BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

DISKOMINFO adalah salah satu perusahaan BUMN dengan salah satu misi untuk meningkatkan kualitas dan kuantitas dan SDM di bidang teknologi informasi. Adapun tugas pokok DISKOMINFO Provinsi Jawa Barat adalah melaksanakan sebagian tugas umum Pemerintahan Provinsi Jawa Barat dalam merumuskan kebijakan teknis dalam melaksanakan kewewenangan di bidang Sitel sesuai kebutuhan Daerah dan Kewenangan yang dilimpahkan kepada Gubernur. Untuk melaksanakan tugas tersebut, DISKOMINFO mempunyai fungsi untuk melakukan perumusan kebijakan teknis di bidang Sitel dan pelaksanaan penunjang Pemerintah Daerah di bidang Sitel. Oleh karena itu dibutuhkan keamanan yang terjamin untuk melakukan segala aktifitas dan dalam pengelolaan *software* maupun *hardware* yang akan dikerjakan oleh DISKOMINFO, dan juga untuk data – data yang ada harus bisa digunakan dengan sebaik – baiknya.

Di dalam DISKOMINFO ada beberapa kelemahan dalam segi keamanan, baik *software*, *hardware* dan juga SDM. Di tiap divisi ada banyak data yang bisa diakses, tetapi untuk mengakses data tersebut perlu sebuah username dan password, dan para pegawai DISKOMINFO memberikan username dan password sesuai dengan nama tiap divisi, dan ini merupakan salah satu kelemahan dalam segi keamanan. Oleh karena itu penulis ingin membantu DISKOMINFO dalam segi keamanan sistem infomasi dengan mengaudit DISKOMINFO menggunakan Cobit Guideliness 4.1 yang akan dipilih 8 proses (DS5, DS11, DS12, PO7, DS7, DS10, DS13, ME1) yang berhubungan dengan masalah keamanan,

baik dalam segi keamanan *hardware*, *software* dan SDM. 8 proses itu dipilih karena semuanya berhubungan 1 sama lain dengan keamanan dalam segi *hardware* dan *software* dan juga untuk SDM. Berikut ini adalah beberapa alasan kenapa memilih 8 proses tersebut dan beberapa masalah DISKOMINFO yang berhubungan dengan 8 proses yang dipilih :

1. *Ensure Systems Security (DS5)* karena didalam DISKOMINFO, masih terdapat beberapa kelemahan dalam segi keamanan sistem informasinya contohnya adalah tidak memasang antivirus untuk server.
2. *Manage Data (DS11)* karena keamanan data tidak terjaga dengan baik dan masih kurangnya kesadaran para pegawai untuk melakukan backup data serta untuk menjaga data yang ada.
3. *Manage the Physical Environment (DS12)* karena masih kurangnya batasan untuk mengakses ruangan server dan kurangnya keamanan di dalam ruangan server, karena jika ada masalah di dalam server, baru server diperhatikan. JIka tidak ada masalah dibiarkan berjalan serperti itu dan *maintenance* yang bisa dikatakan kurang baik
4. *Manage IT Human Resources* (PO7) karena kurangnya kesadaran dari segi SDM akan pentingnya keamanan data, serta ada beberapa pegawai yang kurang menguasai *software* yang ada dan para pegawai kurang mematuhi peraturan yang ada dan tidak terlalu diterapkan di DISKOMINFO.
5. *Educate and Train User* (DS7) karena masih kurangnnya pelatihan yang diberikan kepada para pegawai, dan juga masih ada beberapa pegawai yang kurang menguasi *software* yang ada didalam DISKOMINFO, serta jenjang karir yang kurang jelas.

