BAB I
PENDAHULUAN

1.1. LATAR BELAKANG MASALAH

Permasalahan keamanan komputer selalu menarik untuk dibahas, hal ini karena perkembangan teknologi informasi yang semakin canggih dan meluas. Semakin canggih teknologi informasi ternyata terkadang tidak diikuti dengan penerapan keamanan yang memadai, sehingga ancaman keamanan selalu menjadi momok bagi penerapan sistem komputer dalam sebuah organisasi atau perusahaan [1]. Bisnis *clothing line* atau distro bisa dikatakan bisnis yang sulit. Mengapa? Sebab bisnis ini membutuhkan kepiawaian dan keseriusan dalam memproduksi karya dan mendistribusikannya. Selian itu, dibutuhkan pula strategi pemasaran dalam memperkenalkan *brand*-nya dan melakukan pembuatan sistem keamanan kepada perusahaan yang akan dijalankan. Berkembangnya zaman membuat bisnis ini juga ikut berkembang. Garment Mensamco Indonesia merupakan perusahaan yang bergerak dibidang retail.

Mekanisme penjualan yang terjadi di Garment Mensamco Indonesia adalah konsumen datang ke toko untuk mencari dan memilih barang yang akan dibeli. Saat ini pertokoan Garment Mensamco Indonesia sudah menerapkan sistem dan tekhnologi informasi dalam mendukung operasional perusahaan namun ada berbagai masalah dalam akuntabilitas, tanggung jawab serta efektifitas, dan efensiensi terhadap keamanan TI. Hasil dari pengamatan berbeda dengan ekspektasi Divisi Teknologi Informasi (TI) di toko Garment Mensamco Indonesia selama ini. Sesuai hasil pengamatan keamanan informasi tersebut, keamanan informasi Garment Mensamco Indonesia dinilai masih lemah. Kurangnya *monitoring* dan evaluasi ini menjadi salah

satu penyebab masalah belum terpenuhinya kriteria keamanan informasi di Garment Mensamco Indonesia. Belum tercapainya kriteria keamanan informasi salah satunya disebabkan karena belum adanya kebijakan dan prosedur keamanan informasi komprehensif, baik yang berlaku pada tingkat operasional (teknis) maupun manajerial. Apabila data yang dimiliki oleh suatu institusi dicuri atau disalahgunakan akan memberikan dampak kerugian bagi institusi tersebut [2].

Ekspektasi divisi TI selama ini adalah keamanan informasi perusahaan sudah baik (aman), begitu pula dengan keamanan informasi pelanggan. Hal ini ditunjang dari adanya kebijakan dan prosedur keamanan informasi yang berlaku di Garment Mensamco Indonesia. Ditinjau dari hasil pengamatan tersebut, kami memutuskan melakukan audit kepatuhan keamanan informasi untuk menguji apakah tingkat kepatuhan keamanan informasi perusahaan terhadap visi dan misi yang sudah memenuhi aspek keamanan informasi dan menguji pengaruhnya terhadap keamanan informasi perusahaan. Dari hasil audit kepatuhan keamanan informasi ini, nantinya didapatkan kebijakan dan prosedur yang lebih baik sehingga dapat diberikan rekomendasi kebijakan dan prosedur yang lebih komprehensif.

1.2. RUMUSAN MASALAH

Berdasarkan latar belakang diatas , dapat dirumuskan masalah sebagai berikut:

1. Apakah Kebijakan dan prosedur yang ada sudah dapat dikatakan memenuhi standar terhadap aspek keamanan TI ?
2. Bagaimana akuntabilitas dan tanggung jawab terhadap keamanan TI pada Garment Mensamco Indonesia ?
3. Bagaimana efesiensi dan efektifitas keamanna TI pada Garment Mensamco Indonesia ?

1.3. TUJUAN

Tujuan yang ingin dicapai dari melakukan audit ini yaitu:

1. Mengetahui akuntabilitas dan tanggung jawab terhadap keamanan TI pada Garment Mensamco Indonesia .
2. Memberikan SOP atau prosedur yang sesuai dengan setandar keamanan TI pada Garment Mensamco Indonesia.

1.4. TEKNIK PENGUMPULAN DATA

Penulis melakukan penelitian guna mengumpulkan data dengan cara:

1. Observasi

Pengamatan dilakukan terhadap pengelolaan TI berdasarkan aspek-aspek yang telah ditetapkan dalam COBIT 5 berdomain DSS.

