# BAB II

# LANDASAN TEORI

Pembahasan mengenai DRP tidak dapat dipisahkan dari teori sistem informasi dan *computer security*. Untuk menegaskan kembali beberapa definisi atau terminologi yang terkait dengan DRP juga perlu diuraikan, yaitu mengenai *physical data management*, *enterprise resources planning* (ERP), bencana (*disaster*) dan *disaster recovery plan* (DRP).

## 2. 1. Sistem Informasi

Banyak pengertian sistem informasi yang telah di definisikan. Secara umum sistem informasi adalah sebuah sistem yang terdiri dari berbagai komponen yang berinteraksi dan bertujuan menghasilkan informasi.

Menurut Lauden,[3] sistem informasi adalah hubungan dari berbagai komponen yang di kumpulkan, diproses, disimpan dan informasi tersebut disebarkan untuk mendukung pengambilan keputusan untuk membuat analisa dan memberikan gambaran pada sebuah organisasi.

Sedangkan menurut Whitten,[4] sistem informasi adalah suatu pengaturan orang-orang, data, proses, dan teknologi informasi yang saling berhubungan untuk

---

[3] Lauden (1994,P8)

[4] Whitten (2003,P12)

mengumpulkan, memproses, menyimpan, dan menyediakan keluaran informasi yang diperlukan untuk men-*support* suatu organisasi.

## 2. 2. Computer Security

Oleh Gupta,[5] *Computer Security* didefinisikan sebagai proses menjaga dan melindungi perangkat keras, perangkat lunak, jaringan, fasilitas fisik, data dan orang dari kecelakaan atau hal yang disengaja serta bencana alam.

Jadi salah satu tujuan dari *computer security* adalah menjaga dan melindungi data dari bencana alam/*disaster*, dengan demikian diperlukan sebuah sistem agar terhindar dari bencana tersebut.

Sistem keamanan dari suatu perusahaan harus mempunyai cara untuk menangkal atau meminimalkan/mengurangi resiko yang terjadi, sistem ini harus beroperasi 7 hari dalam seminggu dan 24 jam dalam sehari, serta harus mempunyai layanan yang konsisten dan benar, demikian juga semua perangkat keras, perangkat lunak dan jaringan harus dalam keadaan prima.

Kecelakaan atau *accident* tidak dapat dihindarkan, untuk itu perusahaan harus mendefinisikan apa saja *accident* yang kemungkinan akan dialami oleh perusahaan tersebut.

Berikut ini beberapa terminologi dalam menjaga keamanan informasi:

---

[5] Gupta (2000,P329)

### 2.2.1 Kesengajaan atau *intentional*

Bencana hasil dari kesengajaan biasanya dilakukan oleh orang di dalam perusahaan yang mempunyai pengetahuan untuk melakukannya. Yaitu tindakan-tindakan seperti:

- Mencuri data penting perusahaan
- Menyadap *password* orang lain
- Membuka *email* orang lain
- Membaca arsip penting
- Menghapus data penting perusahaan
- Merusak *hardware* dan *software* dengan sengaja, yaitu seperti dengan sengaja membuka *file* atau *email* yang mengandung virus.

### 2.2.2 *Security Control*

Menurut Gupta, *Security Control* adalah kebijakan, prosedur, alat bantu, teknik, dan metoda yang dirancang untuk mengurangi pelanggaran keamanan, pembinasaan sistem, dan kesalahan sistem dari kecelakaan, kesengajaan dan bencana alam.[6]

Sehingga apabila terjadi *accident, security control* ini diharapkan akan mengurangi dampak yang terjadi.

