	Bagian : NOC - BAPSI	Dibuat oleh : M.Achsan Isa
	PENGAMANAN RUANG SERVER	Direvisi oleh :
	Tgl. Pembuatan: 6 November 2008	Disetujui oleh :
	Tgl. Revisi :	Jumlah Halaman : 13

I. TUJUAN

Pembahasan utama dalam bagian ini mengenai keamanan fisik ruang server. Untuk itu akan dipaparkan terlebih dahulu definisi keamanan fisik. Berikut pengertian keamanan fisik.

- Perlindungan terhadap peralatan pemrosesan informasi dari kehancuran, kerusakan atau kehilangan; fasilitas pemrosesan informasi dari kehancuran, kerusakan dan masukan yang tidak sah; dan personil dari situasi yang berpotensi berbahaya.

- Penggunaan kunci, penjaga, lencana dan ukuran administratif sejenis untuk mengendalikan akses ke komputer dan peralatan yang berhubungan. Dan pengukuran yang dibutuhkan untuk melindungi struktur dari rumah komputer, peralatan yang berhubungan dan isinya dari kehancuran karena kecelakaan, kebakaran, bahaya lingkungan, kejahatan, pengrusakan, spionase industri dan lainnya.

- Keamanan fisik mendeskripsikan ukuran yang mencegah atau menanggulangi dari pengaksesan sebuah fasilitas, sumber daya, atau informasi yang disimpan pada media fisik. Dapat disederhanakan sebagai penguncian pintu atau sebagai rincian lapisan jamak dari penjagaan bersenjata.

- Dapat disimpulkan keamanan fisik adalah tindakan atau cara yang dilakukan untuk mencegah atau menanggulangi dan menjaga orang, hardware, program, jaringan dan data dari bahaya fisik dan kejadian yang dapat menyebabkan kehilangan yang besar atau kehancuran. Keamanan fisik termasuk perlindungan terhadap kebakaran, bencana alam, pencurian, vandalism dan teroris.

II. RUANG LINGKUP

Alat / Barang / Sarana dan Prasarana yang dipertanggungjawabkan kepada NOC-BAPSI ini berasal dari Program Hibah Kompetensi yang telah dimenangkan oleh Universitas Gunadarma dan yang belum di distribusikan secara langsung kepada bagian terkait. Program Hibah tersebut adalah :

1. TPSDP – Program Studi Sistem Komputer
2. TPSDP – Digital Library
3. TPSDP – Career Center
4. PHK A3 Program Studi Manajemen
5. PHK A3 Program Studi Teknik Arsitektur
6. PHK TIK (Inherent) Tahun 2006 dan 2007
7. Program Transfer Teknologi
8. Program Peningkatan Mutu Pendidikan (PMP)
9. Program Penguatan Lembaga Penelitian
10. Hibah dari Perusahaan

Prosedur peminjaman alat / barang / sarana dan prasarana ini meliputi kegiatan-kegiatan :

1. Pengajuan Surat Permohonan Peminjaman
2. Pengesahan Permohonan Pinjaman
3. Pengisian Surat Pinjaman
4. Penyerahan Pinjaman dan Pengecekan Awal
5. Pengembalian Pinjaman dan Pengecekan Akhir
6. Pengisian Surat Pengembalian

III. ACUAN/REFERENSI

1. Rencana Induk Pengembangan Jangka Panjang yang ditetapkan oleh Ketua Yayasan Pendidikan Gunadarma
2. Renstra Universitas Gunadarma Tahun 2007-2011
3. Pedoman Umum Tata Kelola Sarana dan Prasarana melalui SK Rektor Nomor : 065.1/SK/REK/UG/2006

IV. SARANA

1. Komputer
2. Server

3. Router
4. Switch

V. DEFINISI

Aspek Keamanan Data/Informasi server (Virtual)

Aspek keamanan data/informasi atau disebut juga keamanan virtual pada server menyangkut hal-hal sebagai berikut.

