BAB 1

PENDAHULUAN

1.1. Latar Belakang

Pada masa sekarang ini perkembangan teknologi informasi sangatlah cepat, di Indonesia sendiri teknologi informasi sudah menjadi salah satu bagian yang tidak bisa dipisahkan pada setiap pekerjaan. Teknologi Informasi memiliki cakupan yang sangat luas yaitu teknologi komputer, perangkat keras, dan perangkat lunak yang dapat digunakan untuk pengolahan dan penyimpanan informasi dan digunakan untuk berkomunikasi yang bertujuan untuk mengirimkan ataupun menyebarluaskan suatu informasi [1]. Teknologi Informasi tidak akan maksimal tanpa adanya dukungan yang baik dari keamanan informasi. keamanan sistem informasi membantu kita untuk melakukan pencegahan penipuan ataupun pendeketsian sebuah penipuan pada sistem [2]. Sebuah iformasi pada sistem yang mempunyai nilai penting menjadikan informasi tersebut tidak dapat diakses oleh setiap orang melainkan harus diproteksi untuk memastikan hanya orang – orang yang mempunyai wewenang dapat diberi akses. Misalnya dalam suatu persaingan bisnis dan informasi jatuh ke pesaing, dapat membawa kerugian yang besar bagi pemilik binsis tersebut.

Mengelola sebuah sistem informasi tentunya dibutuhkan keamanan sistem informasi yang baik untuk mencegah dan mengantisipasi ancaman yang mungkin akan terjadi, ISO/IEC 27000 adalah standar Sistem Manajemen Keamanan Informasi (SMKI) atau juga dikenal dengan *Information Security Management System (ISMS)* yang melatar belakangi bagaimana sebuah perusahan bisa mengelola dan menerapkan keamanan sistem informasi [3]. ISO/IEC 27000 dibagi menjadi 8 bagian yaitu:

- ISO/IEC 27000:20009 tentang gambaran umum SMKI
- ISO/IEC 27001:2005 tentang persyaratan SMKI
- ISO/IEC 27002:2005 tentang kode praktik SMKI
- ISO/IEC 27003:2010 tentang Implementasi SMKI
- ISO/IEC 27004:2009 tentang evaluasi SMKI
- ISO/IEC 27005:2008 tentang risiko sistem informasi
- ISO/IEC 27006:2007 tentang pemenuhan syarat sertifikasi SMKI
- ISO/IEC 27007 tentang panduan pengujian SMKI

Seri seri ISO/IEC 27000 diatas merupakan pembaharuan dari ISO 17799 dan sudah diadopsi oleh Badan Standarisasi Nasional(BSN) [4].

Manajemen perusahaan seringkali sulit untuk melakukan investasi di bidang keamanan dikarenakan kurangnya kesadaran perusahaan itu sendiri yang masih menganggap bahwa keamanan sistem Informasi bukanlah hal yang penting. Survey yang dilakukan Survey Information Week (USA) terhadap keamanan Sistem Informasi terhadap 1721 sistem, hanya 22% yang menanggap bahwa keamanan sistem adalah penting. Sama hal nya pada PT. Asia Bandar Alam, perusahaan yang berada dibidang kecantikan yang juga menerapkan peranan teknologi informasi untuk menunjang berjalannya bisnis. Pada tahun 2020 ini, telah terjadi *phishing* pada sistem komputer yang digunakan karyawan sehingga menyebabkan file tidak bisa diakses dan hilangnya data perusahaan yang penting. Pishing sendiri bisa terjadi karena lalai nya user dalam memasukan informasi kedalam sebuah situs yang ditiru oleh *pisher* (penjebak) dengan cara menggunakan situsyang tampilannya menyerupai tampilan asli atau situs resmi sebenarnya [5]. Kurangnya edukasi terhadap karyawan dan kurangnya keamanan sistem pada komputer memicu terjadinya *phishing*.

Penerapan keamanan sistem informasi pada PT. Asia Bandar Alam masih terbilang kurang, komputer yang digunakan untuk bekerja menggunakan software yang sudah terbilang lawas, karena masih menggunakan OS windows 7 yang sudah tidak didukung oleh Microsoft

itu sendiri, karena update terakhir Microsoft untuk windows 7 adalah pada 14 Januari 2020 yang menjadikan OS windows 7 lebih rentan terhadap risiko keamanan, ditambah lagi *registry*, *autoplay*, dan *clipboard* pada OS Windows mampu digunakan untuk mendapatkan akses ke sistem [6]. Antivirus yang digunakan juga antivirus *free* yang fitur dan kemampuannya yang terbatas sehingga tidak maksimal untuk menangani komputer.

1.2. Perumusan Masalah

Penggunaan TI pada perusahaan PT. Asia Bandar Alam membantu menjadikan proses bisnis pada perusahaan menjadi lebih efektif dan efisien. Untuk menerapkan manajemen keamanan sistem dengan menggunakan TI, harus adanya tingkat kesadaran yang tinggi maupun komitmen supaya berjalan dengan baik. Di PT. Asia Bandar Alam ini, tingkat kesadaran pengguna terhadap TI masih rendah, sehingga risiko untuk mengalami kegagalan keamanan sistem informasi masih tinggi sehingga dapat merugikan perusahaan.