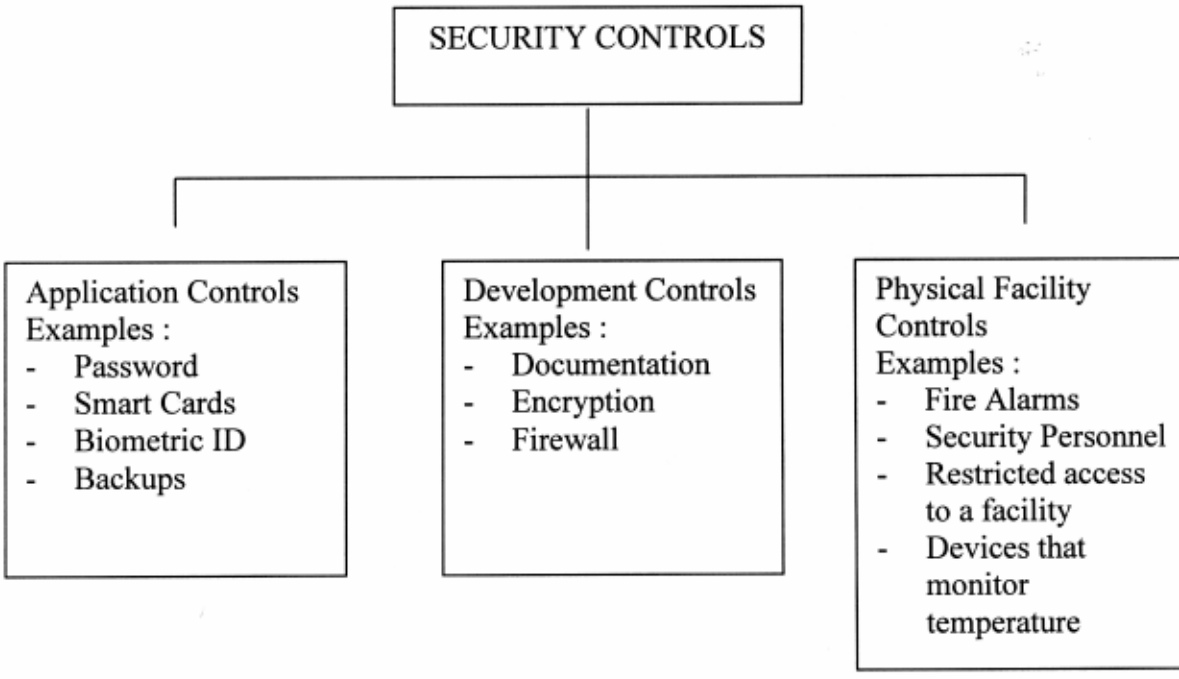
---

[6] Gupta (2000,P329)

Security Control mempunyai tiga fase yaitu :

- *Application Control*
- *Development Control*
- *Physical Facility Control*

Untuk lebih jelas dapat dilihat dari gambar dibawah ini :




**Gambar 2.1 Security Control**

## 2.3. *Physical Data Management*

*Physical data management* adalah suatu kegiatan menjaga, me-maintain, merawat dan menyajikannya kepada pihak-pihak yang membutuhkan. Dalam kaitannya dengan PT. SCU sebagai obyek dari pembahasan ini, *physical data management* adalah kegiatan yang fokus pada kegiatan menjaga, memelihara,

merawat dan menyajikannya kepada pihak-pihak yang membutuhkan data-data hasil eksplorasi perusahaan minyak, yaitu berupa *hard copy document*, bebatuan mineral, cairan sample eksplorasi ataupun berupa gas/uap.

## 2.4. *Enterprise Resource Planning* ( ERP )

ERP menurut situs webopedia[7] adalah *enterprise resource planning*, sistem manajemen bisnis yang mengintegrasikan semua bagian dari bisnis termasuk perencanaan, pembuatan, penjualan, sales dan marketing. Methodology ERP saat ini menjadi populer, aplikasi dari software ini banyak dipakai untuk membantu bisnis manajer untuk memimplementasikan ERP di aktivitas bisnis seperti mengontrol inventaris, mengecek pesanan, pelayanan konsumen, keuangan dan personalia.

Salah satu aplikasi dari ERP adalah SAP. SAP dikenal oleh umum sebagai *System Aplications and Products*. SAP didirikan di Jerman pada tahun 1972. Saat ini SAP adalah salah satu ERP yang terbesar di dunia, dan *software company* yang masuk ke dalam 4 besar di dunia. SAP adalah sistem yang terintegrasi, yang di dalamnya terbagi atas banyak modul yang saling berhubungan satu sama lain.

Modul yang diimplementasikan di PT. SCU dari SAP R/3, yang menjadi bahan saat ini adalah modul FI/CO (*Finance and Controlling*), modul *Asset Management* dan modul *Material Management* .

