Penanggulangan Bencana Teknologi Informasi Di Data Center Perusahaan Dengan Metoda *Disaster Recovery Plan* (DRP)

Akmal Hidayat [1], ***Ade Andri Hendriadi*** [2]
Program Studi Teknik Informatika, Fakultas Ilmu Komputer,
Universitas Singaperbanga Karawang
E-mail: mall_7@yahoo.com, hendri2k@gmail.com

ABSTRAK

Semakin tinggi ketergantungan perusahaan terhadap sistem informasi, semakin rentan pula perusahaan terhadap gangguan atau bencana yang mengganggu sistem informasi yang dimiliki. Rencana penanggulangan bencana (Disaster Recovery Plan) adalah salah rencana darurat dibidang teknologi informasi yang ditujukan untuk memulihkan layanan IT setelah terjadinya suatu gangguan besar/bencana dan membutuhkan relokasi sistem. Hasil analisa menunjukkan terdapat 6 asset IT/aplikasi yang dipandang kritis terhadap 13 ancaman bahaya resiko yang teridentifikasi. Rancangan Disaster Recovery Center yang diterapkan menggunakan teknologi Clustering dan Synchronous Replication. DRC dilengkapi dengan SOP dan fasilitas serta kelengkapan layaknya sebuah Data Center.

Kata Kunci**:** *Disaster Recovery Plan, Business Continuity Plan, IT Contingency Plan*

PENDAHULUAN

Teknologi informasi telah dipergunakan secara meluas didalam proses bisnis organisasi. Beberapa organisasi bahkan memiliki kecendurungan untuk sangat tergantung pada teknologi informasi dalam operasional kesehariannya.

Penerapan IT dalam organisasi memberikan nilai positif dari berbagai aspek, seperti peningkatan efektifitas kerja dan efisiensi, peningkatan marketshare dan lain-lain. Namun disisi lain memberikan aspek yang sangat merugikan bila terjadi kegagalan IT dalam organisasi. Besarnya kerugian ini akan berbanding lurus dengan tingkat penerapan IT dalam suatu organisasi. Semakin besar sebuah organisasi menggantungkan proses bisnisnya pada IT, maka semakin besar pula kerugian yang dialami akibat tidak berlangsungnya proses bisnis.

Kerugian organisasi sangat terkait pada resiko (Risk) yang dihadapi oleh organisasi. Setiap organisasi menghadapi resiko yang berbeda-beda, dan berkaitan erat pada strategi bisnis yang diterapkan dan bidang usaha atau bisnis utama organisasi. Resiko memiliki tingkat intensitas dan dampak kerugian yang berbeda-beda. Resiko secara umum dapat dibagi menjadi beberapa kategori:

1. Bencana alam

2. Manusia
3. Lingkungan (diluar bencana alam)

Sebuah rencana penanggulangan diperlukan untuk memulihkan dukungan IT, sehingga proses bisnis kembali berfungsi normal dalam waktu yang singkat. Rencana tersebut dikenal sebagai Rencana Kelangsungan Usaha (BCP). Rencana Penanggulangan Bencana (DRP) merupakan salah satu bagian dari BCP.

TINJAUAN PUSTAKA

Definisi Rencana Penanggulangan Bencana (*Disaster Recovery Plan*)

DRP didefinisikan secara berbeda-beda oleh oleh masing-masing organisasi. Perbedaan tersebut disebabkan perbedaan persepsi, fungsi dan dan kepentingan setiap organisasi. Namun DRP tidak boleh didefinisikan keluar dari tujuan dan batasan DRP. Berikut adalah beberapa definisi DRP dari lembaga-lembaga internasional yang independen dan referensi yang ada.

Disaster Recovery Plan (DRP). *As suggested by its name, the DRP applies to major, usually catastrophic, events that deny access to the normal facility for an extended period. Frequently, DRP refers to an IT-focused plan designed to restore operability of the target system, application, or computer facility at an alternate site after an emergency. The DRP scope may overlap that of an IT contingency plan; however, the DRP is narrower in scope and does not address minor disruptions that do not require relocation. Dependent on the organization's needs, several DRPs may be appended to the BCP.*

Disaster Recovery Planning (DRP). The actions you would take to recover from disaster. Includes the planning steps to advoid Risks, to mitigate them, or to shift the Risk to somene else through insurance or other means. DRP is applicable to all aspects of a Business but usually used in the context of data processing operation.

