Tugas Kuliah
Proteksi dan Tehnik Keamanan Sistim Informasi
IKI-83408T

Business Continuity and Disaster Recovery Plan

Dikerjakan oleh,
Usep Solehudin
7204000403

Dosen Pembimbing,
Rahmat M. Samik-Ibrahim
Johny Moningka
Arrianto Mukti Wibowo

UNIVERSITAS INDONESIA
Magister Teknologi Informasi

2005

Daftar Isi

Daftar Gambar

Business Continuity and Disaster Recovery Plan

Berdasarkan goal dari (ISC)2 bagi kandidat CISSP:
"Kandidat diharapkan akan mengetahui perbedaan antara business continuity plan dengan disaster recovery plan; perencanaan bisnis dalam konteks perencanaan dan lingkup proyek, analisa dampak bisnis, startegi pemulihan, pengembangan rencana pemulihan, dan implementasinya. Kandidat harus memahami pemulihan bencana dalam konteks pengembangan rencana pemulihan, penerapan dan restorasi."

Domain dari Busines Continuity Plan (Perencanaan Keberlangsungan Bisnis atau BCP) dan Disaster Recovery Plan (Perencanaan Pemulihan dari Bencana atau DRP), semuanya adalah mengenai bisnis. Sementara domain-domain yang lainnya concern dengan pencegahan risiko dan melindungi infrastruktur dari serangan, domain ini berasumsi bahwa kejadian terburuk telah terjadi. BCP adalah mengenai pembuatan perencanaan dan frame-work untuk menjamin bahwa proses bisnis dapat terus berlanjut dalam keadaan emergensi. Sedangkan DRP adalah mengenai pemulihan cepat dari keadaan emergensi atau bencana, sehingga hanya mengakibatkan dampak minimum bagi organisasi atau perusahaan. [1]

Business Continuity Plan (BCP) dan Disaster Recovery Plan (DRP) adalah dua hal yang sangat penting dalam proses bisnis, namun jarang menjadi prioritas karena alasan memerlukan biaya yang mahal dan sulit penerapannya. Apalagi bencana adalah hal yang umumnya diyakini karena faktor alam yang tak dapat diprediksi dan tak dapat dicegah atau pun dihindari, sehingga kalangan bisnis berkeyakinan bahwa pelanggan mereka akan memaklumi hal ini. Maka hal yang terpenting bagi setiap perusahaan yang berniat membangun BCP adalah mendapatkan dukungan dari pihak manajemen. Sudah terlalu sering BCP menempati urutan prioritas terendah, atau proyek ini ditangani staf junior.

Sebagai contoh adalah keberlangsungan pada perusahaan-perusahaan seperti Merrill Lynch dan Deutsch Bank di New York pada 11 September 2001. Bencana ini menghancurkan masing-masing kantor pusat lokalnya dan menewaskan ratusan karyawannya. Namun setelah situasi stabil, masing-masing mampu melanjutkan operasinya dengan mulus dari sebuah lokasi alternatif tanpa hilangnya data-data yang kritis.

Pencapaian luar biasa ini merupakan bukti kecanggihan dari BCP dan DRP perusahaan-perusahaan tersebut. Industri keuangan/perbankan dikenal lekat dengan standar-standar tertinggi

dalam hal pengujian planning mereka secara berkala, untuk menjamin bahwa semua pihak aware terhadap prosedur-prosedur ini, sehingga planning tersebut tetap sejalan dengan realita dan tujuan bisnis. Sementara industri-industri lainnya cukup banyak variasinya dalam hal pengelolaan BCP dan DRP-nya.

Akan ada pembengkakan ongkos kelewat besar yang harus dibayar untuk merespon dan memulihkan diri dari sebuah bencana tanpa ada persiapan rencana mitigasi. Ongkos kuantitatif untuk memperpanjang interupsi bisnis seperti biaya lembur karyawan, penyewaan fasilitas ad hoc, prioritas akuisisi perangkat keras, denda, dan Service Level Agreement (SLA) yang tidak terpenuhi bisa sangat besar.

Perusahaan-perusahaan yang ingin menampilkan tingkat profesionalisme yang lebih baik dan fokus pada perlindungan dan meningkatkan nilai stakeholder, semakin melihat bahwa continuity plan diperlukan sebagai langkah menghindari interupsi bisnis dan dampaknya dalam ongkos maupun hal-hal lainnya yang tinggi nilainya. Dan seiring dengan perkembangan tehnologi informasi, maka ditemukan tehnologi yang dapat menjamin keberlanjutan bisnis dan pemulihan dari bencana, yang lebih murah dan mudah penerapannya. Bahkan BCP dan DRP telah menjadi standar tersendiri bagi kalangan bisnis terutama yang berhubungan jalannya proses bisnis (aplikasi) dan penyimpanan data.

Tujuan dari BCP dan DRP adalah menjaga bisnis tetap beroperasi meskipun ada gangguan dan menyelamatkan sistem informasi dari dampak bencana lebih lanjut. Proses perencanaan suatu business continuity plan (BCP) akan memungkinkan perusahaan menemukan dan mengurangi (reduce) ancaman-ancaman, merespon (respond) suatu peristiwa ketika peristiwa itu terjadi, pulih (recover) dari dampak langsung suatu peristiwa dan akhirnya mengembalikan (restore) operasi seperti semula. Reduce, respond, recover dan restore ini lebih dikenal sebagai Empat R di BCP. [14]

BCP dan DRP adalah merupakan perencanaan yang hanya tertulis dalam kertas, perencanaan yang baik tentunya akan mampu laksana dan tepat guna saat dilaksanakan, atau saat BCP/DRP action. Sehingga penyiapan BCP dan DRP yang baik, serta pengetesan yang qualified (sesuai dengan keadaan sebenarnya) dan serius serta upaya pemeliharaannya menjadi ukuran terhadap kemampuan organisasi dalam menghadapi ancaman atau bencana. Dengan memiliki rencana kongkrit mengenai apa yang harus dilakukan selama dan setelah gangguan serius terjadi, perusahaan dapat memastikan bahwa gangguan itu hanya berdampak minimal pada proses bisnis utamanya, dan layanan yang layak kepada klien tetap bisa berlanjut.

A. Pengertian dan Perbedaan

BCP dan DRP ditujukan untk memenuhi kebutuhan bisnis dalam menghadapi gangguan-gangguan terhadap operasi perusahaan. Business Continuity Plan dan Disaster Recovery Plan adalah meliputi persiapan, pengujian dan pemutakhiran tindakan-tindakan yang diperlukan untuk melindungi proses bisnis fital (critical) terhadap dampak dari kegagalan jaringan dan sistem utama. Kandidat CISSP harus memahami persiapan yang dibutuhkan untuk melakukan tindakan-tindakan spesifik yang diperlukan saat adanya kegagalan atau penundaan operasi bisnis suatu perusahaan atau organisasi. [1]

Proses BCP adalah meliputi:

- Inisiasi Perencanaan dan Lingkup

- Business Impact Assessment (BIA)
- Pengembangan Business Continuity Plan

Proses DRP adalah meliputi:

- Proses Disaster Recovery Planning
- Pengujian Disaster Recovery Plan
- Prosedur Pemulihan Bencana

A.1. Pengertian Business Continuity Plan (BCP)

BCP adalah proses otomatis atau pun manual yang dirancang untuk mengurangi ancaman terhadap fungsi-fungsi penting organisasi, sehingga menjamin kontinuitas layanan bagi operasi yang penting. [16] Perencanaan keberlangsungan bisnis dibuat untuk mencegah tertundanya aktivitas bisnis normal. BCP didisain untuk melindungi proses bisnis vital dari kerusakan atau bencana yang terjadi secara alamiah atau perbuatan manusia, dan kerugian yang ditimbulkan dari tidak tersedianya proses bisnis normal (rutin, seperti biasa). Business Continuity Plan merupakan strategi untuk meminimalisir efek dari ganguan dan mengupayakan berjalannya kembali proses bisnis suatu organisasi atau perusahaan.

Kejadian atau hal-hal yang menahan proses bisnis adalah segala sesuatu gangguan keamanan yang terduga dan tak terduga yang bisa mematikan operasi normal bisnis dalam kurun waktu tertentu. Tujuan dari BCP adalah untuk meminimalisir efek dari kejadian atau bencana tersebut dalam sebuah perusahaan atau organisasi. Manfaat utama dari Business Continuity Plan adalah untuk mereduksi risiko kerugiaan keuangan dan meningkatkan kemampuan perusahaan untuk memulihkan diri dari bencana atau gangguan sesegera mungkin. Perencanaan keberlangsungan bisnis juga harus dapat membantu meminimalisir biaya dan mengurangi risiko sehubungan dengan kejadian bencana tersebut.

Business Continuity Plan perlu memperhatikan semua area proses informasi kritis dari perusahaan, seperti hal di bawah ini; [1]

- LAN, WAN, dan server
- Hubungan telekomunikasi dan komunikasi data
- Lokasi dan ruang kerja
- Aplikasi, software, dan data
- Media dan tempat penyimpanan rekaman/data
- Proses produksi dan staf-staf yang bekerja

Prioritas nomor satu dari semua perencanaan keberlangsungan bisnis dan pemulihan bencana adalah selalu people first, mengutamakan manusianya. Sementara kita membahas mengenai pentingnya kapital, kembali beroperasinya aktivitas bisnis normal, dan issu keberlanjutan bisnis lainnya, perhatian utama yang harus ditangani dalam perencanaan adalah untuk mengeluarkan atau menghindarkan manusia dalam hal ini pegawai akan bahaya dari suatu bencana. Jika pada saat yang bersamaan ada pertentangan apakah menyelamatkan hardware atau data ketimbang manusia terhadap ancaman bahaya fisik, perlindungan untuk manusia harus yang diutamakan. Keselamatan dan evakuasi personnel harus menjadi komponen pertama dalam perencanaan menghadapi bencana. [1]

A.2. Pengertian Disaster Recovery Plan (DRP)

DRP adalah prosedure yang dijalankan saat BCP berlangsung (in action) berupa langkah-langkah untuk penyelamatan dan pemulihan (recovery) khususnya terhadap fasilitas IT dan sistem informasi. Disaster Recovery Plan merupakan pengaturan yang komprehensive berisikan tindakan-tindakan konsisten yang harus dilakukan sebelum, selama, dan setelah adanya kejadian (bencana) yang mengakibatkan hilangnya sumber daya sistem informasi secara bermakna. DRP berisikan prosedur untuk merespon kejadian emergensi, menyediakan operasi backup cadangan selama sistem terhenti, dan mengelola proses pemulihan serta penyelamatan sehingga mampu meminimalisir kerugian yang dialami oleh organisasi.

