4. DESKRIPSI DATA DAN PEMBAHASAN

Aktivitas audit yang dilakukan oleh penulis dilaksanakan pada tanggal 20 Maret sampai dengan 6 November tahun 2010. Dimana aktivitas audit atas *General Control* dilaksanakan di PT. X yang terletak di jalan Raya Sumengko KM 31,6. Data-data yang didapat dari aktivitas audit yang telah dilaksanakan berasal dari hasil wawancara dengan bapak roy selaku pihak *EDP*, Bapak Agus selaku *System Analyst and Programmer*, wawancara dengan para pekerja, uji coba atas sistem serta bukti-bukti dokumentasi berupa foto serta *print screen*.

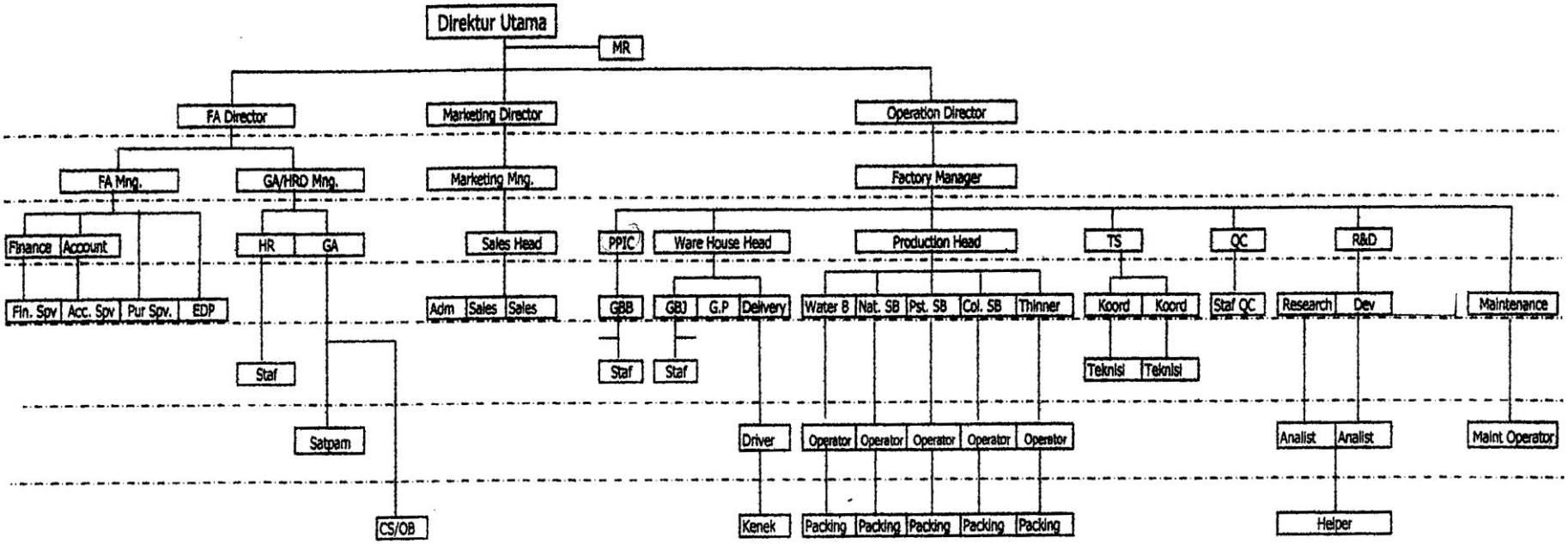
4.1 Gambaran Umum

4.1.1 Sejarah Perusahaan

PT. "X" berdiri sejak tahun 1996 dan berlokasi di daerah Wringin Anom, yaitu di jalan Raya Sumengko KM 31,6. PT "X" merupakan perusahaan yang bergerak di bidang *manufacture*, untuk memproduksi cat dan thinner.

Pada awalnya PT. "X" masih menggunakan sistem manual dalam proses bisnisnya, hal ini disebabkan minimnya pengetahuan akan sistem komputer dan perusahaan merasa belum membutuhkannya. Seiring dengan berkembangnya teknologi, pada tahun 1998 perusahaan mulai menggunakan komputer, namun sistem yang digunakan masih sebatas *microsoft excel* dan *microsoft word* yang berfungsi untuk membantu proses pencatatan dan perhitungan data. Seiring dengan berjalannya waktu, perusahaan memperbarui sistem terkomputerisasinya yang awalnya belum terintegrasi menjadi terintegrasi dengan menggunakan software "BMP" (Business Management Process) di tahun 2002. "BMP" yang diterapkan dalam PT. X ini merupakan program dari hasil outsourcing dari perusahaan *Consulting* PT. Orlansoft. Adapun departemen yang terintegrasi adalah departemen Pembelian / *purchasing*, Penjualan / *marketing*, akuntansi, produksi dan bagian gudang.

4.1.2 Struktur organisasi



Sumber : PT. “X”

4.1.3 *Job Description* organisasi

Tanggung jawab masing-masing bagian tertera dalam *job description* yang tertulis dibawah ini :

1. Direktur

   Direktur memgang jabatan tertinggi dan bertugas memimpin serta mengelola perusahaan secara keseluruhan, merumuskan visi, misi, serta kebijakan perusahaan. Selain itu, juga menetapkan rencana strategis perusahaan, menerima semua laporan atas kinerja perusahaan.

2. FA

   A. Finance

      Finance bertugas memeriksa kelengkapan dokumen untuk pembayaran supplier, menyiapkan dan operasional perusahaan, membuat laporan kas harian, entry data transaksi pada BKK dan BKM, mencocokkan uang tunai yang ada dengan laporan kas harian, entry data pada BBK dan BBM, membuat laporan kas bank harian.

   B. Accounting

      Accounting bertugas memposting transaksi harian yang terjadi, membuat laporan keuangan.

   C. Purchasing

      Purchashing mempunyai tanggung jawab serta otorisasi untuk membuat *PO*, mengubah *master file* yang berhubungan dengan data-data supplier perusahaan, mengakses terhadap file stok barang, membuat dan memeriksa minimum stok barang

   D. EDP

      EDP membuat dan melaksanakan jadwal maintenance computer, menjadwalkan cek rutin sistem jaringan yang ada termasuk keamanannya, melakukan perbaikan terhadap trouble shooting baik pada perangkat computer maupun jaringan, melakukan back up data secara rutin, melakukan kontrol keamanan user dan data, bertanggung jawab pada seluruh proses komputerisasi perusahaan

3. Marketing

   Marketing mempunyai otorisasi serta tanggung jawab untuk membuat SO, mengakses master *file customer* perusahaan, mengakses terhadap *utility*, memiliki otorisasi untuk melakukan *input* ataupun *edit* data-data yang ada di master file

4. Gudang

   Gudang memiliki otorisasi untuk menginputkan jumlah barang yang keluar ataupun masuk ke dalam gudang perusahaan, mengakses master file tentang persediaan barang yang dimiliki oleh perusahaan, serta dapat diaksesnya *utility*.

4.1.4 Job Description terkait fungsi EDP

Bagian EDP PT. "X" terdiri dari 2 orang, yaitu :

- IT Manager

  IT Manager bertugas melakukan perencanaan serta pengotorisasian dalam pengembangan serta perawatan sistem yang terjadi di dalam perusahaan, menyusun prosedur dan kebijakan pemeliharaan dan perbaikan sistem, bertanggung jawab terhadap segala aktivitas perubahan yang terjadi dalam sistem yang ada di dalam perusahaan, menentukan kebijakan user id dan password serta pemberian batas otorisasi atas username tersebut.

  Di PT "X" fungsi IT Manager rangkap tugas dengan fungsi data library, yaitu menyimpan offsite back up. Walau fungsi data library ini juga diserahkan pada outsource, tetapi IT manager juga menyimpan offsite backup.

- Staff

  Bertugas membantu IT Manager dan melakukan pemeliharaan sistem sehari-hari, tetapi apabila tidak dapat diatasi maka staff akan lapor kepada IT Manager dan selanjutnya akan diserahkan kepada pihak outsource.

- *System Analyst and Programmer*

  Fungsi ini diserahkan pada pihak outsource dan bertugas melakukan perawatan sistem secara berkala sesuai dengan yang tertera dalam kontrak, melakukan perbaikan atas hardware apabila terjadi kerusakan serta melakukan perbaikan kesalahan akibat kegagalan sistem, melakukan pengembangan atas sistem yang dimiliki oleh perusahaan berdasarkan otorisasi dari *IT Manager, m*elakukan backup dan offsite backup secara berkala setiap dilakukannya perawatan sistem perusahaan, yang bertanggung jawab atas fungsi tugas *librarian* adalah *System Analyst and Programmer* dan IT Manager.

4.2 Deskripsi Data

4.2.1 Sistem informasi PT. "X"

Pada awalnya PT. "X" masih menggunakan sistem manual dalam proses bisnisnya, hal ini disebabkan minimnya pengetahuan akan sistem komputer dan perusahaan merasa belum membutuhkannya. Seiring dengan berkembangnya teknologi, pada tahun 1998 perusahaan mulai menggunakan komputer, namun sistem yang digunakan masih sebatas *microsoft excel* dan *microsoft word* yang berfungsi untuk membantu proses pencatatan dan perhitungan data. Seiring dengan berjalannya waktu, perusahaan memperbarui sistem terkomputerisasinya yang awalnya belum terintegrasi menjadi terintegrasi dengan menggunakan software "BMP" (Business Management Process) di tahun 2002. "BMP" yang diterapkan dalam PT. X ini merupakan program dari hasil outsourcing dari perusahaan *Consulting* PT. Orlansoft. Dimana sistem yang digunakan diterapkan merupakan sistem yang terintegrasi yang menggabungkan departemen yang satu dengan yang lainnya. Adapun departemen yang terintegrasi adalah departemen Pembelian / *purchasing*, Penjualan / *marketing*, akuntansi, produksi dan bagian gudang.