Disaster Recovery Plan (DRP). A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities.

Disaster Recovery Plan (DRP); The document that defines the resources, actions, tasks and data, which are required to manage the Business recovery process in the event of a Business interruption. The plan is designed to assist in restoring the Business process within the stated disaster recovery goals.

Disaster Recovery Plan (DRP); The disaster recovery plan is a document containing procedures for emergency response, extended backup operations, and recovery should a computer installation experience a partial or total loss of computing resources or physical facilities (or of access to such facilities). The primary objective of this plan, used in conjunction with the contingency plans, is to provide reasonable assurance that a computing installation can recover from disasters, continue to process critical applications in a degraded mode, and return to a normal mode of operation within a reasonable time. A key part of disaster recovery planning is to provide for processing at an alternative site during the time that the original facility is unavailable.

Definisi tersebut menuntut pengetahuan yang dalam atas tantangan yang dihadapi sistem dan kelemahan dari sistem. Sebagai contoh; Bila sistem

menggunakan database SQL, midleware PHP dengan konfigurasi default, maka tantangan yang kita hadapi adalah SQL injection (kasus penggantian nama partai pada situs internet KPU). Hal ini menyebabkan resiko menjadi sangat sulit diidentifikasi, diperlukan pengetahuan teknis yang amat dalam terhadap sistem.

Tantangan yang dihadapi sistem dewasa ini berkembang dengan sangat cepat, diperlukan biaya dan tenaga yang besar untuk mengetahui tantangan-tantangan terbaru sebuah sistem. Masalah yang lebih besar lagi adalah konsep tersebut tidak dengan mudah dimengerti oleh manajer atau pengambil keputusan yang memiliki latar belakang pengetahuan non-teknis IT.

Resiko dikategorikan dalam beberapa jenis, diurutkan berdasarkan frekwensi kejadian dan tingkat kerusakannya. Identifikasi bentuk-bentuk resiko, jenis resiko, frekwensi kejadian dan tingkat kerusakan masing-masing resiko dapat diperoleh dari lembaga-lembaga independen dan pemerintahan baik nasional dan internasional yang terkait. Identifikasi resiko dapat juga dilakukan berdasarkan asumsi-asumsi yang diambil dari pengalaman internal organisasi. Sumber-sumber ancaman yang umum dihadapi :

1. Bencana Alam
   Semua sumber ancaman yang berasal dari alam, seperti banjir, gempa bumi, tornado, tanah longsor, tsunami, petir dan lain-lain
2. Manusia
   Semua sumber ancaman yang berasal dari manusia, seperti DoS, Hacker, Virus, Kesalahan pemasukan data, Teroris dan lain-lain
3. Lingkungan
   Semua ancaman yang berasal dari lingkungan, seperti kegagalan kelistrikan dalam waktu lama, polusi, kebocoran cairan atau bahan kimia dan lain-lain

Manajemen Resiko - NIST SP 800-30

National Institute of Standards and Technology dalam SP 800-30 (*Risk Management Guide for Information Technology Systems*) menjelaskan bahwa rencana penanggulangan bencana (DRP) dibangun berdasarkan analisa-analisa yang dilakukan dalam manajemen resiko. DRP merupakan bagian dari langkah-langkah pengurangan resiko (*Risk mitigation*) dalam manajemen resiko. Manajemen resiko adalah proses dimana manajer IT menyeimbangkan operasional dan biaya-biaya ekonomis untuk melindungi tercapainya misi organisasi dengan melindungi sistem IT yang mendukung misi organisasi. Proses ini tidak khusus pada lingkungan IT, namun meliputi pengambilan keputusan dalam semua area dari aktifitas keseharian. Pemimpin organisasi harus memastikan bahwa organisasi mampu menyelesaikan misinya. Pemimpin organisasi juga harus menentukan kemampuan keamanan yang diperlukan, agar sistem IT dapat memberikan dukungan dalam menghadapi tantangan usaha pada tingkat yang diharapkan.