---

[7] lihat situs http://www.webopedia.com/term/e/erp.html

Sedangkan Menurut Whitten,[8] *Enterprise Resource Planning* adalah suatu aplikasi perangkat lunak yang secara penuh mengintegrasikan sistem informasi yang mencakup semua dan dasar dari fungsi bisnis inti (mencakup proses transaksi dan informasi manajemen )

Beberapa *Vendor* dari ERP adalah:

- SAP AG (penguasa pasar)
- Baan
- J. D. Edwards
- Oracle
- PeopleSoft

## 2. 5. *Disaster Recovery Plan*

Berikut adalah beberapa teori dan definisi yang terkait dengan DRP, yang pada saatnya nanti akan dijadikan acuan dalam bab pembahasan.

### 2.5.1. Definisi Bencana (Disaster)

Bencana menurut situs klikdt[9] adalah peristiwa atau rangkaian peristiwa yang disebabkan oleh alam, manusia dan atau oleh keduanya yang mengakibatkan korban dan penderitaan umat manusia, kerugian harta benda dan kerusakan

---

[8] lihat whitten

[9] lihat situs: http://www.klikdt.com/profile.php?dt=mainprofile&kid=93

lingkungan serta sarana dan prasarana umum sehingga menimbulkan gangguan terhadap tata kehidupan dan penghidupan masyarakat.

Bencana adalah sebuah keadaan tidak normal, yang membuat sebuah sistem menjadi rusak dan tidak berfungsi sebagaimana mestinya. Misal: kerusakan pada gedung akibat bencana gempa sehingga tidak dapat dipergunakan lagi, kerusakan sistem email di perusahaan akibat adanya virus, atau kerusakan komunikasi akibat jaringan telepon terputus.

Bencana baik sebagai ulah manusia, maupun akibat alam atau *natural disaster*, seringkali tidak dapat diprediksi kapan akan terjadi. Untuk itu harus dibuat sistem yang akan mengurangi resiko dan kerugian bila bencana terjadi.

### 2.5.2. Area yang berpotensi terjadinya bencana

Menurut *National Institute of Standards and Technology Special Publication*[10], area yang mempunyai resiko dapat diklasifikasikan menjadi tiga tipe yaitu:

- Alami, seperti: Banjir, angin ribut, tanah longsor, gempa bumi.
- Manusia, seperti: Kesalahan operator, sabotase, *malicious code*.
- Teknologi, seperti: Kesalahan alat, perangkat lunak error, jaringan telekomunikasi tidak berfungsi dan listrik mati.

[10] lihat *NIST Special Publication 800-34 hal 7, Contingency Planning Guide for Information Technology Systems, National Institute of Standards and Technology 2001*

### 2.5.3. Definisi *Disaster Recovery Plan*

DRP menurut Jurnal *Disaster Recovery* dari DRI International adalah dokumen yang menggambarkan sumber daya, tindakan, tugas dan data yang diperlukan untuk mengatur proses *recovery* bisnis pada saat terjadi gangguan yang mengancam bisnis perusahaan. Rencana ini dirancang untuk membantu mengembalikan proses bisnis dari perusahaan.

Sedangkan menurut National *Institute of Standard and Technology*, DRP adalah rencana yang sudah dipersiapkan untuk memproses aplikasi yang penting dalam situasi kerusakan besar dari perangkat keras dan perangkat lunak atau kerusakan yang besar pada fasilitas.[11]

DRP adalah didefinisikan tidak terbatas hanya sebagai tindakan pencegahan dan pemulihan dari infrastruktur IT, tapi adalah *business continuity plan,* yang memiliki fokus dan komponen yang lebih luas, seperti sebuah *crisis management plan* dan *human resources management.*

Diharapkan sebelum terjadi bencana, setiap perusahaan yang mempunyai data yang sangat penting harus mempunyai DRP agar apabila bencana tersebut terjadi kerugian dapat di minimalisasi dan dapat mengembalikan keaadaan perusahaan dengan cepat dan efektif.

---

[11] lihat *NIST Special Publication 800-34 hal D-1, Contingency Planning Guide for Information Technology Systems, National Institute of Standards and Technology 2001*

### 2.5.4 Merencanakan dari DRP

Sebuah rencana dari DRP mempunyai banyak model dan langkah yang berbeda tergantung dari pembuat rencana tersebut. Menurut DRI *international model* dari *Business Continuity Planning* adalah:

1. Fase awal (*project initiation phase*)
2. Fase persyaratan secara fungsi (*functional requirements phase*)
3. Fase desain dan pengembangan (*design and development phase*)
4. Fase penerapan (*implementation phase*)
5. Fase pengujian (*testing and exercising phase*)
6. Fase perawatan (*maintenance and updating phase*)
7. Fase eksekusi (*execution phase*) apabila terjadi bencana.