PT. "X" untuk memproses data menggunakan metode client-server. Dimana setiap komputer yang ada di perusahaan dalam menginputkan data, memproses data, dan menyimpan data langsung terhubung dengan server perusahaan. Untuk operating systemnya PT. "X" menggunakan windows XP.

Sedangkan untuk masuk kedalam sistem operasi perusahaan ini yaitu program BMP para user terlebih dahulu harus melakukan prosedur *log in* dengan memasukkan *user name* dan *password*. Tiap user memiliki hak akses yang berbeda-beda. Hak akses tersebut diatur oleh bagian EDP, disesuaikan dengan kebutuhan masing-masing *user* dalam menjalankan tugasnya. User yang ada didalam perusahaan berjumlah 30 orang

4.2.2 *General Control* atas Sistem Informasi

Berikut ini adalah hasil survey atas beberapa area *general control* sistem informasi di PT. "X" berdasarkan tujuan auditnya dan di sesuaikan dengan tingkat kompleksitas IT yang diterapkan di perusahaan.

4.2.2.1 Pengendalian atas Struktur Organisasi

Tujuan audit pengendalian atas struktur organisasi adalah memastikan bahwa tiap individu dari area yang berbeda dipisahkan sesuai dengan deskripsi kerjanya berkaitan dengan tingkat resiko potensialnya, sehingga tidak ada penyalahgunaan otoritas.

Tabel 4.1 Pengendalian atas Struktur Organisasi

Standar	Bukti Audit			
	Wawancara	Observasi	Uji Coba	Dokumentasi
a. Adanya pembagian fungsi tugas yang ada dalam organisasi.	Menurut keterangan *IT* Manager, computer operator, fungsi administrasi basis data dipegang oleh ITmanager, sedangkan fungsi *computer operation* telah dipisahkan dari fungsi-fungsi lainnya. Fungsi *system analysis and programming* diserahkan kepada pihak outsource (PT Orlansoft), dan fungsi library dipegang oleh pihak outsource dan IT manager. Menurut keterangan pihak outsorce, pihaknya tidak menjalankan fungsi computer operation dan hanya datang ke perusahaan saat melakukan perawatan system dan offsite backup setiap 1 bulan.	Kebijakan perusahaan atas pemisahan tugas, yakni computer operation dan database administrator dilakukan oleh orang yang berbeda dalam perusahaan. Sedangkan programer dan maintenance dilakukan oleh outsourcing (observasi dilakukan di PT.”X”)		

Tabel 4.1 Pengendalian atas Struktur Organisasi (sambungan)

Standar	Bukti Audit			
	Wawancara	Observasi	Uji Coba	Dokumentasi
b. Adanya kebijakan pembagian fungsi serta deskripsi tugas yang ada dalam bagian EDP	Menurut keterangan *IT* Manager, terdapat deskripsi tugas divisi EDP secara tertulis tetapi didalam dokumen tersebut tidak ada pembagian fungsi secara rinci mengenai fungsi-fungsi didalamnya seperti IT Manager, data library, dsb. Tetapi menjadi satu bagian utuh, yaitu *Job Description* divisi EDP. Fungsi computer operations telah dipisahkan dari fungsi-fungsi lainnya. Sisanya yaitu programer, maintenance, diserahkan kepada pihak outsourcing. Walau dalam job description bagian edp disebutkan bertugas sebagai maintenance juga tetapi pada kenyataanya, pihak EDP lebih condong sebagai teknisi, apabila terdapat kerusakan sistem, pihak EDP tidak mengerti dan menyerahkan kepada pihak outsource.			

Berikut ini adalah deskripsi yang didapat melalui aktivitas audit atas struktur organisasi PT. "X" adalah :

1. Berdasarkan bukti audit wawancara dengan IT Manager, computer operator, dan pihak outsource. Fungsi administrasi basis data dipegang oleh ITmanager, sedangkan fungsi *computer operation* telah dipisahkan dari fungsi lainnya. Fungsi *system analysis and programming* diserahkan kepada pihak outsource (PT Orlansoft) yang bertugas melakukan perawatan sistem secara berkala sesuai dengan yang tertera dalam kontrak, melakukan perbaikan atas hardware apabila terjadi kerusakan serta melakukan perbaikan kesalahan akibat kegagalan sistem, melakukan pengembangan atas sistem yang dimiliki oleh perusahaan berdasarkan otorisasi dari *IT Manager, m*elakukan offsite backup secara berkala setiap dilakukannya perawatan sistem perusahaan. Sedang pemeliharaan sistem sehari-hari dipegang oleh bagian EDP. Tetapi apabila terdapat masalah yang tidak dapat ditangani oleh bagian EDP, maka akan menyerahkan pada pihak outsource. Selain itu, fungsi library dipegang oleh Pihak outsource (PT Orlansoft) selaku fungsi *system analysis and programming* dan juga dipegang oleh ITmanager.
2. Berdasarkan wawancara dengan *IT* Manager, terdapat deskripsi tugas divisi EDP secara tertulis tetapi didalam dokumen tersebut tidak ada pembagian fungsi secara rinci mengenai fungsi-fungsi didalamnya seperti IT Manager, data library, dsb. Tetapi menjadi satu bagian utuh, yaitu *Job Description* divisi EDP. Namun deskripsi tugas telah dimengerti oleh masing-masing pekerja yang ada. Fungsi computer operations telah dipisahkan dari fungsi-fungsi lainnya. Sisanya yaitu programer, maintenance, diserahkan kepada pihak outsourcing. Walau dalam job description bagian edp disebutkan bertugas sebagai maintenance juga tetapi pada kenyataanya, pihak EDP lebih mengarah sebagai teknisi, apabila terdapat kerusakan sistem, pihak EDP tidak mengerti dan menyerahkan kepada pihak outsource.

4.2.2.2 Pengendalian atas Pusat Komputer dan Keamanan Pusat Komputer

4.2.2.2.1 Pengendalian atas Pusat Komputer

Tujuan audit pengendalian atas pusat komputer adalah untuk memastikan bahwa pengendalian atas keamanan fisik cukup memadai untuk melindungi pusat komputer dari ancaman-ancaman fisik.

Tabel 4.2 Pengendalian atas Pusat Komputer

Standar	Bukti Audit			
	Wawancara	Observasi	Uji coba	Dokumentasi
a. Lokasi fisik pusat komputer terletak di lokasi yang aman dari bahaya buatan manusia dan alam	Menurut keterangan IT Manager, ruangan server selalu dikunci, dan kunci ruangan dipegang olehnya. Selama ini pernah terjadi lalai lupa mengunci ruangan tersebut, tetapi hal tersebut jarang terjadi.	Letak pusat komputer terletak di lantai 1 dan terkunci. Selain itu, ruang server bersebelahan dengan ruang divisi penjualan yang ramai dilalui orang.		
b. Bahan konstruksi ruang pusat komputer dinding, langit-langit dan lantai anti api serta air	Menurut keterangan IT Manager, konstruksi bangunan di ruangan pusat komputer terbuat dari bahan yang sama dengan ruangan-ruangan yang lainnya.	Adanya barang-barang yang tidak tahan api seperti kardus-kardus yang berada di pusat komputer yang sangat mudah menangkap api.		

Tabel 4.2 Pengendalian atas Pusat Komputer (sambungan)

Standar	Bukti Audit			
	Wawancara	Observasi	Uji coba	Doku-mentasi
c. Kabel listrik dan telepon telah terletak di bawah tanah		Kabel listrik diletakkan di dinding ruangan. Tetapi tidak pernah ada kejadian yang merugikan dari hal ini.		
d. Adanya pengendalian akses secara fisik. Dapat berupa penjagaan, kunci manual atau elektronik, *biometric system*, *badge system*, kamera, dan *alarm system*	Menurut keterangan IT Manager, pusat komputer di PT. "X" selalu terkunci dan kunci dipegang oleh IT Manager	Pengamanan pusat komputer di PT. "X"tidak dilengkapi dengan penempatan penjaga, *biometric system*, *badge system*, kamera, dan *alarm system*. pengendalian fisik yang diterapkan berupa *single entry point* yaitu hanya terdapat satu jalan untuk dapat melakukan akses ke dalam pusat komputer dan terkunci.		
e. Adanya pendingin ruangan dan memastikan tidak ada jendela yang terbuka sehingga pendingin ruangan mampu bekerja dengan baik	Menurut keterangan IT Manager, pusat komputer di PT. "X" dilengkapi dengan 1 unit AC, berdaya 1PK	Pusat komputer di PT. "X" dilengkapi dengan satu unit AC dan tidak terdapat jendela.		-Foto AC
f. Adanya bukti dokumentasi pendingin ruangan telah mendapat perawatan secara berkala	Menurut keterangan IT Manager, *Air condition* yang ada diservis setiap 3 bulan sekali	Kartu servis AC menunjukkan servis dilakukan 3 bln sekali		-Foto kartu servis AC