Tujuan utama dari Disaster Recovery Plan adalah untuk menyediakan kemampuan atau sumber daya untuk menjalankan proses vital pada lokasi cadangan sementara waktu dan mengembalikan fungsi lokasi utama menjadi normal dalam batasan waktu tetentu, dengan menjalankan prosedur pemulihan cepat, untuk meminimalisir kerugian organisasi. [1]

Mungkin saja sebuah organisasi tidak memerlukan disaster recovery plan. Jika organisasi tersebut memiliki unit bisnis yang dapat bertahan selama masa interupsi, atau bisa saja organisasi tersebut tidak memiliki area proses vital yang diperlukan beberapa jenis pemulihan bencana. Dalam hal ini, disaster recovery plan mungkin tidak perlu diterapkan oleh organisasi tersebut. Kita telah tahu bahwa ada perusahaan yang tidak memerlukan beberapa jenis rencana kontingensi plan. [1]

A.3. Perbedaan antara BCP dengan DRP

Tujuan akhir dari Business Continuity Plan dan Disaster Recovery Plan adalah sama yaitu untuk menjamin keberlangsungan proses bisnis penting atau utama. DRP merupakan bagian atau subset dari strategi yang ada pada BCP dalam menghadapi bencana yang mengancam keberlangsungan proses bisnis penting. [10]

Pada saat bisnis requirement berubah dan mengharuskan adanya pemulihan atau penyiapan dari fungsi-fungsi bisnis yang penting, maka solusi/rencana yang dibuat adalah berupa BCP. Dalam banyak kasus BCP tidak dikontrol oleh unit tehnologi Informasi (TI), biasanya ditangani oleh bagian sekuriti organisasi atau keuangan. Sedangkan DRP adalah murni domain dari Tehnologi Informasi, bagian TI-lah yang menghasilkan Disaster Recovery Plan. Segala sesuatu umumnya berfokus kepada “bagaimana memulihkan sistem data mereka”. [14]

Dua konsep ini (BCP dan DRP) adalah sangat berhubungan erat dan perlu memadukannya dalam satu domain. Memang ada beberapa perbedaan, namun pada dasarnya business continuity plan adalah proses dalam membuat perencanaan yang akan menjamin fungsi bisnis vital dapat bertahan dalam berbagai keadaan emergensi. Disaster recovery plan mencakup pembuatan persiapan terhadap bencana dan juga menentukan prosedur yang harus diikuti selama dan setelah interupsi proses bisnis vital. [1]

Namun demikian perencanaan memerlukan keterlibatan unit lain dan dukungan dari DRP yang scopenya lebih besar. Disaster Recovery Plan hanya berfokus pada sumberdaya TI, sedangkan BCP sifatnya lebih luas dengan merencanakan secara menyeluruh keberlanjutan sebuah bisnis. BCP mempertimbangkan akses ke berbagai fasilitas, ketersediaan orang, proses bisnis serta pemulihan TI.

B. Bencana dan Jenisnya

Sebuah bencana (disaster) didefinisikan sebagai apapun peristiwa tak terencana atau tak terduga, yang mengganggu fungsi-fungsi bisnis penting untuk periode waktu tidak tertentu. Jadi, crash-nya sebuah server IVR misalnya, tidak serta merta menjadikan BCP diberlakukan. Namun, peristiwa itu menyebabkan inisiasi DRP, jika diestimasikan dampaknya berupa ketidaktersediaan sumberdaya dalam sebuah periode waktu kritis tertentu. Bencana dalam hal ini adalah yang berpotensi mengancam atau menghentikan keberlangsungan proses bisnis. Bencana meliputi yang alami dan karena manusia baik disengaja maupun tidak. [1]

Kita dapat membedakan bencana sebagai berikut:

1. Bencana alam, yaitu kejadian-kejadian alami seperti banjir, genangan, gempa bumi, gunung meletus, badai, kekeringan, wabah, serangga dan lainnya.
2. Bencana lainnya yang meliputi tabrakan pesawat udara atau kendaraan, kebakaran, huru-hara, sabotase, ledakan, gangguan listrik, ganguan komunikasi, gangguan transportasi dan lainnya.
3. Ancaman yang “bukan bencana”, seperti pemogokan, gangguan perangkat lunak, gangguan perangkat keras, Denial of services, Virus dan lainnya.

Sedangkan berdasarkan cakupan wilayah, bencana terdiri dari: [13]

1. Bencana Lokal. Bencana ini biasanya memberikan dampak pada wilayah sekitarnya yang berdekatan. Bencana terjadi pada sebuah gedung atau bangunan-bangunan disekitarnya. Biasanya adalah karena akibat faktor manusia seperti kebakaran, ledakan, terorisme, kebocoran bahan kimia, dan lainnya. Kita dapat mengharapkan bantuan dari pihak luar dalam merespond kejadian emergensi ini.
2. Bencana Regional. Jenis bencana ini memberikan dampak atau pengaruh pada area geograpis yang cukup luas, dan biasanya disebabkan oleh faktor alam, seperti badai, banjir, letusan gunung, tornado dan lainnya. Pada kejadian ini diperlukan bantuan khusus seperti dari pihak Palang Merah dan lainnya, Kita diharapkan bisa bertahan untuk waktu sekitar 72 jam.

Bencana-bencana tersebut dapat berlangsung beberapa waktu menit, jam dan bahkan berhari-hari, serta dapat memaksa penggunaan fasilitas TI alternatif atau data backup off-site. Adapun antisipasi terhadap kemungkinan terburuk adalah dengan menggunakan 2 strategi: [16]

1. Strategi jangka pendek (short-term), yaitu dengan menyediakan fasilitas TI alternatif.
2. Strategi jangka panjang (long-term), yaitu dengan menyediakan fasilitas TI yang permanen.

C. Business Continuity Plan

Memiliki sebuah BCP dipandang sebagai sebuah jaminan kebijakan yang memberikan kontribusi pada “good governance”-nya sebuah bisnis. Namun, tidak semua industri atau negara di dunia menyadari pentingnya nilai BCP. Di seluruh dunia, industri jasa keuangan adalah terdepan dibanding industri lainnya dalam persyaratan BCP yang up todate dan tested. Regulasi-regulasi ini ditegakkan dengan audit-audit internal dan eksternal dan dalam kasus-kasus ekstrim dengan berbagai sanksi dan denda.

Beberapa badan regulasi tertentu mengawasi persyaratan mutlak untuk BCP di negara-negara yang berbeda. Di AS, ada US Federal Reserve Board yang melakukan tugas ini. Kemudian di Singapura, ada Monetary Authority of Singapore (MAS) dan di Hong Kong ada Hong Kong Monetary Authority (HKMA). Biasanya badan-badan seperti ini selalu mengikuti best practise dari seluruh dunia dan menyebarluaskannya ke institusi-institusi di bawahnya. [14]

Dampaknya, sebagian besar dari masyarakat terjamin dan tenang bahwa jika ada bencana yang menimpa bank, perusahaan sekuritas, asuransi atau institusi keuangan lainnya yang menjadi rekan usaha atau penyedia jasa untuk masyarakat, mereka mampu bertahan dari peristiwa tersebut untuk melanjutkan pelayanan kepada masyarakat sebagai customer atau rekan bisnis dalam periode waktu yang sewajarnya.

Proses perencanaan suatu business continuity plan (BCP) akan memungkinkan perusahaan atau organisasi menemukan dan mengurangi (reduce) ancaman-ancaman, merespon (respond) suatu peristiwa ketika peristiwa itu terjadi, pemulihan (recover) dari dampak langsung suatu peristiwa atau bencana, dan akhirnya mengembalikan (restore) operasi menjadi seperti semula. Reduce, respond, recover dan restore ini lebih dikenal sebagai Empat R di BCP. [14]

C.1. Business Continuity dan Service Level Agreements (SLA)

Umumnya organisasi tidak beroperasi secara terisolasi, keputusan untuk melakukan out source proses bisnis ke vendor eksternal ditentukan berdasarkan beberapa kriteria seperti alasan ekonomis atau harga dan keuntungan fungsional dari suatu tehnologi. Saat suatu bisnis proses di outsource, TOR (Term of Reference), peran dan tanggung jawab akan ditetapkan dalam kontrak, bersamaan dengan dukungan terhadap SLA. Service Level Agreement (SLA) meliputi layanan yang akan diberikan, peran dan tanggung jawab operasional dan ketentuan dalam penyediaan layanan, oprasional dan quality, serta biaya layanan. Intinya adalah menggunakan Service Level Agreement (SLA) untuk menentukan efektivitas dan efisiensi dari performa vendor.

Kunci keberhasilan untuk memadukan business impact analysisn (BIA) dengan service level agreement (SLA) adalah mendapatkan data-data (dokument) dari pemilik/user dan pengembang, sehingga dokumen pada BIA dapat dipadukan dengan SLA. BIA sangat diperlukan untuk menetapkan tingkat critical operasi bisnis. Berdasarkan buku Central Computer and Telecommunication Agency (CCTA), “A Guide to Business Continuity Management,” tahun 1995. BIA mengidentifikasi potensi kerusakan atau kehilangan yang mungkin disebabkan oleh bencana, terhadap proses-proses bisnis yang critis.
Business impact analysis (BIA) juga memberikan informasi mengenai toleransi terhadap bencana, maksimal waktu yang diperkenankan terhadap terhentinya sistem atau aplikasi, dan berbagai tingkatan toleransi terhadap interupsi tersebut pada operasi bisnis yang berbeda-beda. Hal ini menuntut manajemen organisasi untuk mau memastikan bahwa service level agreement (SLA) merefleksikan kerusakan maksimal yang bisa diterima pada operasi-operasi tertentu. Recovery

time objective (RTO) dan a recovery point objective (RPO) perlu dikuantifikasi sehubungan dengan peran vendor yang dipilih.

C.2. Dua puluh Fakta tentang Keberlanjutan Bisnis [5]

Jika seseorang mendapat tangung jawab untuk mengembangkan business continuity plan (BCP) dalam kurun waktu tertentu, maka orang tersebut akan dihadapkan pada beberapa karakteristik program yang harus diperhitungkan. Setelah selama dua puluh tahun membantu beberapa organisasi dalam mengembangkan business continuity dan disaster recovery plan. Minnich mencatat beberapa karakteristik, atau keyakinan yang tak pernah gagal, yaitu sebanyak dua puluh keyakinan, “20 truth” sebagai berikut:

1. Biaya untuk pencegahan adalah lebih murah ketimbang biaya untuk pemulihan, dan pecegahan jauh lebih cepat.
2. Jika real estate itu harganya murah, pasti ada alasannya. Saat mencari fasilitas untuk sumber daya cadangan atau alternatif, pastikan bahwa risiko tidak ada ditempat tersebut.
3. Jangan taruh semua telur dalam satu keranjang. Tempatkan operasi-operasi bisnis vital secara menyebar, jangan memusat, tempatkan pada beberapa lokasi.
4. Saat bencana timbul, hal pertama yang bisa hilang adalah perencanaan. Kondisi yang tenang atau tidak panik, membuat kita mampu mengikuti prosedure yang telah ditetapkan, pada saat terjadi bencana.
5. Saat bencana timbul, para kompetitor akan memanfaatkannya. Pemulihan yang lama akan membuat reputasi perusahaan turun, dan para kompetitor akan memanfaatkan kekosongan tersebut.
6. Polis asuransi menjadi benar-benar jelas setelah adanya bencana. Jangan menunggu adanya bencana, polis asuransi bisa membantu perusahaan dalam menghadapi kerugian akibat bencana.
7. Rumah and, Kehidupan dan kendaraan diasuransikan ... Ini benar-benar sudah melindungi, atau tidak. Perlindungan terhadap bisnis sangat penting. Kegagalan bisnis karena bencana, dan tanpa asuransi, menjadi bencana bagi perusahaan dan individu atau pegawai.
8. Tiga P dalam disaster plan: People, Property, Priorities (business). Ada tiga lagi: Praktek, Praktek, Praktek. Praktek atau berlatih adalah satu-satunya cara untuk kita supaya lebih baik dalam segala hal yang kita lakukan. Jika kita tidak pernah atau jarang mempraktekkan rencana kita, maka kita tidak akan mampu menghadapi bencana selancar yang kita harapkan. Bahkan pemain olah raga profesional pun sering berlatih.
9. Terapkan investasi untuk keberlanjutan bisnis sesuai dengan prioritas dan ancaman yang ada. Pastikan bahwa segala sesuatu yang akan dilindingi memiliki nilai terhadap bisnis dan ancaman yang bisa mengenainya.
10. Lindungilah orang terlebih dahulu, karena jika ada benda yang hilang maka benda-benda lain akan bisa menggantikannya. Kehilangan pegawai akan selalu ada di benak orang-orang dan bisa selama-lamanya.
11. Pemulihan adalah seperti resep; segala sesuatu harus datang bersamaan pada waktu yang tepat dan dalam bentuk yang bisa digunakan. Pemulihan membutuhkan berbagai perangkat pendukung yang tepat waktu dan dapat digunakan, seperti halnya saat memasak.
12. Pastikan pimpinan telah menentukan prioritas, sebelum bencana terjadi. Dan mengapa hal tersebut menjadi prioritas. Jangan sampai bingung menentukan prioritas sementara bencana sudah menimpa.

