TUGAS AKHIR

IF5166 KEAMANAN INFORMASI LANJUT

Audit Keamanan Teknologi Informasi dengan Metodologi BSI

Tanggal Pengumpulan :

18 Desember 2008

Dibuat oleh :

Rosa Ariani Sukamto / 23507024

SEKOLAH TEKNIK ELEKTRO DAN INFORMATIKA

INSTITUT TEKNOLOGI BANDUNG

2008

1 Pendahuluan

Saat ini teknologi informasi (TI) sudah merupakan bagian yang memegang peranan penting di dunia industri. Banyak kemudahan diberikan oleh teknologi informasi dalam menyelesaikan masalah manusia di bidang industri. Namun di lain sisi, untuk membangun sebuah teknologi informasi yang andal memerlukan biaya yang tidak sedikit. Teknologi informasi dalam sektor perusahaan publik dan privat, administrasi publik dan bagian lain sangat rentan pada berbagai ancaman, misalnya virus, serangan *hacking* pada kegagalan sistem. Proses bisnis dapat menjadi tidak berjalan dengan baik sebagai akibatnya. Secara periodik, teknologi informasi harus dilindungi agar resiko fungsional tidak menjadi rusak. Dalam implementasinya, biaya akan sangat dibutuhkan dan digunakan seefisien mungkin. Semuanya juga harus proporsional dilakukan berdasarkan prediksi resiko yang mungkin terjadi [1].

Selain perlindungan terhadap resiko, perlu adanya pemeriksaan terhadap implementasi perlindungan sercara periodik untuk mengidentifikasi jika terjadi penyelewengan implementasi perlindungan. Hasil dari pemeriksaan ini juga dapat dipergunakan untuk memperbaiki standar implementasi perlindungan di masa mendatang.

Keamanan teknologi informasi banyak tidak diperhatikan karena beberapa hal berikut:

- permasalahan banyaknya biaya,
- dianggap menghabiskan biaya yang mahal,
- menghalangi pemakai melakukan pekerjaannya,
- menambah pekerjaan untuk administrasi teknologi informasi,
- dianggap hanya dibutuhkan untuk perusahaan besar.

Keamanan teknologi informasi perlu diperhatikan karena hal-hal berikut:

- di masa mendatang semua perusahaan akan menggunakan teknologi informasi
- di masa mendatang semua proses bergantung pada teknologi informasi
- persiapan perkembangan jaringan lokal maupun global
- teknologi informasi menjadi semakin kompleks
- sistem teknologi informasi menjadi terbuka (melalui internet dan akses secara *remote*)

Demi keperluan perbaikan sistem teknologi informasi di masa mendatang maka sangat dibutuhkan proses audit teknologi informasi.

2 Audit Teknologi Informasi

Audit sendiri sebenarnya adalah proses pengawasan dan pengendalian. Audit teknologi informasi adalah bentuk pengawasan dan pengendalian dari infrastruktur teknologi informasi secara menyeluruh. Audit teknologi informasi ini dapat berjalan bersama-sama dengan audit finansial dan audit internal, atau dengan kegiatan pengawasan dan evaluasi lain yang sejenis. Audit teknologi informasi secara umum merupakan proses pengumpulan dan evaluasi dari semua kegiatan sistem informasi dalam perusahaan itu. Istilah lain dari audit teknologi informasi adalah audit komputer yang banyak dipakai untuk menentukan apakah aset sistem informasi perusahaan itu telah bekerja secara efektif, dan integratif dalam mencapai target organisasinya [2].

Keuntungan adanya audit antara lain:

- menilai keefektifan aktivitas aktifitas dokumentasi dalam organisasi,
- memonitor kesesuaian dengan kebijakan, sistem, prosedur dan undang-undang perusahaan,
- mengukur tingkat efektifitas dari sistem,
- mengidentifikasi kelemahan di sistem yang mungkin mengakibatkan ketidaksesuaian di masa datang,
- menyediakan informasi untuk proses peningkatan,
- meningkatkan saling memahami antar departemen dan antar individu,
- melaporkan hasil tinjauan dan tindakan berdasarkan resiko ke manajemen.