Di lain pihak, menurut *National Institute of Standard and Technology*,[12] DRP juga harus berperan dalam koridor *Contingency Planning Process*, yaitu yang terdiri dari fase-fase sebagai berikut :

1. Pengembangan kebijakan *contingency planning*, berupa:
   - Identifikasi kebutuhan saat ini (*existing requirements*).
   - Mengidentifikasikan program dan rencana bersama (*associated plans and programs*).
   - Mendapatkan dukungan dan persetujuan dari *senior management*.

---

[12] lihat *NIST Special Publication 800-34 hal 14, Contingency Planning Guide for Information Technology Systems, National Institute of Standards and Technology 2001*

2. Menjalankan *business impact analysis.*
   - Mengidentifikasi *critical IT resources.*
   - Mengidentifikasi *outage impacts* dan *allowable outage times.*
   - Mengembangkan proritas *recovery.*
3. Menetapkan *preventive controls.*
   - *Implement controls.*
   - *Maintain controls.*
4. Mengembangkan *recovery strategy.*
   - Mengidentifikasikan metodenya.
   - Mengintegrasikan pada sebuah *system architecture.*
5. Mengembangkan *contingency plan.*
   - Mendokumentasikan *recovery strategy.*
6. Merencanakan, mengujinya, melaksanakan training dan *exercises.*
   - Mengembangkan tujuan dari pengujian (*test objectives*).
   - Mengembangkan *success criteria.*
   - Mendokumentasikan pelajaran yang diperoleh dari test tersebut.
   - Memasukannya ke rencana secara keseluruhan (*incoporate into the plan*).
   - Melakukan pelatihan/training.
7. Merencanakan *maintenance.*
   - Melakukan *review* dan meng-*update plan.*
   - Mengkoordinasikan dengan organisasi internal dan eksternal.

- Mengendalikan distribusi kewenangan (*control distribution*).
- Mendokumentasikan setiap perubahan yang terjadi.

Model tersebut harus dilaksanakan dan diterjemahkan ke dalam bentuk kegiatan–kegiatan yang saling mendukung agar proyek ini berjalan sesuai dengan rencana. Secara garis besar proyek ini mempunyai tiga rencana besar yaitu :

1. **Tahap proteksi**

   Tahap proteksi adalah tahap pencegahan, bila bencana yang sesungguhnya terjadi harus siap menghadapi dan segera melakukan pelbagai antisipasi. Tahap ini terjadi pada keadaan normal dan bencana belum terjadi.

2. **Tahap bencana**

   Tahap masa bencana adalah masa bencana yang masih berjalan atau sedang berjalan. Dalam tahap ini, langkah-langkah yang harus diambil adalah harus relevan/sesuai dengan kondisi dan situasi bencana yang sedang terjadi saat itu.

3. **Tahap recovery atau pemulihan**

   Tahap pemulihan adalah masa perbaikan untuk dikembalikan ke situasi seperti kondisi normal pasca bencana.

### 2.5.5 Perancangan *Disaster Recovery Planning*

Perancangan *disaster recovery planning* menggunakan *System Development Life Cycle* ( SDLC )[13] dengan tahapan–tahapan sebagai berikut:

1. Tahap Inisiasi atau *Initiation Phase*

   Dalam tahap ini kebutuhan akan suatu sistem dinyatakan dan tujuan sistem dan kebutuhan tingkat tinggi atau *high level* di dokumentasikan.

2. Tahap Pengembangan atau *Development / Acquisition Phase.*

   Dalam tahap pengembagan sistem, sistem dirancang, dibeli, deprogram dan dikembangkan.

3. Tahap Implementasi atau *Implementation Phase.*

   Pada tahap ini setelah sistem di tes, kemudian sistem diimplementasikan.

4. Tahap Pemeliharaan atau *Maintenance Phase*

   Sistem telah bekerja setelah dikembangkan kemudian sistem di pelihara/maintenance.