Sebagian besar organisasi memiliki dana yang sangat terbatas untuk keamanan IT, oleh karena itu pengeluaran bidang keamanan IT harus ditinjau ulang secara menyeluruh seperti pada pengambilan keputusan lainnya. Sebuah metode manajemen resiko yang terstruktur baik, bila dipergunakan secara efektif dapat membantu manajemen untuk mengidentifikasi pengamanan yang sesuai terhadap misi utama organisasi.

Manajemen resiko meliputi tiga proses yaitu :

- Penilaian resiko.
- Peringanan resiko.
- Evaluasi dan penilaian.

Integrasi Manajemen Resiko Ke Dalam *System Development Life Cycle*

Mengurangi dampak negatif terhadap organisasi adalah alasan yang paling mendasar pengambil keputusan menerapkan proses manajemen resiko untuk sistem IT mereka. Manajemen resiko yang efektif harus terintegrasi secara keseluruhan kedalam SDLC. Dalam bidang IT SDLC memiliki lima tahap yaitu:

1. Initiation.
2. Development atau Acquisition.
3. Implementation.
4. Operation atau Maintenance.
5. Disposal.

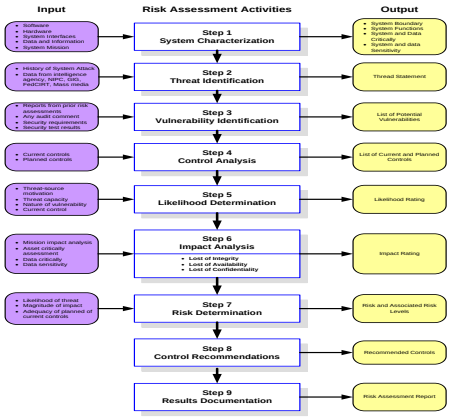
Dalam beberapa hal sistem IT menempati beberapa tahap dalam waktu yang sama. Namun metodologi manajemen resiko memiliki kesamaan dengan tahapan SDLC dalam melakukan penilaiaan. Tabel berikut menjelaskan karakteristik keduanya.

Penilaian Resiko (Risks Assessment)

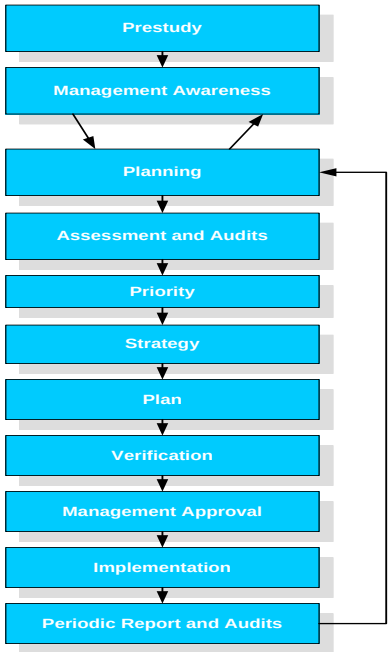
Penilaian resiko adalah proses pertama dalam metodologi manajemen resiko. Organisasi menggunakan penilaian resiko untuk menentukan tingkat ancaman dan resiko terhadap sistem IT mereka. Hasil dari proses ini akan membantu mengidentifikasi pengendalian resiko yang sesuai untuk mengurangi atau menghilangkan resiko-resiko tersebut pada proses pengurangan resiko. Proses penilaian resiko dapat dibagi menjadi sembilan tahap sebagai berikut:

1. ***System Characterization***; Identifikasi resiko dalam lingkungan IT memerlukan pengetahuan mengenai lingkungan sistem dalam melakukan proses. Berikut adalah aspek aspek yang harus dikumpulkan :
   - Hardware.
   - Software.
   - System interfaces.
   - Data dan informasi.
   - Personel yang mendukung dan menggunakan sistem IT.
   - Misi dari sistem.
   - Sistem dan data kritisnya.
2. ***Threat Identification***; Tujuan dari langkah ini adalah mengidentifikasi sumber-sumber tantangan yang potensial dan membuat daftar sumber ancaman yang potensial mengganggu sistem IT yang dievaluasi.
3. ***Vulnerability Identification***; analisa ancaman suatu sistem IT harus memasukkan sebuah analisa kelemahan yang dihubungkan dengan lingkungan sistem tersebut. Tujuan langkah ini adalah membuat daftar kelemahan yang mungkin dieksploitasi oleh sumber ancaman potensial.
4. ***Control Analysis***; Tujuan dari langkah ini adalah menganalisa kontrol yang pernah dibangun atau yang pernah direncanakan untuk dibangun, oleh organisasi untuk meminimalkan atau mengurangi kemungkinan sebuah ancaman menyerang kelemahan sistem.