Tabel 4.2 Pengendalian atas Pusat Komputer (sambungan)

Standar	Bukti Audit			
	Wawancara	Observasi	Uji coba	Dokumentasi
g. Adanya *fire suppression*, alarm kebakaran manual, *smoke detectors*	Menurut keterangan IT Manager, pusat komputer PT. "X" tidak dilengkapi dengan *fire suppression*, alarm kebakaran manual, *smoke detectors*.	Tidak terdapatnya *fire suppression*, alarm kebakaran manual, *smoke detectors* di dalam pusat komputer PT. "X". Namun, terdapat tabung pemadam kebakaran di luar ruangan pusat		
h. Adanya perlindungan ketidakstabilan listrik berupa UPS	Menurut keterangan IT Manager, pusat komputer di PT. "X" telah dilengkapi dengan 1 buah unit UPS.	Pusat komputer di PT."X" dilengkapi dengan 1 buah unit UPS		-Foto UPS
i. Adanya asuransi atas *asset* perusahaan	Menurut keterangan Direktur, untuk pusat komputer tidak diasuransikan secara khusus, tetapi menjadi 1 dengan asuransi keseluruhan perusahaan.			-Polis asuransi

Berikut ini deskripsi yang didapat melalui aktivitas audit atas pengendalian pusat komputer adalah :

1. Berdasarkan bukti audit obervasi di ruang pusat komputer, pengamanan pusat komputer secara fisik tidak menggunakan peralatan yang modern namun hanya dengan menggunakan *single entry point* dan kunci dipegang oleh manajer IT, pernah terjadi kelalaian mengunci ruangan namun hal ini jarang terjadi. Sedangkan lokasi ruang pusat komputer perusahaan terletak di lantai 1, hal ini secara tidak langsung menimbulkan resiko kebanjiran walau hal ini tidak pernah terjadi sebelumnya. Selain itu, ruang server juga bersebelahan dengan ruang divisi penjualan yang ramai dilalui orang.
2. Berdasarkan bukti audit wawancara dengan IT Manager, konstruksi bangunan di ruangan pusat komputer terbuat dari bahan yang sama dengan ruangan-ruangan yang lainnya.

   Berdasarkan bukti audit observasi di ruang pusat komputer ditemukan adanya barang-barang yang tidak tahan api seperti kardus-kardus yang berada di pusat komputer yang sangat mudah menangkap api.
3. Berdasarkan bukti audit observasi di ruang pusat komputer terlihat bahwa kabel listrik tidak terletak di bawah tanah. Hal ini dapat memicu kebakaran jika terjadi korsleting listrik, tetapi tidak pernah terjadi peristiwa seperti ini.
4. Berdasarkan bukti audit wawancara dengan IT Manager, pusat komputer di PT. "X" selalu terkunci dan kunci dipegang oleh IT Manager Pendingin udara digunakan di setiap ruangan yang terdapat komputer, dimana hal tersebut dilakukan demi menunjang kinerja para pekerja dan juga kinerja dari komputer tersebut sehingga dapat meminimalisasikan terjadinya kerusakan komputer yang berdampak pada terhambatnya kinerja para pekerja. Berdasarkan bukti audit observasi di ruang pusat komputer, Pengamanan pusat komputer di PT. "X"tidak dilengkapi dengan penempatan penjaga, *biometric system*, *badge system*, kamera, dan *alarm system*. pengendalian fisik yang diterapkan oleh perusahaaan berupa *single entry point* yaitu hanya terdapat satu jalan untuk dapat melakukan akses ke dalam pusat komputer dan terkunci.

   Berdasarkan bukti audit dokumentasi didapat foto pusat komputer.

5. Berdasarkan bukti audit wawancara dengan IT Manager, pusat komputer di PT. “X” dilengkapi dengan 1 unit AC, berdaya 1PK.
   Berdasarkan bukti audit observasi di ruang pusat komputer terlihat bahwa pusat komputer di PT. ”X” dilengkapi dengan satu unit AC dan tidak terdapat jendela.
   Berdasarkan bukti audit dokumentasi terdapat foto AC
6. Berdasarkan bukti audit wawancara dengan IT Manager, *Air condition* yang ada diservis setiap 3 bulan sekali
   Berdasarkan bukti audit observasi di ruang pusat komputer ditemukan kartu servis AC menunjukkan servis dilakukan 3 bln sekali.
   Berdasarkan bukti audit dokumentasi, didapat foto kartu servis AC.
7. Berdasarkan bukti audit wawancara dengan IT Manager, pusat komputer PT. “X” tidak dilengkapi dengan *fire suppression*, alarm kebakaran manual, *smoke detectors*.
   Berdasarkan bukti audit observasi di ruang pusat komputer terlihat tidak adanya *fire suppression,* alarm kebakaran manual, *smoke detectors* di dalam pusat komputer PT. “X”. Namun, terdapat lat pemadam kebakaran berada di lantai 1 tetapi terletak di luar ruang pusat komputer.
8. Berdasarkan bukti audit wawancara dengan IT Manager, pusat komputer di PT. “X” telah dilengkapi dengan 1 buah unit UPS. Berdasarkan bukti audit observasi terlihat adanya i unit UPS. Berdasarkan bukti dokumentasi adanya foto UPS yang terpakai.
   Semua komputer yang terhubung dengan sistem dilengkapi dengan *UPS,* dimana dengan adanya *UPS* maka *computer user* masih sempat melakukan penyimpanan data dan kemudian mematikan komputer. Pusat komputer juga dilengkapi dengan *UPS* dimana hal tersebut juga bertujuan untuk dapat dilaksanakannya proses menyimpan data yang telah diinputkan dan juga menjaga agar *hardware* komputer tidak mengalami kerusakan akibat tegangan yang tidak stabil tersebut.

9. Berdasarkan bukti audit wawancara dengan Direktur, untuk pusat komputer tidak diasuransikan secara khusus, melainkan menjadi satu dengan asuransi keseluruhan perusahaan. Berdasarkan bukti audit dokumentasi adanya dokumen polis asuransi perusahaan.

4.2.2.2.2 Pengendalian atas *DRP*

Tujuan audit pengendalian atas Disaster Recovery Planning adalah untuk melakukan pencegahan serta pemulihan sistem atas kemungkinan terjadinya kerusakan ataupun kehilangan data yang mana hal tersebut mungkin disebabkan oleh adanya penghapusan ataupun kerusakan.

Tabel 4.3 Pengendalian *Disaster Recovery Planning*

Standart	Bukti Audit			
	Wawancara	Observasi	Uji coba	Dokumentasi
a. Adanya kebijakan tentang prosedur dalam pemulihan sistem dan siapa yang bertanggung jawab	Menurut keterangan IT Manager, tidak terdapat kebijakan tentang langkah-langkah dalam pemulihan sistem dan siapa yang bertanggung jawab jika terjadi bencana. Namun perusahaan telah memiliki kontrol pengganti yaitu melakukan back up data. *Off site back up* dilakukan oleh manager IT setiap hari jumat dan oleh pihak outsource setiap bulannya. Selain itu dari wawancara dengan manager IT juga didapat keterangan bahwa selama ini perusahaan tidak pernah mengalami bencana alam didaerah tersebut. Lingkungan perusahaan merupakan daerah industri.	Lingkungan perusahaan merupakan daerah industri.		

Berikut ini deskripsi yang didapat melalui aktivitas audit pengendalian atas DRP adalah :

- Berdasarkan wawancara dengan IT manager, tidak adanya kebijakan prosedur DRP yang diterapkan oleh perusahaan.

4.2.2.3 Pengendalian atas Manajemen Data

Tujuan audit atas pengendalian Manajemen Data adalah memastikan bahwa kontrol terhadap manajemen data sudah cukup untuk menjaga integritas dan keamanan fisik basis data yaitu cadangan file data sudah memadai untuk memfasilitasi pemulihan ketika terjadi hal yang tidak diinginkan, individu yang telah diberi otorisasi telah menggunakan basis data secara terbatas, individu yang tidak memiliki otoritas ditolak aksesnya.

Tabel 4.4 Pengendalian atas Manajemen Data

Standart	Bukti Audit			
	Wawancara	Observasi	Uji coba	Dokumentasi
a. Individu dapat mengakses file sesuai dengan otoritasnya	Menurut keterangan IT manager *User*ID dan *password* yang diminta pada waktu ingin mengakses ke program aplikasi menentukan sampai *file* mana *user* boleh mengakses *file* yang ada dalam *database*.. Menurut computer operator, pihaknya tidak dapat mengakses data yang berada di luar otoritasnya.	*Computer operator* tidak dapat membuka file yang bukan otoritasnya. Adanya tampilan yang mengatakan user tidak memiliki akses.		- *Access Control Matrix*
b. Adanya fitur kontrol lain untuk menghentikan akses	Menurut keterangan IT Manager, fitur kontrol perusahaan hanya pada *user*Id dan *password*. Tidak ada kontrol lain seperti	Tidak ada fitur *biometric device*.		