13. Libatkan pimpinan dalam proses perencanaan. Jika pimpinan tidak terlibat dalam perencanaan, jangan harapkan mereka akan mengikuti perencanaan, padahal mereka yang akan memimpin proses pemulihan. Jangan sampai rencana tak digunakan, jadi sia-sia.
14. Prioritas pertama pegawai adalah keluarga mereka. Pada saat bencana yang cakupan wilayahnya luas atau regional, pastikan pegawai anda sudah memastikan kondisi keluarganya, sehingga mereka bisa bekerja, melakukan pemulihan bisnis dengan tenang.
15. Pegawai pasti akan membantu proses pemulihan. Tapi pastikan adanya petunjuk yang telah disiapkan sebelumnya. Sehingga karyawanan tahu apa yang harus dilakukannya dan tidak jalan sendiri-sendiri.
16. Bencana membuat kita paham siapa sahabat sebenarnya. Sahabat-sahabat sejati pasti akan bersedia saling bantu.
17. Pastikan kita telah berkonsultasi dengan petugas pemadam, polisi dan lainnya sebelum membuat rencana pemulihan. Karena pada kondisi bencana, terutama yang bersifat regional, mereka lah yang memegang kendali, terkadang membuat pegawai tersinggung.
18. Software rencana pemulihan mengelola rencana data, tidak bisa membuat rencana untuk manusia. Software tersebut tidak akan bisa mengambil alih strategi pemulihan, tidak akan mengurangi risiko dari ancaman, dan tidak bisa mengambil alih sisi kemanusiaan dalam pemulihan bisnis. Tempatkan software pada waktu yang tepat saat proses perencanaan pemulihan.
19. Jangan pernah mudah percaya dengan apa yang dibaca, terutama dalam perencanaan pemulihan dari bencana. Lakukan pengetesan!
20. Selalu dapatkan persetujuan dari atasan. Perencanaan tanpa persetujuan pihak manajemen tidak akan mampu laksana, karena pada implementasinya tidak akan mendapatkan dukungan sumber daya dan kepemimpinan yang dibutuhkan.

C.3. Pengembangan BCP

Untuk membangun sebuah BCP dibutuhkan informasi-informasi dari beberapa bagian yang berbeda seperti pengetahuan mengenai pengoperasian, pemahaman mengenai fungsi-fungsi bisnis yang penting di dalam pengoperasian, penentuan waktu sasaran pemulihan (recovery) untuk fungsi-fungsi ini, memahami ancaman lokal, pengetahuan mengenai regulasi lokal, dan beberapa hal lainnya.

Orang yang bertugas sebagai koordinator BCP harus memimpin usaha ini selayaknya seorang project manager, seperti halnya inisiatif-inisiatif formal lainnya yang lazim dilakukan sebuah perusahaan. Namun demikian, memahami seluk beluk pengoperasian perusahaan atau organisasi akan sangat membantu dalam menyiapkan planning yang relevan dan praktis. Beberapa team leader yang bertanggung jawab terhadap berbagai aspek pengoperasian perusahaan harus dilibatkan untuk membantu memahami fungsi-fungsi bisnis yang penting, dan membantu membuat prioritas dan menentukan recovery time objectives (RTO).

Ada empat element atau langkah-langkah dalam membangun sebuah BCP yang baik, yaitu meliputi: [1]

Pembuatan Cakupan dan Rencana. Tahapan ini menandai dimulainya proses BCP. Hal yang dilakukan adalah membuat lingkup dan elemen lainnya yang diperlukan untuk menentukan parameter dari rencana.

Business Impact Assassment (BIA). Proses ini dilakukan sebelum membuat Disaster Recovery Plan. BIA digunakan untuk membantu unit bisnis memahami dampak dari bencana. Tahapan ini

adalah meliputi pelaksanaan analisa risiko dan menentukan dampak terhadap perusahaan jika potential loss yang teridentifikasi oleh risk analysis sungguh-sungguh terjadi.

Pembuatan Business Continuity Plan. Tahapan ini menggunakan informasi yang didapat pada proses BIA untuk mengembangkan business continuity plan yang sebenarnya. Proses pengembangannya adalah meliputi rencana implementasi, rencana pengujian, dan pemeliharaan rencana yang dijalankan. Tahapan ini juga menentukan strategi pengoperasian business recovery alternatif untuk pemulihan bisnis dan kapabilitas TI di dalam periode recovery time yang sudah ditentukan.

Persetujuan dan Implementasi. Proses ini terdiri dari mendapatkan persetujuan akhir dari manajemen senior, penyiapan sebuah program awareness korporat dan menerapkan prosedur pemeliharaan untuk meng-update rencana sesuai dengan kebutuhan.

Business Impact Assassment (BIA) seringkali dijalankan dengan fokus utamanya pada potensi dampak atau kebalikan dari BAU (business as usual). BIA perlu menilai risiko berdasarkan catatan historis dari bencana alam dan konsekuensinya terhadap proses bisnis, dan menimbang risiko-risiko ini terhadap fungsi-fungsi penting yang dijalankan sebuah perusahaan. Biasanya fungsi-fungsi yang menuntut down time paling kecil ini adalah fungsi-fungsi yang memiliki dampak finansial yang signifikan (misalnya sebuah bank tidak mampu menerima telepon dari seorang customer untuk memblokir pembayaran sebuah cek) atau yang menyebabkan terjadinya pelanggaran Service Level Agreement (SLA).

Perusahaan-perusahaan lainnya mungkin akan menganggap ketidaktersediaan selama periode inbound yang kritis (misalnya setelah kampanye promosi diluncurkan) atau periode-periode sibuk yang sudah jadi tradisi (misalnya saat lebaran, natal atau tahun baru) akan berdampak sangat besar sehingga memerlukan kelonggaran dan memiliki strategi pelaksanaan recovery. Segera setelah direncanakan, BCP harus diuji atau di-exercise. Untuk hal ini, pengetahuan tentang seluk beluk proses bisnis sebuah perusahaan menjadi syarat mutlak bagi seorang koordinator BCP yang berusaha merancang latihan (exercise) yang secara realistis memasukkan seluruh skenario kedalamnya, tanpa harus mengganggu BAU.

Dengan BCP, perusahaan bisa memformulasikan rencana kelanjutan bisnisnya secara jelas ketika bencana terjadi dan dapat mengurangi potensi gangguan-gangguan terhadap pengoperasian perusahaan serta mengembalikannya ke keadaan semula seefisien mungkin.

C.3.1. Pembuatan Cakupan dan Rencana

Tahapan pembuatan cakupan dan rencana adalah langkah pertama untuk membuat business continuity plan. Tahap ini menandai dimulainya proses BCP. Hal yang dilakukan adalah membuat lingkup dan elemen lainnya yang diperlukan untuk menentukan parameter dari rencana. Aktivitas pembuatan cakupan (lingkup) meliputi pembuatan detail pekerjaan yang diperlukan, membuat list sumber daya yang akan digunakan, dan menetapkan praktek manajemen yang akan dikerjakan.

Dengan adanya personal komputer di tempat kerja, proses yang terdistribusi memberikan masalah khusus kepada BCP proses. Sangatlah penting, bahwa upaya perencanaan terpusat dapat mempersingkat semua sistem dan proses yang terdistribusi. [1]

Proses BCP melibatkan banyak personnel dari berbagai bagian di perusahaan. Pembentukan komite BCP akan menempatkan keterlibatan pimpinan perusahaan terhadap unit bisnis yang memiliki fungsi vital. Semua unit bisnis lainnya akan terlibat sesuai dengan kebutuhan, terutama selama implementasi dan tahap peningkatan kepedulian.

Komite BCP
Komite atau tim BCP perlu dibentuk dan diberikan tanggung jawab untuk membuat, menerapkan, dan menguji rencana. Komite ini terbentuk atas perwakilan dari senior manajemen, seluruh unit bisnis fungsional, sistem informasi, dan administrasi sekuritas. Komite berupaya menentukan lingkup dari perencanaan, yang harus berhubungan dengan upaya pemulihan awal dari dampak bencana dan mengurangi dampak finansial dan kehilangan sumber daya karena bencana atau ancaman tersebut. [1]

Peran Manajer Senior
Manajemen Senior memiliki tanggung jawab yang menentukan pada setiap tahap perencanaan, yang tidak hanya termasuk menginisiasi proses perencanaan namun juga mengelola dan memonitoring rencana selama pengujian serta mensupervisi dan menerapkannya selama terhentinya proses bisnis utama. [1]

C.3.2. Business Impact Assessment

Tujuan dari BIA adalah untuk membuat sebuah dokument yang akan digunakan untuk membantu memahami dampak yang terjadi dari bencana terhadap proses bisnis suatu perusahaan. Dampak bisa secara finansial (kuantitatif) atau operasional (kualitatif, seperti ketidak mampuan untuk merespon komplain dari pelanggan). Analisa Risiko sering menjadi bagian dari proses BIA.

Business Impact Assessment memiliki tiga tujuan utama; [1]

Prioritas Kritis. Setiap proses unit bisnis yang kritis harus diidentifikasi dan dibuat prioritasnya, dan dampak dari kejadian bencana harus dievaluasi. Lebih jelasnya, proses bisnis yang tidak terikat waktu akan diterapkan memiliki tingkat prioritas yang lebih rendah untuk dipulihkan dari pada proses bisnis yang terikat dengan waktu.

Perkiraan Downtime. BIA digunakan untuk membantu memperkirakan *MaximumTolerable Downtime* (MTD) atau maksimal lamanya waktu downtime yang dapat ditolerir dan dipraktekan oleh perusahaan.

Kebutuhan Sumberdaya. Kebutuhan sumber daya untuk proses yang vital juga bisa diidenfikisai pada saat ini, proses yang sangat tergantung pada waktu akan lebih diutamakan untuk mendapatkan alokasi sumber daya.
Bisnis Impact Assessment (BIA) secara umum melakukan empat tahapan berikut;

1. Mengumpulkan materi-materi assessment yang dibutuhkan
2. Melakukan Analisa risiko
3. Menganalisa informasi yang didapatkan
4. Mendokumentasikan hasil dan mempresentasikan rekomendasi

Mengumpulkan Materi-Materi Assessment
Tahap awal dari BIA adalah mengidentifikasi unit bisnis mana yang paling penting (vital, kritikal) untuk tetap dijalankan pada tingkat operasi yang diperkenankan. Sering kali titik awalnya adalah sebuah struktur organisasi simple yang memperlihatkan hubungan antara unit bisnis. Dokumen lainnya yang perlu dikumpulkan adalah berupa hubungan kegiatan-kegiatan fungsional antar unit bisnis.

Hal-hal yang perlu ditanyakan dalan BIA ini adalah meliputi; [16]

- Informasi sumber daya yang penting bagi organisasi
- Proses bisnis yang kalau tidak berjalan akan memberikan dampak negatif yang fatal bagi perusahaan

Setiap proses perlu 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

Setelah bahan-bahan terkumpulkan dan fungsi-fungsi operasai bisnis teridentifikasi, proses BIA akan mencoba hubungan antar fungsi bisnis ini terhadap beberapa faktor seperti kesuksesan bisnis, skala prioritas antar unit bisnis, dan prosedure proses alternatif yang dapat digunakan.

Analisa Risiko [1]
Fungsi dari analisa ini adalah untuk melakukan analisa terhadap dampak bencana. Akan ada 2 bagian analisa yaitu secara finansial (kuantitatif) dan operasional (kualitatif).