Informasi audit harus disimpan dan dijaga sehingga sebuah aksi dapat ditelusuri. Data audit harus dijaga dari modifikasi dan perusakan dari pihak yang tidak bertanggung jawab.

Pada audit teknologi informasi, area yang harus dicakup antara lain:

- perencanaan,
- organisasi dan manajemen,
- kebijakan dan prosedur,

- keamanan,
- regulasi dan standar.

Dalam tulisan ini nantinya hanya akan dibahas audit teknologi informasi pada area keamanan dengan pendekatan metodologi BSI yang akan dibahas berikutnya.

Jenis-jenis audit teknologi informasi antara lain:

- audit sistem;
  audit terhadap sistem terdokumentasi untuk memastikan sudah memenuhi standar nasional atau internasional,
- audit pemenuhan (*compliance*);
  untuk menguji efektifitas implementasi dari kebijakan, prosedur, kontrol dan unsur hukum yang lain,
- audit produk atau layanan;
  untuk menguji suatu produk atau layanan telah sesuai seperti spesifikasi yang telah ditentukan dan cocok digunakan.

Berikut adalah pihak-pihak yang perlu diaudit dalam proses audit teknologi informasi:

- pihak management,
- manajer teknologi informasi,
- spesialis teknologi informasi seperti *technical support*, *network administrator*, *database admin*, *system analyst*, *programmer*, dan lain ,
- *user*.

Kesuksesan proses audit tergantung pada hal-hal berikut:

- pemilihan auditor yang tepat,
- persiapan yang matang dan adanya respon,
- adanya laporan yang berarti,
- adanya aksi yang tepat yang diminta oleh auditor.

Seorang auditor yang tepat harus mampu melakukan hal-hal berikut:

- memastikan sisi-sisi penerapan teknologi informasi memiliki kontrol yang diperlukan,
- memastikan kontrol tersebut diterapkan dengan baik sesuai yang diharapkan.

Langkah-langkah yang harus dilakukan oleh seorang auditor adalah sebagai berikut:

- persiapan,
- *review* dokumen,
- persiapan kegiatan *on-site* audit
- melakukan kegiatan *on-site* audit
- persiapan, persetujuan dan distribusi laporan audit,
- *follow up* audit.

Keterampilan yang harus dimiliki oleh seorang auditor adalah sebagai berikut:

- *audit skill*: sampling, komunikasi, melakukan *interview*, mengajukan pertanyaan, mencatat,
- *generic knowledge*: pengetahuan mengenai prinsip-prinsip audit, prosedur dan teknik, sistem, manajemen dan dokumen-dokumen referensi, organisasi, peraturan-peraturan yang berlaku
- *specific knowledge*: latar belakang teknologi informasi/sistem informasi, bisnis, *specialist technical skill*, pengalaman audit sistem manajemen, perundangan.

Audit teknologi informasi secara internal meliputi hal-hal berikut:

- acuan di dalam proses audit secara internal,
- kunci obyektif dan kebutuhan;
    - global dan independen,
    - fokus pada resiko,
    - keahlian dalam mengontrol teknologi informasi internal,
    - keterlibatan proyek teknologi informasi,
    - *review* secara teratur,
    - adanya standardisasi dan *review* yang dalam,
    - rekomendasi,
    - teknologi informasi dan pengetahuan,
    - koordinasi yang efektif dengan pihak luar dan bagian regulasi,
    - aplikasi/infrastruktur koordinasi audit,
- metodologi kerangka kerja;
    - Area penggunaannya meliputi:
        - audit teknologi informasi,

        - analisis resiko,
        - pengecekan kesehatan (perbandingan keamanan),
        - konsep keamanan,
        - manual keamanan,
- organisasi internal audit teknologi informasi dan ruang lingkupnya,
- pendekatan yang diajukan dan metodologi audit:
    - COBIT,
    - BS7799,
    - BSI - *IT Baseline Protection Manual*,
    - ITSEC,
    - Common Criteria (CC),
- koordinasi dengan regulator eksternal dan bagian audit
- pembuatan kesimpulan

Pada tulisan ini metodologi yang dibahas adalah metodologi audit BSI - *IT Baseline Protection Manual*.