1.3. Pertanyaan Penelitian

Dari pemaparan perumusan di atas, pertanyaan penelitian yang dihasilkan adalah sebagai berikut:

1. Bagaimana menganalisa proses keamanan sistem informasi PT. Asia Bandar Alam sesuai dengan standar ISO 27002:2013 menggunakan metode SSE-CMM?

1.4. Batasan Masalah

Dari pemaparan perumusan di atas, batasan masalah yang dihasilkan adalah sebagai berikut:

1. Analisis tingkat keamanan sistem informasi PT. Asia Bandar Alam dilakukan pada divisi IT yang berada pada kantor pusat di Juanda Jakarta Pusat
2. Penelitian ini menggunakan standar ISO 27002:2013
3. Penelitian ini menggunakan metodologi SSE-CMM
4. Keluaran yang dihasilkan pada penelitian ini merupakan rekomendasi untuk keamanan sistem informasi PT. Asia Bandar Alam

1.5. Tujuan Penelitian

Dari pemaparan perumusan masalah dan pertanyaan penelitian di atas, tujuan penelitian yang dihasilkan adalah sebagai berikut:

1. Menganalisis tingkat keamanan sistem informasi PT. Asia Bandar Alam menggunakan metode SSE-CMM untuk mengidenfifikasi risiko berupa *maturity level* untuk bisa menilai apakah sudah sesuai standar ISO27002:2013 atau belum.

1.6. Manfaat Penelitian

Bagi Keilmuan

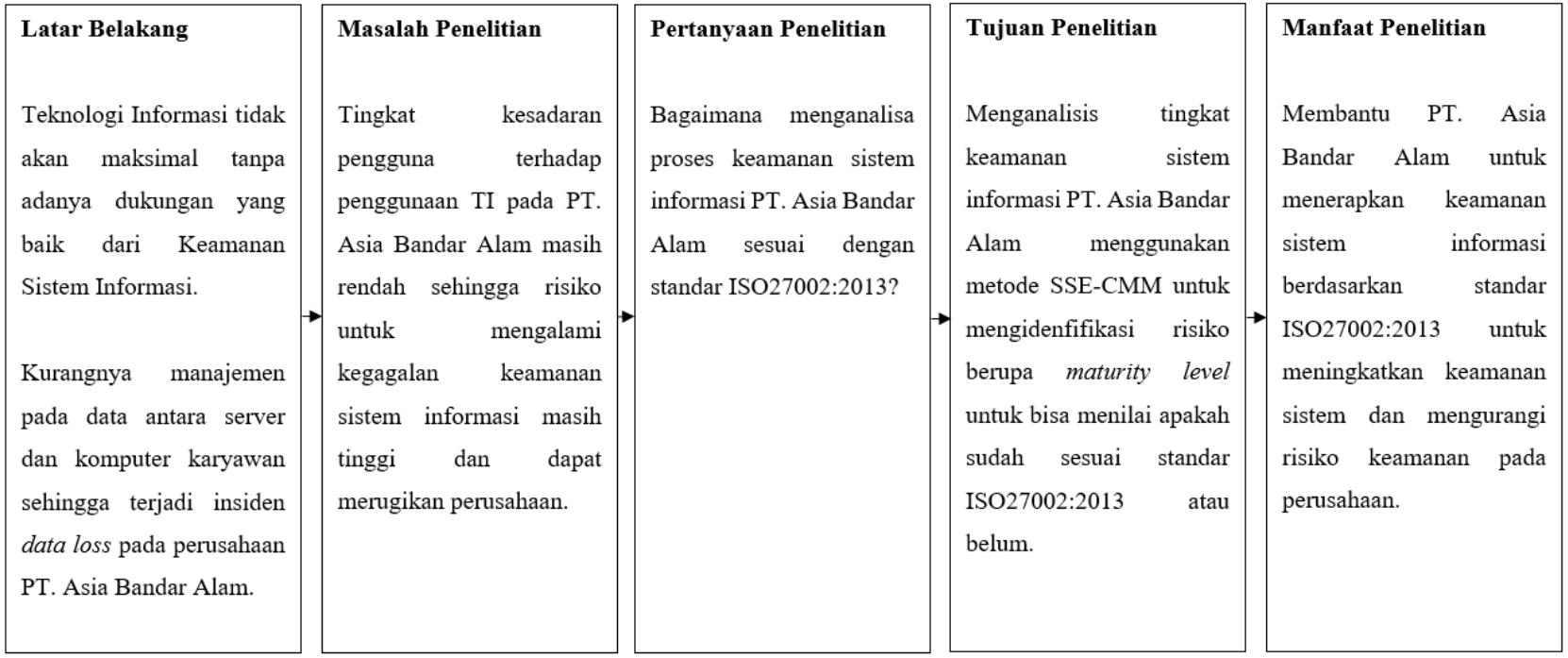
1. Peneliti berkontribusi untuk menganalisa keamanan sistem informasi menggunakan kerangka kerja ISO 27002:2013 pada perusahaan PT. Asia Bandar Alam

Bagi Praktisi

1. Perusahaan dapat meningkatkan kesadaran dalam penggunaan TI dan menangani risiko risiko yang mungkin akan terjadi sesuai dengan ISO 27002:2013

1.7. Bagan Keterkaitan

Bagan keterkaitan untuk Analisis Keamanan Sistem Informasi PT. Asia Bandar Alam Sesuai Standar ISO27002:2013 Menggunakan Metode SSE-CMM



Gambar 1.1 Bagan Keterkaitan