan menganalisis risiko keamanan informasi sesuai standar ISO 27001:2022.

- BAB 4 HASIL DAN PEMBAHASAN

Bab ini menyajikan hasil penelitian yang diperoleh di PT XYZ, termasuk analisis kesenjangan, evaluasi tingkat risiko, serta interpretasi dari data yang telah dikumpulkan berdasarkan kerangka ISO 27001:2022.

- BAB 5 KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan dari hasil penelitian yang dilakukan, serta saran-saran yang dapat dijadikan acuan untuk peningkatan pengelolaan keamanan informasi di PT XYZ.