**LECTURE NOTES**

**IT Risk Management and Disaster Recovery**

**KDS – Name SME**

**Session 13**

**Disaster Recovery – Preparation, Operation and Maintenance**

1. **Disaster planning functions**

Jika terjadi bencana, maka organisasi harus memobilisasikan semua kemampuan dan sumber daya yang dibutuhkan untuk melanjutkan kegiatan operasionalnya dan mengembalikan keadaan menjadi normal secepat mungkin karena waktu adalah uang. Bencana adalah sebuah kejadian yang memberikan akibat negatif dalam skala yang relatif sangat besar. Kejadian yang mengakibatkan kegagalan sistem dan memberikan dampak yang membahayakan terhadap bisnis yang dijalankan. 50% dari perusahaan yang pernah mengalami kegagalan sistem akibat bencana, tidak akan bertahan hidup dan 90% nya akan mati dalam 2 tahun.

Disaster planning functions merupakan proses, kebijakan dan prosedur mengembalikan fungsi-fungsi kritikal perusahaan, mencakup akses ke data (dokumen, perangkat keras, perangkat lunak, dsb), akses komunikasi, akses ke lokasi kerja dan proses bisnis lain setelah terjadinya bencana. Untuk meningkatkan peluang pemulihan dari dokumen-dokumen penting, sebuah Disaster Recovery Plan harus dikembangkan dan diuji secara seksama. Tugas ini menuntut kerja sama lintas bagian di perusahan. Disaster Recovery Plan difokuskan pada perlindungan data perusahaan, dan sebaiknya mencakup tindakan mengatasi terputusnya jalur komunikasi dan kehilangan personil-personil kunci. DRP merupakan bagian dari proses lebih besar yang dikenal sebagai Business Continuity Plan (BCP).

Business Continuity Planning (BCP) adalah konsep pembuatan dan pengujian rencana logistic perusahaan untuk mengembalikan dan memperbaiki sebagian atau seluruh fungsi-fungsi kritikal yang terganggu dalam jangka waktu tertentu setelah terjadinya gangguan. BCP bertujuan mengurangi risiko operasional akibat kurangnya kendali informasi di tingkat manajemen, dan proses ini umumnya terintegrasidengan kebijakan Manajemen Risiko. Pada Desember 2006, British Standards Institute menerbitkan standar independen baru untuk BCP, yaitu BS 25999 yang dapat diterapkan di semua organisasi, baik perusahaan kecil dan besar, swasta atau pemerintah, di sektor industri manapun. BCP umumnya berupa pedoman tertulis sebagai referensi sebelum/selama/sesudah gangguan terjadi. Pedoman BCP perusahaan kecil/menengah bisa berupa dokumen yang disimpan di tempat yang berbeda dengan lokasi kerja, berisi daftar nama, alamat dan nomor telepon dari karyawan, klien, pemasok dan informasi-informasi terpenting untuk kelanjutan hidup perusahaan. Dalam format yang kompleks. Pedoman BCP juga memuat lokasi kantor/fasilitas produksi cadangan, kesiapan dan kebutuhan teknis, langkah pemulihan operasi, metode mendapatkan kembali dokumen perusahan, jalur suplai, dan sebagainya. Pedoman harus disusun secara realistis dan mudah dijalankan di dalam masa krisis.

**Tujuan Adanya DRP:**

* Mempersiapkan organisasi dalam menghadapi bencana
* Meningkatkan Kepuasan Konsumen dan Kepercayaan masyarakat
* Melindungi dan memelihara citra positif organisasi di mata masyarakat umum Meningkatkan Kepercayaan investor atau stakeholder
* Meminimasi kerusakan atau gangguan akibat bencana
* Mengembalikan kegiatan operasional menjadi normal kembali secepat mungkin setelah terjadi bencana

Dalam membuat dokumen DRP perlu dibentuk sebuah tim dengan seorang koordinator yang tanggungjawabnya adalah:

