# PERANCANGAN PROSEDUR *DISASTER RECOVERY PLAN* (DRP) ATAS ASET TEKNOLOGI INFORMASI PADA PT. XXX

# DESIGNING PROCEDURES DISASTER RECOVERY PLAN(DRP) TO INFORMATION TECHNOLOGY ASSETS IN PT XXX

**Berka Irfansyah[1], RD Rohmat Saedudin ST., MT.,[2], Dr. Basuki rahmat CISA CIRM CRISC[3]**

**[123]Program Studi Sistem Informasi, Fakultas Rekayasa Industri, Telkom University**

berkairfansyah@gmail.com 1, roja2128@gmail.com 2, azkaku@gmail.com 3

**Abstrak**

Didirikan sejak tahun 1965, PT XXX kemudian bertransformasi menjadi sebuah Badan Usaha Milik Negara (BUMN) pada tahun 1991. Sejak saat itu, PT XXX telah menjadi sebuah entitas bisnis profesional dengan nama PT XXX Industri. Dari hasil wawancara yang dilakukan diketahui PT XXX Industri belum menerapkan *Disaster Recovery Plan* dalam proses bisnisnya, akan tetapi pada *master plan* PT XXX sudah tercantum perencanaan dokumen *Disaster Recovery Plan (DRP).* Fokus perancangan *Disaster Recovery Plan* ini dilakukan untuk menentukan prosedur dalam menghadapi bencana yang mungkin terjadi, meliputi prosedur dalam Identifikasi dan Deklarasi Bencana, prosedur *Recovery*, prosedur dalam melakukan *Resumption*, dan pelaksanaan *Testing Disaster Recovery Plan*, serta penetapan tim untuk *disaster recovery team* yang bertanggung jawab dalam menghadapi bencana tersebut. Penelitian ini dilakukan melalui pengumpulan data untuk memeriksa dokumen yang terkait dengan penelitian. Serta melakukan wawancara kepada pihak yang terkait dengan penelitian.

Hasil akhir dari penelitian berupa rekomendasi perancangan dokumen, sehingga diharapkan perancangan *Disaster Recovery Plan* ini dapat di terapkan pada PT. XXX Industri dalam kelangsungan proses bisnis ke depannya.

Kata Kunci : *Disaster Recovery plan*, Prosedur, Struktur organisasi

**Abstract**

PT. XYZ is an electronics and infrastructure industry company. PT. XYZ has a finished good warehouse that is used as storage for solar modul product. There is a problem in the warehouse that the warehouse cannot accommodate the goods in it. This is caused by storage system in the warehouse using floor stake with only one level tall and the storage media is the pallets with size (1.7m x 1.1m) with maximum limit is 10 stacks for each pallet. Furthermore, the initial height is used only 1.19m tall while the overhead height is 6m tall. It responsibles for a very low utility of the warehouse that only 18% in volumetric.

The objective of the research is to increase the capacity and utility of the warehouse. The problems are solved using dynamic programming by combining the selective rack and non-selective rack (drive-in) to increase the rack's lane.

The result of the research is the capacity of PT.XYZ's warehouse increased, in initial capacity warehouse can hold 156 pallets position increased to 492 pallets position.

Keywords : Optimization, warehouse capacity, dynamic programming algorithm, racking system, rack combination, lane depth

## I. Pendahuluan

Teknologi Informasi (TI) adalah seperangkat alat yang membantu pekerjaan dengan informasi serta melakukan tugas-tugas yang berhubungan dengan pemrosesan informasi (Haag & Keen, 1996). TI merupakan suatu kebutuhan yang menjadi pendorong bagi kemajuan bisnis pada pemerintahan dan memberikan manfaat yang baik bagi keberlangsungan kinerja perusahaan. BCM (*Business Continuity Management*) adalah pengembangan strategi, rencana, dan tindakan yang memberikan perlindungan atau mode alternatif operasi untuk kegiatan atau proses bisnis yang, jika mereka terganggu, mungkin sebaliknya membawa kerugian serius merusak atau berpotensi untuk perusahaan (Protiviti, 2013).

BCM pada umumnya terdiri atas 3 elemen penting yaitu:

a) Krisis manajemen dan komunikasi ialah proses yang dirancang untuk memungkinkan tanggapan yang efektif terhadap suatu peristiwa.

b) Perencanaan dimulainya kembali proses bisnis ialah proses yang melibatkan pemulihan dari fungsi bisnis dan proses yang terlibat dalam hal yang berhubungan dengan pelanggan.

c) *Disaster recovery* ialah dokumen yang ditujukan untuk pemulihan aset-aset penting dari TI, termasuk sistem, aplikasi, database, storage, ataupun jaringan.

