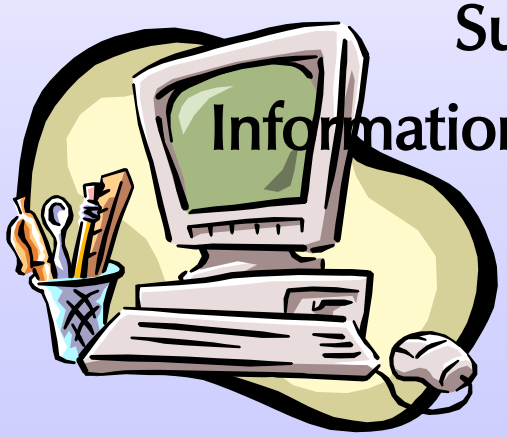
Business Continuity Plan & Disaster Recovery Plan



Sumber : CISA Review Manual,

Information Systems Audit & Control Association

Arrianto Mukti Wibowo, CISA
08568012508
amwibowo@cs.ui.ac.id

Tujuan DRP / BCP

Agar bisnis bisa tetap beroperasi meskipun ada gangguan dan selamatnya sistem informasi terhadap bencana.

Definisi (1)

BCP : proses (otomatis maupun manual) yang dirancang untuk mengurangi ancaman terhadap fungsi-fungsi penting organisasi, sehingga menjamin kontinuitas layanan bagi operasi yang penting.

Definisi (2)

DRP : saat BC action sedang berlangsung, maka juga dimulailah langkah-langkah untuk 'penyelamatan' (*recovery*) terhadap fasilitas IT dan sistem informasi. Dapat juga dikatakan bahwa DRP merupakan bagian / subset dari BCP.

Beberapa definisi lainnya

	Disaster Recovery	Business Recovery	Business Resumption	Contingency Planning
Objective	Mission-critical applications	Mission-critical business processing (workspace)	Business process workarounds	External event
Focus	Site or component outage (external)	Site outage (external)	Application outage (internal)	External behavior forcing change to internal
Deliverable	Disaster recovery plan	Business recovery plan	Alternate processing plan	Business contingency plan
Sample Event(s)	Fire at the data center; critical server failure	Electrical outage in the building	Credit authorization system down	Main supplier cannot ship due to its own problem
Sample Solution	Recovery site in a different location	Recovery site in a different power grid	Manual procedure	25% backup of vital products; backup supplier
Crisis Management				

Source: Gartner Research

Bencana / Disaster (1)

Bencana bisa 1 jam – berhari-hari, dan bisa memaksa menggunakan fasilitas IT alternatif dengan menggunakan data backup off-site.

Bencana / Disaster (2)

Bencana alam :

- Gempa.
- Banjiiiiiirrr !
- Topan.
- Kebakaran

Bencana lainnya :

- Masalah aliran listrik (misal : putus).
- Tidak adanya saluran telekomunikasi.
- Tidak adanya transportasi.

Bencana / Disaster (3)

- Tapi ada pula ancaman yang tidak dianggap bencana tetapi tetap dianggap sebagai “high-risk” misalnya virus dan denial of service (DoS).
- Ancaman tsb harus diperhitungkan dalam pembuatan BCP.
- Guna mengantisipasi kasus terburuk, BCP harus mempertimbangkan strategi short-term dan strategi long-term.
- Misalnya untuk short term harus ada fasilitas IT alternatif, sedangkan long-term strategi misalnya menyiapkan fasilitas IT yang permanen.

Boeing Syndrome

- *The ultimate disaster scenario for contingency planning purposes.*
- *The name, allegedly, comes from a conference in which IT specialists, administrators, planners, etc were asked first to imagine that a Boeing 747 Jumbo fell out of the air onto their computer centre (with the resulting complete loss of systems) and then asked to prepare a contingency/disaster recovery plan to keep their organisation going in such circumstances.*
- *A very useful exercise - even for small companies, who often do not realise just how important their computer systems are to their continued existence as a viable business.*

Business Impact Analysis (1)

Dilakukan sebelum membuat BPC/DRP.