Secara kuantitatif akan meliputi:

- Kerugian secara finansial terhadap pendapatan, pengeluaran modal, atau tanggung jawab personal.
- Pengeluaran operasional tambahan dalam perbaikan dampak dari bencana
- Kerugian finansial berkaita dengan persetujuan kontrak kerja
- Kerugian finansial karena adanya tuntutan dari pihak lain

Secara kualitatif analisa risiko meliputi;

- Kehilangan keunggulan kompetitif atau market share
- Kehilangan kepercayaan public atau kredibilitas

Salama melakukan analisa risiko, area-area pendukung yang utama harus bisa ditetapkan dalam rangka menilai dampak dari kejadian bencana. Area pendukung utama adalah unit atau fungsi bisnis yang harus ada untuk mempertahankan keberlanjutan proses bisnis, menjaga keselamatan jiwa, atau menghindari hubungan ke masyarakat yang memalukan. Area pendukung utama dapat berupa hal-hal berikut;

- Telekomunikasi, komunikasi data, atau area tehnologi informasi
- Infrastruktur fisik atau fasilitas pabrik, layanan transportasi
- Akunting, neraca pembayaran, proses transaksi, layanan pelanggan

Adapun klasifkasi dari analisa risiko adalah meliputi: [16]

1. **Critical.** Fungsi-fungsi ini tidak bisa bekerja kecuali digantikan oleh fungsi yang serupa. Tidak bisa digantikan dengan metode manual.

2. **Vital.** Bisa dilakukan secara manual pada rentang waktu yang pendek sekali. Sebaiknya direstore dalam waktu tidak lebih dari 5 hari.

3. **Sensitive.** Bisa dilakukan secara manual dalam waktu yang relatif lama, namun meskipun dilakukan secara manual pasti tetap sulit untuk melakukannya dan membutuhkan keterlibatan staf yang lebih banyak.

4. **Noncritical.** Bisa diinterupsi sampai waktu yang lama, dengan sedikit beban atau tidak ada beban biaya bagi perusahaan.

Menganalisa Informasi
Aktifitas yang dilakukan adalah mendokumentasikan proses yang dibutuhkan, identifikasi hubungan atau ketergantungan antar unit bisnis, dan menentukan lamanya waktu penundaan proses bisnis yang dapat diterima. Tujuan dari analisa informasi ini adalah untuk menggambarkan secara jelas mengenai dukungan apa yang dibutuhkan oleh fungsi-fungsi bisnis utama. Komponen analisa akan disusun berdasarkan unit-unit bisnis yang ada pada perusahaan.

Mendokumentasikan hasil dan mempresentasikan rekomendasi
Tahap akhir business impact assessment (BIA) adalah membuat sebuah dokumentasi lengkap dari semua proses, prosedur, analisa dan hasil serta presentasi rekomendasi kepada senior manajemen yang sesuai. Laporan kan berisikan bahan-bahan yang telah dikumpulkan, daftar dukungan kristis yang teridentifikasi, ringkasan analisa dampak kuantitatif dan kualitatif, dan memberikan rekomendasi prioritas pemulihan berdasarkan proses analisa tersebut.

Sistem Toleransi Kegagalan [4]
“Maaf, sistem komputer kami sedang tidak dapat digunakan” adalah kalimat yang akrab bagi banyak pemakai akhir. Berbagai pengendalian dapat mencegah kegagalan komputer semacam itu atau dapat meminimalkan pengaruhnya. Sistem komputer gagal karena beberapa alasan –listrik mati, tidak berfungsinya sirkuit elektronik, masalah dalam jaringan telekomunikasi, kesalahan pemrograman yang tersembunyi, virus komputer, kesalahan operator komputer, dan vandalisme elektronik. Contohnya, komputer tersedia dengan kemampuan untuk pemeliharaan jarak jauh dan otomatis. Program pemeliharaan dan perawatan untuk hardware serta pembaruan manajemen software adalah hal biasa. Kemampuan sistem komputer cadangan dapat diatur dengan organisasi pemulihan bencana. Perubahan hardware dan software utama biasanya dijadwalkan secara hati-hati serta diimplementasikan untuk untuk menghindari masalah. Personel pusat data yang terlatih baik dan penggunaan software manajemen kinerja serta keamanan membantu menjaga sistem komputer perusahaan dan jaringannya untuk bekerja dengan benar.

Banyak perusahaan juga menggunakan sistem komputer pentoleransi kegagalan (fault tolerant) yang memiliki banyak prosesor, periferal, dan software yang memberikan kemampuan fail over untuk mendukung berbagai komponen ketika terjadi kegagalan sistem. Sistem ini dapat memberikan kemampuan fail safe dengan sistem komputer tetap beroperasi di tingkat yang sama bahkanjika terdapat kegagalan besar pada hardware atau software. Akan tetapi banyak sistem komputer pentoleransi kegagalan menawarkan kemampuan fail soft yang memungkinkan sistem komputer terus beroperasi dalam tingkat yang lebih rendah tetapi dapat diterima jika ada kegagalan sistem yang besar. Gambar berikut memberikan garis besar tentang beberapa kemampuan toleransi atas kegagalan yang digunakan dalam banyak sistem komputer serta jaringan.

Lapisan	Ancaman	Metode Toleransi Kegagalan
Aplikasi	Lingkungan, kegagalan hardware dan software	Redundansi khusus aplikasi dan kembali ke titik pemeriksaan sebelumnya
Sistem	Interupsi	Isolasi sistem, keamanan data, integritas sistem
Data Base	Kesalahan dan Kerusakan data	Pemisahan transaksi dengan pembaruan simpanan, sejarah transaksi yang lengkap, file cadangan
Jaringan	Kesalahan transmisi	Pengendalian yang andal; asynchrony dan handshaking yang aman; routing alternatif; kode pendeteksi kesalahan dan perbaikan kesalahan
Proses	Kegagalan hardware dan software	Komputasi alternatif, kembali ke titik pemeriksaan
File	Kesalahan media	Replikasi data penting dalam lokasi dan situs yang berbeda; pembentukan archive, pembuatan cadangan, dan penarikan data
Prosesor	Kegagalan hardware	Mencoba kembali perintah; kode perbaikan kesalahan dalam memori dan pemrosesan; replikasi; multi prosesor dan memori

Gambar 1.; Berbagai metode toleransi atas kegagalan dalam sistem informasi berbasis komputer.

Visa International: Sistem Pentoleransi Kegagalan

"Tidak ada yang disebut keandalan 99.9 persen; seharusnya 100 persen," kata Richard L. Knight, wakil direktur utama senior untuk operasi di Inovant Inc., anak perusahaan Visa International yang menjalankan pusat datanya. "Jika ada apa pun yang kurang dari 100 persen, saya akan mencari pekerjaan baru." Perusahaan itu mengalami waktu kegagalan selama 98 menit dalam 12 tahun. Visa berjuang dalam perang melawan interupsi dan kecacatan sebagai dua dasar utama; Gedung pemrosesan fisiknya dilindungi oleh beberapa lapis redundancy dan cadangan, serta belanja TI perusahaan itu telah meningkatkan proses pengujian software menjadi suatu karya seni.

Terdapat lebih dari 1 milyar kartu pembayaran Visa yang beredar di seluruh dunia, menghasilka transaksi senilai $2 trilliun per tahun untuk 23 juta pedagang dan ATM serta 21.000 anggota lembaga keuangan Visa. "Kami menjalankan mesin pembayaran terbesar di dunia," kata Sara Garrison, wakil direktur utama senior bagian pengembangan sistem di Visa U.S.A. Inc. Yang berlokasi di Foster City, California. "Jika anda mengambil semua lalu lintas transaksi di seluruh pasar modal di dunia dalam 24 jam, kami melakukan transaksi sejumlah itu selama waktu istirahat minum kopi. Selain tiu, kapasitas Kami tumbuh 20 hingga 30 persen dari tahun ke tahun, hingga setiap tiga tahun, kapasitas kami meningkat dua kali lipat."

Visa memiliki empat pusat pemrosesan global untuk menangani beban itu, tetapi fasilitas di Washington D.C. adalah yang terbesar, dengan separuh dari transaksi pembayaran global mengalir melalui gedung tersebut. Fasilitas itu berbagi lalu lintas di AS dengan sebuah pusat di San Mateo, California, tetapi dapat secara instan mengambil alih seluruh beban di AS jika San Mateo mengalami kegagalan.

Bahkan, segala sesuatu dalam infrastruktur pemrosesan Visa –dari seluruh pusat data hingga komputer, setiap prosesor, dan switch komunikasi- memiliki cadangan. Bahkan, cadangan-cadangan tersebut memiliki cadangan juga.

C.3.3. Pembuatan Business Continuity Plan [1]

Penyusunan business continuity plan adalah bedasarkan informasi yang didapatkan saat business impact assessment (BIA), dalam rangka membuat rencana strategi pemulihan untuk mendukung fungsi-fungsi bisnis critical tersebut. Di sini kita mengambil informasi yang dikumpulkan saat BIA dan mulai memetakan strategi untuk membuat sebuah rencana keberlangsungan bisnis.

Tahapan ini terdiri dari:

1. Menentukan strategi keberlangsungan
2. Mendokumentasikan strategi keberlangsungan

Penentuan strategi keberlangsungan meliputi;

- Komputer; yaitu komponen hardware, software, jalur komunikasi, aplikasi dan data.
- Fasilitas; yaitu gedung utama atau kampus, dan fasilitas remote lainnya.
- People; yaitu operator, manajemen, dukungan tehnis.
- Perlengkapan dan bahan; yaitu kertas, formulir, HVAC, atau perlengkapan khusus untuk pengamanan

Pendokumentasisn strategi keberlangsungan cukup mengacu pada pembuatan dokumentasi hasil-hasil dari proses penentuan strategi keberlangsungan. Dokumentasi diperlukan hampir pada semua bagian, dan ini adalah hal yang alami dari BCP dan DRP dan tentnya memerlukan banya kertas untuk mencetaknya.

Departemen TI memiliki peranan yang penting dalam mengidentifikasi dan melindungi ketergantungan internal dan eksternal informasi sebuah perusahaan. Komponen tehnologi informasi dalam Business Continuity Plan juga harus memenuhi beberapa issu utama, termasuk;

- Menyediakan backup data, proses restorasi, termasuk media penyimpanan off-site yang memadai bagi pegawai sebuah organisasi
- Menyediakan mekanisme pengamanan fisik untuk menjamin ketersediaan jaringan vital dan komponen hardware, termasuk file dan print server.
- Menyediakan pengamanan logik (otentifikasi, otorisasi, dll) terhadap data yang sensitif
- Memastikan bahwa tiap departemen menerapkan sistem administrasi yang tepat, termasuk up-date inventori hardware, software, dan media penyimpanan

---

Pertimbangan Dalam Business Continuity Plan

Saat membangun BCP, prosesnya harus melibatkan seluruh perusahaan, tidak hanya bagian TI saja. Sehingga semua pihak merasa memiliki Business Plan yang dikembangkan dan merasa bertanggunng jawab dalam implementasinya. Oleh karena itu pengembangan BCP ini sering dikategorikan sebagai “Operation Risk”, karena bila tidak melibakan banyak pihak maka kepedulian perusahaan secara luas akan rendah dan mengakibatkan beban atau kerugian yang sangat besar terhadap perusahaan bila terjadi bencana yang menghentikan proses bisnis utama. Dengan melibatkan banyak pihak maka peluang terjadinya bencana terutama karena faktor manusia bisa ditekan, dan upaya pemulihan bisa lebih cepat dan murah dilakukannya. Kerugian suatu perusahaan, umumnya akan langsung berdampak pada pegawainya.

Kalau tidak ada Business Continuity Plan pada level perusahaan, maka BCP pada sistem informasi perlu menyertakan unit bisnis lain yang terkait dengan BCP tersebut.