Aspek-aspek yang menjadikan perbedaan dalam BCM digunakan oleh industri, meski memiliki perbedaan akan tetapi ada sejumlah istilah yang sama dengan BCM namun memiliki makna yang berbeda sebagai contoh;

- *Disaster Recovery* adalah istilah untuk pemulihan dan dimulainya kembali aset teknologi penting dalam bencana. Pemulihan bencana dapat mencakup tugas-tugas seperti melanjutkan sistem individu atau memulihkan semua aspek penting dari lingkungan TI. *Disaster Recovery* merupakan bagian secara keseluruhan dari program BCM.
- *Resumption Planning* adalah disiapkan untuk pemulihan fungsi bisnis secara kritis yang telah berhenti dan terpisah dari pemulihan TI.
- *Contingency Planning* mengacu pada solusi taktis menangani sumber daya inti atau proses. Sebagai lawan BCM, *contingency planning* adalah tindakan terisolasi dan tidak menyerupai program atau tindakan terkait.
- *Recovery Planning* merupakan hal yang paling terkait dengan BCM. kedua istilah ini dapat digunakan bergantian

*Emergency Response* termasuk tindakan yang harus segera diambil untuk melestarikan kehidupan dan menjaga properti dan aset. *Emergency response* merupakan bagian dari program manajemen krisis yang lebih luas.

Pada saat ini PT XXX belum memiliki dokumen *Disaster Recovery Plan (DRP)* pada proses bisnisnya, akan tetapi pada *master plan* PT XXX sudah tercantum dokumen *Disaster Recovery Plan (DRP).* Tujuan utama dari *Disaster Recovery Plan (DRP)* 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 tertentu, dengan menjalankan prosedur pemulihan cepat, untuk meminimalisir kerugian organisasi (Usep, 2005).

## II. Dasar Teori dan Metodologi Penelitan

### A. Bencana

Bencana (*disaster*) didefinisikan sebagai kejadian luar biasa, tiba-tiba dan tidak direncanakan yang dapat menyebabkan kerusakan dan kehilangan besar sebagaimana yang didefinisikan atau diidentifikasi melalui penilaian risiko (risk assessment) dan analisis dampak bisnis *Business Impact Analysis* (BIA) (Yunita, Kridanto, 2008).

Berdasarkan penyebabnya, bencana dapat dikelompokkan sebagai berikut:

- *Natural*: bencana disebabkan oleh kejadian alam seperti angin topan, banjir atau kebakaran.

- *Human*: bencana/ kerusakan yang disebabkan oleh manusia, misalnya kesalahan operator, sabotase, pembajakan atau kode-kode yang berbahaya (*malicious*), dan serangan teroris.
- *Environment*: disebabkan oleh faktor lingkungan, misalnya kesalahan peralatan, kesalahan sistem perangkat lunak, kerusakan jaringan telekomunikasi dan sumber daya listrik.

B. ***Disaster Recovery Plan (DRP)***

***Disaster recovery plan*** adalah rencana yang terfokus yang telah dirancang untuk mengembalikan proses pengoperasian sistem ataupun aplikasi setelah keadaan darurat. Sebuah *Disaster Recovery Plan (DRP)* dengan gangguan yang cukup besar membutuhkan sebuah tempat relokasi (Charlotte, Matthew, Igor, John, 2002). Dokumen *Disaster Recovery Plan (DRP)* yang telah diterbitkan biasanya berfokus pada infrastruktur TI yang dirancang untuk melindungi kelangsungan beroperasinya database, aplikasi, jaringan, maupun infrastruktur pendukung (power, cooling, space). Pada sisi lain *Disaster Recovery Plan (DRP)* cukup bergantung pada *Business Continuity Plan (BCP)* yang menggambarkan metode dan prosedur yang telah digunakan untuk menjalankan bisnis untuk menjamin bahwa fungsi penting perusahaan harus berjalan sesuai rencana.

C. **Lingkup prosedur**

Merupakan prosedur-prosedur yang dapat mengatur semua aktivitas sebagai respon dalam menghadapi bencana hingga pemulihan kembali seperti kondisi normal (Buti pama, 2015). Terdapat beberapa fase yang dapat dijalankan berikut dibawah ini penjelasannya.