Area-area teknologi informasi yang perlu diaudit antara lain:

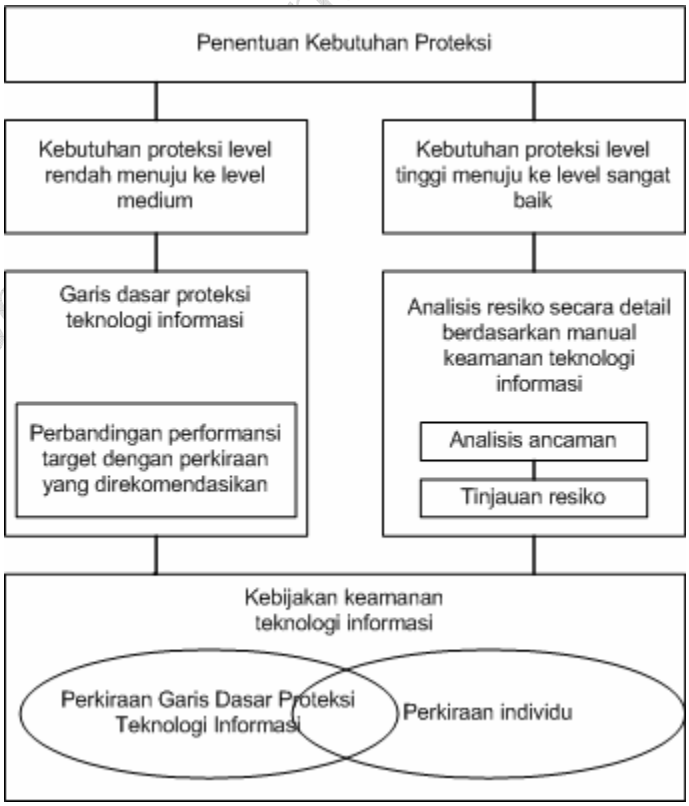
Area	Keterangan
Manajemen	Aspek-aspek keamanan yang relevan dengan perencanaan dan proses operasi khususnya pada bidang teknologi informasi
Organisasi/ Personel	Aspek-aspek keamanan yang relevan untuk rekruitmen staf dan pelatihan sesuai dengan aturan-aturan fungsi-fungsi kunci, secara individu didesain pertanggungjawabannya sesuai dengan isu-isu keamanan teknologi informasi
Kontraktor Eksternal	Aspek-aspek keamanan yang relevan dalam seleksi kontraktor eksternal teknologi informasi, mendefinisikan termin kontrak dan kerjasama
Alarm-Manajemen dan Perbaikan dari Kerusakan	Identifikasi dan pemrosesan kejadian-kejadian yang relevan dengan keamanan teknologi informasi. Standar/aturan-aturan, pengukuran perbaikan bisnis untuk teknologi informasi untuk kejadian-kejadian mayor yang mungkin terjadi setelahnya.

Area	Keterangan
Manajemen *Account*	Manajemen *user account*
Pusat Komputer dan Layanan Teknologi Informasi	Aspek-aspek keamanan yang relevan dari konfigurasi, operasi dan proses *backup* sistem multi-*user* dan aplikasi yang berjalan didalamnya
Sistem Proses Kontrol	Aspek-aspek keamanan yang relevan dari arsitektur, konfigurasi, dan sistem kontrol proses operasi untuk proses produksi yang bersifat kritis
Infrastuktur Kerja dan Sistem Mobil	Aspek-aspek keamanan yang relevan yang terfokus pada konfigurasi dan penggunaan PC, PC kantor, laptop, PDA, dan sistem *workstation* lainnya
Jaringan Data	Aspek-aspek keamanan yang relevan dari arsitektur, konfigurasi, dan operasi jaringan
Infrastruktur Keamanan Teknologi Informasi	Aspek-aspek keamanan yang relevan dari arsitektur, konfigurasi, dan operasi anti virus, keamanan *gateway*
Perubahan Cabang Privat	Aspek-aspek keamanan yang relevan dari arsitektur, konfigurasi, dan operasi perubahan cabang privat
Infrastruktur Fisik	Konstruksi usaha perlindungan dari infrastruktur fisik dimana operasi teknologi informasi bernaung, ditambah dengan penyediaan perangkat teknologi informasi seperti *power*, AC, dan kabel
Kesadaran Keamanan	Adanya kesadaran keamanan yang sesuai dan sesuai pula diantara *user*