- Kontrol akses logikal, menyangkut apa, siapa dan bagaimana data diakses secara virtual. Contohnya seperti password untuk menentukan hak akses.
- Kontrol penyimpan, menyangkut berapa lama data disimpan dan jenis keamanan apa yang digunakan pada media penyimpan dan data yang disimpan. Contohnya sistem backup data yang dipakai dan enkripsi yang digunakan.
- Keamanan jaringan baik jaringan intranet maupun internet terkait dengan konfigurasi jaringan, hak akses jaringan, firewall, intrusion detection dan lainnya.
- Keamanan sistem terkait dengan sistem operasi yang digunakan.

Kebijakan Keamanan Ruang server

Keamanan fisik dan keamanan virtual dalam ruang server tidak terlepas dari kebijakan keamanan yang diterapkan di sebuah ruang server. Prosedur dan kebijakan yang diterapkan harus dapat berhasil dengan efektif. Namun kebijakan dan prosedur yang diterapkan sangat terkait sumber daya manusia yang akan melakukan kebijakan. Secara umum kebijakan keamanan menyangkut pengaturan terhadap sistem, pengaturan terhadap hak akses dan pengguna, pengaturan pengoperasian, prosedur backup dan pengaturan penyimpanan, serta kebijakan yang terkait dengan kontrol akses fisik dan lainnya. Memberikan pelatihan kepada staf tentang pentingnya mematuhi dan menjalankan prosedur serta kebijakan yang berlaku merupakan sebuah cara yang dapat dilakukan agar kebijakan keamanan dapat mencapai tujuannya.

Keamanan Fisik Ruang server

Jika dahulu keamanan fisik dianggap tidak penting dan sering diabaikan, namun sekarang pandangan tersebut telah mulai berubah. Ada banyak kejadian yang membuat pandangan ini berubah. Sebagai contoh adanya penelitian dari computer forensics experts Pinkerton bahwa 70% data dicuri dari sebuah perusahaan adalah pencurian fisik, dari laptop dan harddisk ke CD atau peningkatan tinggi kapasistas penyimpanan mini menyebabkan kemudahan dalam pencurian data.

Selain itu juga bencana alam, membuat orang menjadi berubah pandangan akan pentingnya keamanan fisik. Bagaimana menjaga data agar tetap aman jika terjadi bencana alam, bagaimana strategi pemulihan kembali setelah terjadi bencana adalah topik hangat yang diperbincangkan pada banyak artikel-artikel keamanan di internet.

Hal-hal tersebut di atas menjadi pertimbangan dalam pengamanan fisik ruang server. Keamanan fisik mulai diperhatikan, kebijakan keamanan yang terkait dengan keamanan fisik mulai dilihat ulang dan diperbaiki. Bagaimanan pengontrolan akses fisik, bagaimana standar ruangan server, bagaimana penyimpanan data, bagaimana prosedur backup, bagaimana standar keamanan gedung tempat ruang server dan lainnya, mulai mengimplementasikan aspek-aspek keamanan fisik. Untuk itu perlu mengetahui lebih lanjut mengenai resiko dan ancaman keamanan fisik serta metoda pengamanannya, sehingga dapat dilakukan tindakan pencegahan dan penanggulangan untuk bahaya keamanan fisik.

Jenis-Jenis Ancaman dan Resiko Keamanan Fisik pada Ruang server

Ancaman dan resiko pada ruang server adalah sebagai berikut.

- Keamanan fisik dan faktor lingkungan
  Penerapan keamanan fisik harus memperhatikan faktor lingkungan dan menerapkan kontrol keamanan lingkungan. Dari hasil survei yang dilakukan, 70% manajer mengatakan resiko terbesar adalah bahaya lingkungan sebagai ancaman terbesar. Bahaya lingkungan ini berupa kebakaran, banjir, embun, suhu, listrik, gempa bumi dan bentuk-bentuk bencana alam lainnya yang memberikan pengaruh negatif untuk

peralatan yang ada dalam ruang server. Namun banyak yang belum siap untuk mengatasi bahaya ini, karena menganggap bahwa bencana belum tentu akan terjadi.