5. ***Likelihood Determination***; Tujuan dari langkah ini adalah memperoleh gambaran tingkat kemungkinan sumber ancaman menyerang kelemahan sistem.
6. ***Impact Analysis***; Langkah berikutnya adalah menentukan tingkat resiko berdasarkan dampak yang ditimbulkan dari sebuah ancaman yang berhasil mengekspoitasi kelemahan sistem. Dampak tersebut dapat diukur atas hilangnya tujuan dari keamanan sistem informasi, yaitu
   - Lost Integrity.
   - Lost Availability.
   - Lost Confidetiality.



Gambar 1. Penilaian Resiko



Gambar 2. Diagram Aliran Kerja Mengelola DRP

Kesadaran Manajemen (*Management Awareness*)

Kesadaran manajemen adalah langkah awal dan langkah yang terpenting dalam menyusun DRP. Untuk mendapatkan sumberdaya yang diperlukan dan

waktu yang dibutuhkan dari setiap area dalam organisasi, manajemen senior harus memahami dan mendukung proses analisa dampak usaha dan analisa resiko. Beberapa tugas penting dalam proses pembangunan DRP memerlukan kesadaran manajemen.

- Identifikasi skenario kemungkinan bencana; Langkah pertama adalah mengidentifikasikan sepuluh besar bencana dan menganalisa dampaknya terhadap usaha. Analisa tersebut harus meliputi pengaruh pada komunikasi dengan supplier dan pelanggan, dampak terhadap operasional dan gangguan pada proses bisnis utama.
- Membangun kesadaran manajemen; Manajemen senior perlu untuk terlibat dalam proses perencanaan DRP, dan harus sadar terhadap resiko dan potensi dampaknya terhadap organisasi. Analisa pertama dari DRP harus memasukkan sebuah estimasi biaya dan waktu pembangunan stategi DRP. Ketika manajemen mengerti aspek finansial, fisikal dan bidang usaha yang terkait sebuah bencana, manajemen senior akan dapat membangun strategi dan memastikan strategi tersebut diterapkan dalam organisasi.
- Mendapatkan persetujuan dan pembiayaan dari manajemen; Ketika senior manajemen setuju atas proyek DRP dan dana serta sumberdaya yang diperlukan telah diberikan, langkah pertama adalah membentuk tim perencana atau sterring committe yang dipimpin oleh salah satu senior manajemen.

Proses Perencanaan DRP

Dalam melakukan perencanaan DRP, dilakukan identifikasi misi utama organisasi (mission-critical), penting dan tidak pentingnya proses, sistem dan layanan dalam jaringan untuk memastikan perlindungannya terhadap resiko bencana yang ada. Elemen kunci dari perencanaan DRP adalah :

1. Membentuk tim perencana; Tim yang dibentuk terdiri dari pengambil keputusan dari setiap unit usaha atau area operasional, bertanggung jawab atas semua aktivitas DRP, perencanaan dan melaporkan perkembangan yang terjadi setiap bulannya pada manajemen senior.
2. Melakukan penilaian resiko dan audit; Untuk membuat rencana DRP tim tersebut harus memahami proses bisnis, teknologi, jaringan dan layanan. Analisa resiko dan analisa dampak usaha setidaknya dilakukan terhadap 10 besar potensi bencana. Analisa dilakukan dengan mempertimbangkan skenario terburuk yaitu dari kehilangan atau kerusakan total fasilitas. Analisa juga dilakukan dengan mempertimbangkan aspek geografis, rancangan sistem IT saat ini dan layanan yang tersedia. Setiap analisa harus menggambarkan dampak finansial dari pernggantian perangkat, alokasi sumberdaya tambahan dan kontrak pemasangan layanan tambahan.
3. Menentukan prioritas terhadap jaringan dan aplikasi; prioritas pada masing-masing proses bisnis dan komponen IT yang digunakan dapat dikategorikan sebagai berikut:
    - Mission Critical; Kegagalan sistem IT akan menyebabkan gangguan yang sangat besar terhadap usaha, menyebabkan kerugian hukum dan finansial atau dapat mengancam keselamatan seseorang.
    - Important; Kegagalan sistem IT dapat menyebabkan gangguan yang bersifat moderat pada bisnis, menyebabkan kerugian kecil pada hukum dan finansial atau menyebabkan masalah akses ke sistem lain.