3 BSI – *IT Baseline Protection Manual*

Salah satu metodologi audit yang banyak digunakan adalah BSI - *IT Baseline Protection Manual*. BSI merupakan singkatan dari *Bundesamt fur Sicherheit in der Informationstechnik* yang dalam bahasa Inggris *Federal Office for Security in Information Technology*. *IT Baseline Protection Manual* yang diperkenalkan oleh BSI dan dikembangkan oleh BSI Jerman berisi kumpulan rekomendasi standar kontrol keamanan atau perlindungan sebagai referensi di dalam manual. Tujuan dari publikasi BSI manual adalah untuk mencapai level keamanan untuk sistem teknologi informasi yang beralasan dan cukup memuaskan proteksi kebutuhan normal dan juga dapat memberikan layanan sebagai basis untuk kebutuhan sistem dan aplikasi teknologi informasi akan perlindungan [4].

Dokumen BSI memberikan deskripsi yang luas mengenai kebijakan keamanan informasi, meliputi tanggung jawab manajemen pada kebijakan, menyatukan sebuah tim yang bertanggung jawab pada pengembangan kebijakan, baik dari segi isi kebijakan maupun penyebaran kebijakan [3]. Berikut adalah diagram pendekatan BSI:



3.1 Garis Dasar Proteksi Teknologi Informasi (*IT-Baseline Protection*)

Penggunaan teknologi informasi meningkat secara kontinyu. Di satu sisi hal ini merupakan sebuah perubahan, evaluasi dan mengumpulkan informasi menjadi lebih efektif, tapi di sisi lain akan ada resiko yang baru. Saat ini banyak perusahaan federal tidak dapat memenuhi kewajibannya dengan benar tanpa menggunakan teknologi informasi. Untuk alasan ini, informasi dalam sistem teknologi informasi harus dijaga untuk mencegah hal-hal berikut:

- pengaksesan oleh pihak yang tidak berhak
- perubahan oleh pihak yang tidak berhak
- penurunan atau kehilangan fungsi

Perencanaan keamanan teknologi informasi, realisasi, dan kontrol harus mempertimbangkan area infrastruktur, organisasi, personil, dan teknologi. Hal tersebut didesain untuk memastikan kepercayaan, integritas, dan ketersediaan sistem teknologi informasi dan informasi itu sendiri. Untuk perkantoran federal, sebuah penurunan dari fungsi dasar keamanan teknologi informasi akan mengakibatkan hal-hal berikut:

- pelanggaran hukum, regulasi, atau kontrak,
- rusaknya performansi,
- rusaknya bidang keuangan,
- rusaknya reputasi.

Kebutuhan proteksi pada sebuah sistem teknologi informasi merupakan roda penggerak yang dapat mengakibatkan kerusakan yang potensial. Berikut adalah kategori kebutuhan proteksi:

- dasar;
  dampak kehilangan atau kerusakan dibatasi,
- tinggi;
  dampak kehilangan atau kerusakan menjadi pertimbangan,
- sangat tinggi;
  dampak kehilangan atau kerusakan dapat mengancam kelangsungan perusahaan.

Untuk menentukan pengukuran keamanan dalam hubungannya dengan kebutuhan proteksi maka diperlukan adanya proses perkiraan resiko. Langkah berikutnya adalah

memperkirakan probabilitas kejadian-kejadian yang mengancam keamanan. Setelah itu pengukuran keamanan teknologi informasi harus diimplementasikan.

IT Baseline Protection Manual mendukung perkantoran federal (termasuk perusahaan) dalam mengimplementasilan konsep keamanan teknologi informasi dengan mudah, ekonomis, dan efektif. Idenya adalah dengan berbasis pada asumsi bahwa sebuah paket pengukuran keamanan teknologi informasi harus *up-to-date*, diterima, dan terbukti, mencakup ancaman dan resiko dengan lingkup yang besar. Sehingga perkiraan resiko secara mendalam tidak terlalu dibutuhkan.