Hal-hal yang harus ditanyakan antara lain :

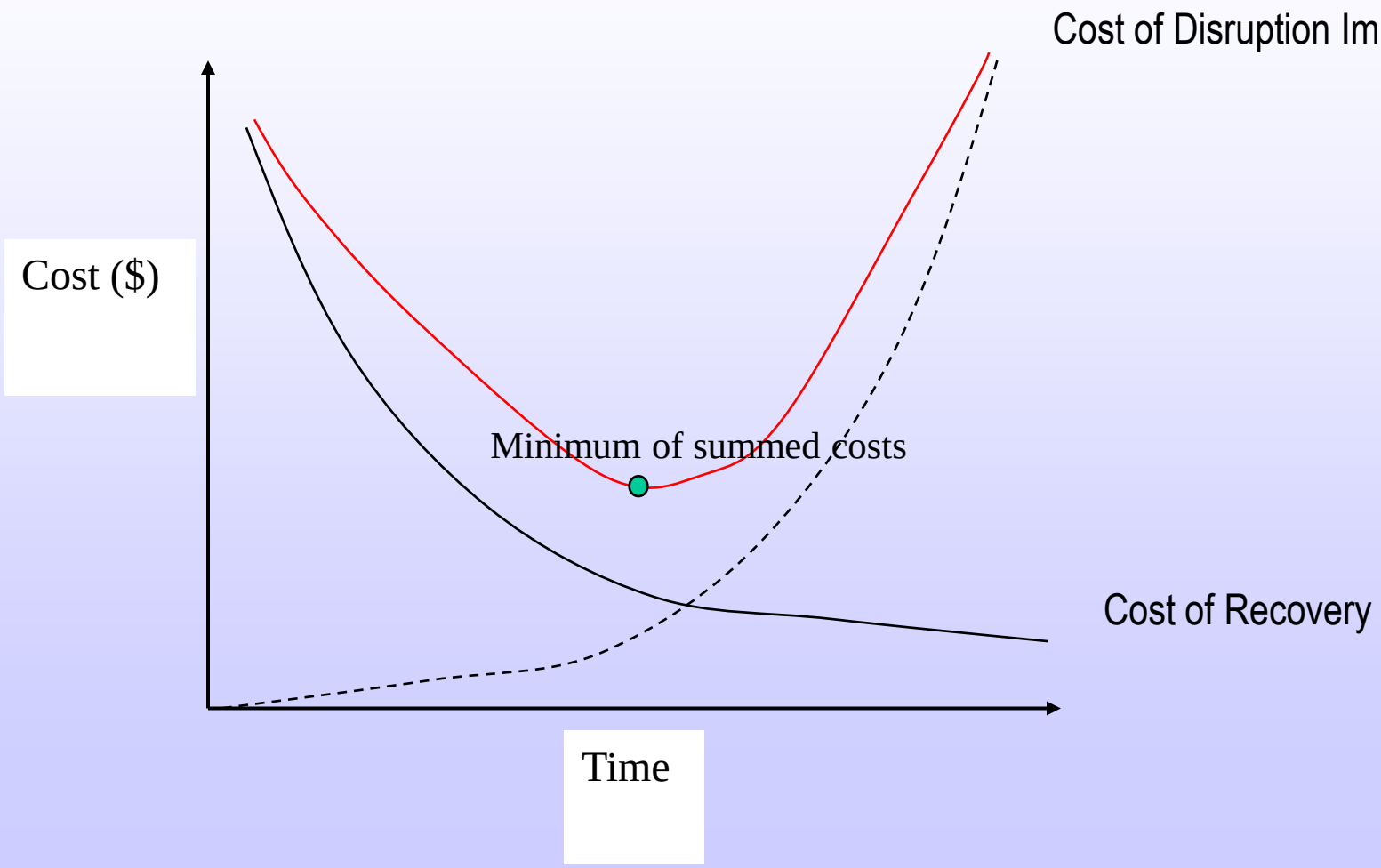
- *Information resource* apa yang penting bagi organisasi ?
- *Business process* apa yang kalau tidak berjalan akan memberikan dampak negatif yang fatal bagi perusahaan ?