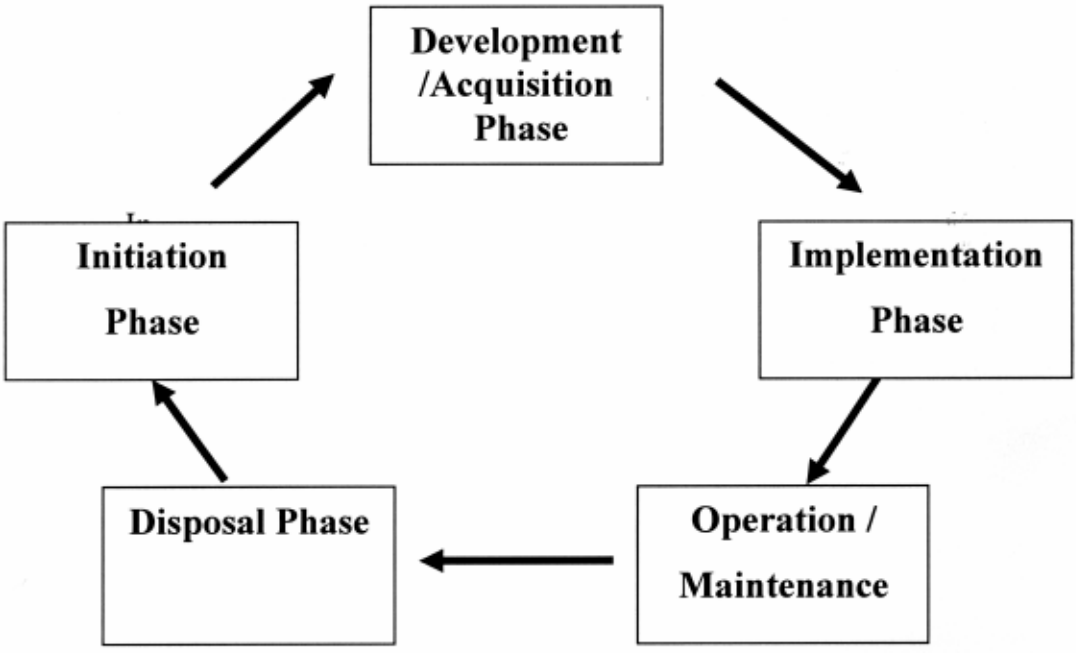
5. Tahap Penyelesaian atau *Disposal Phase*

   Pada tahap ini sistem telah selesai dibuat

---

[13] lihat *NIST Special Publication 800-34 hal 14, Contingency Planning Guide for Information Technology Systems, National Institute of Standards and Technology 2001*

Atau agar lebih jelas hubungan dari tahap - tahap dapat terlihat dari gambar berikut ini :




**Gambar 2.2 System Development Life Cycle**

Bila penerapan proyek ini berhasil maka *rewards* yang akan didapat oleh PT. SCU adalah sebagai berikut [14]:

1. Meningkatkan produktifitas.
2. Lebih hemat.
3. Permintaan pelanggan lebih meningkat.
4. *Service* meningkat/lebih baik.

---

[14] lihat *NIST Special Publication 800-34 hal 14, Contingency Planning Guide for Information Technology Systems, National Institute of Standards and Technology 2001*

5. Meningkatkan keuntungan.
6. Meningkatkan koleksi.
7. Meningkatkan *compliance.*
8. Meningkatkan moral.

### 2.5.6 Tier dari Disaster Recovery Planning[15]

Konsep *tier* saat ini banyak dipakai untuk desain dari *disaster recovery planning*. Konsep ini *powerful* dan terpusat untuk memilih metodologi karena konsep *tier* dikenal untuk memberikan klien *Recovery Time Objective* (RTO )[16].

Dengan mengkategorisasikan teknologi DRP ke berbagai macam *tier*, akan lebih mudah untuk mencocokan RTO yang diinginkan dengan teknologi yang optimal.