- Keamanan fisik dan faktor manusia

  Manusia merupakan faktor penting dalam keamanan fisik. Eksploitasi keamanan komputer kebanyakan dilakukan oleh manusia. Jika menganggap bahwa sesorang yang tidak sah tidak mungkin masuk ke ruang server atau ruang penyimpanan data adalah sebuah hal yang salah. Hal ini dapat menjadi ancaman terbesar untuk ruang server. Namun demikian kita tidak hanya memperhatikan eksploitasi keamanan oleh orang dari luar, namun harus peduli pula dengan orang yang berasal dari dalam. Hal ini adalah ancaman terbesar karena orang berasal dari dalam dan lebih mengetahui dibandingkan penyusup dari luar.

- Keamanan fisik dan faktor finansial

  Perlu investasi yang cukup lumayan untuk mengimplementasikan keamanan fisik yang terintegrasi di sebuah ruang server. Namun terkadang karena alasan keuangan pengimplementasian tidak jadi dilakukan. Jika para manejer mengabaikan hal tersebut bisa jadi hal tersebut merupakan tindakan yang benar. Namun pandangan yang demikian adalah salah, pengimplementasian keamanan fisik harus diinvestasikan seefisien dan seefektif mungkin, karena jika terjadi sesuatu karena faktor lingkungan atau faktor manusia telah ada pencegahan dan penanggulangannya. Dengan penerapan keamanan fisik resiko kehilangan baik pada data ataupun perangkat keras menjadi lebih kecil, kerugian yang didapat tidak sebesar tanpa penerapan keamanan fisik. Jadi wajar saja jika diinvestasikan untuk keamanan fisik.

Metoda Pengamanan Fisik pada Ruang server

Dalam bagian sebelumnya telah membahas resiko dan ancaman keamanan fisik dari berbagai faktor. Selanjut akan dibahas mengenai metoda keamanan untuk mengatasi dan menanggulangi kerugian serta

ancaman dari faktor lingkungan dan faktor manusia. Banyak cara dan metoda yang dapat digunakan mulai dari cara sederhana sampai menggunakan teknologi canggih, namun perlu diingatkan manusia adalah faktor penentu untuk keberhasilan keamanan di sebuah ruang server. Selain itu juga cara yang akan digunakan terkait dengan kebijakan yang akan diterapkan, jadi pada dasarnya penerapan keamanan fisik haruslah terintegrasi dan menyeluruh dengan keamanan informasi.

VI. PROSEDUR

Bangunan Tempat Ruang server

Faktor lingkungan berkaitan erat dengan bangunan tempat ruang server didirikan untuk itu sebagai awal pembahasan akan dimulai mengenai lokasi bangunan dan fisik bangunan untuk ruang server sebagai langkah awal pengamanan data.