IT Baseline Security Manual berisi:

- standar perlindungan keamanan untuk sistem teknologi informasi dengan kebutuhan proteksi “normal”,
- sebuah deskripsi skenario ancaman yang diasumsikan secara global,
- deskripsi detail dari perlindungan untuk memandu implementasi,
- sebuah deskripsi proses yang terlibat pencapaian dan pemeliharaan level yang sesuai pada keamanan teknologi informasi,
- sebuah prosedur yang simpel untuk mengidentifikasi level keamanan teknologi informasi yang dicapai dilihat dari target yang dibandingkan dengan aktualisasi.

IT Baseline Security Manual distrukturkan menjadi bentuk modular dan menyediakan modul-modul berikut secara individual yang merefleksikan area dimana aset teknologi informasi digunakan:

- komponen generik (manajemen keamanan teknologi informasi, organisasi, personil, konsep perencanaan kontingensi, kebijakan *back up* data, menangani kecelakaan keamanan, dan lain-lain)
- infrastruktur (gedung, ruangan, kabel, pusat komputer, tempat kerja, dan lain-lain)
- sistem non-jaringan (DOS-PC, laptop, PC, sistem UNIX, Windows 2000, klien, dan lain-lain)
- sistem jaringan (server UNIX, jaringan Windows-NT, server Windows 2000, dan lain-lain)
- sistem transmisi data (modem, *firewall*, e-Mail, Exchange 2000, Outlook 2000, dan lain-lain)

- telekomunikasi (mesin fax, sistem telekomunikasi, server fax, telepon mobil, dan lain-lain)
- komponen teknologi informasi lainnya (basis data, dan lain-lain)

Setiap modul dari *IT Baseline Protection Manual* berisi deskripsi subyek, daftar yang berisi referensi pada ancaman yang relevan, dan standar pengukuran keamanan yang relevan pada setiap kasus. BSI secara kontinyu melakukan *update* pada manual dan menambahnya dengan subyek-subyek baru yang berbasis survei *user* [3].

3.2 Instruksi Menggunakan IT Baseline Protection Manual

Berikut adalah instruksi menggunakan *IT Baseline Protection Manual*:

1. analisis struktur teknologi informasi,
2. perkiraan kebutuhan proteksi,
3. memodelkan,
4. pengecekan keamanan dasar

Pada kasus menggunakan sistem teknologi informasi dengan kebutuhan proteksi yang tinggi, penyedia analisis keamanan harus berhati-hati mengalokasikan biaya secara efektif. Secara umum kepuasan akan pembuatan rekomendasi dalam *IT Baseline Protection Manual* dengan diberikan oleh orang yang sesuai dan pengukuran yang tepat. Setelah itu pengukuran garis dasar proteksi teknologi informasi dan pengukuran yang tepat harus dikonsolidasikan untuk mendapatkan sudut pandang umum dari semua pengukuran yang muncul [3].

3.3 Standar Audit BSI

Ketika proses audit keamanan teknologi informasi dalam perkantoran federal, *IT Baseline Protection Manual* digunakan sebagai standar untuk sistem teknologi informasi dengan kebutuhan proteksi “normal”. Jika semua rekomendasi yang dibuat dalam *Baseline Protection Manual* tetap konsisten, pengukuran keamanan akan selalu dapat sesuai dengan permintaan dari sistem teknologi informasi dengan kebutuhan proteksi yang tinggi.