2. Wawancara

Kegiatan ini dilakukan untuk menangkap deskripsi lebih lengkap mengenai masalah yang diteliti yang tidak terjaring melalui kuesioner. Untuk pedoman wawancara, meneliti juga berpedoman pada model kematangan dan *Control Objectives COBIT.* Penulis melakukan wawancara langsung dengan salah satu karyawan di bagian IT pada perusahaan Garment Mensamco Indonesia yang bernama Bapak Indra Susilo pada tanggal 20 Mei 2020 pukul 13.00 WIB, dan membahas mulai dari proses jual beli, transaksi hingga keamanan informasi pelanggan.

3. Studi Pustaka

Studi pustaka cara pengumpulan data dan mempelajari dari teori-teori dengan melihat sumber kepustakaan seperti situs web, jurnal ilmiah, skripsi dan sebagainya yang dapat dipertanggung jawabkan untuk dijadikan bahan referensi dalam pembuatan makalah ini.

BAB II
LANDASAN TEORI

2.1. LANDASAN TEORI

1. Control Objective for Information and related Technology (COBIT)

Arensdan Loebbecke [3] berpendapat *COBIT* adalah suatu proses pengumpulan dan pengevaluasian Bahan bukti tentang informasi yang dapat diukur mengenai suatu entitas ekonomi yang dilakukan seorang yang kompeten dan independen untuk dapat menentukan danmelaporkan kesesuaian informasi dengan kriteria-kriteria yang telah ditetapkan. Auditing seharusnya dilakukan oleh seorang yang independent dan kompeten.

Sukrisno Agoes [4] berpendapat *COBIT* adalah pemeriksaan yang dilakukan secarakritis dan sistematis oleh pihak yang independen, terhadap laporan keuangan yang telah disusun oleh manajemen beserta catatan-catatan pembukuan danbukti-bukti pendukungnya, dengan tujuan untuk dapat memberikan pendapat mengenai kewajaran laporan keuangan tersebut.

COBIT merupakan suatu kerangka kerja atau panduan best practices manajemen dan teknologi informasi [5]. Fokus utama dari *COBIT* ini adalah harapan bahwa melaui adopsi *COBIT* ini, perusahaan akan mampu meningkatkan nilai tambah melalui penggunaan TI dan mengurangi resiko-resiko inheren yang teridentifikasi didalamnya. COBIT dikembangkan oleh *IT Governance Institute (ITGI),* yang merupakan bagian dari *Information Systems Audit and Control Association (ISACA).* Saat ini pengembangan terbaru dari standar ini adalah COBIT Edisi 5.0. COBIT 5 merupakan pengembangan dari COBIT 4.1 yang merupakan salah satu framework yang digunakan untuk melakukan proses audit.

Manfaat yang diberikan oleh informasi dan teknologi pada perusahaan:

1. Menjaga kualitas informasi untuk mendukung pengambilan keputusan bisnis
2. Menghasilkan nilai bisnis dari investasi pemanfaatan IT , yaitu mencapai tujuan strategis dan merealisasikan manfaat bisnis melalui penggunaan IT yang efektif dan inovatif.
3. Mencapai keunggulan operasional melalui penerapan teknologi yang handal dan efisien.
4. Menjaga resiko yang behubungan dengan penerapan pada tingkat yang masih bisa ditoleransi mengoptimalkan biaya penggunaan it service dan teknologi

2. Information Security

G.J. Simons [6] berpendapat bahwa *Information Security* adalah bagaimana kita dapat mencegah penipuan *(cheating)* atau,paling tidak, mendeteksi adanya penipuan di sebuah sistem yang berbasis informasi, dimana informasinya sendiritidak memiliki arti fisik. Menurut Commite on National Security System [7] berpendapat bahwa Information Security adalah perlindugan informasi dan elemenelemen didalamnya termasuk sistem dan perangkat kerasnya. Sarno dan Iffano [8] menjelaskan bahwa Information Securityadalah adalah suatu upaya untuk mengamankan asetinformasi terhadap ancaman yang mungkintimbul.

Keamanan informasi adalah untuk melindungi kerahasiaan, integritas dan ketersediaan aset informasi, baik dalam penyimpanan, pengolahan, atau transmisi. Hal ini dicapai melalul penerapan kebijakan, pendidikan, pelatihan dan kesadaran, dan teknologi. Dalam keamanan informasi saat ini telah berkembang menjadi tiga konsep utama yang menjadi standar utama dalam industry keamanan yang disebut dengan CIA triangle yaitu: *Confidentiality (*usaha untuk menjaga informasi), *Integrity* (keaslian pesan yang dikrim), dan *Availability* (ketersediaan berhubungan dengan ketersediaan infromasi ketika dibutuhkan)

BAB III

PEMBAHASAN

1.1. DOMAIN *Delivery, Services and Support (DSS)*

Muhammad Tanzir Wilson [10] berpendapat bahwa Domain yaitu sebuah URL yang unik di internet sehingga situs anda bisa diakses oleh pengunjung di seluruh dunia. Irene Joos dan Nancy [11] berpendapat bahwa Domain ialah suatu identitas sebuah website di internet. Sebuah domain terdiri dari nama domain dan ekstensi.