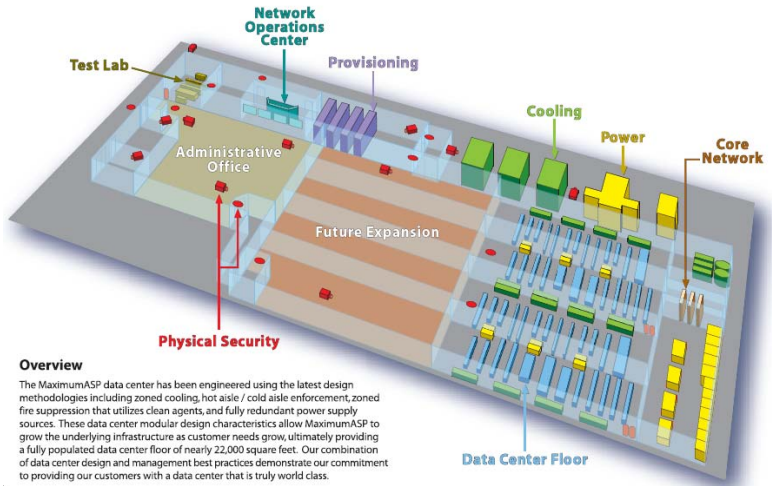
- Lokasi Ruang server

  Pemilihan lokasi bagunan mejadi hal yang harus diperhatikan. Kesadaran ini muncul sejak peristiwa 11 September, runtuhnya WTC membuat orang menjadi memperhatikan pemilihan lokasi yang tepat untuk Ruang server. Hal-hal berikut dapat dijadikan bahan pertimbangan dari segi aspek keamanan dalam pemilihan lokasi. Lokasi yang dipilih sebaiknya yang memiliki sedikit resiko baik dari ancaman bencana alam (jalur gempa, daerah rawan banjir atau daerah rawan tornado) maupun dari ancaman teroris dan vandalisme. Ruang server sebaiknya dibangun terpisah dari kantor pusat. Cukup jauh dari jalan raya utama. Tidak bertetangga dengan bandar udara, pabrik kimia, jalur pipa gas, pusat keramaian (pasar, stadium olahraga) dan pusat pembangkit listrik. Dan juga lokasi memiliki fasilitas yang memadai, seperti kecukupan tenaga listrik.

- Kontruksi Bangunan Ruang server

  Setelah memilih lokasi yang baik selanjutnya kita harus memperhatikan bagunan yang akan didirikan untuk ruang server. Bangunan harus memperhatikan masalah sirkulasi udara karena hal ini terkait dengan suhu, ventilasi udara yang cukup, penggunaan AC yang direncanakan

dengan baik. Karena biasanya bangunan ruang server dibuat dengan sedikit/bahkan tidak ada jendela dan tertutup. Bahan bangunan yang dipakai harus tidak mudah terbakar serta kontruksi bangunan yang tahan gempa. Adanya ruangan terpisah antara ruangan administratif dengan ruangan server dan data. Gunakan standar pendingin ruangan seperti TIA-942 dan perhatikan pengaturan kabel yang melalui bawah lantai. Menyiapkan kabel standar untuk instalasi listrik yang dibutuhkan dan konstruksi bangunan harus memperhatikan hal tersebut. Pintu masuk dirancang sangat terbatas. Pintu kebakaran dirancang untuk keluar saja. Segala aspek keamanan dalam bangunan sebuah ruang server harus direncanakan dengan baik. Kontruksi dan arsitektur bangunan harus dapat mengakomodasi semua hal berkaitan dengan keamanan fisik. Layout berikut ini menggambarkan contoh ruangan yang ada dalam Ruang server.



Gambar Layout bangunan ruang server.

- Pengamanan disekililing bangunan

  Disekeliling bangunan ruang server seharusnya adalah bidang kosong, bangunan ruang server sebaiknya memiliki jarak ± 10 meter dengan bangunan lain atau tanaman dan pohon, hal ini dimaksudkan untuk memudahkan pengawasan. Dinding dan tembok yang ada disekitar ruang server harus dapat dimonitor dengan baik. Penggunaan kamera CCTV sebagai pengawas adalah hal minimal yang harus dilakukan. Selain itu juga kamera yang digunakan sebaiknya memiliki kemampuan terhadap cahaya rendah, tahan terhadap suhu dan cuaca. Selain itu

juga penggunaan landscape setelah bidang kosong pada ruang server baik dilakukan, adanya pepohonan dan taman akan membuat ruang server tersembunyi dari orang yang lewat disekitar ruang server serta pengintai.

Pengawasan juga tidak terlepas dari areal parkir yang ada didekat ruang server. Pengawasan orang yang masuk dan keluar di kawasan ruang server harus dimonitor dengan baik. Penggunaan detektor bom perlu dilakukan untuk memeriksa setiap mobil yang masuk ke kawasan ruang server. Penggunaan penjaga atau petugas keamanan yang profesional merupakan sebuah hal yang harus dilakukan. Intinya jadikanlah bangunan ruang server sebagai sebuah benteng yang harus memiliki pengamanan baik diluarnya, agar orang yang tidak berkepentingan tidak mudah untuk masuk kedalam bangunan.

- Pengamanan didalam bangunan
  Pengamanan didalam bangunan juga terkait dengan hal-hal lain seperti faktor manusia. Penggunaan kamera pengawas, sensor asap, sensor kebakaran merupakan hal standar yang harus diterapkan. Pengawasan terhadap pintu masuk dan keluar orang harus diperhatikan dengan baik. Pintu masuk yang menggunakan bahan dari baja serta penggunaan kaca dan dinding yang aman akan sulit dilalui. Namun penggunaan pendeteksi penyusup dapat pula diaplikasikan pada bangunan ruang server.