Business Impact Analysis (2)

Setiap proses harus diperhatikan *criticality*-nya, dengan indikasi antara lain :

- Proses yang berkaitan dengan nyawa seseorang.
- Proses yang akan menyebabkan kerugian finansial yang luar biasa.
- Proses yang harus mematuhi aturan yang berlaku (misalnya : sektor keuangan, atau Air Traffic Control).

Cost of recovery vs Impact of distruption



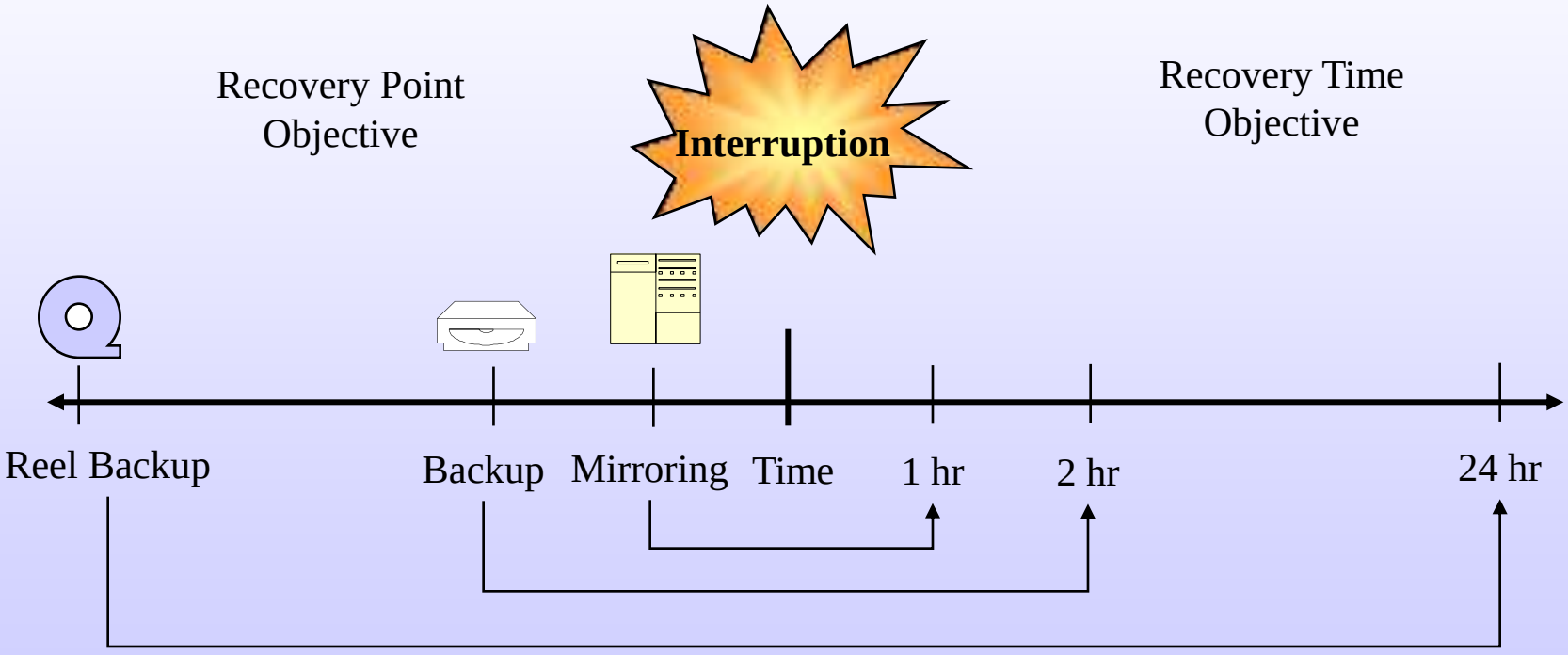
Risk Analysis (1)

Melakukan risk analysis (ingat soal SLE, ALE, ARO, dsb ?), kadang-kadang juga dilakukan pendekatan kualitatif,

Risk Analysis (2)