* Melaporkan progress ke manajer tingkat atas
* Menyusun budget untuk DRP
* Menyimpan file anggota tim DRP
* Menjadwalkan meeting Tim
* Memimpin meeting tim
* Mendokumentasikan kebijakan dan prosedur DRP
* Menangani hubungan dengan pihak penyedia jasa luar untuk mendukung DRP Mengawasi hasil kerja antar departemen dan bawahan
* Penjadwalan Test dan latihan Mengatur pemeliharaan DRP
* Mengupdate Dokumentasi jika diperlukan

1. **Disaster response phase**

Penyusunan strategi Disaster Recovery harus didasarkan pada Business Continuity Plan yang berisi targe Recovery Point Objective (RPO) dan Recovery Time Objective (RTO) untuk berbagai proses bisnis perusahaan. Kedua target ini harus dipadankan dipadankan dengan sistem dan infrastruktur IT pendukungnya. Kemudian ditentukan strategi pemulihan yang paling tepat untuk setiap sistem. Perlu diingat bahwa pencapaian RPO dan RTO sesungguhnya tergantung anggaran yang tersedia. Walau semua manajer bisnis menginginkan “zero data loss” dan “zero time loss”, biaya perlindungan dan ketersediaan setinggi ini sulit diwujudkan. Berikut adalah beberapa startegi umum untuk perlindungan data:

* Backup ke tape dan dikirim keluar kantor ke tempat aman secara regular
* Backup ke disk di lokasi dan salin secara otomotamis ke lokasi luar kantor
* Replikasi data ke lokasi luar kantor, sehingga mengurangi kebutuhan restorasi data (hanya system yang harus direstorasi)
* Sistem high availability untuk menjaga data dan sistem direplikasi ke lokasi luar kantor. Dalam banyak kasus, perusahaan akan lebih efisien menggunakan disaster recovery provider yang memiliki lokasi dan sistem pelindung daripada menggunakan fasilitas milik sendiri.

**Contoh Manajemen Risiko dalam Penggunaan Teknologi Informasi di Perbankan**

Peraturan Bank Indonesia Nomor 9/15/PBI/2007 tanggal 30 November 2007 Tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum.

**Latar Belakang**

* Peningkatan efisiensi kegiatan operasional dan mutu pelayanan Bank kepada nasabah melalui perkembangan Teknologi Informasi;
* Penggunaan Teknologi Informasi meningkatkan risiko yang dihadapi Bank;
* Penerapan manajemen risiko secara efektif sejalan dengan meningkatnya risiko yang dihadapi;
* Perlunya ditetapkan ketentuan yang mengatur Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum dalam Peraturan Bank Indonesia.

**Kerangka PBI**

* PBI berisi pokok-pokok ketentuan Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum yang meliputi :
  + Ruang Lingkup Manajemen Risiko
  + Penerapan Manajemen Risiko
  + Penyelenggaraan Teknologi Informasi oleh Pihak Penyedia Jasa Teknologi Informasi
  + Electronic Banking
  + Pelaporan
  + Ketentuan Peralihan

**Ruang Lingkup Manajemen Risiko Teknologi Informasi**

* Bank wajib menerapkan manajemen risiko secara efektif dalam penggunaan Teknologi Informasi
* Ruang lingkup penerapan manajemen risiko paling kurang mencakup:

1. Pengawasan aktif dewan Komisaris dan Direksi;
2. Kecukupan kebijakan dan prosedur penggunaan Teknologi Informasi;
3. Kecukupan proses identifikasi, pengukuran, pemantauan dan pengendalian risiko penggunaan
4. Teknologi Informasi; dan
5. Sistem pengendalian intern atas penggunaaan Teknologi Informasi.