Kebakaran

Bahaya kebakaran sangat mungkin terjadi di ruang server. Kumpulan peralatan elektronik yang ada berpotensi untuk menyebabkan kebakaran. Suplai tenaga yang baik harus diperhatikan, bangunan yang tidak mudah terbakar, penggunaan sensor asap, sensor panas, pemadam api dan sistem penyemprot air merupakan hal-hal yang harus dilakukan untuk mengurangi dan menanggulangi bahaya kebakaran. Pemasangan detektor dan sensor baik pada rungan komputer maupun di luar ruangan. Penggunaan alarm kebakaran dapat dilakukan baik secara manual maupun otomatis. Selain itu juga gunakan pemadam api yang sesuai dengan jenis kebakaran yang terjadi. Ada dua jenis pemadam api yaitu pemadam kimia

kering dan pemadam dari gas halon. Serta perhatikan juga efek yang dapat ditimbulkan dari penggunaan pemadam api.

Berikut ini langkah-langkah yang ditulis oleh Lance D. Harry seorang manejer pengembang bisnis di Fenwal Protection System, yang dapat dilakukan untuk perencanaan kebakaran.

1. Proteksi = deteksi + suppresi
   Idealnya proteksi yang dilakukan yaitu dengan menerapkan deteksi asap dan sistem suppresi kebakaran. Suppresi kebakaran dapat dilakukan dengan pemasangan detektor asap dan sensor udara pada langit-langit. Dan lengkapi dengan sistem penyemprot air baik skala kecil maupun besar seperti FM200.
2. Memahami secara keseluruhan strategi FP perusahaan.
3. Dapatkan ahli yang terpercaya untuk memberikan saran penanggulangan bahaya kebakaran.
4. Pahami kebutuhan lokal
   Selain menerapkan standar tapi juga melihat kebutuhan perusahaan.
5. Lakukan penilaian resiko yang mencakup analisis TCO dalam fasilitas.
6. Lakukan perawatan sistem supaya dapat bertahan lama.
7. Didik dan latih pekerja.
   Diharapkan dengan pendidikan dan latihan pekerja dapat memahami bahaya kebakaran dan peduli untuk mencegah terhadap kemungkinan timbulnya bahaya.

Suhu

Ruang server sangat rentan terhadap temperatur yang tinggi. Oleh sebab itu penggunaan sensor suhu yang diletakkan di rack server menjadi sebuah solusi untuk mengendalikan suhu. Selain memperhatikan panas pada server, yang perlu diperhatikan adalah suhu ruangan. Untuk itu diperlukan sistem pendingin yang baik. Sejak mulai awal pembangunan ruang server hendaknya sudah diperhitungkan berapa kapasitas yang diperlukan untuk membuat ruangan tetap dingin, sehingga tidak kesulitan dalam menghitung listrik yang dibutuhkan. Meningkatnya suhu dapat diatasi dengan penambahan AC, namun akan dapat menimbulkan masalah karena membutuhkan listrik yang cukup besar.

Ada beberapa pendekatan yang dikembangkan untuk menghitung besarnya kebutuhan pendinginan. Pada dasarnya hal ini bergantung dari banyaknya jumlah peralatan yang ada didalam ruang komputer yang harus didinginkan. Cara sederhananya mungkin dengan melihat kapasitas ruangan yang dapat menampung berapa banyak rack server kemudian dari hal tersebut dapat diperkirakan berapa kebutuhan pendinginan yang diperlukan.

Sebuah teknologi baru yang dapat diterapkan untuk menyesuaikan kapasitas pendinginan dengan kebutuhan ruang komputer. Lantai terbaru meningkatkan ketepatan sistem pendingin yang secara otomatis menyesuaikan kapasitas dengan kebutuhan ruangan tanpa memutar kompresor dan meningkatkan efisiensi dan realibilitas. Hal ini memungkinkan peningkatan kapasitas ekstra dalam sistem tanpa peningkatan dalam biaya energi. Keuntungan menggunakan pre-piping adalah kemudahan untuk menambahkan atau memindahkan model pendingin, selain itu juga realibilitas akan dapat tercapai.