Klasifikasi	Deskripsi
Critical	Fungsi-fungsi ini tidak bisa bekerja kecuali digantikan dengan fungsi serupa. Tidak bisa digantikan dengan metode manual.
Vital	Bisa dilakukan secara manual pada rentang waktu yang pendek sekali. Sebaiknya bisa direstore dalam waktu 5 hari atau kurang.
Sensitive	Bisa dilakukan secara manual dalam waktu yang relatif lama, namun meskipun dilakukan secara manual pasti tetap sulit melakukannya dan membutuhkan staf lebih banyak.
Noncritical	Bisa diinterupsi sampai waktu yang lama, dengan sedikit beban / tidak ada beban biaya bagi perusahaan.

Recovery Point Objective & Recovery Time Objective



Selection of Recovery Strategies

Rumusnya:

- Tentukan cara/strategi untuk melakukan recovery fasilitas IT.
- Tentukan aktifitas bisnis apa saja yang harus dilakukan selama fasilitas IT sedang di-recover.

Selection of Recovery Strategies

- Asuransi : perencanaannya sendiri tidak bisa diasuransikan tetapi kalau ada kecelakaan baru bisa diasuransikan…. (tentunya ☺)
- Namun dengan adanya rencana yang memadai, maka biaya premi asuransinya biasanya lebih kecil.

Selection of Recovery Strategies

Untuk mainframe atau fasilitas jaringan :

1. Duplicate information processing facilities
2. Hot sites
3. Warm sites
4. Cold sites
5. Mobile site dengan mobil trailer, biasanya juga dilengkapi microwave dan/atau telekomunikasi satelit.
6. Reciprocal Agreement

Duplicate Processing Facility

- Dibuat ‘sama persis’
- Hot site yang selalu ‘stand-by’
- Hal harus diperhatikan:
  - Tidak berada dalam resiko bencana alam yang sama
  - Kesamaan hardware/software

Hot Sites

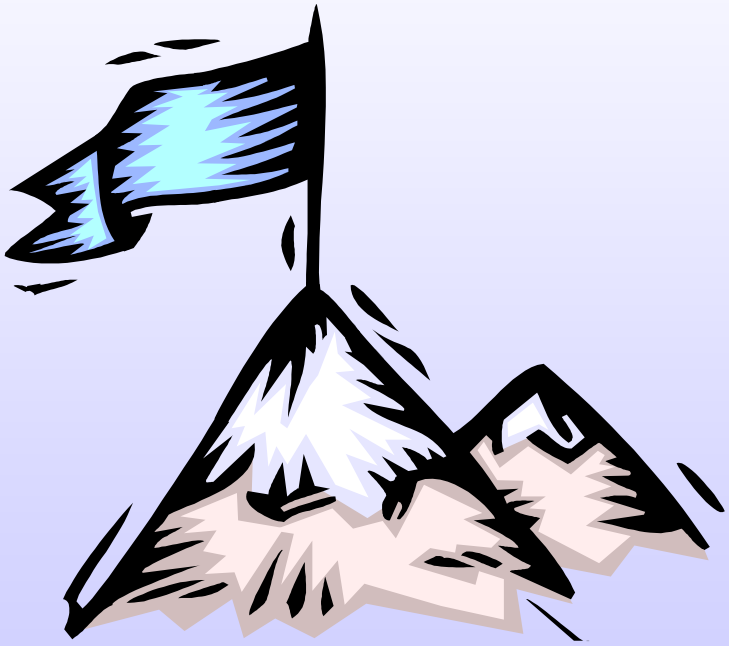
- Fully configured & readily operational offsite data processing facility equipped with hardware & software in event of a disaster.
- Ini penting untuk aplikasi yang critical.
- Namun biayanya sangat mahal.
- Bisa jalan dalam waktu beberapa jam saja.
- Hanya perlu staff, program, data dan dokumentasi.

Warm Sites

- Fasilitas alternatif yang memiliki sarana yang lebih sedikit.
- Misalnya ada listrik, jaringan, telepon, meja-meja, printer, tetapi tanpa komputer yang mahal.
- Kadang-kadang ada komputer, tetapi less processing power.