Hal lain yang juga perlu dipertimbangkan dalam membuat Business Continuity Plan adalah staf-staf yang diperlukan untuk menjalankan fungsi bisnis yang penting saat terjadi bencana, dan konfiguras gedung, meja, kursi telepon dan lainnya. Pemilihan staff yang tepat yaitu yang bisa mengambil keputusan dan penyampaian informasi secara cepat dan tepat selama masa dampak bencana. Bila terjadi bencana, dengan adanya arahan dan kepemiminan yang jelas dan konfigurasi fasilitas dan dukungan untuk saat bencana (antisipasi) yang baik, maka proses pemulihan bencana bisa dilakukan lebih cepat dan tentunya akan bisa menekan biaya sekaligus kerugian yang dialami.

Komponen BCP [16]
Komponen pada proses pengembangan business continuity plan adalah mencakup;

- Penanggung jawab utama dari Busisiness Continuity Plan
- Backup dari supplies yang dibutuhkan oleh organisasi
- Pengorganisasian dan penanggung jawab dari tiap aktivitas BCP dan DRP
- Fasilitas jaringan dan komputer yang mampu mendukung
- Asuransi

Dalam proses pengembangan business continuity plan perusahaan atau tim pengembang harus menyepakati;

- Tujuan dari setiap tahapan pemulihan yang ditentukan
- Lokasi dan fasilitas alternatif saat terjadinya bencana
- Penanggung jawab
- Sumber daya termasuk dana yang perlu disediakan
- Prioritas penanganan, kegiatan dan jadwalnya

Bussines continuity plan (BCP) harus mencakup masalah asuransi dan cara klaimnya. Beberapa hal yang mungkin diasuransikan antara lain:

- Peralatan dan fasilitas IT
- Software reconstruction, termasuk juga backup yang ada
- Extra expense, karena harus beroperasi dari fasilitas alternatif
- Business interuption cost, kerugian akibat berhentinya aktifitas perusahaan dalam kurun waktu tertentu
- Valuable papers dan records, akibat hilangnya surat-surat dan rekaman-rekaman berhaga
- Media transportasi, kendaraan.
- Errors dan Omissions
- Fidelity coverage, akibat ketidakjujuran pegawai, dapat berupa blanket bonds, menilep uang (korupsi)

C.3.4. Persetujuan dan Implementasi

Tahap akhir dari pengembangan business continuity plan (BCP) adalah implementasinya. Perencanaannya sendiri harus mengandung urutan dalam implementasinya. Implementasi di sini tidak berarti mengeksekusi skenario bencana dan menguji rencana, tapi lebih mengacu pada tahapan berikut: [1]

1. Persetujuan oleh manajemen senior
2. Menciptakan kepedulian dan ketrampilan
3. Memelihara rencana, termasuk updating jika diperlukan

Senior manajemen memiliki tanggung jawab utama pada setiap tahapan dalam perencanaan. Mereka memiliki tanggung jawab untuk melakukan supervisi dan eksekusi rencana selama kejadian bencana, mereka perlu memberikan persetujuan final. Disaat bencana terjadi, senior manajemen harus mampu menginformasikan keputusan yang cepat selama upaya pemulihan.
Kepedulian perusahaan terhadap rencana adalah penting. Ada beberapa alasan untuk ini, termasuk bukti bahwa kemampuan organisasi untuk pulih dari bencana akan sangat bergantung pada upaya-upaya tiap individu. Kepedulian dan pemahaman pegawai terhadap rencana akan memperkuat komitmen organisasi terhadap karyawannya. Training khusus atau simulasi kedaan bencana mungkin diperlukan bagi beberapa karyawan untuk menjalankan tugasnya, dan training yang berkualitas akan meningkatkan minat dan komitmen pegawai terhadap BCP proses.

Berikut ini adalah 9 langkah mempromosikan Business Continuity Plan: [2]

1. Visualisasikan fungsi-fungsi bisnis secara top down
2. Buatlah item-item dari tugas-tugas yang dijalankan secara bottom up
3. Prioritaskan pekerjaan hanya pada fungsi-fungsi utama
4. Buat kategori dan organisasikan masalah menjadi bagaian-bagian pekerjaan yang dapat dikelola
5. Minimalkan risiko, ini adalah tujuan utama dari business continuity plan
6. Organisir staff untuk bereaksi pada satt bencana terjadi
7. Praktekan kejadian bencana (simulasi), sehingga staff familiar dengan prosedure respon
8. Sponsor/Champion, partisipasi untuk mendemonstrasikan dan mengkomunikasikan pentingnya rencana pemulihan.
9. Monitor supply chain dan rencana-rencana partner

Business continuity plan (BCP) terkadang sudah tidak cocok lagi, perkembangan tehnologi komputer, jaringan dan komunikasi sering mendorong perusahaan untuk membuat perencanaan ulang dan melakukan pelatihan yang diperlukan.

D. Disaster Recovery Plan

Bencana alam dan buatan manusia dapat terjadi. Angin puyuh, gempa bumi, kebakaran, banjir, tindakan kriminal dan teroris, serta kesalahan manusia dapat sangat parah merusak sumber daya komputasi suatu organisasi, dan kemudian kesehatan organisasi itu sendiri. Banyak perusahaan terutama peritel e-commerce online dan grosir , penerbangan, bank, serta ISP, dibuat tidak berdaya karena kehilangan kekuatan komputasi selama beberapa jam. Itulah alasan mengapa organisasi mengembangkan prosedur pemulihan dari bencana (disaster recovery) serta mensahkannya sebagai rencana pemulihan dari bencana (disaster recovery plan, DRP). Rencana itu menspesifikasikan karyawan mana yang akan berpartisipasi dalam pemulihan dari bencana serta apa tugas mereka nantinya; hardware, software, dan fasilitas apa yang akan digunakan; serta prioritas aplikasi yang akan diproses. Kesepakatan dengan berbagai perusahaan lainnya untuk penggunaan fasilitas alternatif sebagai lokasi pemulihan dari bencana dan penyimpanan di luar kantor dari data base organisasi, juga merupakan bagian dari usaha pemulihan dari bencana yang efektif [4].

Disaster Recovery Plan atau DRP adalah penerapan dari Business Continuity Plan (BCP) atau disebut juga “BCP in action” yaitu implementasi BCP saat terjadi bencana. DRP memberikan langkah-langkah pada organisasi jika kejadian bencana timbul. DRP akan mengurangi kebingungan yang terjadi saat ada bencana dan meningkatkan kemampuan organisasi saat menghadapi keadaan krisis.

Pada saat ada kejadian bencana tentunya organisasi tidak akan memiliki waktu banyak untuk membuat rencanan pemulihan dilokasi bencana saat terjadi. Dengan perencanaan yang baik dan proses simulasi sebelum benar ada kejadian bencana, maka organisasi akan dapat memperkirakan kemampuannya dalam menghadapi suatu bencana. Supaya perbaikan dapat dilakukan dengan lancar, maka perlu adanya perencanaan untuk ini yang biasanya disebut dengan disaster recovery plan (DRP).

Secara umum manfaat atau tujuan penyusunan disaster recovery plan (DRP) bagi perusahaan adalah sebagai berikut; [1]

- Melindungi organisasi dari kegagalan layanan komputer utama
- Meminimalisasi risiko organisasi terhadap penundaan (delay) dalam penyediaan layanan
- Menjamin kehandalan dari sistem yang sedia melalui pengetesan dan simulasi
- Meminimalisasi proses pengambilan keputusan oleh personal/manusia selama bencana.

D.1. Proses Pengembangan DRP

Proses ini adalah berupa pengembangan dan pembuatan rencana pemulihan yang sama dengan BCP proses. Dengan telah dilakukannya proses pengembangan business continuity maka proses pengembangan DRP tidak perlu melakukan lagi identifikasi dan justifikasi. Perencanaan dibuat hanya untuk menghadapi bencana, yaitu dengan menentukan strategi dan prosedur yang akan dilakukan bila bencana benar-benar terjadi.

Intinya proses perencanaan pemulihan bencana meliputi dua hal berikut, yaitu: [1]

- **Perencanaan Keberlanjutan Pemrosesan Data**; Perencanaan terhadap adanya bencana dan membuat rencana untuk menanganinya.
- **Pemeliharaan Rencana Pemulihan Data**; Menjaga rencana tetap up to date dan sesuai dengan kondisi dan kebutuhan organisasi.

Pemilihan Strategi Pemulihan

Pemilihan strategi pemulihan meliputi dua hal yaitu: penentuan cara atau strategi untuk melakukan pemulihan fasilitas tehnologi informasi dan aktifitas bisnis apa saja yang harus dilakukan selama fasilitas tehnologi informasi sedang dipulihkan.

Asuransi tidak bisa digunakan untuk perencanaan, tapi pada saat ada bencana atau kecelakaan baru bisa diasuransikan. Namun dengan adanya perencanaan yang memadai, maka biaya premi asuransi biasanya akan lebih kecil. Asuransi sangat bermanfaat untuk mengurangi atau bahkan mengganti kerugian finansial yang ditimbulkan karena bencana atau kecelakaan.

Strategi bisnis continuity saat terjadi bencana antara lain adalah sebagai berikut: [16]

- Tidak melakukan apa-apa sampai pemulihan fasilitas sudah beroperasi kembali, contoh adalah pada sistem perpustakaan. Jika sistem sudah beroperasi, maka petugas kembali menggunakan aplikasi tersebut.
- Melakukan prosedur secara manual. Sambil menunggu sistem kembali beroperasi, transaksi dilakukan secara manual, atau dicatat pada form off line.
- Memfokuskan pada proses yang penting seperti yang berhubungan dengan pelanggan, produksi, dan lainnya.
- Menggunakan PC untuk data capture (pencataan saja) dengan pengolahan minimal. Pengolahan normal baru dilakukan setelah pemulihan fasilitas bekerja kembali.

Perencanaan Keberlangsungan Pemrosesan Data adalah menentukan proses backup atau alternatif pemrosesan data saat terjadinya bencana yang menginterupsi aplikasi bisnis yang berjalan. Berikut adalah strategi yang dapat dipilh dalam menentukan alternatif data prosessing saat terjadi bencana: [16]

- Melakukan duplikasi terhadap fasilitas proses informasi. Ada komputer lain atau cadangan di lokasi tertentu yang memiliki fungsi yang sama dan selalu diupdate sesuai dengan transaksi yang berjalan.

- Hot sites: Sepenuhnya dijalankan oleh fasilitas operasi dan data alternatif yang dilengkapi dengan perangkat keras dan perangkat lunak yang memadai selama dampak bencana masih berlangsung. Cara ini penting untuk aplikasi yang kritical, namun biayanya sangat mahal.

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

- Perjanjian dengan perusahaan lain (mutual aid agreement), yaitu bekerja sama dengan perusahaan lain yang memiliki kebutuhan sistem komputer yang sama seperti pada konfigurasi hardware atau software, atau kesamaam jaringan komunikasi data atau akses Internet. Dalam kerja sama ini, ke dua perusahaan setuju untuk saling mendukung bila terjadi bencana

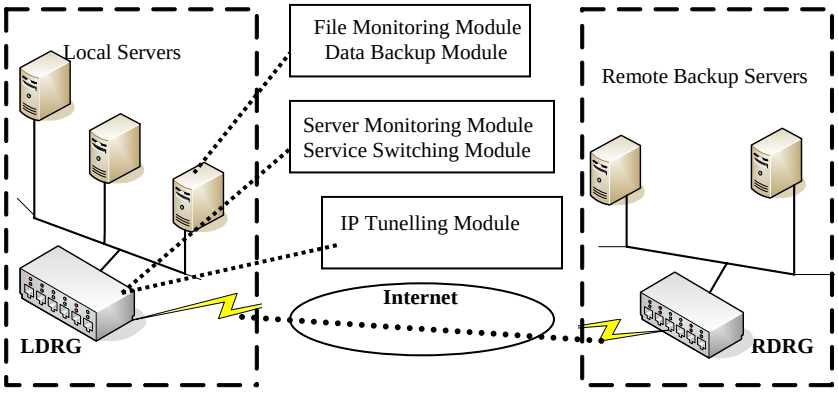
- Multiple Center: Proses sistem dan data tersebar di masing-masing unit organisasi. Strategi ini hampir sama dengan mutual aid agreement, namum dilaksanakan secara internal dalam satu organisasi atau perusahaan, dan memerlukan regulasi atau standar internal yang disepakati dan dipatuhi bersama.