Listrik/Tenaga

Kebutuhan listrik merupakan hal yang penting pada sebuah ruang server. Karena semua peralatan komputer, peralatan komunikasi dan jaringan serta pendingin membutuhkan energi. Selain itu juga penggunaan listrik cadangan seperti Genset dan UPS harus dilakukan. UPS yang digunakan harus memenuhi kebutuhan listrik dari semua peralatan yang ada. Batere UPS diharapkan dapat bertahan cukup lama sebelum digantikan dengan listrik cadangan dari Genset.

Banyak metoda yang dapat diterapkan untuk menghitung kebutuhan tenaga pada ruang server. Berikut ini contoh penghitungan tenaga listrik yang dibutuhkan.

Tabel 2.1 Informasi kebutuhan ruang server

Data	Value	Units	Comment
Total IT racks available	28	#	Some of the space in the data center is consumed by power and cooling equipment
Total initial power requirement	47	kW	At least 47 kW of power and cooling equipment must be installed initially. Using Figure 1, based the density of Row 1, 2 and 3, the number of IT racks spaces available is 6, 4, and 5 respectively (6 x 2 kW / rack + 4 x 5 kW / rack + 5 x 3 kW / rack = 47 kW)
Total final power requirement	104	kW	The remainder of the power and cooling equipment, as much as 60 kW, is deferred until the remaining rows are determined (28 IT racks x 3.7 kW / rack = 104 kW)
Peak power density	15	kW / rack	Cooling at this high density narrows the options available and increases the cost. A further attempt to spread these peak loads should be considered before committing the design at this density
Average data center power density	3.7	kW / rack	This data center, as specified, is more than twice the density of the average existing data center. Less than 2% of data centers today achieve this density

Sekarang ini telah timbul semacam pandangan untuk mengurangi konsumsi energi pada sebuah ruang server, misalnya penggunaan teknologi pendingin terbaru, penggunaan energi lain seperti matahari atau hidrogen. Teknologi untuk hal ini masih terus dikembangkan seiring dengan kesadaran para manajer untuk lebih mengefisiensikan konsumsi energi di sebuah ruang server.

Bencana Alam

Bencana alam memang tak dapat dihindari, namun kita dapat mengantisipasi untuk mengurangi resiko yang disebabkan oleh bencana alam. Pada awal telah disebutkan bangunan ruang server harus jauh dari daerah yang sering dilanda bencana alam seperti gempa bumi, gunung meletus, banjir, tornado dan sebagainya. Kontruksi bangunan yang memiliki ketahanan terhadap gempa adalah suatu cara yang dapat diterapkan. Selain itu juga rak server ditempatkan pada platform isolasi seismic sehingga resiko kerusakan jika terjadi gempa berskala kecil dapat dikurangi.

Namun demikian bencana alam bukan itu saja, untuk itu pentingnya penerapan backup yang kontinu pada sebuah ruang server dan tempat penyimpanan data hasil backup harus terpisah dari ruang server dan disimpan pada tempat yang aman pula. Antisipasi terhadap bencana alam,

kebakaran atau kerusakan pada ruang server hanya dengan cara backup data. Teknologi backup data yang digunakan terkait erat dengan keamanan data secara virtual. Oleh sebab itu konvergensi keamanan fisik dan virtual pada keamanan ruang server merupakan hal yang tidak dapat ditawar. Backup dapat dilakukan langsung di ruang server menggunakan media backup seperti tape, cd, dvd atau alainnya. Namun dapat pula dilakukan secara virtual melalui jaringan. Backup yang dilakukan ini disebut dengan istilah *remote replication* jadi backup dilakukan dari hard disk ke hard disk. Karena dilakukan melalui jaringan diperlukan bandwidth yang cukup untuk melakukan hal ini dan aspek keamanan virtual harus lebih diperhatikan. Penyimpanan terhadap data hasil backup perlu diperhatikan. Gudang penyimpanan harus aman dari penyusup dan ruangan penyimpan harus baik, bebas debu, tidak lembab dan tidak mudah terbakar agar data tetap terjaga.