Cold Sites

- Fasilitas yang memiliki prasarana penunjang untuk operasi komputer, misalnya ruangan yang memiliki listrik dan AC.
- Tapi belum ada komputernya, namun siap dipasangi komputer.



Reciprocal Agreement

- Perjanjian dengan perusahaan lain
- This is a less frequently used method between two or more organizations with similar equipment or applications.
- Under the typical agreement, participants promise to provide computer time to each other when an emergency arises.
- Keuntungan:
  - Murah
  - Kalau vendornya jarang, bisa jadi cuma satu-satunya pilihan
- Kerugian:
  - Perbedaan konfigurasi hardware/software bisa memaksa perlunya modifikasi aplikasi komputer

Pengadaan Hardware Cadangan

- **Vendor or third-party**

  Hardware vendors are usually the best source for replacement equipment; however, this may often involve a waiting period that is not acceptable for critical operations. It is unlikely that any vendor will guarantee specific reaction to a crisis. Vendor arrangements are best utilized when planning to move from a hot site to a warm or cold site. The arrangements should be planned in advance.
- **Off-the-shelf**

  Such components are readily available from the inventory of suppliers on short notice and with minimum need for special arrangements. To make use of this approach, several strategies must be utilized, including:
  - Jangan menggunakan hw/sw yang sulit didapatkan.
  - Meng-update equipment agar tetap yang terbaru (atau agak baru).
  - Maintaining software compatibility to permit the operation of newer equipment
- **Credit agreement or emergency credit cards**

  Ensuring the recovery plans include instructions on how such equipment is to be paid for. This could be by a credit agreement with suppliers or by the provision of an emergency credit card, with a sufficiently high credit limit. It should not be left to individual employees, even managers, to take responsibility for such purchases on their own account.

Strategi business continuity

- Tidak melakukan apa-apa sampai *recovery facility* sudah 'on'.
- Melakukan prosedur manual.
- Memfokuskan diri pada proses yang penting saja : customer, products, dsb.
- Menggunakan PC untuk *data capture* (pencatatan saja) dengan pengolahan minimal. Pengolahan baru dilakukan setelah *recovery facility* sudah bekerja.

Pertimbangan dalam BCP (1)

- Saat membangun BCP, harus melibatkan seluruh perusahaan, tidak hanya bagian IT saja.
- Oleh karena itu sering masuk dalam bagian “Operation Risk”
- Kalau tidak ada BCP lapisan perusahaan, maka BCP dari sistem informasi harus menyertakan bagian lain yang terkait dengan BCP.

Pertimbangan dalam BCP (2)

Hal lain yang harus dipertimbangkan dalam membuat BCP :

- Staf-staf yang diperlukan untuk menjalankan fungsi bisnis yang penting saat terjadi bencana.
- Konfigurasi gedung, meja, kursi, telepon, dsb.

Komponen BCP (1)

Yang harus disepakati dalam BCP :

- Tujuan dari setiap tahap recovery
- Fasilitas alternatif
- Penanggung jawab
- Sumber daya yang akan disediakan
- Prioritas dan jadual aktifitas.

Komponen BCP (2)

Komponen BCP mencakup :

- Siapa penanggung jawab utama.
- Backup dari supplies yang dibutuhkan.
- Pengorganisasian dan penanggung jawab setiap aktifitas.
- Jaringan komputer.
- Asuransi.

Organization & Assignment of Responsibilities

- Ada tim-tim yang bertugas melakukan fungsi tertentu dalam BCP, dan dipimpin seorang *team leader*.

Tim-tim itu antara lain:

1. Emergency action team :
   - Tugas utamanya adalah seperti “pemadam kebakaran”, dan bertugas untuk menyelamatkan jiwa.
2. Damage assessment team :
   - Harus bisa mengkalkulasi dampak bencana.
   - Bisa memperkirakan kapan lokasi bisa kembali normal.
3. Emergency management team :
   - Berkewajiban mengkoordinasikan aktifitas tim-tim lainnya.
   - Melakukan decision making: apakah akan menjalankan DRP atau tidak
   - Termasuk menangani masalah hukum dan public relations.
4. Off site strorage team

   Packing dan shipping dari media dan records ke offsite facility.