6. *Manage Problems* (DS10) karena tidak ada manajemen untuk mengatasi masalah yang ada, walaupun sudah melakukan identifikasi masalah dan pengelompokan masalah dalam segi *software* dan *hardware*.
7. *Manage Operations* (DS13) karena masih kurangnya keahlian para pegawai jika terjadi masalah dan juga peraturan yang kurang dipatuhi oleh beberapa pegawai walaupun suda ada peraturan yang jelas.
8. *Monitor and Evaluate IT Performance* (ME1) karena belum ada monitoring method untuk memonitor dan mengevaluasi kinerja dari proses bisnis yang terjadi, terutama di dalam bagian Telematika

1.2 Rumusan Masalah

Berdasarkan uraian permasalahan tersebut, maka dapat dirumuskan sebagai berikut :

1. Apakah solusi terbaik untuk masalah keamanan *hardware* dan *software* di dalam DISKOMINFO agar kinerja IT bisa lebih baik?
2. Bagaimana cara untuk meningkatkan kesadaran para pegawai IT akan pentingnya menjaga kemanan sistem informasi didalam DIKSOMINFO?
3. Apakah server dan data yang ada sudah terjaga dengan baik dari berbagai masalah yang ada ?

1.3 Tujuan Pembahasan

Tujuan yang ingin dicapai oleh penulis adalah sebagai berikut :

1. Memberikan solusi yang terbaik untuk masalah keamanan dalam segi *hardware* dan *software* di DISKOMINFO.

2. Memberikan seluruh hasil dokumentasi dan observasi kepada DISKOMINFO sebagai bahan referensi untuk bahan pertimbangan maupun informasi yang berguna untuk segi keamanan.
3. Belum terjaga dengan baik, oleh karena itu penulis memberi tahukan dampak yang mungkin terjadi jika para pegawai tidak memiliki kesadaran yang tinggi akan pentingnya menjaga keamanan system informasi yang ada di dalam DISKOMINFO

1.4 Ruang Lingkup Kajian

1. Hanya menangani masalah keamanan data dan SDM yang berhubungan dengan sekuritas.
2. Menganalisis dan riset dengan menggunakan COBIT 4.1
3. Proses analisis dan evaluasi proses DS5, DS11, DS12, PO7, DS7, DS10, DS13, ME1 menggunakan COBIT 4.1.

1.5 Sumber Data

Sumber data yang digunakan untuk mendapatkan data yang diperlukan oleh penulis adalah sebagai berikut :

1. Observasi di DISKOMINFO
2. Wawancara dengan pimpinan , staff yang berada dalam divisi tersebut
3. Studi pustaka, buku ataupun internet

1.6 Sistematika Penulisan

Adapun sistematika penulisan laporan tugas akhir sebagai berikut :

BAB I Pendahuluan

1. Latar Belakang Masalah

Yaitu profil perusahaan dan hal-hal yang melatarbelakangi penulis melakukan tugas akhir

2. Perumusan Masalah

   Yaitu proses-proses yang akan diaudit oleh penulis

3. Tujuan

   Yaitu tujuan dari tugas akhir ini

4. Batasan Masalah

   Yaitu hal-hal yang membatasi penulis melakukan penelitian dan pengauditan di perusahaan.

5. Sistematika Penulisan

   Yaitu berisi kerangka laporan tugas akhir

6. Metode dan Teknik Penelitian

   Yaitu hal hal yang dilakukan oleh penulis dalam pelaksanaan penelitian tugas akhir ini, yakni meliputi metode metode dan teknik teknik penelitiannya.

BAB II Kajian Teori

Teori-teori yang menjadi dasar bagi penulis dalam melakukan tugas akhir ini. Yaitu teori mengenai COBIT *framework* dan penjelasan mengenai proses-proses yang akan diaudit.

BAB III Analisis

Proses pengauditan berdasarkan COBIT 4.1 *guideline.* Menjelaskan bagaimana proses yang dilakukan untuk menilai kepatuhan terhadap kontrol yang sudah ditetapkan. Apakah sistem yang telah diterapkan saat ini sudah sesuai dengan standar dari COBIT

BAB IV Hasil Penelitian

Berisi tentang hasil yang didapatkan dari proses analisis berdasarkan COBIT 4.1 *guideline*.

BAB V Simpulan dan Saran

Kesimpulan dari seluruh hasil tugas akhir dan saran bagi perusahaan berdasarkan hasil audit.