- Out source: Organisasi melakukan kontrak dengan pihak ke tiga untuk memberikan alternatif layanan proses backup.

Selain itu perusahaan juga perlu menentukan strategi dalam memulihkan telekomunikasi seperti, melalui; [16]

- Network redundancy, memiliki kapasitas yang lebih atau ekstra gate gateway.
- Alternative routing, menggunakan media komunikasi alternatif, mis. kalau sebelumnya antar cabang menggunakan VSAT, maka dicoba alternatif menggunakan POST (plain old telephone system), juga jaringan fiber optik yang memiliki 2 jalur routing.
- Diverse routing, menggunakan kabel duplikat, dan menjamin bahwa kabel-kabel tersebut memiliki jalur/path yang berbeda. Kalau kabel-kabel tersebut berada pada jalur yang sama persis, maka akan kena jenis ancaman yang sama.
- Long haul network diversity, sebuah recovery facility (off site alternate facility). Banyak yang memiliki banyak jalur keluar ke beberapa penyelenggara jasa telekomunikasi. Hal ini untk menjamin tersedianya jasa telekomunikasi kalau yang satu crash.
- Protection of local loop (last mile circuit), menggunakan banyak metode akses komunikasi keluar, kalau ada bencana di off site facility.
- Voice recovery, pemulihan sarana telekomunikasi terutama untuk melakukan hubungan komunikasi suara, lewat telepon.

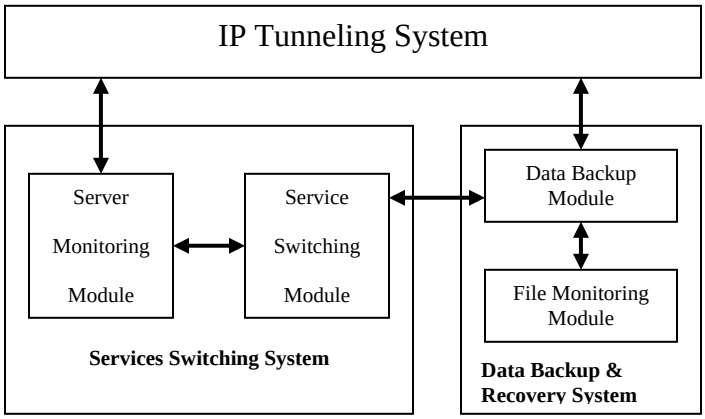
Sistem pemulihan berbasis Internet [8]
Arsitektur dari sistem pemulihan berbasis Internet terdiri dari dua bagian fisik yaitu local data center (LDC) dan remote backup center (RBC). Gambar berikut memperlihatkan arsitektur LDC terdiri dari group server-server yang memberikan layanan untuk bisnis dan local disaster recovery gateway (LDRG), dimana setiap server terhubung dengan Internet. LDRG meng-inspect status tiap server dan mengontrol akses user Internet ke layanan yang diberikan oleh server di LDC.



Gambar 2.; Arsitektur Sistem Pemulihan Bencana Berbasis Internet

Sama dengan LDC, RBC terdiri dari group server-server backup dan remote disaster recovery gateway (RDRG), tapi jumlah server backup dapat ebih sedikit dari lokal server. Ada satu server di RBC yang berfungsi sebagai backup server untuk beberapa server di LDC.

Sistem terbentuk dari tiga sub sistem fungsional yaitu data backup recovery sistem (DBRS), IP tunneling system (IPTS) dan services switching system (SSS). Gambar berikut memperlihatkan tiga sub sistem dan hubungannya.



Gambar 3.; Module Sistem dan Hubungannya

Sistem backup real time berbasis Internet memungkinkan Internet mentransfer data antara LDC dan RBC tanpa dedicated lines, sehingga jarak antar LDC dan RBC tidak terbatas dan biaya lebih rendah dari dedicated liness. IP tunelling akan memastikan kerahasiaan data yang ditransmisikan lewat Internet. Tehnologi backup dan recovery yang otomatis dapat meminimalisir kehilangan data, sedangkan service switching memungkinkan operasi bisnis berlanjut terus meskipun terjadi bencana seperti banjir, kebakaran dan bahkan gempa bumi. Ini adalah salah satu solusi pemulihan bencana bagi bisnis kecil dan menengah yang tidak mahal dan aman.

Integrasi backup and recovery [3]
Pengendalian backup dan recovery diperlukan untuk berjaga-jaga bila file atau data base mengelami kerusakan atau kehilangan data. Back up adalah salinan dari file atau data base di tempat yang terpisah dan recovery adalah file atau data base yang telah dibetulkan dari kesalahan atau kerusakan.

Karena file atau data base dapat mengalami kerusakan atau kehilangan data, maka sangat perlu untuk membuat backup-nya yang berfungsi sebagai cadangan bila yang asli mengalami kerusakan. Ada beberapa strategi untuk melakukan backup dan recovery, yaitu strategi file bertingkat (kakek-bapak-anak), strategi pencatatan ganda, dan strategi dumping. File tersebut dapat disimpan di luar gedung utama, sebuah lokasi yang jauh dari pusat data perusahaan, yang kadang merupakan gudang penyimpanan di lokasi yang jauh.

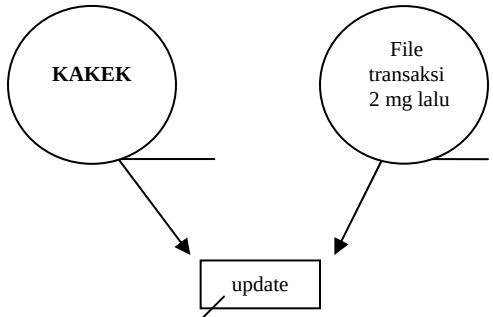
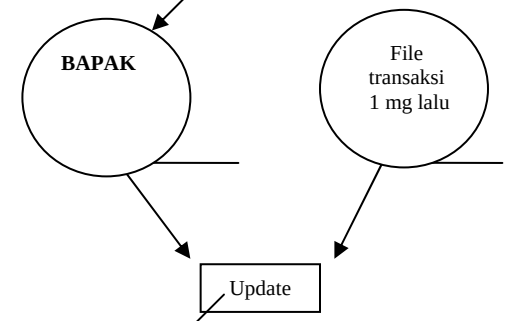
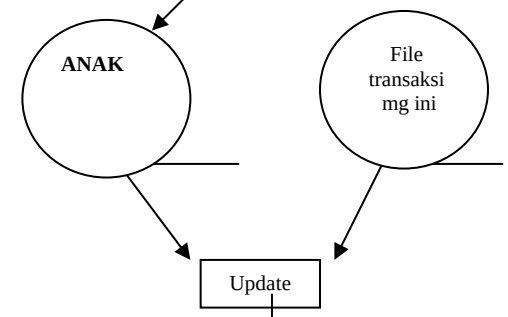
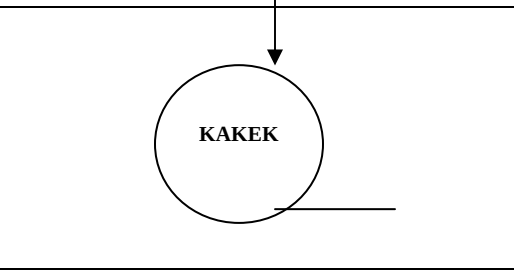
Strategi kakek-bapak-anak biasanya digunakan untuk file yang berada di media simpanan luar pita magnetik. Strategi ini dilakukan dengan menyimpan tiga generasi file induk bersama-sama dengan file transaksinya. Gambar 4. berikut ini menunjukkan strategi ini dengan periode waktu pemutakhirannya 1 minggu. Selama periode 3 minggu, maka akan didapatkan 3 buah file induk yang disimpan di tempat yang berbeda.

Selama periode tersebut akan didapat file-file sebagai berikut:

a. File induk kakek (grand father) dan file transaksi 2 minggu yang lalu
b. File induk bapak (father) dan file transaksi 1 minggu yang lalu
c. File induk anak (son) dan file transaksi minggu ini

Ketiga file induk dan transaksi tersebut akan disimpan secara terpisah. Bila terjadi kerusakan atau kehilangan data didalam file, maka akan dapat dibetulkan kembali. Misalnya kasus-kasus sebagai berikut;

a. File induk anak mengalami kerusakan atau hilang, maka dapat dibetulkan dari file induk bapak yang diupdate ulang dengan file transaksi minggu kemarin.
b. File induk anak dan file induk bapak, kedua-duanya mengalami kehilangan atau kerusakan, maka dapat dibetulkan dari file induk kakek yang diupdate ulang dari file transaksi 2 minggu lalu dan file transaksi minggu kemarin.

Proses 2 minggu yang lalu: Setelah digunakan untuk update, file induk (kakek) dan file transaksi disimpan oleh librarian di tempat A.	
Proses 1 minggu yang lalu: Setelah digunakan untuk update, file induk (bapak) dan file transaksi disimpan oleh librarian di tempat terpisah dari file induk (kakek) yaitu di tempat B.	
Proses minggu ini: Setelah digunakan untuk update, file induk (anak) dan file transaksi disimpan oleh librarian di tempat terpisah dari file induk (kakek) dan file induk (bapak) yaitu di tempat C.	
Untuk update berikutnya, file induk (kakek) digunakan kembali dan proses kembali dari atas lagi	

Gambar 4.; Strategi Backup Kakek-Bapak-Anak

Pencatatan Ganda (dual recording) dilakukan dengan menyimpan dua buah salinan data base yang lengkap secara terpisah. Bila terjadi transaksi, keduanya diupdate secara bersamaan. Untuk mengatasi kegagalan dari perangkat keras, sebuah processor ke dua dapat dipergunakan. Processor ke dua ini akan menggantikan fungsi dari processor utama bila mengalami kerusakan. Kalau hal ini terjadi, yaitu prosessor utama tidak berfungsi, secara otomatis program akan merubah dari processor utama ke processor ke dua, dan data base ke dua menjadi data base utama. Dual recording sangat tepat untu aplikasi-aplikasi yag data base-nya tidak bolah terganggu

dan harus selalu siap. Akan tetapi, sebagai pertimbangannya, strategi ini mahal, karena menggunakan dua buah processor dan dua buah data base.

Dumping dilakukan dengan menyalinkan semua atau sebagian dari data base ke media backup yang lain, dapat berupa pita magnetik atau disket (CD/DVD). Recovery pada strategi ini dapat dilakukan dengan merekam kembali (restore) hasil dari dumping kembali ke data base di simpanan luar utama dan melakukan proses transaksi yang terakhir yang sudah mempengaruhi data base sejak proses dumping trakhir. Misalnya dumping untuk membackup data base dilakukan seminggu sekali, yaitu pada hari sabtu. Pada hari Kamis berikutnya, diketahui bahwa data base mengalami kerusakan. Untuk membetulkannya dapat dilakukan dengan cara berikut ini;

1. Back up data base terakhir, yaitu pada hari Sabtu kemarin direkamkan kembali ke simpanan luar utama.
2. Akan tetapi data base hasil perekaman dari back up masih belum lengkap, karena sudah terjadi proses transaksi sejak hari Sabtu sampai dengan hari Kamis (saat terjadi kerusakan), sehingga transaksi-transaksi ini harus diupdatekan kembali ke data base.