5. Software team :

   Restore operating system.

6. Applications team :

   Pergi ke recovery site dan menginstall kembali aplikasi komputer.

7. Emergency operations team :

   - Shift operators & shift supervisors yang harus menjalankan recovery site (alternate facility)

8. Salvage team

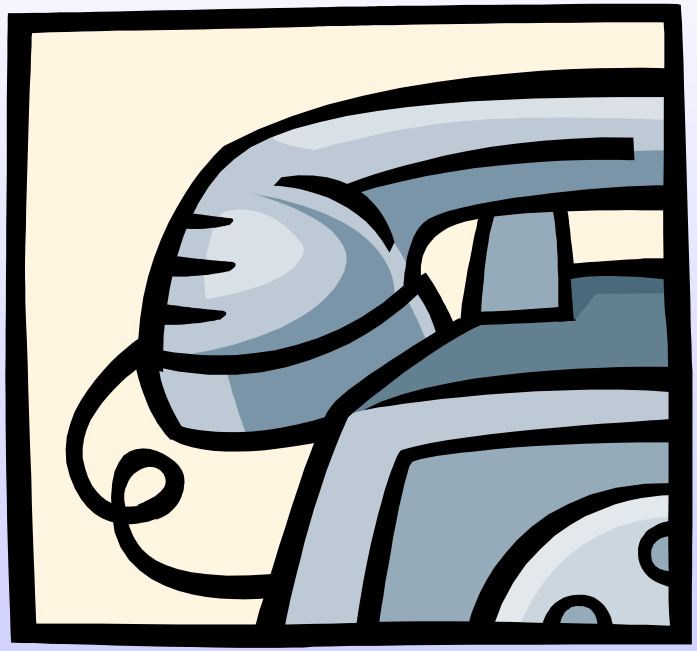
   - Melakukan analisis lebih mendalam terhadap dampak bencana.
   - Menentukan apakah akan memperbaiki lokasi yang kena bencana, atau melakukan proses relokasi.
   - mengisi form klaim asuransi

9. Relocation team

   - Mengembalikan dari recovery site ke lokasi awal atau ke lokasi baru yang permanen.

Key Decision Making Personel

- Berisi daftar orang yang harus menginisiasi dan melaksanakan kegiatan recovery.
- Biasanya berupa daftar nomor telepon.



Key Decision Making Personel

Daftar itu sepatutnya mencakup :

1. Siapa yang harus di-contact terlebih dahulu.
2. Emergency telephone numbers, termasuk ketua tim.
3. Telepon vendor-vendor, termasuk supplier.
4. Telepon dari recovery facility.
5. Telepon penyelenggara jasa telekomunikasi.
6. Telepon dari orang yang menyimpan backup data.
7. Telepon asuransi.
8. Telepon orang-orang kontrakan (jika yang melakukan recovery bukan orang operasional), terutama jika alternate facility ada di daerah lain.

Backup of Required Supplies

Harus ada pula persediaan kertas-kertas (berlogo perusahaan) dan formulir-formulir perusahaan agar siap untuk dipakai.

Telecommunication Networks

Beberapa strategi DRP untuk telekomunikasi :

1. Redundancy :
   - Involves providing extra capacity with a plan to use the surplus capacity should the normal primary transmission capability not be available.
   - In the case of a LAN, a second cable could be installed through an alternate route for use in the event the primary cable is damaged.
2. Alternative routing :
   - Menggunakan media komunikasi alternatif, misalnya kalau dulu antar cabang pakai VSAT, maka dicoba alternatifnya pakai POTS (plain old telephone system).

Telecommunication Networks

3. Diverse routing
   - Menggunakan duplicate cable, dan menjamin bahwa kabel-kabel tersebut memiliki jalur/path yang berbeda. Hal ini disebabkan kalau kabel-kabel itu berada pada satu jalur yang sama persis, maka akan kena jenis ancaman yang sama.