Tabel 4.4 Pengendalian atas Manajemen Data (sambungan)

Standart	Bukti Audit			
	Wawancara	Observasi	Uji coba	Dokumentasi
yang tidak terotorisasi jika *user*ID dan *password* tertembus	*biometric device* dan sebagainya. *Password control* di perusahaan juga sangat lemah (*password control* lebih lanjut dibahas dalam pengendalian sistem operasi).			
c. Adanya prosedur *backup* yang ditetapkan perusahaan	Menurut keterangan IT Manager setelah data diproses akan langsung tersimpan ke *server*. Data dalam *server* akan di *back up* setiap hari jumat oleh pihak EDP, dan tiap 1 bulan oleh pihak outsource. Menurut pihak outsource, pihaknya melakukan backup dan *offsite back up* tiap bulannya.	Saat observasi terlihat proses *back up* data		Print screen logs backup database. Terdapat jobdesc tertulis backup dilakukan secara rutin namun tidak terdapat dokumen tertulis atas rincian prosedur aturan aktivitas backup

Tabel 4.4 Pengendalian atas Manajemen Data (sambungan)

Standart	Bukti Audit			
	Wawancara	Observasi	Uji coba	Dokumentasi
d. Kepastian lokasi *backup* telah terpisah	Menurut keterangan IT Manager *Back-up* di PT. "X" ini ditempatkan secara terpisah (*offsite)*. Data back up disimpan di usb dan dibawa oleh IT Manager dan pihak outsource. Menurut pihak outsource, backup tiap bulan ilakukan dan ditempatkan di lokasi terpisah.	USB dibawa oleh IT Manager (Bapak Roy) dan bapak Agus selaku pihak outsource.		
e. Adanya cadangan hardware yang dapat digunakan sewaktu-waktu.	Menurut keterangan IT Manager dimilikinya 2 (dua) buah komputer cadangan yang diletakkan di ruangan pusat komputer yang dapat digunakan terlebih dahulu sebagai *backup* apabila terdapat komputer yang mengalami kerusakan *hardware* dan masih harus menunggu pihak outsourcing	Terdapat 2 buah hardisk cadangan yang tidak terpakai.		

Berikut ini deskripsi yang didapat melalui aktivitas audit pengendalian atas pengendalian manajemen data adalah :

1. Berdasarkan bukti audit wawancara dengan IT Manager, *User*ID dan *password* yang diminta pada waktu ingin mengakses ke program aplikasi menentukan sampai *file* mana *user* boleh mengakses *file* yang ada dalam *database*. Berdasarkan bukti audit

wawancara dengan computer operator, pihaknya tidak dapat mengakses data yang berada di luar otoritasnya. Berdasarkan bukti audit observasi terlihat bahwa *Computer operator*tidak dapat membuka file yang bukan otoritasnya.

Bukti audit dokumentasi berupa *access control matrix*, dimana setiap *computer operator* hanya dapat mengakses *file* yang mereka perlukan saja. Seperti yang terlampir dalam lampiran, acces control matrix yang terlihat adalah berisi kontrol akses atas nama siapa saja yang dapat mengakses ke dalam data inventory master list.

2. Berdasarkan bukti audit wawancara dengan IT Manager, fitur kontrol perusahaan hanya pada *user*Id dan *password*. Tidak ada kontrol lain seperti *biometric device* dan sebagainya. *Password control* di perusahaan juga sangat lemah (*password control* lebih lanjut dibahas dalam pengendalian sistem operasi).Berdasarkan bukti audit observasi tidak ditemukan adanya fitur *biometric device*.
3. Berdasarkan bukti audit wawancara dengan IT Manager, setelah data diproses akan langsung tersimpan ke *server*. Data dalam *server* akan di *back up* setiap hari jumat oleh pihak EDP, dan tiap 1 bulan oleh pihak outsource.

   Berdasarkan bukti audit wawancara dengan pihak outsource, pihaknya melakukan backup dan *offsite back up* tiap bulannya.Setelah data diproses, data akan secara otomatis tersimpan ke *server* dan data tersebut tidak dapat dibuka oleh *computer user*.

   Berdasarkan bukti audit observasi terlihat proses back up data.

   Berdasarkan bukti audit dokumentasi terdapat print screen logs backup database.
4. Berdasarkan bukti audit wawancara dengan IT Manager, *Back-up* di PT. “X” ini ditempatkan secara terpisah (*offsite)*. Data back up disimpan di usb dan dibawa oleh IT Manager dan pihak outsource. Berdasarkan bukti audit wawancara dengan pihak outsource, backup tiap bulan ilakukan dan ditempatkan di lokasi terpisah.

   Berdasarkan bukti audit observasi terlihat bahwa usb dibawa oleh IT Manager (Bapak Roy) dan bapak Agus selaku pihak outsource.

5. Berdasarkan bukti audit wawancara dengan IT Manager, dimilikinya 2 (dua) buah komputer cadangan yang diletakkan di ruangan pusat komputer yang dapat digunakan terlebih dahulu sebagai *backup* apabila terdapat komputer yang mengalami kerusakan *hardware* dan masih harus menunggu pihak outsourcing.

Berdasarkan bukti audit observasi terlihat adanya 2 komputer cadangan. Perusahaan tidak memiliki orang yang bertanggung jawab secara khusus atas kerusakan hardware yang dialami oleh komputer yang ada di perusahaan. Hal tersebut dikarenakan adanya kontrak dengan pihak outsourcing yang mana perbaikan atas kerusakan hardware tersebut merupakan tanggung jawab dari pihak outsourcing. Walaupun tidak memiliki divisi ataupun orang yang bertanggung jawab secara khusus atas kerusakan hardware, perusahaan memiliki backup komputer sebanyak 2 (dua) komputer yang diletakkan di dalam ruangan pusat komputer yang dapat digunakan sewaktu terjadi kerusakan hardware dan selama komputer sedang dalam tahap perbaikan.

4.2.2.3 Pengendalian atas Sistem Operasi

Tujuan audit atas sistem operasi adalah :

a. Memastikan pemberian hak akses yang konsisten dengan kebutuhannya untuk memisahkan fungsi-fungsi yang berbeda sesuai dengan kebijakan perusahaan.

Tabel 4.5 Hak Akses atas *File* dan *Program*

Standar	Bukti Audit			
	Wawancara	Observasi	Uji coba	Dokumentasi
a. Adanya proses *log on* untuk masuk ke	Menurut keterangan *computer operator*, prosedur log on dilakukan	Saat log on ke sistem operasi akan muncul	Uji coba dilakukan dengan memasukkan *password* dan	- *print screen* prosedur *log on*

Tabel 4.5 Hak Akses atas *File* dan *Program* (sambungan)

Standar	Bukti Audit			
	Wawancara	Observasi	Uji coba	Dokumentasi
dalam sistem operasi.	saat akan akses ke dalam sistem operasi yaitu dengan memasukkan *user name* dan *password*	tampilan *user name* dan *password.*	*username* yang tidak tepat dan tidak dapat masuk ke dalam program aplikasi	
b. Adanya pesan jika proses *log on* gagal	Menurut keterangan computer operator, jika proses log on gagal maka akan keluar kotak pemberitahuan.	Terlihat kotak pemberitahuan "*invalid login*" apabila password yang dimasukkan salah	Saat uji coba memasukkan password yang salah ada tampilan kotak "*invalid login*"	- *printscreen* kotak pemberitahuan "invalid login"
c. Adanya kontrol yang mengatur otorisasi akses untuk masuk ke sistem operasi.	Menurut keterangan IT manager, hak akses ke program aplikasi BMP hanya diberikan kepada user-user yang terlibat. Hal ini telah diatur dalam *acces control matrix.* *keterangan mengenai acces control matrix ada di deskripsi.	Computer operator tidak dapat membuka modul yang bukan merupakan hak aksesnya, akan adanya tampilan yang mengatakan user tidak memiliki akses.		-*Acces control matrix*

b. Memastikan bahwa perusahaan memiliki *password control* yang memadai dan efektif untuk mengendalikan akses ke sistem operasional.

Tabel 4.6 *Password Control*

Standar	Bukti Audit			
	Wawancara	Observasi	Uji coba	Dokumentasi
a. Adanya kontrol yang menjaga kerahasiaan password	Menurut keterangan IT manager dan computer operator, di PT. "X hanya adanya *hide password* namun tidak adanya kontrol lain yang menjamin kerahasiaan *password*	Adanya *hide password* saat memasukkan *password*	Uji coba dilakukan dengan memasukkan *password* dan *password* tampil secara *hide*.	
b. Adanya kebijakan mengenai masa aktif *user ID dan password*	Menurut keterangan IT Manager tidak ada prosedur tertulis mengenai penghapusan *user name* dan *password*, tetapi apabila ada karyawan yang keluar maka bagian HRD akan memberitahu bagian EDP agar dapat menghapusnya. Menurut keterangan divisi HRD, adanya pemberitahuan kepada divisi EDP saat ada computer operator yang keluar dari perusahaan.			

Tabel 4.6 *Password Control* (sambungan)

Standar	Bukti Audit			
	Wawancara	Observasi	Uji coba	Dokumentasi
c. Adanya kebijakan jumlah *digit password* dan pembatasan percobaan *entry password*	Menurut keterangan IT Manager, password dibuat berdasarkan keinginan dari karyawan tetapi sesuai persetujuan IT manager. Selain itu, tidak ada batasan pemasukan password		Uji coba dilakukan dengan memasukkan password yang salah dan tidak ada batasan pemasukan password walau berulang-ulang salah.	

c. Memastikan adanya kebijakan dan prosedur manajemen yang efektif untuk mencegah masuk dan menyebarnya program yang bersifat merusak.