BSI juga memiliki standar *checklist* yang digunakan untuk melakukan audit keamanan teknologi informasi. Menurut petunjuk keamanan teknologi informasi dari BSI, berikut

adalah hal-hal yang penting untuk diukur dalam proses audit keamanan teknologi informasi:

- manajemen keamanan teknologi informasi,
  - apakah manajemen sudah mendefinisikan obyek keamanan teknologi informasi dan menerima bahwa mereka bertanggung jawab untuk keamanan teknologi informasi? apakah semua isu legal dan kotraktual telah dipertimbangkan?
  - apakah ada seorang petugas keamanan teknologi informasi?
  - apakah kebutuhan keamanan teknologi informasi telah dipertimbangkan di awal pada setiap proyek (mulai perencanaan dari jaringan baru, pembelian baru aplikasi dan sistem teknologi informasi, perjanjian *outsourcing* dan layanan)?
  - apakah ada rangkuman mana yang paling penting dari aplikasi dan sistem teknologi informasi dan kebutuhan proteksi mereka?
  - apakah ada sebuah rencana aksi yang memprioritaskan obyek keamanan dan kumpulan kemajuan yang menyatakan bagaimana perjanjian pengukuran keamanan teknologi informasi diimplementasikan?
  - apakah pengukuran keamanan teknologi informasi telah ditentukan di semua kasus yang sering terjadi maupun yang jarang? (misal melakukan *update* pada *virus scanner*)
  - apakah tanggung jawab telah didefinisikan untuk semua pengukuran keamanan teknologi informasi?
  - apakah pengaturan pewakilan yang tepat dengan jabatannya pada pertanggungjawaban dan pekerjaan yang harus dilakukan sudah sesuai dengan kapasitas yang bersangkutan? apakah *password* yang paling penting sudah aman pada saat pengiriman pada saat keadaan darurat?
  - apakah semua orang yang menjadi target sudah kenal dengan kebijakan dan tanggung jawab yang ada?

- apakah ada *checklist* faktor cakupan yang butuh dipertimbangkan ketika ada staf baru atau ada staf yang keluar dari perusahaan? (masalah akses sistem, pelatihan, dan lain-lain)
- apakah pengukuran keamanan teknologi informasi yang efektif dicek secara teratur?
- apakah ada dokumentasi konsep keamanan teknologi informasi?

- keamanan sistem teknologi informasi,
  - apakah mekanisme proteksi ada dalam aplikasi dan program yang digunakan?
  - apakah perangkat lunak anti virus memang digunakan dan dijalankan?
  - apakah aturan dan profil telah diberikan pada semua sistem *user*?
  - apakah ada kontrol setiap kali anggota staf diijinkan mengakses data? apakah ada batasan yang cukup?
  - apakah ada aturan dan profil yang berbeda untuk administrator atau apakah semua administrator bebas melakukan apapun?
  - apakah ijin dan hak akses dari program diketahui dan telah dikontrol?
  - apakah standar keamanan yang relevan telah diset pada program dan sistem teknologi informasi yang sesuai dengan adaptasi?
  - apakah program atau fungsi keamanan yang relevan tapi sebenarnya tidak penting sudah di-*uninstall* atau di-*disabled*?
  - apakah manual dan dokumentasi produk telah dibaca dengan benar?
  - apakah instalasi dan dokumentasi sistem dibuat dan di-*update* secara teratur?
- jaringan dan koneksi internet,
  - apakah sudah ada *firewall*?
  - apakah konfigurasi dan fungsionalitas *firewall* telah diawasi dan diperiksa secara periodik (jangka waktu teratur)?
  - apakah ada konsep kemana data akan dikirimkan di dunia luar?
  - apakah telah dispesifikasikan seberapa bahaya program tambahan (*plug-in*) dan konten aktif yang harus dihindari?

- apakah semua layanan dan fungsi program yang tidak perlu telah di-*disabled*?
- apakah *web browser* dan program email telah dikonfigurasi pada kondisi aman?
- apakah semua staf sudah cukup diberi pelatihan?