Telecommunication Networks

4. Long haul network diversity
   - Sebuah recovery facility (offsite alternate facility) banyak yang memiliki banyak jalur interlokal/internasional ke luar ke beberapa penyelenggara jasa telekomunikasi. Hal ini untuk menjamin tersedianya jasa telekomunikasi kalau yang satu crash.
   - Misalnya: Jakarta-Singapore

Telecommunication Networks

5. Last mile circuit protection
   - Menggunakan banyak metoda akses komunikasi keluar, kalau ada bencana di recovery/off-site facility
   - Banyak recovery facilities menyediakan kombinasi redundant dari penyedia jasa T1s, microwave and/or coaxial cable access ke dalam local communications loop.
6. Voice recovery : supaya bisa telepon-teleponan!

Server Disaster Recovery Methods

- The loss of or disruption to, the organization's servers that are managing sensitive and critical business processes could have a catastrophic effect on the organization.
- Plans should include operational failover methods to prevent servers from going offline for any extended period of time.
- Some of the techniques for providing failover or fault tolerant capabilities include uninterruptible power supply and the use of failover systems to prevent power failures of varying levels.

Fault-Tolerant Servers

- Fault-tolerant servers provide for fail-safe redundancy through mirrored images of the primary server.
- Using this approach also may entail distributed processing of a server load, a concept referred to as load balancing or clustering, where all servers take part in processing.
- In this arrangement, there is an "intelligent" cluster unit that provides for load balancing for improved performance.
- This type of server architecture, however, is transparent to the user.
- The only thing that may be noticeable to a user is performance degradation, if a server fails.

Redundant Array of Inexpensive Disks

- RAID provides performance improvements and fault-tolerant capabilities via hardware or software solutions, breaking up data and writing it to a series of multiple disks to simultaneously improve performance and/or save large files.
- These systems provide the potential for cost effective mirroring offsite for data backup.
- A variety of methods categorized into 11 levels, the most popular being 0, 3 and 5 are defined for combining several disk drives into what appears to the system as a single disk drive.
- RAID improves upon the single-drive-only solution as it offers better performance and/or data redundancy.

Asuransi (1)

BCP harus mencakup masalah asuransi dan cara klaim-nya juga.

Beberapa yang mungkin diasuransikan antara lain:

1. Peralatan dan fasilitas IT.
2. Software reconstruction (termasuk dari backup yang ada).
3. Extra expense, karena harus beroperasi dari alternate facility.

Asuransi (2)

4. Business interuption cost: kerugian akibat berhentinya aktifitas perusahaan.
5. Valuable papers & records, akibat hilangnya surat-surat berharga.
6. Media transportation.
7. Errors & Omissions.
8. Fidelity coverage : akibat ketidakjujuran pegawai.

Permasalahan Kontrak dengan Fasilitas Alternatif

Sebaiknya mencakup hal-hal di bawah ini :

1. Configuration – apakah konfigurasi hardware & software sudah tepat ?
2. Definisi “bencana” / disaster.
3. Speed of availability.
4. Subscribers per site.
5. Subscribers per area.

Permasalahan Kontrak dengan Fasilitas Alternatif

6. Preference: siapa yang didahulukan kalau ada bencana umum regional
7. Usage periode: kalau ada bencana, berapa lama boleh menggunakan fasilitas alternatif?
8. Audit: apakah kita boleh mengaudit alternate site/facility?
9. Testing: apakah testing diperkenankan.
10. Reliability: sepatutnya vendor pun harus bisa menjamin kehandalannya.

Library Off-site(1)

- Library berisi antara lain backup source code, program-program komputer dan data-data.
- Dokumentasi dari program-program juga harus ada di off-site facility.
- Dokumen BCP/DRP
- Dokumen SOP

Library (2)

Syarat-syaratnya antara lain :

1. Secure physical access : yang boleh masuk hanya terbatas.
2. Bangunan bisa tahan api 2 jam.
3. Lokasi library jauh dari ruang komputer, agar kalau terjadi apa-apa dengan ruang komputer, harapannya librarynya masih aman
4. Materi yang keluar-masuk library harus tercatat.
5. Memastikan kebenaran catatan yang berisi informasi file-file, versi dan lokasinya di mana.