- Minor; Kegagalan sistem IT hanya menyebabkan sebuah gangguan kecil pada bisnis.

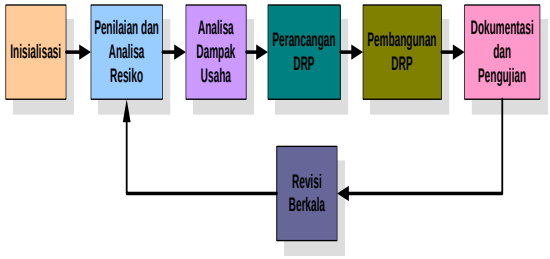
4. Merancang resiliency dan strategi recovery; dengan merancang resiliency dalam infrastruktur jaringan, layanan dan sumberdaya dapat disebar kedalam area geografis yang lebar, untuk membentuk fault tolerant pada site yang diproritaskan dan lokasi dimana layanan utama berada. Strategi recovery harus ditujukan pada manusia, fasilitas, layanan jaringan, perangkat komunikasi, aplikasi, client dan server, kontrak support dan maintenance, layanan tambahan vendor, lead-time layanan Telco dan lingkungan. Strategi recovery harus menyertakan estimasi down time layanan, rencana aksi dan prosedur pemulihan. Rencana tersebut juga menentukan ambang batas, seperti level minimum layanan agar usaha dapat tetap beroperasi, sistem yang harus berfungsi penuh dan lain-lain.
5. Menyiapkan sebuah inventory yang terbaru dan dokumentasi rencana; Sangatlah penting memiliki inventori yang selalu diperbaharui dan memiliki daftar lengkap semua lokasi, perangkat, vendor, pengguna layanan dan contact name. Inventory dan dokumentasi adalah bagian dari perencanaan dan pembangunan DRP. Dokumentasi DRP setidaknya mengandung aspek-aspek sebagai berikut :
   - Inventory lengkap, termasuk prioritas sumberdaya
   - Tinjauan ulang penilaian struktur proses, audit dan laporan-laporan.
   - Analisa resiko dan gap berdasarkan hasil penilaian resiko dan audit.
   - Rencana yang diterapkan untuk menghilangkan resiko dan gap.
   - Prosedur aksi.
   - Materi pelatihan.

METODE PENYUSUNAN DAN PERANCANGAN DRP

Tahap/Proses Penyusunan DRP (*Life Cycle*)

Setiap referensi yang ada memiliki perbedaan-perbedaan dan kesamaan-kesamaan dalam menentukan tahapan penyusunan DRP. Merujuk dari kepustakaan yang ada, secara umum proses penyusunan DRP mengandung aspek-aspek dasar sebagai berikut:

1. Inisialisasi.
2. Penilaian dan Analisa Resiko.
3. Analisa Dampak Usaha.
4. Perancangan DRP.
5. Pembangunan DRP.
6. Dokumentasi dan Pengujian.
7. Revisi secara berkala.



Gambar 3. Tahap (Life Cycle) Pembangunan DRP

Inisialisasi

Inisialisasi adalah tahap awal pembangunan DRP dimana semua aspek dan regulasi yang mendasari implementasi DRP dibangun, Tahap ini diperlukan untuk memberi landasan yang kuat pada DRP yang akan dirancang.

Tujuan tahap inisialisasi adalah :

- Membentuk landasan awal DRP.
- Membangun kesadaran perlunya DRP dalam perusahaan.
- Mendefinisikan DRP perusahaan.
- Menentukan ruang lingkup DRP.
- Membentuk tim-tim yang diperlukan dalam kondisi darurat.