- pemenuhan kebutuhan keamanan,
  - apakah informasi dan media data telah disimpan dengan hati-hati?
  - apakah informasi yang dihapus dari media data atau sistem teknologi informasi dapat tetap diperlihara dan diperbaiki jika ada kesalahan?
  - apakah staf yang dikenai pelatihan reguler dengan subyek keamanan yang relevan?
  - apakah ada pengukuran yang dilakukan untuk kewaspadaan keamanan?
  - apakah obyek keamanan yang ada diawasi dan dilakukan dengan disiplin?
- pemeliharaan sistem teknologi informasi: menangani *update*,
  - apakah instalasi keamanan di-*update* secara regular?
  - apakah sesorang sudah ditugaskan untuk menjaga karateristik keamanan dari perangkat lunak dengan *update* keamanan yang relevan?
  - apakah ada konsep pengetesan untuk perangkat lunak yang dimodifikasi?
- ekripsi dan *password*,
  - apakah aplikasi dan program menyediakan mekanisme keamanan seperti proteksi dengan *password* dan enkripsi? apakah mekanisme keamanan sudah diaktifkan?
  - apakah *pasword* kosong atau standar sudah diubah?
  - apakah semua staf sudah diberi pelatihan memilih *password* yang aman?

- apakah *workstation* dilindungi ketika penggunaannya sedang tidak ada dengan *password* atau *screensaver*?
- apakah data dan sistem dilindungi dengan ekripsi dan *safeguard*?

- perencanaan kontingensi,
  - apakah ada rencana yang kontingen dengan instruksi dan alamat kontak?
  - apakah semua situasi kontingensi yang peting sudah dicakup?
  - apakah setiap anggota staf kenal dengan rencana kontingensi dan mudah untuk diakses?
- *backup* data,
  - apakah ada strategi *backup*?
  - apakah ada aturan kapan data harus di-*backup* dan untuk berapa lama?
  - apakah *backup* juga termasuk data pada laptop atau komputer yang tidak terhubung dengan sistem jaringan?
  - apakah isi hasil *backup* dicek secara teratur?
  - apakah *backup* dan prosedur penyimpanan didokumentasikan?
- keamanan infrastruktur,
  - apakah sistem teknologi informasi cukup dilindungi dari api, kerusakan akibat terkena air, kelebihan voltase, dan kegagalan *power*?
  - apakah akses pada sistem teknologi informasi yang penting dan ruangan penting telah dikontrol? apakah jika ada orang yang masuk atau mengakses akan ditemani atau dibimbing?
  - apakah proteksi yang ada sudah cukup untuk melawan pengganggu?
  - apakah ada persediaan perangkat keras dan perangkat lunak yang direkam dalam daftar inventori?
- perubahan cabang privat.
  - seorang manajer dan deputi cabang privat harus ditunjuk,
  - fitur yang tidak diperlukan harus diidentifikasi dan diblok,
  - beberapa *password* konfigurasi perusahaan harus dimandatkan,

- *password* yang dibutuhkan untuk proses konfigurasi dan pemeliharaan harus disimpan di lingkungan yang aman untuk keadaan darurat,
- petunjuk nomor panggilan layanan dan panggilan internasional harus diisukan,
- *file log* harus dianalisis secara regular sehingga sesuatu yang tidak biasa bisa ditandai.
- konfigurasi cabang privat harus diawasi secara regular,
- dokumentasi teknik dan kumpulan petunjuk yang digunakan sehari-hari harus dibuat atau didapat dari proses manufaktur,
- cabang privat harus memperhatikan aturan di dalam *Emergency Procedure Manual* (berisi *troubleshooting* yang dapat dilakukan, nomor telepon layanan teknik perbaikan, dan lain-lain),

  staf harus diberitahu informasi mengenai ancaman yang mungkin terjadi, jika memungkinkan keamanan cabang privat harus dicek secara reguler oleh ahli dari luar [3].

4 Referensi

[1] _____. 2005. *IT Security Audit Material For Site Surveys in Critical Infrastructures*. Bundesamt fur Sicherheit in der Informationstechnik: Bonn, Jerman.

[2] _____. 2008. *Audit Teknologi Informasi*, [html], (*http://id.wikipedia.org/wiki/Audit_IT* , diakses tanggal 17 Desember 2008).

[3] Fasswald , Jan. 2004. *Federal Court of Audit (Bundesrechnungshof), Audit Unit IV 3. 2004: 2nd Seminar on IT-Audit September 1st to 4th, 2004 in Nanjing*. Bundesrechnungshof.

[4] Hone, Karin dan J.H.P. Eloff. 2001. *Information Security Policy: What do International Information Security Say?*. Rand Afrikaans University.