Delivery, Services and Support Domain ini memberikan fokus utama pada aspek penyampaian atau pengiriman dan pelayanan dari IT. Domain ini mencakup area-area seperti pengoperasian aplikasi aplikasi dalam sistem IT dan hasilnya, dan juga, proses dukungan yang memungkinkan pengoperasian sistem IT tersebut dengan efektif dan efisien. Proses dukungan ini termasuk isu atau masalah keamanan dan juga pelatihan.

Delivery, Service, and Support (DSS) Domain merupakan salah satu dari lima domain COBIT 5 yang termasuk Management of Enterprise IT. Domain DSS mempunyai focus pada pengiriman data, layanan, dan dukungan yang diberikan untuk sistem informasi yang efektif dan efisien. Domain DSS memiliki enam proses, yaitu [9]:

a. *DSS01 Manage Operation*
b. *DSS02 Manage Service Requests and Incidents*
c. *DSS03 Manage Problems*
d. *DSS04 Manage Continuity*
e. *DSS05 Manage Security Services*
f. *DSS06 Manage Business Process Controls*

Dalam bab ini, peneliti akan membahas hasil audit dari masing-masing sub-domain yang dipilih yaitu *DSS (Delivery, suport, and service)* dan juga akan membahas rekomendasi untuk setiap sub-domain. Rekomendasi akan diberikan oleh peneliti berdasarkan gap antara current level dan expected level, expected level yang diharapkan perusahaan pada domain DSS 4:

1. DSS Maturity Level 0 Non Exsistent

Mengetahui prosedur atau proses keamanan komputer yang ada pada perusahaan dan penerapannya apakah pihak internal menyadari tentang pentingnya keamanan komputer terhadap sistem yang sedang berjalan pada perusahaan. Pada level ini ada 5 pernyataan yang di tanyakan pada responded.

2. DSS Maturity Level 1 Initian atau Ad Hoc

Merupakan proses lanjutan dari peroses level 0 non exsistent yang dibutuhkan oleh peneliti dalam mengaudit keamanan sebuah sistem. Proses ini akan memberikan pengetahuan awal dari pihak internal atau orang yang berinteraksi langsung pada sistem tentang kesadaran kemamanan komputer dan adanya ancaman akan pelanggaran keamanan komputer. Pada level ini terdapat 6 pernyataan yang diajukan pada responded.

3. DSS Maturity Level 2 Repetable but Intuitif

Mengulang atau memahami dan memiliki kesadaran atas tanggung jawab terhadap keamanan sebuah sistem yang sedang berjalan pada perusahaan. Bagaimana pengelolaan akuntabilitas dan tanggung jawab tersebut mendapat kejelasan dari pengelola dan ditetapkannya oleh perusahaan. Pada level ini terdapat 8 pernyataan yang diajukan pada responded.

4. DSS Maturity Level 3 Defined

Merupakan proses selanjutnya dimana hasil dari yang sudah dilakukan, disini menerangkan definisi dari pengertian pengelola akan kesadaran keamanan yang sudah ditetapkan pihak perusahaan atau manajemen dan juga prosedur – prosedur yang berlaku di perusahaan tentang pentingnya tanggung jawab keamanan sebuah sistem (keamanan TI). Pada level ini terdapat 5 pernyataan yang di tanyakan pada responded.

5. DSS Maturity Level 4 Managed and Masurable

Merupakan pengelolaan yang terukur dimana pengelola sadar akan dampak yang terjadi dari keamanan komputer (keamanan TI) prosedur dan kebijakan keamanan TI sudah konsisten dilakukan oleh pengelola dan diminimalisisr resikonya serta dianalisi kekurangannya. Identifikasi, otentikasi, otorisasi pengguna sudah tersetandarisasi. Pada proses ini terdapat 10 pernyataan yang diajukan pada responded.

6. DSS Maturity Level 5 Optimised

Merupakan pengoptimalan atau proses terakhir dari audit yang dilakukan, kebutuhan keamanan TI sudah ditetapkan, dioptimalisasi dengan jelas dan sudah dimasukan kedalam rencana keamanan yang sudah di setujui. Penilaian keamanan secara periodik dilakukan untuk mengevaluasi keefektifan dan implementasi rencana keamananroses dan teknologi keamanan sudah terintegrasi didalam keseluruhan perusahaan. Pada proses level ini terdapat 9 pernyataan yang diajukan pada responded.