Tabel 4.7 Pengendalian atas Virus

Standar	Bukti Audit			
	Wawancara	Observasi	Uji coba	Dokumentasi
a. Adanya antivirus yang digunakan oleh perusahaan	Menurut keterangan IT Manager, PT. "X" menggunakan anti virus Smadav2010			-Tampilan anti virus Smadav2010
b. Adanya kebijakan untuk pencegahan masuknya virus	Menurut keterangan IT Manager, Setiap karyawan melakukan *scan* pada setiap		Saat flash disk dimasukkan scan secara otomatis dimulai	

Tabel 4.7 Pengendalian atas Virus (sambungan)

Standar	Bukti Audit			
	Wawancara	Observasi	Uji coba	Dokumentasi
	penggunaan *flash disc*, atau *hardware* lain. *Scan* dilakukan secara berkala setiap 1 minggu sekali. Menurut keterangan computer operator, scan secara otomatis berjalan saat memasukkan USB.			
c. Digunakannya anti virus yang kompeten	Menurut keterangan IT Manager, anti virus yang digunakan adalah Smadav *free charge demo* yang didapatkan secara gratis ketika membeli komputer. Anti virus ini tidak berlangganan dan tidak mampu mendeteksi virus jenis baru (.TR, .m3x) sehingga membuat data terkorupsi dan hilang.			
d. Adanya kebijakan tentang *update* anti virus secara berkala	Menurut keterangan IT Manager, anti virus yang dipakai tidak dapat melakukan *update* karena tidak berlangganan.			

d. Memastikan bahwa pemeriksaan dan pengawasan terhadap *users* dan *events* cukup memadai untuk mencegah dan mendeteksi penyalahgunaan sistem.

Tabel 4.8 Pengendalian atas Jejak Audit (*Audit trail*)

Standar	Bukti Audit			
	Wawancara	Observasi	Uji coba	Dokumentasi
a. Adanya *audit logs* untuk melihat aktivitas karyawan	Menurut keterangan IT Manager, adanya *Audit Log* dalam sistem namun tidak digunakan oleh perusahaan dikarenakan terlalu rumit dalam proses membaca *audit log*. *Audit logs* tidak direview apabila pihak EDP merasa tidak ada hal yang janggal. Namun pihak EDP tidak dapat mengakses *audit log* tanpa bantuan pihak *outsourcing*.			Print Screen *Audit Log*

e. Memastikan bahwa perusahaan menerapkan tingkat *fault tolerance* yang tepat

Tabel 4.9 Pengendalian atas *Fault Tolerance*

Standar	Bukti Audit			
	Wawancara	Observasi	Uji coba	Dokumentasi
a. Adanya prosedur yang menanggulangi pemadaman listrik	Menurut IT Manager, perusahaan memiliki *diesel genset* untuk mengaktifkan kembali aliran listrik sementara. Perusahaan juga memiliki UPS untuk mematikan komputer secara normal ketika sumber listrik padam.	*Diesel genset* terletak di gudang . *Genset* tidak menyala otomatis ketika listrik mati, *genset* harus dinyalakan secara manual.		

Berikut deskripsi yang didapat melalui aktivitas audit pengendalian atas sistem operasi adalah :

1. Berdasarkan bukti audit wawancara dengan *computer operator*, prosedur log on dilakukan saat akan akses ke dalam sistem operasi yaitu dengan memasukkan *user name* dan *password* . berdasarkan bukti audit observasi terlihat saat akan masuk ke system operasi muncul kotak prosedur untuk memasukkan user name dan password. Berdasarkan bukti audit uji coba dilakukan dengan memasukkan *password* dan *username* yang tidak tepat dan tidak dapat masuk ke dalam program aplikasi. Berdasarkan bukti audit dokumentasi terdapat print screen tampilan prosedur log on.
2. Berdasarkan bukti audit wawancara dengan computer operator, jika proses log on gagal maka akan keluar kotak pemberitahuan. Berdasarkan bukti audit observasi terlihat kotak pemberitahuan "*invalid login*" apabila password yang dimasukkan salah.

Berdasarkan bukti audit uji coba saat memasukkan password yang salah ada tampilan kotak "*invalid login*". Berdasarkan bukti audit dokumentasi terdapat print screen kotak "*invalid login*".

3. Berdasarkan bukti audit wawancara dengan pihak outsource, hak akses ke program aplikasi BMP hanya diberikan kepada user-user yang terlibat. Hal ini telah diatur dalam *acces control matrix.*

   Berdasarkan bukti dokumen terdapatnya *acces control matrix.* Pengendalian terhadap hak akses telah diatur dalam *access control matrix*. Dalam *access control matrix* telah diatur batasan-batasan mengenai hak akses ke program aplikasi yang disesuaikan dengan kebutuhan *user* untuk mengerjakan tugas masing-masing.

   Berdasarkan bukti audit observasi, komputer operator tidak dapat membuka modul yang bukan merupakan hak aksesnya, akan adanya tampilan yang mengatakan user tidak memiliki akses.

   *keterangan mengenai *access control matrix*

   access control matrix yang terdapat di lampiran bukan berupa table hak akses yang secara detail menjelaskan seorang user dapat mengakses modul apa saja. Namun, harus terlebih dahulu masuk ke dalam modul, seperti yang tertera di lampiran modul inventory master list. Setelah membuka modul tersebut baru terlihat siapa saja yang dapat mengakses ke dalam modul tersebut. Didalam set user access terdapat operator name, acces, insert, change, delete, resetflg, all. Access adalah keterangan bahwa diperbolehkan atau tidaknya operator masuk ke dalam modul tersebut, insert adalah keterangan boleh tidaknya operator menginputkan data, change adalah keterangan boleh tidaknya operator mengubah data, delete adalah keterangan boleh tidaknya operator menghapus data, reset flg adalah keterangan boleh tidaknya operator mengakses data yang telah ditutup, seperti data 3 bulan lalu, all adalah keterangan boleh tidaknya operator mengakses semua data.

4. Berdasarkan bukti audit wawancara dengan IT Manager di PT. “X hanya adanya *hide password* namun tidak adanya kontrol lain yang menjamin kerahasiaan, sehingga orang lain tidak dapat melihat password apa yang dimasukkan. Berdasarkan wawancara dengan computer operator, pihaknya menyatakan bahwa memang terdapat *hide password*. Berdasarkan bukti audit observasi terlihat saat *computer operator* mencoba memasukkan password, password terhide. Bukti audit uji coba adalah saat dimasukkan password, yang tampil di layar adalah tampilan *** sebagai *hide password*. Namun tidak terdapat control lain yang menjamin kerahasiaan password.
5. Berdasarkan bukti audit wawancara dengan IT Manager tidak ada prosedur tertulis mengenai penghapusan *user name* dan *password*, tetapi apabila ada karyawan yang keluar maka bagian HRD akan memberitahu bagian EDP agar dapat menghapusnya. Berdasarkan bukti audit wawancara dengan divisi HRD, adanya pemberitahuan kepada divisi EDP saat ada computer operator yang keluar dari perusahaan.
6. Berdasarkan bukti audit wawancara dengan IT Manager, password Tidak adanya kebijakan jumlah digit *userID* serta *password* yang ada di dalam perusahaan dan penentuan password sesuai keinginan karyawan tetapi tetap disetujui oleh IT Manager, dimana hanya IT Manager yang dapat membuat, mengubah, menghapus serta memberikan otorisasi atas *username* serta *password.* Selain itu, tidak ada batasan pemasukan password.

   Bukti audit uji coba adalah dengan memasukkan password yang salah dan tidak ada batasan pemasukan password walau berulang-ulang salah.
7. Berdasarkan bukti audit wawancara dengan IT Manager, PT. “X” menggunakan anti virus Smadav2010. Bukti audit dokumentasi terdapatnya Tampilan anti virus Smadav2010

8. Berdasarkan bukti audit wawancara dengan IT Manager, Setiap karyawan melakukan *scan* pada setiap penggunaan *flash disc*, atau *hardware* lain. *Scan* keseluruhan computer dilakukan secara berkala setiap 1 minggu sekali. Berdasarkan bukti audit wawancara dengan computer operator, scan secara otomatis berjalan saat memasukkan usb.
   Berdasarkan bukti audit uji coba adalah berjalannya scan otomomatis saat usb dimasukkan.
9. Berdasarkan bukti audit wawancara dengan IT Manager, anti virus yang digunakan adalah Smadav *free charge demo* yang didapatkan secara *free* atas pembelian komputer dari *vendor*. Anti virus ini tidak berlangganan dan tidak mampu mendeteksi virus jenis baru (.TR, .m3x) sehingga membuat data terkorupsi dan hilang.
10. Berdasarkan bukti audit wawancara dengan IT Manager, anti virus yang dipakai tidak dapat melakukan *update* karena tidak berlangganan.
11. Berdasarkan bukti audit wawancara dengan IT Manager, adanya *Audit Log* dalam sistem namun tidak digunakan oleh perusahaan dikarenakan terlalu rumit dalam proses membaca *audit log*. *Audit logs* tidak direview apabila pihak EDP merasa tidak ada hal yang janggal. Pihak EDP tidak dapat mengakses *audit log* tanpa bantuan pihak *outsourcing*. Namun selama ini tidak pernah ada hal yang janggal sehingga perusahaan tidak merasa perlu melakukan review.
12. Berdasarkan bukti audit wawancara dengan IT Manager ,perusahaan memiliki *diesel genset* sebagai fitur toleransi kesalahan ketika aliran listrik mati. Tetapi *genset* ini tidak secara otomatis menyala ketika aliran listrik mati. *Genset* harus dinyalakan secara manual. Perusahaan juga memiliki UPS untuk mematikan komputer secara normal ketika sumber listrik padam. Berdasarkan bukti audit observasi, didapati *diesel genset* terletak di gudang.