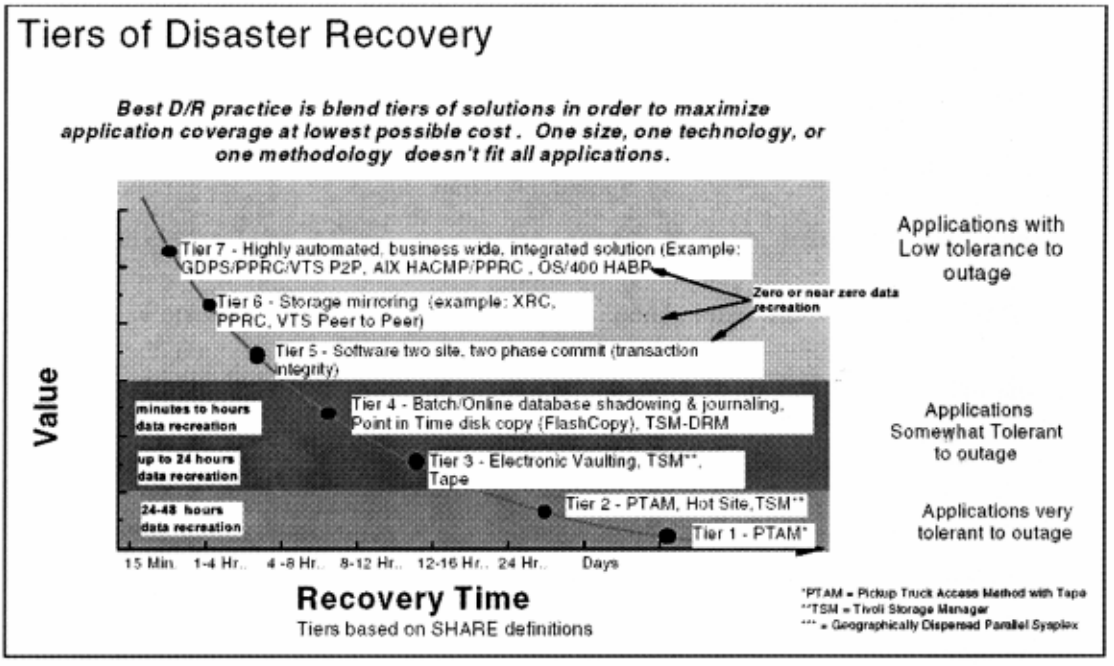
Konsep *tier* adalah fleksibel, apabila produk dan fungsi telah berubah sejalan dengan waktu maka *tier* ini harus di *update* sesuai dengan *tier* yang sudah dipakai sebelumnya.

Dengan melihat gambar dibawah ini dapat disimpulkan bahwa semakin besar *tier* maka biaya untuk implementasi *disaster recovery planning* semakin besar, dan semakin besar tier juga akan memerlukan waktu *recovery* yang semakin cepat.

---

[15] lihat IBM Total Storage for Disaster Recovery hal 47,*Redbook January 2004*

[16] RTO (Recovery Time Objective ) adalah waktu yang bisa ditoleransi oleh sistem selama kejadian / bencana berlangsung




**Gambar 2.3 Konsep dari tier IBM**

### 2.5.7 Site dari Disaster Recovery Planning

DRP harus mempunyai lokasi/*site* yang ideal agar apabila lokasi utama dari peusahaan mengalami bencana, lokasi tersebut dapat bekerja menggantikan lokasi utama dengan cepat dan akurat.[17]

Lokasi cadangan dapat dipelihara sendiri atau menggunakan jasa vendor yang dapat dipercaya.

*Site* cadangan dapat dibagi menjadi 5 yaitu :

1. *Cold Site*

Biasanya terdiri dari fasilitas dengan ruang dan infrastruktur yang cukup

[17] lihat NIST

(listrik, koneksi komunikasi, kontrol lingkungan atau ruangan) untuk men-*support* sistem IT. Ruangan dapat memiliki *raised floors* dan peralatan lain yang mendukung operasi IT. Site tidak mempunyai peralatan IT dan tidak memiliki peralatan *office outomation,* seperti telepon, mesin fax dan poto kopi. Perusahaan yang menggunakan *cold site* ini berusaha untuk menyediakan dan meng-install peralatan yang perlu di site tersebut dan site tersebut mempunyai kemampuan komunikasi apabila dibutuhkan.

2. *Warm Site*

Di *site* ini sebagaian peralatan sudah ada dan berisi sistem perangkat keras, perangkat lunak, telekomunikasi dan tenaga listrik. *Warm site* dipelihara dan dalam status siap apabila akan digunakan. Site harus dipersiapkan lagi sebelum menerima sistem dan *recovery personal*. Dibanyak kasus, *warm site* mungkin dapat diibaratkan sebagai fasilitas operasi yang normal untuk sistem atau fungsi yang lain. Dan apabila terjadi bencana harus dipersiapkan terlebih dahulu sebelum sistem dipindahkan.

3. *Hot Site*

Adalah ruangan yang sama dengan kantor untuk men-*support* kebutuhan sistem dan dikonfigurasi dengan baik semua sistem perangkat keras, *supporting infrastructure*, dan pegawai yang men-support lokasi tersebut.