Backup (1)

- Periode backup tergantung program aplikasi atau software.
- Jadi jika ada proses yang dilaksanakan sekali sebulan dimana master file diupdate, maka backup juga dilakukan sebulan sekali.
- Di sisi lain, kadang kalau untuk on-line / real-time system perlu menggunakan *mirrored master file* di lokasi yang berbeda.

Backup (2)

- Proses backup bisa diotomasi dengan menggunakan *job scheduling software*, sehingga bisa menghindar dari kesalahan backup dan lupa membackup.

Backup (3)

Hal-hal yang perlu dipertimbangkan dalam backup adalah:

- Frekuensi backup untuk setiap data file.
- DBMS biasanya menyediakan teknik backupnya sendiri.
- Sebaiknya ada perjanjian dengan vendor soal backup software.

Recovery Plan Testing (1)

- Untuk membukti bahwa BCP bekerja, maka BCP harus diuji.
- Tes dilakukan saat gangguan pada operasi dinilai kecil, misalnya weekend.
- Seluruh anggota recovery team harus ikut.

Recovery Plan Testing (2)

Yang harus dilakukan dalam pengujian BCP :

1. Memeriksa kelengkapan dan ketepatan dari BCP.
2. Mengevaluasi kinerja dari orang-orang yang terlibat dalam uji coba.
3. Menilai cara training dan program penyadaran staf-staf lain.

Recovery Plan Testing (3)

4. Mengevaluasi koordinasi antara tim BC dan external entity, seperti vendor, supplier dan penyelenggara jasa lainnya.
5. Mengukur kapasitas situs alternatif.
6. Mengukur tingkat *retrieveablitiy* dari informasi penting.
7. Mengukur kinerja operasional dari bisnis secara umum.

Tahapan Pengujian

1. Pretest :
   - Persiapan sebelum pengujian, misalnya memasang kabel-kabel di alternate facility atau membawa peralatan komunikasi ke alternate facility.
   - Jadi esensinya memastikan bahwa fasilitas alternatif selalu siap.
2. Test
   - Seluruh kegiatan operasional untuk mendukung business objectives tertentu dilaksanakan. Misalnya: data entry, telephone calls, information systems processing, penanganan order, workflow, dsb.
3. Post-test
   - Mengembalikan alat-alat yang perlu dikembalikan ke tempatnya semula. Tapi yang paling penting adalah analisis formal dan perbaikan-perbaikan BCP

Jenis-jenis test

1. Paper test.

   Walkthrough pada BCP, dengan melibatkan tim BCP serta staf inti yang terlibat.

2. Preparedness test.

   Localized version of full test, actual resource tidak boleh dipakai untuk mensimulasikan system crash. Pengujian dilakukan pada bagian-bagian tertentu, dan mungkin bisa cost effective.

3. Full operational test.

Ukuran-ukuran Pengujian

- Waktu dari tugas-tugas tertentu, pengiriman peralatan/dokumentasi/data, persiapan staf, dsb
- Banyaknya pekerjaan yang dilakukan oleh staf di lokasi fasilitas alternatif
- Jumlah benda yang diminta untuk dipindahkan dan yang sebenarnya diterima
- Keakuratan data dan keakuratan pengolahan data

Pemeliharaan dan Perubahan BCP

BCP jangan dibiarkan bertahun-tahun tanpa ditinjau kembali.

Perubahan bisa disebabkan karena :

1. Aplikasi baru telah dikembangkan.
2. Perubahan strategi bisnis, menyebabkan aplikasi yang dianggap kritis berubah.
3. Perubahan hardware & software.

Pemeliharaan dan Perubahan BCP

Untuk melakukan maintenance BCP dapat dilakukan antara lain :

1. Periodic review.
2. Komentar terhadap hasil review.
3. Melakukan pengujian BCP terjadual maupun mendadak.
4. Melakukan updating BCP.
   - Updating BCP, termasuk daftar nama & nomor telepon.