Tahap ini diperlukan dengan mempertimbangkan hal-hal sebagai berikut:

1. DRP tidak dapat dibangun tanpa dukungan dan komitmen yang tegas dari management, karena strategi DRP merupakan strategi Top-Down dari pemimpin perusahan.
2. Pembangunan DRP memerlukan tim yang memiliki kompetensi yang sesuai dan akses ke dalam perusahaan yang baik dalam melakukan tugas-tugasnya.
3. DRP memerlukan pengelolaan tim khusus.

Pada tahap ini dibangun keperdulian dan kesadaran dalam internal organisasi tentang fungsi dan perlunya pembangunan DRP. Manajemen tingkat atas harus memberikan dukungan yang penuh pada pembangunan DRP dengan memberikan sebuah regulasi tentang DRP. Pembentukan tim dalam membangun DRP dilakukan dalam tahap ini. Tim DRP tersebut harus terdiri dari personel-personel di bidang IT dan personel-personel di bidang non IT. Personel-personel tersebut harus memiliki pengetahuan yang cukup mengenai sistem IT dan proses bisnis organisasi serta memiliki wewenang yang cukup untuk mencari data, melakukan asumsi-asumsi dan analisa yang terkait dengan pembanguan DRP.

Penilaian Dan Analisa Resiko

Tahap penilaian resiko adalah proses identifikasi dan penilaian resiko serta analisa dampak kerugian atas kehilangan asset yang ditimbulkan masing-masing resiko terhadap perusahaan. Tujuan penilaian resiko dan analisa resiko adalah :

1. Mengidentifikasi resiko-resiko yang mengancam.
2. Melihat dampak resiko terhadap asset IT/aplikasi dari sudut pandang kehilangan asset.
3. Memetakan ancaman resiko dalam beberapa kategori.
4. Memperkirakan besarnya investasi DRP.
5. Menghitung efektifitas pembangunan DRP.
6. Mengetahui asset IT/aplikasi kritis.

Analisa Dampak Usaha (*Business Impact Analysis* – BIA)

Tahap analisa dampak usaha (*Business Impact Analysis – BIA*) adalah sebuah proses analisa dampak kerugian masing-masing resiko atas kehilangan produktifitas perusahaan. Secara umum analisa ini dilakukan dengan dua pendekatan yaitu :

1. Kualitatif; Analisa kualitatif dilakukan untuk memperoleh penilaian dari sudut padang pengelola sistem dan pemakai (user) mengenai tingkat kritisisasi setiap asset IT yang ada.
2. Kuantitatif; Analisa kuantitatif dilakukan untuk memperoleh penilaian dari sudut padang produksivitas sistem yang ada dan untuk mempertajam hasil-hasil kuantitatif. Berbeda dengan pendekatan kualitatif, pendekatan kuantitatif menentukan RTO dan RPO didasarkan perhitungan matematis dari produktivitas masing-masing sistem.

Perancangan DRP

Tahap pencangan DRP adalah tahap dimana proses perancangan DRC dan aspek-aspek DRP lainnya dilakukan. Tahap ini merupakan tahap yang lebih menitikberatkan pada faktor-faktor teknis DRP. Tujuan dari perancangan DRP adalah:

1. Menentukan teknologi, kebutuhan minimum DRC.
2. Menentukan lokasi DRC yang digunakan.
3. Merancang infrastruktur DRC dan aspek-aspek teknis/non-teknis yang terkait dengan DRP.

Perancangan dibutuhkan mengingat aspek-aspek sebagai berikut :

- Terdapat banyak teknologi backup & recovery yang ada di pasar, perusahaan memilih teknologi yang tepat berdasarkan RTO dan RPO yang diharapkan.
- Terdapat banyak lokasi yang dapat dipilih sebagai lokasi DRP, perusahaan menentukan lokasi yang tepat berdasarkan kebutuhan perusahaan.

Perancangan dilakukan oleh :

- Tim Pembangunan DRP.
- Vendor/Konsultan atau Pakar IT khususnya bidang Backup & Recovery.