*Hot site* adalah site yang harus beroperasi 24 jam per hari, 7 hari seminggu, pegawainya harus siap apabila *contingency plan* diaktifkan.

4. *Mobile Site*

Adalah site yang dapat berpindah/*transportable* (mobil kontainer) dengan alat komunikasi khusus dan peralatan IT yang memenuhi syarat sebuah *site*. Biasanya perusahaan menyewa *site* ini dari *vendor* dengan *service-level agreement* (SLA) yang jelas.

5. *Mirrored Site*

*Mirrored site* adalah fasilitas yang *full redundant* dengan *full real-time information mirroring*.

*Site* identik dengan *site* utama dengan fasilitas lengkap dan menyediakan kesediaan yang *highest degree* karena data diproses dan disimpan dalam site utama dan site yang lain secara simultan. Site di disain, dibuat dan dioperasikan dan di pelihara oleh perusahaan.

### 2.5.8 Alasan penggunaan DRP

Menurut *CBK review August 1999* alasan sebuah perusahaan menggunakan *Disaster Recovery Plan* adalah[18] :

1. Proaktif dari pada reaktif.

   Perusahaan diharapkan proaktif yaitu mempersiapkan rencana penanggulangan bencana sebelum terjadi bencana.

2. Maintain aktifitas bisnis.

   Apabila suatu perusaan tidak mempunyai *disaster recovery plan* akan mengakibatkan kerugian dalam jangka pendek dan jangka panjang.

3. Dampak terhadap pelanggan.

   Kehilangan citra perusahaan dimata pelanggan.

4. Undang – undang yang mengharuskan.

   Undang–undang suatu negara yang mengharuskan suatu perusahaan mempunyai *disaster recovery plan.*

### 2.5.9 Kerugian apabila tidak mempunyai DRP

Bencana dapat meliputi suatu wilayah yang luas, tetapi hasilnya dapat juga bervariasi tergantung pada sifat alami dari bencana. Seperti yang dapat dijelaskan di bawah ini: [19]

---

[18] lihat CBK review
[19] lihat NIST

- **Kerugian langsung (direct losses).**

  Kerugian langsung mempresentasikan nilai dari semua aset yang mungkin telah hilang/musnah dan dapat meliputi *key personel*, data, infrastruktur, jaringan, dan sebagainya. Kerugian ini secara langsung dihubungkan dengan nilai aset dari perusahaan.

- **Kerugian tidak langsung.**

  Kerugian tidak langsung adalah disebabkan oleh ketidakmampuan sistem untuk beroperasi, atau dapat mengoperasikannya tapi levelnya telah turun karena tidak ketersediaan sumber daya seperti akses data, listrik, layanan telepon dan yang lainnya.

  Biasanya kerugian ini akan berlanjut atau menjadi lebih buruk sampai gangguan dapat dikurangi/diatasi. Kerugian meliputi produktivitas yang hilang seperti halnya pendapatan/*revenue*.

- **Kerugian sebagai akibat**

  Kategori ini adalah disebabkan oleh *outage*, tetapi konsekuensi yang dihadapi perusahaan akan bertahan lama walaupun perusahaan sudah beroperasi kembali. Kerugian tersebut meliputi citra perusahaan, harga saham, dan hilangnya pelanggan dan penguasaan pasar.

Selain dampak yang disebut di atas, juga terdapat dampak dari segi financial, yaitu:

- **Laba yang hilang.**

  1. Kompensasi yang harus dibayar.
  2. Kehilangan pendapatan masa depan.
  3. Kerugian investasi.

- **Kerugian Produktivitas.**

  Dampak jumlah sumber daya manusia yang dipakai.

- **Pengumpulan tagihan/collection yang di/tertunda.**

  1. Kerugian pembayaran.
  2. Diskon terlewatkan.

- **Biaya Ekstra.**

  1. *Cost* untuk pemulihan.
  2. Biaya *overtime.*
  3. Resiko penipuan.
  4. *Error rate* meningkat.
  5. Biaya perjalanan.
  6. Karyawan sementara.

- **Hukuman.**

  1. Berdasarkan kontrak.
  2. Pemerintah.

3. Legal.

- **Merusak Reputasi.**

  Reputasi kepada *Customer*, Penyalur, Mitra, Bank, Pasar Uang, dan *Rating* dari kredit yang menurun.