4.2.2.4 Pengendalian atas Pengembangan dan Pemeliharaan Sistem

Tujuan audit atas pemeliharaan sistem adalah memastikan prosedur pemeliharaan program melindungi aplikasi dari perubahan yang tidak terotorisasi dan memastikan bahwa program terbebas dari *material error*.

Tabel 4.10 Pengendalian atas Pengembangan dan pemeliharaan Sistem

Standar	Bukti Audit			
	Wawancara	Observasi	Uji coba	Dokumentasi
a. Adanya kepastian bahwa aktivitas perubahan program dan perawatan sistem merupakan aktivitas yang terotorisasi	Menurut keterangan IT Manager, apabila dia menerima keluhan atas sistem dari user, maka IT manajer akan mencatatnya dan memberikannya kepada pihak outsourcing agar diperbaiki, catatan tersebut dibawa oleh pihak outsourcing. Namun, tidak terdapat bukti prosedur secara tertulis yang mengindikasikan adanya otorisasi, hanya berupa lisan dan catatan saja. Setiap perubahan program harus dilakukan di komputer server. Akses ke komputer *server* dilindungi dengan *password*. Hanya pihak EDP dan pihak outsource yang mengetahui *password* ini.			

Tabel 4.10 Pengendalian atas Pengembangan dan pemeliharaan Sistem (sambungan)

Standar	Bukti Audit			
	Wawancara	Observasi	Uji coba	Dokumentasi
	Jadi setiap aktivitas perubahan program dan perawatan sistem diawasi secara langsung oleh pihak EDP			
b. Adanya aktivitas perawatan system secara berkala	Menurut keterangan IT Manager, terdapat aktivitas perawatan sistem secara berkala setiap bulan yang dilakukan oleh PT. Orlansoft selaku *System Analyst and Programmer*.Menurut keterangan pihak outsource, pihaknya datang tiap bulan untuk melakukan perawatan sistem.	Observasi dilakukan saat PT. Orlansoft selaku *System Analyst and Programmer* datang ke perusahaan.		
c. Adanya dokumentasi atas aktivitas perubahan program dan perawatan system	Menurut keterangan IT Manager, Awal penerapan sistem di tahun 2002 dokumentasi dilakukan, saat ini proses dokumentasi perubahan tidak dilakukan lagi dan hanya dilakukan secara lisan saja. Menurut pihak outsource, dokumentasi mengenai perawatan sistem disimpan oleh pihaknya.			

Berikut deskripsi yang didapat melalui aktivitas audit pengendalian atas pemeliharaan sistem adalah :

1. Berdasarkan bukti audit wawancara dengan IT Manager, apabila dia menerima keluhan atas sistem dari user, maka IT manajer akan mencatatnya dan memberikannya kepada pihak outsourcing agar diperbaiki, catatan tersebut dibawa oleh pihak outsourcing. setiap perubahan program harus dilakukan di komputer server. Akses ke komputer *server* dilindungi dengan *password*. Hanya pihak EDP dan pihak outsource yang mengetahui *password* ini. Jadi setiap aktivitas perubahan program dan perawatan sistem diawasi secara langsung oleh pihak EDP.
2. Berdasarkan bukti audit wawancara dengan IT Manager, terdapat aktivitas perawatan sistem secara berkala setiap bulan yang dilakukan oleh PT. Orlansoft selaku *System Analyst and Programmer*.

   Berdasarkan bukti audit wawancara dengan pihak outsource, pihaknya datang tiap bulan untuk melakukan perawatan sistem.

   Berdasarkan bukti audit bservasi dilakukan saat teknisi PT. Orlansoft selaku *System Analyst and Programmer* datang ke perusahaan.
3. Berdasarkan bukti audit wawancara dengan IT Manager, Menurut keterangan IT Manager, Awal penerapan sistem di tahun 2002 dokumentasi dilakukan, saat ini proses dokumentasi perubahan tidak dilakukan lagi dan hanya dilakukan secara lisan saja. Menurut pihak outsource, dokumentasi mengenai perawatan sistem disimpan oleh pihaknya.

   Aktivitas maintenance dilakukan secara rutin oleh PT. Orlansoft selaku *System Analyst and Programmer* setiap bulan, hal tersebut dilakukan untuk menjaga supaya sistem tetap terawat dan dapat beroperasi dengan baik. Dimana dokumentasi atas sistem tersebut disimpan oleh pihak outsourcing dan bukan pihak PT. X.

4.2.2.5 Pengendalian atas Jaringan dan Internet

Tujuan audit dari pengendalian atas jaringan dan internet adalah untuk memastikan keamanan dan integritas, juga mencegah dan mendeteksi akses tidak sah penggunaan internet.

Tabel 4.11 Pengendalian atas Jaringan dan Internet

Standart	Bukti Audit			
	Wawancara	Observasi	Uji coba	Dokumentasi
a. Ada pengendalian pencegahan dan pendeteksi terhadap akses ilegal penggunaan jaringan dan internet	Menurut keterangan IT Manager, perusahaan memperbolehkan semua user akses dan terhubung ke internet, Untuk masuk ke jaringan internet, *user* tidak harus memasukkan *user*Id dan *password.* Menurut computer operator, tidak adanya permintaan memasukkan userID dan password untuk masuk ke jaringan internet.		*User*Id dan *password* hanya digunakan untuk akses ke sistem. Untuk akses ke internet dapat dilakukan langsung ketika menyalakan komputer.	
b. Adanya pemakaian anti virus yang kompeten		Digunakannya anti virus smadav2010 yang merupakan *free charge demo*		

Berikut deskripsi yang didapat melalui aktivitas audit pengendalian atas Jaringan dan Internet adalah :

1. Berdasarkan bukti audit wawancara dengan IT Manager, semua komputer diperusahaan telah terhubung ke internet, untuk masuk ke jaringan internet, *user* tidak harus memasukkan *user*Id dan *password*.

   Berdasarkan bukti audit wawancara dengan computer operator, tidak adanya permintaan memasukkan userID dan password untuk masuk ke jaringan internet.Tidak ada prosedur pencegahan dan pendeteksi terhadap akses ilegal penggunaan jaringan internet. Semua komputer diperusahaan telah terhubung keinternet, Untuk masuk ke jaringan internet, *user* tidak harus memasukkan *user*Id dan *password*.
2. Berdasarkan bukti audit uji coba adanya pemakaian anti virus Smadav2010. Tetapi antivirus ini dianggap kurang kompeten untuk mengatasi virus-virus jenis baru.

4.3 Analisa dan Pembahasan

Di dalam analisa dan pembahasan terdapat dua kriteria penilaian yang digunakan, yaitu:

- Sesuai

  Suatu pengendalian dikatakan sesuai, apabila kondisi dari standar telah terpenuhi berdasarkan bukti-bukti yang diperoleh. Dengan asumsi memperhatikan kondisi perusahaan terlebih dahulu, kemudian akan disesuaikan dengan standart untuk memenuhi tujuan perusahaan.

- Tidak sesuai

  Suatu pengendalian dikatakan tidak sesuai, apabila kondisi dari standart tidak terpenuhi dan tidak tercapainya tujuan pengendalian perusahaan berdasarkan bukti-bukti yang diperoleh.

4.3.1. Pengendalian atas Struktur Organisasi

Dari 2 standar, terdapat 1 yang tidak sesuai

1. Berhubungan dengan standar adanya pembagian fungsi tugas yang ada dalam organisasi tidak sesuai. Berdasarkan bukti audit wawancara dengan IT Manager, pihak *outsource,* ditemukannya ada rangkap tugas antara fungsi *system analysis and programming* dengan fungsi *information system library*. Pihak outsource bertanggung jawab melakukan *offsite back up* setiap bulannya sekaligus melakukan perawatan terhadap system. Sedangkan kondisi didalam perusahaan telah memiliki manajer IT, yang juga bertanggung jawab melakukan *offsite backup*. Hal ini dapat menimbulkan resiko terancamnya keberadaan data perusahaan (data *leakage*) sebab data dipegang oleh pihak luar.
2. Berhubungan dengan standar adanya kebijakan pembagian fungsi dan tugas yang ada dalam bagian EDP telah sesuai. Berdasarkan wawancara dengan *IT* Manager dan observasi terdapat 2 orang yang bertugas didalam divisi EDP yaitu IT manager dan staff. Terdapat deskripsi tugas divisi EDP secara tertulis tetapi didalam dokumen tersebut tidak ada pembagian fungsi secara rinci mengenai fungsi-fungsi didalamnya seperti IT Manager, data library,

dsb. Tetapi menjadi satu bagian utuh, yaitu *Job Description* divisi EDP. Namun didalam perusahaan deskripsi tugas telah dimengerti oleh masing-masing pekerja yang ada sehingga tugas dapat dilaksanakan dengan baik.

4.3.2 Pengendalian atas pusat komputer dan Keamanan Pusat Komputer

4.3.2.1 Pengendalian atas pusat komputer

Dari 9 standar terdapat 2 yang tidak sesuai.