Dalam membangun dokumen Disaster Recovery plan terdiri dari lima phase yaitu:

1. Preparation
2. Response
3. Recovery
4. Resumption
5. Restoration

Dalam proses preparation atau persiapan untuk membuat sebuah organisasi siap untuk kemungkinan untuk menghadapi bencana maka ada hal hal khusus yang harus diperhatikan, yaitu:

* Menghilangkan atau mengurangi potensi cedera atau hilangnya nyawa,
* Mengurangi kerusakan fasilitas, dan hilangnya aset
* Meminimalkan gangguan dan kerugian finansial
* Menstabilkan efek bencana untuk memungkinkan upaya pemulihan untuk memulai peenerapan prosedur DR

Peraturan pada bank untuk penyelenggaraan Pusat Data (Data Center) dan/atau Disaster Recovery Center

* 1. Data Center dan atau Disaster Recovery Center diselenggarakan di dalam negeri.
  2. Apabila Bank menggunakan Penyedia Jasa TI *(outsourcing)*, maka persyaratannya adalah:

**a. Syarat bagi Bank:**

* 1. Bertanggung jawab atas penerapan manajemen risiko;
  2. Mampu melakukan pengawasan atas pelaksanaan kegiatan Bank yang dilakukan oleh penyedia jasa TI;

Memilih pihak penyedia jasa TI berdasarkan cost and benefit analysis;

* + - 1. Wajib memantau dan mengevaluasi kehandalan pihak penyedia jasa;
      2. Tetap memberikan akses kepada auditor intern, ekstern dan Bank Indonesia;
      3. Memberikan akses kepada Bank Indonesia terhadap database secara tepat waktu.

**b. Syarat bagi Pihak Penyedia Jasa:**

* + - Menerapkan IT control secara memadai, dibuktikan hasil audit independen;
    - Menyediakan akses bagi auditor intern Bank, ekstern dan auditor dari BI;
    - Menyatakan tidak keberatan bila BI hendak melakukan pemeriksaan;
    - Sebagai pihak terafiliasi, harus menjamin keamanan seluruh informasi;
    - Melakukan subkontrak sebagian kegiatannya berdasarkan persetujuan Bank, dibuktikan dengan dokumen tertulis.
    - Melaporkan setiap kejadian kritis yang dapat mengakibatkan kerugian keuangan dan mengganggu operasional Bank;
    - Menyampaikan secara berkala hasil audit TI yang dilakukan auditor independen pada penyelenggaraan TI DC, DRC dan atau Pemrosesan Transaksi Berbasis Teknologi kepada BI melalui Bank yang bersangkutan;
    - Menyediakan DRP yang teruji dan memadai;
    - Bersedia untuk memungkinkan early termination.

Apabila Bank akan menyelenggarakan Data Center dan atau Data Recovery Center di luar negeri,Bank harus mendapat persetujuan Bank Indonesia dan memenuhi persyaratan yaitu Syarat bagi Bank (a) dan Syarat bagi pihak penyedia jasa (b) diatas.

**c. Syarat tambahan bagi Bank :**

* + menyampaikan hasil analysis Country Risk;
  + penyelenggaraan DC dan DRC di LN tidak mengurangi efektivitas pengawasan BI;
  + informasi mengenai rahasia Bank hanya dapat diungkapkan sepanjang mematuhi perundangundangan di Indonesia;
  + perjanjian tertulis antara Bank dan penyedia jasa harus memuat klausula choice of law;

**SIMPULAN**

Disaster Recovery Plan difokuskan pada perlindungan data perusahaan, dan sebaiknya mencakup tindakan mengatasi terputusnya jalur komunikasi dan kehilangan personil-personil kunci. DRP merupakan bagian dari proses lebih besar yang dikenal sebagai Business Continuity Plan (BCP).

Penyusunan strategi Disaster Recovery harus didasarkan pada Business Continuity Plan yang berisi targe Recovery Point Objective (RPO) dan Recovery Time Objective (RTO) untuk berbagai proses bisnis perusahaan

**DAFTAR PUSTAKA**

1. Whitman, M.E., Mattoro, H.J. (2013). ***Principles of Incident Response and Disaster Recovery***.