Pemilihan lokasi pemulih dari bencana [6]

Dalam pemilihan lokasi alternatif untuk memulihkan bisnis dari bencana, maka perlu dipertimbangkan hal-hal berikut:

- Jarak dari Fasilitas Utama; pilihlah lokasi yang tidak terlalu dekat dan juga terlalu jauh dari gedung utama yaitu sekitar 30 kilo meter.
- Potensi Risiko dari Bencana: apakah lokasi tersebut juga memiliki risiko terkena bencana, carilah tempat yang minim terkena ancaman atau dampak bencana.

Primary Location

Facility Name:	
Street Address:	**Floor:**
City/State/Zip:	
Contact Person: **Alternate Contact:**	**Phone No:** **24 Hour No:** **FAX No:** **Other No.:**
Security Considerations:	

Alternate Location

Facility Name:	
Street Address:	**Floor:**
City/State/Zip:	
Contact Person: **Alternate Contact:**	**Phone No:** **24 Hour No:** **FAX No:** **Other No.:**
Security Considerations:	

Directions to the Business Recovery Site

TBD

Gambar 5.; Contoh Business Recovery Site Information

- Ketersediaan staff setempat: apakah ada staff setempat yang bisa mengoperasikan proses bisnis utama.
- Ketersediaan dan kualitas tenaga listrik/baterei; apakah tenaga listrik atau baterai tersedia, dan apakah mencukupi untuk waktu lebih dari 27 jam.
- Nearby Fiber Routes: untuk kepentingan jaringan komunikasi data, alangkah lebih baik kalau tidak jauh dari jarul kabel fiber, dan kalau memungkinkan kita bisa minta ijin atau mendaftar menggunakan jalur kabel tersebut.
- Specific IT Criteria; Tehnologi informasi dapat berfungsi pada lokasi tersebut, batasan jarak harus menjadi perhatian perlengkapan jaringan.
- Tax Incentive; Lokasi tertentu atau di luar perkotaan mungkin akan jauh lebih murah biayanya.

Pemeliharaan Rencana Pemulihan Data [1]

Disaster recovery plan sering sudah out of date atau tidak sesuai lagi dengan kondisi organisasi atau perkembangan yang terjadi disekitar baik ancaman bencana maupun tingkat persaingan. Organisasi mungkin telah mereorganisasi dan mungkin saja unit bisnis critical telah berbeda dari saat direncanakan dahulu. Perubahan infrastruktur jaringan juga akan merubah lokasi atau konfigurasi dari hardware, software dan komponan lainnya. Juga mungkin karena masalah administrasi seperti turn over dari pegawai dan berkurangnya ketertarikan pegawai terhadap masalah Business Continuity Plan dan Disaster Recovery Plan.

Apa pun alasannya, pemeliharaan perlu direncanakan sebelumnya supaya BCP dan DRP selalu up date dan berguna. Sangatlah penting untuk membuat prosedure pemeliharaaan BCP dan DRP dalam sebuah organisasi dengan menggunakan job description yang mensetralisasi tanggung jawab pengupdate-an. Mungkin juga diperlukan prosedur audit yang melaporkan secara periodik mengenai status dari perencanaan. Juga penting adalah jangan sampai berbagai versi rencana masih ada, in akan menimbulkan kebingungan dan bisa memperparah kondisi emergensi. Jangan lupa untuk selalu menganti versi yang lama dengan yang baru dan menuliskan teks versi pada tiap perencaaan.

Pengujian Disaster Recovery Plan

Pengujian DRP sangatlah penting, DRP memiliki banyak elemen yang berupa teori sampai mereka benar-benar diuji dan disahkan. Pengujian rencana harus dilaksanakan sesuai dengan urutannya, mengikuti standar yang ditetapkan, dan disimulasikan pada keadaan sebenarnya.

Ada lima bentuk pengujian disaster recovery plan yaitu: [1]

1. Check List tes. Ini adalah preliminary step dari pengujian. Setiap unit manajemen akan mereview apakah perencanaan sesuai dengan prosedur dan critical area dari organisasi.
2. Structured walk-through test. Tes dilakukan melalui pertemuan antar perwakilan dari tiap unit manajemen untuk membahas seluruh isi dari perencanaan. Tujuannya adalah untuk memastikan bahwa perencanaan secara akurat merefleksikan kemampuan organisasi dalam memulihkan diri dari bencana secara sukses, setidaknya on paper.
3. Simulation test. Salama pengujian dengan melakukan simulasi, semua orang dibagian operasional dan support harus memandang bahwa keadaan emergensi terjadi seperi sebenarnya agar sesuai dengan kenyataannya nanti. Simulasi tes ini bertujuan untuk melihat kesiapan personnel bila ada kejadian bencana.

4. Paralel test. Simulasi dilakukan pada semua rencana pemulihan. Parallel berarti proses pengujian berjalan secara paralel dengan proses sebenarnya. Tujuanya adalah memastika supaya sistem yang utama (critical) dapat tetap berjalan pada lokasi alternatif backup.
5. Full-interuption test. Ini adalah tes yang sangat berisiko karena kejadian bencana (dampak) benar-benar diterapkan. Namun ini adalah cara terbaik untuk menguji recovery plan, apakah dapat berjalan atau tidak.

D.2. Disaster Recovery Procedures

Pada bagian ini, perencanaan akan secara detil menjelaskan peranan dari setiap orang yang akan terlibat dalam implemantasi disaster recovery plan. Tugas apa yang mesti dijalankan untuk memulihkan dann menyelamatkan lokasi. Ada dua tim yang akan berperan saat terjadi bencana yaitu tim pemulihan dan tim penyelamatan. Tim pemulihan bertanggung jawab terhadap pemulihan fungsi bisnis kritis (utama), langkah awalnya adalah memastikan penggunaan alternatif operasi dan data bisa berlangsung baik secara otomatis maupun manual. Sedangakan tim penyelamatan terpisah dari tim pemulihan dan memiliki tanggung jawab yang berbeda. Tim penyelamat bertanggung jawab untuk secara cepat membersihkan, mengurangi bahaya/dampak, memperbaiki, menyelamatkan infrastruktur utama setelah bencana terjadi. Ini temasuk juga penyelamatan manusia. [1]

Sasaran utama dari rencana **pemulihan bencana** ini adalah untuk membantu meyakinkan sistem operasional yang berkelanjutan mencakup ketersediaan data. Sasaran khusus dari rencana ini termasuk :

- Untuk menjelaskan secara rinci langkah-langkah yang harus diikuti
- Untuk meminimisasi kebingungan, kekeliruan, dan biaya bagi perusahaan.
- Untuk bekerja cepat dan lengkap atas **pemulihan dan penyelamatan dari bencana**.
- Untuk menyediakan proteksi yang berkelanjutan terhadap aset IT.

Tugas-Tugas:

1. Manajemen Team Leader

   Bertanggung jawab penuh untuk mengkoordinir strategi **pemulihan bencana**. Meyakinkan bahwa seluruh karyawan sadar atas kebijakan **pemulihan bencana** dan tanggung jawab mereka untuk melindungi informasi perusahaan. Tugas-tugasnya antara lain:

   * Memimpin **pemulihan dan penyelamatan dari bencana**
   * Mengumumkan rencana **pemulihan dan penyelamatan bencana**.
   * Menunjuk Koordinator **pemulihan bencana**.
   * Menunjuk Koordinator **penyelamatan bencana**.

2. Koordinator **Pemulihan Bencana**

   Bertanggung jawab Untuk mengkoordinir **pemulihan bencana** seperti digambarkan oleh kebijakan. Mengarahkan implementasi dan uji coba rencana.

   Tugas-tugasnya antara lain:

   * Mengkoordinasikan seluruh aktifitas karyawan terhadap **pemulihan bencana**.
   * Menyelenggarakan program kesadaran **pemulihan bencana** ke Departemen IT dan departemen terkait.
   * Bertanggung jawab untuk menjaga inventori aset IT yang terkini.
   * Mengelola pengetesan dan laporan hasil tes.
   * Mengupayakan pemulihan fungsi bisnis utama saat terjadi bencana

3. Koordinator **Penyelamatan Bencana**

Bertanggung jawab Untuk mengkoordinir **penyelamatan bencana** seperti digambarkan oleh kebijakan. Mengarahkan implementasi dan uji coba rencana.

Tugas-tugasnya antara lain.

* Mengkoordinasikan seluruh karyawan terhadap **penyelamatan diri dari bencana**.
* Menyelenggarakan program kesadaran penyelamatan dar bencana ke Departemen IT dan departemen terkait.
* Bertanggung jawab untuk menjaga inventori aset IT yang terkini.
* Mengelola pengetesam dan laporan hasil tes
* Mengupayakan pengurangan dampak bencana terhadap keselamatan manusia, fasilitas infrastruktur dan proses bisnis utama.

Selain itu ada beberapa tim lainnya yang bisa dibentuk; [16]

a. Emergency action team, tugas utamanya seperti “pemadam kebakaran”, dan bertugas untuk menyelamatkan jiwa.
b. Damage assassment team, tugasnya mengkalkulasi dampak bencana dan memperkirakan kapan lokasi bisa kembali normal
c. Emergency management team, bertugas mengkoordinasi aktifitas antar tim dan melakukan decision making, termasuk masalah hukum dan public relation
d. Off site storage team, melakukan packing dan shipping media dan records ke off site facilitiy
e. Software team, bertugas merestore sistem operasi
f. Applications team, bertugas di recovery site unttuk menginstal kembali aplikasi komputer
g. Emergency operations team, mengatur shift operator dan supervisor yang harus menjalankan recovery site (fasilitas alternatif)
h. Salvage team, bertugas menganalisa dampak bencana lebih dalam, menentukan apakah akan melakukan relokasi atau perbaikan, dan mengisi form asuransi.
i. Reocation team, bertugas mengembalikan fasilitas dari lokasi cadangan atau recovery ke lokasi baru yang permanen atau lokasi awal setelah kondisi pulih.

Disaster Recovery Center

Sejak semester ke dua tahun 2002, seluruh saham diperdagangkan tanpa warkat (*scripless*). Saat itulah ketergantungan pelaku pasar pada sistem penyimpanan dan penyelesaian transaksi tanpa warkat, yakni C-BEST makin tinggi. Nah, apa jadinya bila sistem utama tersebut mengalami gangguan sehingga tidak bisa berfungsi?

"Siapa sih yang mengharapkan kejadian buruk seperti kebakaran atau bencana lain. Tetapi kalau itu terjadi di lokasi tempat C-BEST dioperasikan, apakah aktivitas perdagangan juga berhenti?" demikian pertanyaan yang kerap dilontarkan pelaku pasar. Untuk mengantisipasi kemungkinan gangguan pada sistem utama tersebut, KSEI telah mempersiapkan mekanisme yang memungkinkan tetap berjalannya perdagangan tanpa warkat pada saat terjadinya kegagalan total dari sistem produksi.

Sejak 13 September 2001 pusat pemulihan bencana atau yang dikenal dengan *Disaster Recovery Center (*DRC) telah berfungsi. Di pusat pemulihan bencana itu ditempatkan sistem dan data yang sama dengan sistem produksi, namun dengan kapasitas dan kinerja yang relatif lebih kecil. Pada saat terjadi bencana terhadap sistem produksi, dalam waktu yang tidak terlalu lama sistem yang ada di DRC ini akan mengambil alih peranan sistem utama, sehingga perdagangan tanpa warkat akan tetap berjalan sebagaimana mestinya

DRC dianggap sangat penting meskipun perangkat keras, perangkat lunak dan perangkat jaringan yang digunakan untuk aplikasi C-BEST sebenarnya sudah dilengkapi r*edudancy*, yang memungkinkan tetap berjalannya sistem meskipun salah satu perangkatnya mengalami kerusakan. Kelemahannya, *redudancy* tersebut tidak akan memberisolusi dalam hal bencana total yang dialami di lokasi sistem produksi seperti gempa, bom, kebakaran, kerusuhan dan sebagainya.