Backup yang dilakukan merupakan salah satu cara dalam perencanaan pemulihan bencana atau lebih dikenal dengan *disaster recovery planning* (DR *planing*). Dengan adanya perencanaan ini dimaksudkan setelah becana selesai dapat terus melanjutkan operasi bisnis. Data yang telah dibackup akan direstore sehingga bisnis dapat terus berlanjut.

Berikut ini cek list yang ditulis oleh Denis C. Brewer di newsletter searchdatacenter.com mengenai DR *planning*.

Rule 0

identifikasi semua proses bisnis kritikal dan aplikasi-aplikasi, bersama dengan perangkat keras, perangkat lunak, bisnis, dukungan staf IT yang menjalankan, dan LAN serta WAN yang mengkoneksikan mereka ke pengguna akhir. Kelanjutan bisnis dan rencana pemulihan IT harus memasukkan semua tindakan dalam setiap elemen yang diidentifikasi.

Rule 1

setiap harinya buat replika (dalam disk atau tape) dari "digital trio", yaitu :

Sistem operasi tempat aplikasi berjalan dan patch level saat itu yang ditampilkan pada lingkungan produksi.

Aplikasi kritis yang berjalan pada system operasi pada patch saat ini.

Data.

Jangan ada istilah "no data loss." Bit-by-bit backup data adalah berharga.

Rule 2

Miliki "carbon copy" dari perangkat keras yang dibutuhkan untuk menjalankan tiruan digital. Penggunaan media backup terbaik adalah nilai kecil, jika tidak memiliki perangkat keras yang tepat ketika dan dimana data diperlukan dengan cepat untuk merestore digital trio ke peralatan baru atau yang siap.

Rule 3

Tulis langkah demi langkah untuk merestore tiruan digital ke carbon copy perangkat keras.

Rule 4

Selalu lakukan percobaan. Baik tiruan digital, perangkat keras dan dokumentasinya.

Rule 5

Capai praktek maksimum atau pemisahan yang mampu antar lokasi yang digunakan untuk operasi harian dan tempat penyimpanan tiruan, pemulihan perangkat keras dan dokumentasi. Lokasi backup pada kota yang sama hendaknya dihindari. Perhatikan batasan dari metoda komunikasi yang didukung oleh strategi jalur backup.

Rule 6

Respon dengan segera untuk kondisi yang beresiko tinggi. Badai Katrina memberikan pelajaran ketika kota tidak dapat berfungsi. Latihan teknis dan peroses bisnis untuk staf pada lokasi kerja alternatif.

Rule 7

Miliki dan sedikitnya identifikasi, koneksi alternatif, rute transmisi data dan sumber tenaga listrik. Bergantung di mana lokasi bisnis, alternatif rute dan sumber mungkin terbatas. Pelajari pilihan yang pada lokasi. Jika kantor cabang terhubung dengan kabel, putuskan investasi lain seperti penggunaan jalur satelit.

Rule 8

Aplikasikan konsep "Fort Knox", terapkan keamanan fisik lebih dari satu pada tempat penyimpanan tiruan.

Rule 9

Dokuentasi dan latihan perencanan bisnis keseluruhan. Uji coba dan recanakan dan jawab pertanyaan : Apakah proses bisnis operasi staf efisien setelah kejadian kurang baik.

Rule 10

Miliki dan operasikan alternative pengganti tenaga. Pertimbangkan tenaga generator listrik multi-fuel.

Rule 11

Tetapkan dan uji secara kontinu pada kondisi karantina.

Rule 12

Aplikasikan sumber daya yang diperoleh dan dirawat dari aturan 0-11 melalui daur hidup dalam aplikasi kritis.

Selain cek list diatas juga diperlukan strategi untuk menjalankan DR *planning* yang menyangkut hal-hal berikut : penilaian dampak bisnis, penemuan, anggaran, aturan dasar tim, proteksi data, logistik dan semiannual tes.