1. Berhubungan dengan standar lokasi fisik pusat komputer terletak di lokasi yang aman dari bahaya buatan manusia dan alam tidak sesuai. Berdasarkan bukti audit obervasi, ruang pusat komputer terletak di lantai 1. Kondisi perusahaan berada di lokasi kawasan industri yang jarang terjadi banjir, gempa, hanya memiliki 1 server saja, namun pusat komputer terletak disebelah divisi penjualan, banyak orang yang lalu-lalang melewati ruang server, sedangkan pengendalian fisik hanya berupa pintu yang terkunci. Didukung pula dengan pernah terjadinya kelalaian manajer IT lupa dalam mengunci rung server walau hal ini jarang terjadi, sehingga beresiko orang yang tidak mempunyai hak dapat masuk ke dalam ruang server apabila ruang server lupa dikunci. Selain itu perusahaan memiliki ruang kosong di lantai 2, disebelah ruang direktur, dan jarang dilewati karyawan. Sehingga ruang kosong ini sebenarnya dapat dimanfaatkan sebagai ruang server sebab lokasi dapat lebih aman.
2. Berhubungan dengan standar bahan konstruksi ruang pusat komputer dinding, langit-langit dan lantai anti api serta air tidak sesuai namun tidak signifikan. Walau berdasarkan bukti audit wawancara dengan IT Manager dan observasi ruang pusat komputer konstruksi bangunan di ruangan pusat komputer terbuat dari bahan yang sama dengan ruangan-ruangan yang lainnya dan adanya barang-barang yang tidak tahan api seperti kardus-kardus yang berada di pusat komputer yang sangat mudah menangkap api. Namun, selain karena biaya yang mahal, perusahaan juga hanya mempunyai 1 server, ruangnya tidak terlalu besar, dan terdapat tabung pemadam di lokasi yang dekat dengan pusat komputer, jika terjadi sesuatu

yang tidak diinginkan, akan mudah dilakukan penyelamatan. Sehingga berhubungan dengan standart ini tidak signifikan terhadap perusahaan.

3. Berhubungan dengan standar kabel listrik dan telepon telah terletak di bawah tanah tidak sesuai namun tidak signifikan. Namun, berdasarkan bukti audit observasi di ruang pusat komputer hanya terdapat 1 server saja, dan kabel yang ada hanya sedikit, selain itu juga tidak pernah terjadi peristiwa korsleting yang menyebabkan kebakaran sehingga berhubungan dengan standart ini tidak signifikan untuk perusahaan.
4. Berhubungan dengan standar adanya pengendalian akses secara fisik yang berupa penjagaan, kunci manual atau elektronik, *biometric system*, *badge system*, kamera, dan *alarm system* tidak sesuai. Walau berdasarkan bukti audit wawancara dengan IT Manager dan observasi pusat komputer di PT. "X" selalu terkunci dan kunci dipegang oleh IT Manager namun pusat komputer PT "X" terletak dilokasi yang dilalui oleh banyak orang, jika IT manager lalai mengunci ruangan dapat memperbesar resiko adanya org yang tidak mempunyai hak akses masuk ke dalam ruang server dan melakukan tindak kecurangan. Sehingga diperlukannya pengendalian akses fisik lain seperti kamera, selain itu dilihat dari sisi harga kamera yang relatif murah dan tidak memberatkan perusahaan.
5. Berhubungan dengan standar adanya pendingin ruangan telah sesuai. Berdasarkan bukti observasi pusat komputer di PT. "X" dilengkapi dengan 1 unit AC, berdaya 1PK dan tidak terdapat jendela. Hal ini meminimalisasi resiko komputer panas dan ruangan yang lembab.
6. Berhubungan dengan standar adanya bukti dokumentasi pendingin ruangan telah mendapat perawatan secara berkala telah sesuai. Berdasarkan bukti audit wawancara dengan IT Manager,observasi,dan dokumentasi *Air condition* yang ada diservis setiap 3 bulan sekali
7. Berhubungan dengan standar adanya *fire suppression*, alarm kebakaran manual, *smoke detectors* telah sesuai. Berdasarkan bukti observasi, walau pusat computer PT. "X" tidak dilengkapi dengan *fire suppression*, alarm kebakaran manual, *smoke detectors*. Namun terdapat tabung pemadam

kebakaran berada di lantai 1 dan letaknya berdekatan dengan ruang pusat computer. Hal ini dianggap sesuai karena di ruang pusat computer juga hanya terdapat 1 server saja, sehingga upaya penyelamatan apabila terjadi kebakaran mudah diatasi.

8. Berhubungan dengan standar adanya perlindungan ketidakstabilan listrik berupa UPS telah sesuai. Berdasarkan bukti observasi dan dokumentasi, pusat komputer di PT. "X" telah dilengkapi dengan 1 buah unit UPS.
9. Berhubungan dengan standar adanya asuransi atas *asset* perusahaan tidak sesuai namun tidak signifikan. Berdasarkan bukti audit wawancara dengan Direktur dan dokumentasi, untuk pusat komputer tidak diasuransikan secara khusus, melainkan menjadi satu dengan asuransi keseluruhan perusahaan. Namun, berdasarkan kondisi perusahaan yang hanya memiliki 1 server, dan perusahaan menilai akan membutuhkan biaya yang besar jika hanya mengasuransikan pusat computer maka untuk kapasitas perusahaan ini standart adanya asuransi tidak signifikan.

4.3.2.2 Pengendalian atas *DRP*

Berhubungan dengan standar adanya kebijakan tentang prosedur dalam pemulihan sistem dan siapa yang bertanggung jawab dinilai tidak sesuai namun tidak signifikan. Berdasarkan bukti audit wawancra dengan IT manager bahwa tidak terdapatnya kebijakan dan prosedur DRP. Namun, berdasarkan kondisi perusahaan yang tidak terlalu besar dimana hanya terdapat 1 server saja, dan perusahaan juga terletak di daerah industri yang selama ini tidak pernah terjadi bencana. Selain itu, Perusahaan telah melakukan *offsite backup* sebagai antisipasi jika terjadi hal yang tidak diinginkan. *offsite backup* dilakukan oleh manager IT setiap jumat dan oleh pihak outsource setiap bulannya. Namun, dalam hal ini terdapat resiko atas offsite backup yang dilakukan oleh pihak outsource dan dapat mengancam keberadaan data perusahaan (berhubungan dengan offsite backup yang dilakukan oleh pihak outsource lebih dalam dibahas di dalam pengendalian struktur organisasi). Maka untuk kapasitas perusahaan ini,

pengendalian atas *Disaster Recovery Planning (DRP)* dinilai tidak signifikan bagi perusahaan.

4.3.3 Pengendalian atas Manajemen Data

Dari 5 standar, terdapat 2 yang tidak sesuai.

1. Berhubungan dengan standar individu dapat mengakses file sesuai dengan otoritasnya telah sesuai. Berdasarkan bukti audit wawancara dengan IT Manager dan dokumentasi, *User*ID dan *password* yang diminta pada waktu ingin mengakses ke program aplikasi menentukan sampai *file* mana *user* boleh mengakses *file* yang ada dalam *database*. Bukti audit dokumentasi berupa *access control matrix*, dimana setiap *computer operator* hanya dapat mengakses *file* yang mereka perlukan saja. Seperti yang terlampir dalam lampiran, acces control matrix yang terlihat adalah berisi kontrol akses atas nama siapa saja yang dapat mengakses ke dalam data inventory master list.
2. Berhubungan dengan standar adanya fitur kontrol lain untuk menghentikan akses yang tidak terotorisasi jika *user*ID dan *password* tertembus tidak sesuai. Berdasarkan wawancara dengan IT Manager, Tidak ada kontrol lain seperti *biometric device* dan sebagainya yang digunakan. Selain itu, *Password control* di perusahaan juga sangat lemah dimana tidak adanya kontrol yang menjamin kerahasiaan password, tidak adanya kebijakan mengenai masa aktif user id dan password, tidak adanya kebijakan jumlah digit password dan pembatasan percobaan entry password (*password control* lebih dalam dibahas dalam pengendalian sistem operasi).
3. Berhubungan dengan standar adanya prosedur *backup* yang ditetapkan perusahaan tidak sesuai. Berdasarkan bukti audit wawancara dengan IT Manager dan pihak outsource, tidak ada prosedur tertulis mengenai aturan back up, tetapi tugas backup telah dimengerti, setelah data diproses akan langsung tersimpan ke *server*. Data dalam *server* akan di offsite *back up* setiap hari jumat oleh pihak EDP, dan tiap 1 bulan oleh pihak outsource.

4. Berhubungan dengan standar kepastian lokasi *backup* telah terpisah telah sesuai. Berdasarkan bukti audit wawancara dengan IT Manager,dan observasi *Back-up* di PT. "X" ini ditempatkan secara terpisah (*offsite)*. Data back up disimpan di usb dan dibawa oleh IT Manager dan pihak outsource. Berdasarkan bukti audit observasi terlihat bahwa usb dibawa oleh IT Manager (Bapak Roy) dan bapak Agus selaku pihak outsource.
5. Berhubungan dengan standar adanya cadangan hardware yang dapat digunakan sewaktu-waktu telah sesuai. Berdasarkan bukti audit wawancara dengan IT Manager dan observasi dimilikinya 2 (dua) buah komputer cadangan yang diletakkan di ruangan pusat komputer, 1 komputer cadangan dapat digunakan terlebih dahulu sebagai *backup* apabila terdapat komputer yang mengalami kerusakan *hardware* dan masih harus menunggu pihak outsourcing. Sedangkan 1 komputer lainnya sebagai cadangan bagi computer user yang membutuhkan.