Sejalan dengan rencana pembuatan DRC tersebut, Bapepam telah mengatur mengenai DRC, yang salah satu peraturannya mewajibkan KSEI untuk memiliki DRC dengan jarak minimum 30 KM. Hal itu diperlukan untuk menjaga kemungkinan terjadi bencana yang sama antara lokasi sistem utama dan lokasi DRC. Aturan tersebut juga mengatur mengenai waktu beroperasinya DRC setelah terjadinya bencana pada sistem utama. DRC harus bisa beroperasi selambat-lambatnya dua jam setelah kejadian. Konsekuensinya, DRC harus dibuat dengan arsitektur dan infrastruktur dengan spesifikasi yang cukup tinggi untuk bisa mencapai target waktu tersebut.

Dalam hal ini KSEI memilih alternatif "warm stand by", dimana sistem tidak secara otomatis berpindah tapi proses manual dilakukan seminimal mungkin. Untuk itu KSEI akan menggunakan fasilitas database standby dari oracle. Alternatif ini tidak memerlukan perangkat keras dan perangkat lunak untuk replikasi hardware yang relatif mahal. Selain itu, kapasitas jalur komunikasi data yang diperlukan juga tidak terlalu besar.

E. Implementasi (BCP/DRP untuk small bisnis)

Berdasarkan pengertian, BCP atau Business Continuity Plan adalah rencana bisnis yang berkesinambungan, sedangkan DRP atau Disaster Recovery Plan adalah rencana pemulihan dari kemungkinan kerusakan-kerusakan yang terjadi. Aspek yang terkandung di dalam suatu rencana bisnis yang berkesinambungan yaitu rencana pemulihan dari kemungkinan kerusakan-kerusakan yang terjadi. Dengan kata lain, DRP terkandung di dalam BCP.

Rencana untuk pemulihan dari kerusakan, baik yang disebabkan oleh alam maupun manusia, tidak hanya berdampak pada kemampuan proses komputer suatu perusahaan, tetapi juga akan berdampak pada operasi bisnis perusahaan tersebut. Kerusakan-kerusakan tersebut dapat mematikan seluruh sistem operasi. Semakin lama operasi sebuah perusahaan mati, maka akan semakin sulit untuk membangun kembali bisnis dari perusahaan tersebut.

Konsep dasar pemulihan dari kemungkinan kerusakan-kerusakan yang terjadi yaitu harus dapat diterapkan pada semua perusahaan, baik perusahaan kecil maupun perusahaan besar. Hal ini tergantung dari ukuran atau jenis prosesnya, baik yang menggunakan proses manual, proses dengan menggunakan komputer, atau kombinasi dari keduanya. Pada perusahaan kecil atau usaha kecil menengah (UKM), biasanya proses perencanaannya kurang formal dan kurang lengkap. Sedangkan pada perusahaan besar, proses perencanaannya formal dan lengkap. Apabila rencana tersebut diikuti maka akan memberikan petunjuk yang dapat mengurangi kerusakan yang sedang atau yang akan terjadi. [13]

Pengembangan perencanaan keberlangsungan bisnis mengambil jam kerja beberapa staff untuk menerapkannya dan sumber pembiayaan yang memadai. Untuk mendapatkan sumber daya tersebut, manajemen perlu berkomitmen terhadap proses ini. Dan untuk mendapatkan persetujuan, diperlukan beberapa justifikasi yang perlu dipresentasikan.

Untuk memulainya, teliti beberapa hukum, peraturan atau ketentuan-ketentuan sehubungan dengan bisnis yang dijalankan (ini sering juga diterapkan pada pelayanan kesehatan, asuransi, institusi keuangan, dan sektor pemerintahan). Juga, lihatlah kontrak yang dimiliki dengan kostumer yang membuat bisnis memerlukan perencanaan terhadap keadaan emergensi. Jika hal tersebut sudah ada, maka proses justifikasi relative menjadi mudah.

Tambahan alasan lainnya mungkin bisa meliputi; kebutuhan audit, mengurangi kerugian yang dihadapi pihak manajemen, menyediakan keunggulan kompetitif pada bisnis di masa mendatang, issu kehidupan, kesehatan dan keselamatan, menghindari kehilangan pelanggan, atau memiliki alternatif proses dan data di suatu tempat untuk mengantisipasi adanya bencana.

Setelah mengidentifikasi berbagi alasan untuk mengembangkan rencana keberlangsungan bisnis, kita harus menyusun dokumen untuk dipresentasikan kepada manajemen. Sehubungn dengan dokument tersebut, maka perlu; [13]

- Mengidentifikasi potensi risiko pada bisnis
- Menentukan lingkup rencana keberlangsungan bisnis tersebut
- Membuat daftar tahapan yang diperlukan dalam penerapannya
- Menyediakan time line dari implementasinya
- Mendokumentasikan justifikasi
- Menghitung perkiraan biaya
- Menyimpulkan dan memberikan rekomendasi

Perkiraaan diperlukan waktu sekita 4-6 jam total pertemuan untuk bersama-sama menentukan rekomendasi tersebut. Peserta pertemuan perlu memahami bahwa keberlangsungan bisnis adalah bagian dari tanggung jawab bisnis tersebut, setiap individu harus berasumsi sebagi pemilik dari proses BCP ini. Setiap individu akan melakukan analisa risiko, mengembangkan rencana dan memeliharanya, menentukan lokasi backup dan lokasi kerja alternative, serta melatih dan menguji BCP tersebut.

Untuk usaha kecil menengah (UKM) yang kira-kira memiliki pegawai kurang dari 20 orang tidaklah perlu memiliki tim DRP (recovery team). Sebuah usaha kecil menengah hanya perlu memiliki sebuah document yang berisikan prosedur 5 tahapan dalam menghadapi bencana; [13]

1. Response. Tindakan yang segera dilakukan saat ada bencana. Perhatian utamanya adalah pada kehidupan, kesehatan dan keselamatan manusia. UKM perlu menyediakan perlengkapan pertolongan pertama pada kecelakaan, sarana evakuasi, daftar telepon bantuan emergensi, telepon team leader lain, dan lainnya.
   Pada tahap ini tidak ada upaya pemulihan, namun terbatas pada pengurangan dampak, pemberian peringatan, dan pembuatan keputusan oleh pihak manajemen.

2. Recovery. Tindakan pemulihan terhadap area kerja dan sumber daya. Jika keadaan sudah cukup aman, mulailah diupayakan pemulihan proses bisnis UKM tersebut terutama yang vital, dan bisa juga dilakukan pada lokasi alternative.

3. Resumption. Pengaktifan kembali fungsi-fungsi bisnis. Pada tahap ini, mengikuti pekerjaan pada tahap recovery. UKM mulai menyiapkan fungsi-fungsi bisnis yang diperlukan. Tergantung pada situasi, beberapa fungsi bisnis akan diupayakan beroperasi secara sistematis berdasarkan skala prioritasnya, dalam kurun waktu tertentu.

4. Reconstruction. Rekonstruksi fasilitas yang rusak. Tahap ini berisikan langkah-langkah yang akan dilakukan untuk membersihkan kerusakan dan memperbaiki beberapa fasilitas yang rusak. Jika bangunan hancur, maka perlu pindah ke lokasi lain yang permanen.

5. Relocation. Setelah fasilitas-fasilitas diperbaiki, maka terakhir adalah kembali ke fasilitas yang telah diperbaiki dan menjalankan proses bisnis kembali secara normal.

Jika memang membutuhkan dan mampu membentuk DRP team (recovery team) maka setidaknya ada 4 anggota atau tanggung jawab pemulihan, yaitu: [13]

1. Emergency Respons dan Analisa kerusakan
2. Administrasi dan Manajemen Krisis
3. Voice, Data dan Sistem Informasi
4. Core bisnis dan fungsi pendukung

Dari segi software, maka yang dibutuhkan oleh UKM adalah cukup software untuk membuat kerangka kerja dan dokumen BCP/DRP tersebut. Word dan atau Excel Program sudah cukup membantu. Sedangkan untuk menyimpan backup data dan aplikasi, adalah dengan menerapkan metode dumping dengan menyalinkan semua atau sebagian dari data base ke media backup yang lain, dapat berupa disket, flash disk, external harddisk atau CD/DVD, yang dilakukan seminggu sekali. Masing-masing fungsi atau unit bisnis perlu menyimpan backup tersebut ditempat yang lebih aman misalkan dirumah pegawai yang dipercaya atau kantor cabang lainnya bila berdekatan. Recovery dilakukan dengan merekam kembali (restore) hasil dari dumping kembali ke data base di komputer utama atau alternatif dan melakukan penambahan proses transaksi yang terakhir yang sudah mempengaruhi data base sejak proses dumping trakhir.

Referensi:

Buku

1. Ronald L. Krutz dan Russell Dean Vines, "*The CISSP Prep Guide*", Gold Edition, Wiley Publishing Inc., 2003.
2. Jerry N. Luftman, "*Managing the Information Technology Resource Resources*", International Edition, First Edition, Pearson Education Inc., 2004.
3. Jogiyanto Hartono, "*Sistem Teknologi Informasi, Pendekatan Terintegrasi: Konsep Dasar, Teknologi, Aplikasi, Pengembangan dan Pengelolaan*", Edisi 1, Penerbit Andi Yogyakarta, 2003.
4. James A. O'Brien, "*Introduction to Information System*", 12th Edition, The McGraw-Hill Companies, Inc. 2005. Terjemahan Penerbit Salemba Empat, 2005.

Internet (diakses pada tanggal 27 Oktober 2005)

www.drj.com

5. Gerard Minnich, "*The 20 Truths of Business Continuity*", Disaster Recovery Journal, Volume 17, Issue 1, Systems Support Inc., Winter 2004.
6. Bill Bick, "*Choosing a Location For Your Disaster Recovery Facility*", Disaster Recovery Journal, Volume 17, Issue 1, Systems Support Inc., Winter 2004.
7. Kevin Roden, "*Building a Business Case For Disaster Recovery Planning*", Disaster Recovery Journal, Volume 17, Issue 3, Systems Support Inc., Summer 2004.

8. Pin Yang, Tao Li, Kui Zhao, Jun Kai Liao, "*An Internet Based Disaster Recovery System*", Disaster Recovery Journal, Volume 18, Issue 1, Systems Support Inc., Winter 2005.
9. Duane Abbott, Alan Carlson, "*Small Corporation Stretches Resources to Make Disaster Recovery Strategy a Reality*", Disaster Recovery Journal, Volume 18, Issue 1, Systems Support Inc., Winter 2005.
10. Greg Holdburg, "*DR vs. BC: Dueling Recovery Plans*", Disaster Recovery Journal, Volume 18, Issue 2, Systems Support Inc., Spring 2005.
11. L.D. Weller, "*Best Practices for Prevention, Recovery*", Disaster Recovery Journal, Volume 18, Issue 2, Systems Support Inc., Spring 2005.
12. Garry Bond, "*Modeling Events To Affect a Recovery*", Disaster Recovery Journal, Volume 18, Issue 3, Systems Support Inc., Summer 2005.
13. Norm Koehler, "*The Small And Medium Size Businesses Guide To A Successful Continuity Program*", DRJ's Small Business Center Articles, Systems Support Inc., 2002.
14. http://ebizzasia.com/0109-2003/callcenter,0109,02.htm, "*Perlunya BCP Untuk Contact Center*", E-BizzAsia, Volume I, Nomor 09, Juli 2003.
15. http://www.chiefsecurityofficers.com/bcp.html, "*Business Continuity Planning: Is your business prepared for whatever lies ahead?*".

Materi Kuliah

16. Rahmat Samik-Ibrahim, "*Business Continuity Plan (BCP) & Disaster Recovery Plan (DRP)*", Bahan Kuliah Proteksi dan Teknik Keamanan Sistem Informasi, MTI-UI, November 2005.