BAB I PENDAHULUAN

1.1 Latar Belakang Masalah

PT Indonesia Computer Square adalah perusahaan yang bergerak dalam bidang penjualan komputer dan alat – alat elektronik lainnya. Memiliki 5 cabang yang tersebar di wilayah Jabodetabek. Sebagai sebuah vendor dalam bidang teknologi dan elektronik, menyediakan beragam produk TI yang lengkap dengan harga kompetitif, mulai dari *PC desktop* dan *notebook* merek global dan lokal terkemuka maupun produk-produk *Apple*, komponen/periferal *PC* seperti *hard disk, motherboard, keyboard*, memori, *casing*, kartu grafis, printer, proyektor, monitor, dan *flash disk*, hingga *gadget* seperti *PDA, PDA Phone, dan iPod*. Teknologi dan sistem informasi mempunyai peranan yang besar dalam penyampaian informasi. Informasi atau data adalah aset bagi perusahaan. Keamanan data secara tidak langsung dapat memastikan kontinuitas bisnis, mengurangi resiko, dan mencari kesempatan bisnis. Semakin banyak informasi perusahaan yang disimpan, dikelola dan di-*sharing* maka semakin besar resiko terjadinya kerusakan, kehilangan atau terekspos nya data ke pihak eksternal yang tidak diinginkan.

Agar kinerja IT pada suatu organisasi dapat berjalan dengan baik maka diperlukan suatu kendali *control* internal atau sebuah *framework* yang dapat mengontrol seluruh proses proses yang terdapat pada IT.

1.2 Rumusan Masalah

Rumusan masalah penelitian ini adalah :

Apakah PT.Indonesia Computer telah melakukan penjagaan aset (*asset safeguarding*) khususnya dalam hal data dengan baik?

1.3 Tujuan Pembahasan

Tujuan dilakukan pembahasan ini adalah :

Untuk mengetahui apakah PT.Indonesia Computer telah melakukan penjagaan aset (*asset safeguarding*) khususnya dalam hal data dengan baik dengan cara melakukan audit teknologi informasi.

1.4 Ruang Lingkup

- Audit yang dilakukan mengacu kepada *COBIT Framework*
- Sasaran kontrol (*control objectives*) yang harus dipenuhi sebagai acuan pengauditan adalah :
  - *Accuracy, Completeness and Authenticity Checks*
    Kontrol ini membahas mengenai bahwa data adalah akurat, lengkap dan *valid* menvalidasi data yang di*input*, dan mengedit atau mengirim kembali untuk koreksi
  - *Application Security*
    Kontrol ini membahas mengenai menjaga keamanan aplikasi.
  - *Training*
    Kontrol ini membahas mengenai pelatihan *staf* dan kelompok IT sesuai dengan pelaksanaan rencana dan terkait bahan, sebagai bagian dari setiap sistem informasi
  - *Performance and Capacity Planning*
    Kontrol ini membahas mengenai proses perencanaan untuk meninjau kinerja dan kapasitas sumber daya IT
  - *Exchange of Sensitive Data*
    Kontrol ini membahas mengenai pertukaran data transaksi sensitif melalui jalur yang terpercaya atau dengan kontrol untuk menyediakan konten keaslian, bukti penyerahan, dan bukti penerimaan

- *User Account Management*

  Kontrol ini membahas mengenai hak dan kewajiban berkaitan dengan akses ke sistem perusahaan dan informasi harus diatur dalam kontrak untuk semua jenis pengguna
- *Business Requirements for Data Management*

  Kontrol ini membahas mengenai memverifikasi bahwa semua diharapkan untuk memproses data yang diterima dan diproses sepenuhnya, akurat dan pada waktu yang tepat, dan semua *output* disampaikan sesuai dengan kebutuhan bisnis.
- *Storage and Retention Arrangements*

  Kontrol ini membahas mengenai mendefinisikan dan menerapkan prosedur yang efektif dan efisien untuk penyimpanan data.
- *Disposal*

  Kontrol ini membahas mengenai mendefinisikan dan menerapkan prosedur untuk memastikan bahwa persyaratan bisnis untuk perlindungan data sensitif dan *software* telah terpenuhi
- *Backup and Restoration*

  Kontrol ini membahas mengenai mendefinisikan dan menerapkan prosedur untuk *backup* dan pemulihan sistem, aplikasi, data dan dokumentasi
- *Security Requirements for Data Management*

  Kontrol ini membahas mengenai menentukan dan melaksanakan kebijakan dan prosedur untuk mengidentifikasi dan menerapkan persyaratan keamanan yang berlaku untuk penerimaan, pengolahan, penyimpanan dan *output* data untuk memenuhi tujuan bisnis

- *Sensitive Documents and Output Devices*
  Kontrol ini membahas mengenai menetapkan perlindungan fisik yang sesuai pengelolaan aset IT yang lebih sensitif

1.5 Sumber Data

- Sumber data diambil dari perusahaan yang bersangkutan, yang dalam hal ini PT Indonesia Computer Square
- Wawancara dengan staff dan pimpinan
- Studi pustaka,buku ataupun internet

1.6 Sistematika Penyajian

- Bab I Pendahuluan
  Bab ini berisikan Latar Belakang Masalah, Perumusan Masalah, Tujuan, Batasan Masalah, Sistematika Penulisan, Metode dan Teknik Penelitian
- Bab II Landasan Teori
  Bab ini berisikan Teori-teori yang menjadi dasar bagi penulis dalam melakukan kerja praktek ini. Yaitu teori mengenai *COBIT framework* dan penjelasan mengenai proses proses yang akan diaudit.
- Bab III Analisis
  Bab ini menjelaskan perancangan rencana audit dan proses *evidence collection*.
- Bab IV Hasil Tercapai
  Bab ini akan menjelaskan mengenai proses *evidence evaluation*.
- Bab V Penutup (Kesimpulan dan Saran)
  Bab ini berisikan kesimpulan dari seluruh hasil kerja praktek dan Saran bagi perusahaan berdasarkan hasil audit.