BAB 1

PENDAHULUAN

1.1 Latar Belakang

Keberadaan teknologi informasi sebagai sumber daya ini penting dalam upaya pengambilan sebuah keputusan di organisasi (Galbraith, 2012)[8]. Berkembangnya teknologi membuat aspek keamanan informasi dan proses bisnis layanan operasionalnya menjadi hal yang harus dijadikan prioritas oleh manajemen teknologi informasi dan perlu diberlakukan tolak ukur upaya menjaga keamanan informasi yang telah diterapkan organisasi. Masalah keamanan sistem informasi seringkali kurang diperhatikan oleh para pemangku kepentingan dan pengelola sistem informasi khususnya pada bagian *cyber*, yang diharapkan agar lebih mempertimbangkan masalah keamanan informasi untuk meminimalisir kerugian dan masuknya ancaman risiko kedalam sistem komputer pada sebuah perusahaan.

Aspek yang berdampak pada teknologi informasi merupakan keamanan informasi (Bernard, 2011)[3]. Sistem manajemen keamanan dapat mengendalikan keamanan informasi dalam layanan, berperan dalam mengatur dan menjalankan keamanan sistem informasi sesuai prosedur yang ditetapkan. Tujuannya dalam memastikan kerahasiaan, integritas, dan ketersediaan data dan informasi (Sheikhpour & Modiri, 2012)[17].

Dengan memperhatikan keamanan informasi, kebijakan pengamanan informasi harus melibatkan langkah seperti pengelolaan aset, pengolahan sumber daya, pengamanan fisik pada lingkungan, pengamanan *logical security*, dan terhadap keamanan operasional teknologi informasi (Direktorat Penelitian dan 2 Pengaturan Perbankan, 2007: 52)[4].

PT.XYZ merupakan perusahaan yang saat ini mengandalkan akses dan penggunaan teknologi informasi dalam operasionalnya. PT.XYZ merupakan unit bisnis yang menerapkan teknologi informasi dalam mendukung layanan. Untuk meningkatkan efektivitasnya dan memastikan perlindungan keamanan informasi yang baik. Langkah ini diharapkan dapat meningkatkan kepercayaan pelanggan, memenuhi persyaratan regulasi dan hukum yang berlaku. Berdasarkan hasil observasi dan wawancara bahwa pengelolaan TI pada PT.XYZ ditemukan kendala yang dihadapi dalam pengolahan Sistem Informasi yang dimiliki perusahaan yaitu serangan untuk mencoba masuk ke dalam *database* perusahaan dalam

penggunaan Aset TI. Dengan demikian, isu keamanan menjadi permasalahan yang penting bagi organisasi tersebut.

Keamanan sistem informasi diperlukan di PT.XYZ untuk menjamin suatu keamanan informasi sesuai dengan prosedur yang ditetapkan . Kriteria pada standar yang diperlukan untuk sistem informasi yaitu penggunaan ISO/IEC 27001:2013. Pemilihan ISO 27001:2013 tidak hanya untuk menetapkan persyaratan sistem keamanan tetapi juga memberikan pendekatan dalam mengidentifikasi, mengurangi, dan mengelola risiko keamanan informasi. ISO 27001:2013 juga menempatkan penekanan pengelolaan aset informasi secara efektif dan menyeluruh, serta pengembangan kebijakan dan prosedur yang sesuai dengan kebutuhan organisasi (Nasher, F, 2018)[13].

Meskipun ISO/IEC 27002:2022 merupakan standar yang baru diterbitkan, pemilihan ISO/IEC 27001:2013 dapat dipertahankan atas dasar bahwa standar ini telah terbukti dan telah banyak diterapkan di berbagai organisasi. Oleh karena itu, menggunakan ISO 27001:2013 saat ini masih merupakan pilihan yang rasional dan efektif bagi PT.XYZ.

1.2 Perumusan Masalah

Rumusan masalah yang dipaparkan penulis sebagai berikut :

1. Bagaimana hasil analisis penerapan standar dalam manajemen keamanan informasi ISO 27001:2013 pada PT.XYZ?
2. Bagaimana kesenjangan hasil analisis dari perusahaan berdasarkan ISO 27001:2013?
3. Apa saja rekomendasi yang dibutuhkan berdasarkan Kontrol *Annex* standar ISO 27002:2013 pada PT.XYZ?

1.3 Batasan Masalah

Batasan yang diterapkan pada penelitian sebagai berikut :

1. Data yang digunakan pada penelitian ini berasal dari hasil observasi, wawancara, dan kuesioner.
2. Kriteria standar yang digunakan adalah ISO dengan versi yang dikeluarkan pada tahun 2013.
3. Fokus dari penelitian ini adalah menganalisis portal web internal pada PT.XYZ.
4. Pada penelitian ini hanya mencakup tahap analisis dan rekomendasi saja, tidak sampai tahap implementasi sertifikat.

1.4 Tujuan

Tujuan penerapan penelitian :

1. Menganalisis manajemen keamanan di PT.XYZ menggunakan standar ISO 27001:2013 dengan Kontrol *Annex* berlandaskan ISO 27001:2013.
2. Menganalisis tingkat kesenjangan keamanan sistem dari PT.XYZ berdasarkan ISO 27001:2013.
3. Memberikan rekomendasi berdasarkan analisis dari hasil kontrol *Annex* ISO 27002:2013 pada PT.XYZ.