Tahap perancangan membutuhkan data-data sebagai berikut:

- Daftar/petunjuk umum spesifikasi teknologi backup dan recovery.
- Daftar RTO dan RPO asset IT/aplikasi kritis.
- Daftar kandidat lokasi DRC.
- Daftar detail spesifikasi teknologi yang dipilih.

Berikut adalah langkah-langkah yang dilakukan dalam perancangan DRP:

- Mengumpulkan informasi tentang teknologi backup & recovery dan kemampuan setiap teknologi yang ada.
- Menentukan teknologi yang tepat dengan kebutuhan RTO dan RPO setiap asset IT/aplikasi kritis

KESIMPULAN

1. DRP dibangun dengan menggunakan metodologi ilmiah, langkah-langkah kerja terstruktur yang merujuk pada resiko yang dapat mengancam, proses bisnis dan aplikasi penting perusahaan serta dampak setiap resiko terhadap perusahaan.
2. Karakteristik kekuatan rancangan terletak pada analisa resiko, functional preparedness dan maintenance procedure.
3. Kelemahan rancangan terletak pada aspek insurance yang tidak dapat dipenuhi secara menyeluruh serta aspek testing dan recovery procedure. Sebagian besar dari tidak

terpenuhinya persyaratan tersebut karena terdapatnya aspek-aspek yang terkait dengan vendor atau aspek-aspek yang tidak dapat dilakukan sebelum rancangan DRP selesai dibangun.

SARAN

1. Pembangunan DRP sebaiknya didahului oleh penerapan manajemen resiko di perusahaan, pengalaman selama di lapangan menunjukkan bahwa analisa resiko sulit dilakukan tanpa data-data manajemen resiko perusahaan.
2. Anggota Tim pembangunan DRP sebaiknya dibentuk dari kalangan internal perusahaan pada tingkat manajer bidang, pengalaman di lapangan menunjukkan bahwa data-data yang diperlukan untuk membangun DRP banyak yang bersifat strategis dan rahasia perusahaan dan memerlukan pengetahuan perusahaan serta analisa yang cukup mendalam. Hanya pegawai pada level-level tertentu yang dapat mengakses data tersebut dan melakukan pengambilan keputusan dalam pembangunan DRP.Hal tersebut juga untuk mengurangi kebocoran informasi penting perusahaan.

DAFTAR PUSTAKA

Allberts, Christopher, Dorofee, Audrey. (2004), Managing Information Security Risks - The Octave Approch, Pearson Education Inc.

Bahan, Chad. (2003), The Disaster Recovery Plan.

Business Continuity Glossary of Disaster Recovery Journal homepage. (24th December, 2003), Disaster Recovery Journal, "Business Continuity Glossary," URL: http://www.drj.com/glossary/drjglossary.html

Cisco.(2003). Cisco - Disaster Recovery: Best Practices White Paper, Cisco Systems Ltd,

Cougias, Dorian J. (2005), The Backup Book - 3rd Edition, Disaster Recovey From Destop To Data Center, The Network Frontier,

Farley, Marc (2005), Building Storage Network - Second Edition, Osborne/McGraw-Hill.

Indrajid, Richardus Eko. (2004) , Kajian Strategi Cost Benefit Teknologi Informasi.

International Standard Organization.(2000), ISO 17799 – 2000 Information Security Management, International Standard Organization.

Maiwald, Eric, Sieglein, William. (2002), Security Planning & Disaster Recovery, McGraw-Hill/Osborne.

Martin, Bryan C. (2002), Disaster Recovery Plan Strategies and Processes, SANS Institute.

Krause, Micki, F, Harold. (1993), Handbook of Information Security Management, CRC Press LLC.

Microsoft Corp, NSI Software. (2003), Six Tips Small and Midsize Businesses Can Use to Protect Their Critical Data, White Paper, Microsoft Corp, NSI Software.

Mott, Graham. (2002), Accounting For Managers, Elex Media Komputindo.

National Institute of Standards and Technology. (2002), Contingency Planning Guide for Information Technology Systems, National Institute of Standards and Technology.

National Institute of Standards and Technology. (2002), Risk Management Guide for Information Technology System.

Pepple, Ken, Hornby, David. (2005), Consolidation In The Data Center, Sun Microsystems.