4.3.4 Pengendalian atas Sistem Operasi

Dari 12 standar, terdapat 6 yang tidak sesuai

1. Berhubungan dengan standar adanya proses *log on* untuk masuk ke dalam system operasi telah sesuai. Berdasarkan bukti audit wawancara dengan *computer operator* dan observasi, uji coba, dan dokumentasi prosedur log on dilakukan saat akan akses ke dalam sistem operasi yaitu dengan memasukkan *user name* dan *password*.
2. Berhubungan dengan standar adanya pesan jika proses *log on* gagal telah sesuai. Berdasarkan bukti audit wawancara dengan computer operator,observasi, serta uji coba jika proses log on gagal maka akan keluar kotak pemberitahuan *"invalid login*".
3. Berhubungan dengan standar adanya kontrol yang mengatur otorisasi akses untuk masuk ke sistem operasi telah sesuai. Berdasarkan bukti audit wawancara dengan IT manajer, observasi dan dokumen, hak akses ke program aplikasi BMP hanya diberikan kepada user-user yang terlibat. Namun, *access control matrix* yang terdapat di lampiran bukan berupa

table hak akses yang secara detail menjelaskan seorang user dapat mengakses modul apa saja. Namun, harus terlebih dahulu masuk ke dalam modul, seperti yang tertera di lampiran modul inventory master list. Setelah membuka modul tersebut baru terlihat siapa saja yang dapat mengakses ke dalam modul tersebut.

4. Berhubungan dengan standar adanya kontrol yang menjaga kerahasiaan password tidak sesuai. Berdasarkan bukti audit wawancara dengan IT Manager dan computer operator, observasi, serta uji coba hanya terdapat hide password yaitu password yang masuk hanya tampak ***, sehingga orang lain tidak dapat melihat password apa yang dimasukkan. Namun, tidak ada kontrol lain yang menjamin kerahasiaan password terjamin sehingga beresiko password dapat diketahui oleh orang lain yang tidak memiliki hak akses.
5. Berhubungan dengan standar adanya kebijakan mengenai masa aktif *user ID dan password* tidak sesuai. Berdasarkan bukti audit wawancara dengan IT Manager dan HRD tidak ada prosedur tertulis mengenai penghapusan *user name* dan *password*, tetapi apabila ada karyawan yang keluar maka bagian HRD akan memberitahu bagian EDP agar dapat menghapusnya. Hal ini menimbulkan resiko apabila bagian HRD lalai memberitahu ada user yang keluar, user id dan password user dapat dipakai oleh orang yang tidak berkepentingan.
6. Berhubungan dengan standar adanya kebijakan jumlah *digit password* dan pembatasan percobaan *entry password* tidak sesuai. Berdasarkan bukti audit wawancara dengan IT Manager dan uji coba password, tidak adanya kebijakan jumlah digi*t userID* serta *password* yang ada di dalam perusahaan dan penentuan password sesuai keinginan karyawan tetapi tetap disetujui oleh IT Manager, dimana hanya IT Manager yang dapat membuat, mengubah, menghapus serta memberikan otorisasi atas *username* sert*a password.* Selain itu, tidak ada batasan pemasukan password.Bukti audit uji coba adalah dengan memasukkan password yang salah dan tidak ada batasan pemasukan password walau berulang-ulang

salah. Hal ini dapat menimbulkan resiko dapat dicobanya pemasukan password berulang-ulang untuk mencari celah masuk ke dalam program.

7. Berhubungan dengan standar adanya antivirus yang digunakan oleh perusahaan telah sesuai. Berdasarkan bukti audit wawancara dengan IT Manager dan dokumentasi PT. "X" menggunakan anti virus Smadav2010.
8. Berhubungan dengan standar adanya kebijakan untuk pencegahan masuknya virus tidak sesuai. Walau berdasarkan bukti audit wawancara dengan IT Manager dan uji coba, tidak terdapat prosedur tertulis namun setiap karyawan melakukan *scan* pada setiap penggunaan USB, atau *hardware* lain. Namun, terdapat virus-virus yang ada dalam USB atau hardware lain yang dapat masuk ke dalam komputer. Sehingga, pemakaian USB dihentikan, lebih baik perusahaan menggunakan jaringan LAN untuk mentransfer data sehingga tidak ada virus yang masuk dari penggunaan USB.
9. Berhubungan dengan standar digunakannya anti virus yang kompeten tidak sesuai. Sebab berdasarkan bukti audit wawancara dengan IT Manager, anti virus yang digunakan adalah Smadav *free charge demo* yang didapatkan secara *free* atas pembelian komputer dari *vendor*. Anti virus ini tidak berlangganan dan tidak mampu mendeteksi virus jenis baru sehingga membuat data terkorupsi dan hilang.
10. Berhubungan dengan standar adanya kebijakan tentang *update* anti virus secara berkala tidak sesuai sebab berdasarkan bukti audit wawancara dengan IT Manager, anti virus yang dipakai tidak dapat melakukan *update* karena tidak berlangganan. Sehingga tentunya anti virus tidak dapat mengatasi virus jenis baru dan membuat anti virus tidak kompeten.
11. Berhubungan dengan standar adanya *audit logs* untuk melihat aktivitas karyawan telah sesuai. Berdasarkan bukti audit wawancara dengan IT Manager dan dokumentasi terdapat *Audit Log* dalam sistem namun tidak pernah direview oleh perusahaan dikarenakan terlalu rumit dalam proses membaca *audit log*. *Audit logs* tidak direview apabila pihak EDP merasa tidak ada hal yang janggal. Pihak EDP tidak dapat mengakses *audit log*

tanpa bantuan pihak *outsourcing*. Namun selama ini tidak pernah ada hal yang janggal sehingga perusahaan tidak merasa perlu melakukan review.

12. Berhubungan dengan standar adanya prosedur yang menanggulangi pemadaman listrik telah sesuai sebab berdasarkan bukti audit wawancara dengan IT Manager, perusahaan memiliki *diesel genset* yang terletak di gudang sebagai fitur toleransi kesalahan ketika aliran listrik mati. Tetapi *genset* ini tidak secara otomatis menyala ketika aliran listrik mati. *Genset* harus dinyalakan secara manual. Perusahaan juga memiliki UPS untuk mematikan komputer secara normal ketika sumber listrik padam.

4.3.5 Pengendalian atas Pengembangan dan Pemeliharaan Sistem

Dari 3 standar, terdapat 2 yang tidak sesuai

1. Berhubungan dengan standar adanya kepastian bahwa aktivitas perubahan program dan perawatan sistem merupakan aktivitas yang terotorisasi tidak sesuai. Berdasarkan bukti audit wawancara dengan IT Manager, apabila dia menerima keluhan atas sistem dari user, maka IT manajer akan mencatatnya dan memberikannya kepada pihak outsourcing agar diperbaiki, catatan tersebut dibawa oleh pihak outsourcing. Namun, tidak terdapat bukti prosedur secara tertulis yang mengindikasikan adanya otorisasi, hanya berupa lisan dan catatan saja. Hal ini menimbulkan resiko pihak outsource dapat melakukan perubahan program atau perawatan system tanpa sepengetahuan dari manager IT karena tidak adanya bukti hitam diatas putih.
2. Berhubungan dengan standar adanya aktivitas perawatan sistem secara berkala telah sesuai. Berdasarkan bukti audit wawancara dengan IT Manager dan outsource, terdapat aktivitas perawatan sistem secara berkala setiap bulan yang dilakukan oleh PT. Orlansoft selaku *System Analyst and Programmer*.
3. Berhubungan dengan standar adanya dokumentasi atas aktivitas perubahan program dan perawatan system tidak sesuai. Sebab berdasarkan bukti audit wawancara dengan IT Manager, saat ini proses

dokumentasi perubahan tidak dilakukan dan hanya berupa catatan permintaan perubahan dari IT manajer yang diberikan kepada pihak outsource saja. Menurut pihak outsource, dokumentasi mengenai perawatan sistem disimpan oleh pihaknya. Aktivitas maintenance dilakukan secara rutin oleh PT. Orlansoft selaku *System Analyst and Programmer* setiap bulan, hal tersebut dilakukan untuk menjaga supaya sistem tetap terawat dan dapat beroperasi dengan baik. Dimana dokumentasi atas sistem tersebut disimpan oleh pihak outsourcing dan bukan pihak PT. X.hal ini beresiko sebab perusahaan tidak memiliki dokumentasi sehingga tidak dapat mereview perubahan yang dilakukan oleh pihak outsource.

4.3.6 Pengendalian atas Jaringan dan Internet

1. Berhubungan dengan standar pengendalian pencegahan dan pendeteksi terhadap akses ilegal penggunaan jaringan dan internet telah sesuai. Berdasarkan bukti audit wawancara dengan IT Manager dan computer operator, perusahaan memperbolehkan semua komputer diperusahaan telah terhubung ke internet, untuk masuk ke jaringan internet, *user* tidak harus memasukkan *user*Id dan *password*. Sehingga tidak ada akses yang ilegal.
2. Berhubungan dengan standar adanya pemakaian anti virus yang kompeten tidak sesuai. Berdasarkan bukti observasi adanya pemakaian anti virus Smadav2010. Tetapi anti virus ini dianggap kurang kompeten untuk mengatasi virus-virus jenis baru yang dapat masuk melalui pemakaian internet sebab hanya berupa *free charge demo* yang didapatkan secara grati