- Acivation phase
- Recovery phase
- Resumption phase
- Testing

D. ***Roles and Responsibilities***

Menurut (Marianne, Amy, Lucinda, Joan, Tim, Ray, 2002) setelah memilih dan menerapkan strategi backup dan pemulihan sistem, organisasi harus menunjuk tim yang tepat untuk menerapkan strategi. Setiap tim harus dilatih dan siap untuk merespon jika terjadi situasi yang membutuhkan aktivasi *recovery*.

## III. Pembahasan

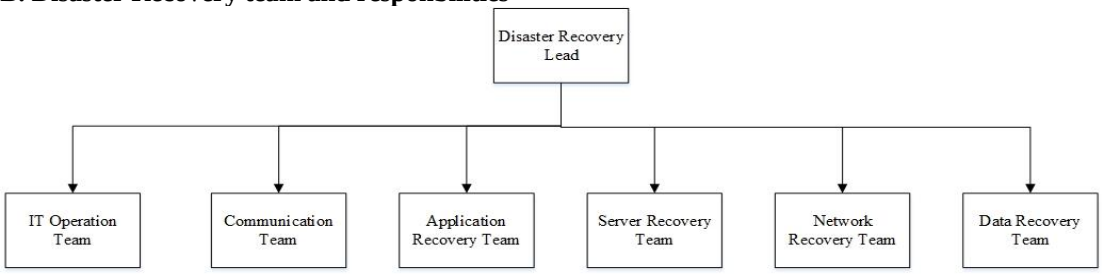
A. **Disaster**

Sebuah bencana (disaster) didefinisikan sebagai apapun peristiwa tak terencana atau tak terduga, yang mengganggu fungsi bisnis penting untuk periode waktu yang tidak tertentu. Bencana dapat disebabkan oleh beberapa faktor yaitu faktor manusia maupun faktor alam. Berikut dibawah ini tipe insiden maupun bencana yang dapat diaktifkannya DRP.

Tabel V.1 Tipe insiden

| Tipe insiden | Deskripsi | Risk response | Keterangan |
|---|---|---|---|
| Minor | Berpengaruh terhadap proses, tujuan, sasaran unit kerja relatif dan terdapat konsekuensi waktu yang masih dapat ditolerir. | Accept | Manajemen insiden |
| Major | Berpengaruh terhadap proses unit kerja lain dan terdapat konsekuensi waktu dan biaya / tambahan anggaran. Serta berdampak terganggunya pada beberapa layanan di perusahaan. | Mitigate | Perlu dijalakannya *Disaster Recovery Plan* (hanya beberapa prosedur saja) |
| Worst case | Berpengaruh signifikan terhadap organisasi, sehingga kegiatan proses bisnis organisasi berhenti secara total. | Mitigate | Perlu dijalankannya *Disaster Recovery Plan* secara keseluruhan |

**B. Disaster Recovery team and responbilities**




**1. Disaster Recovery Lead**

*Disaster Recovery Lead* bertanggung jawab untuk membuat semua keputusan yang terkait dengan upaya pemulihan bencana. Seseorang yang berperan sebagai *disaster recovery lead* ini bertugas memandu proses pemulihan bencana dan semua individu lain yang terlibat dalam proses pemulihan bencana akan melaporkannya kepada orang tersebut jika terjadi bencana

- Membuat keputusan bahwa telah terjadi bencana dan memicu *Disaster Recovery Plan (DRP*) serta segala prosesnya yang terkait.
- Menjadi satu satunya kontak yang berguna untuk mengawasi semua tim Disaster Recovery
- Mengorganisir serta memimpin pertemuan rutin tim *Disaster Recovery* selama bencana berlangsung
- Mengatur, mengawasi dan mengelola semua tes *Disaster Recovery*.

**2. IT Operation Team**

*IT Operation Team* merupakan pihak yang mengawasi seluruh sistem TI yang berjalan pada perusahaan. Tim ini tidak hanya bertugas ketika adanya insiden maupun bencana yang terjadi pada perusahaan, akan tetapi pada saat kondisi normal pun tim ini akan tetap bertugas sebagai pengawas seluruh sistem TI yang berjalan. Tim ini merupakan pihak pertama yang mengetahui adanya gangguan pada sistem TI perusahaan.

- Menentukan besaran dan kelas insiden yang terjadi
- Melaporkan kepada *disaster recovery lead* bahwa telah terjadi bencana.
- Melakukan perbaikan jika gangguan hanya bersifat insiden.

**3. Communication Team**

Tim ini akan bertanggung jawab atas semua komunikasi saat terjadi bencana. Secara teknis mereka akan berkomunikasi dengan karyawan, klien, vendor, bank, serta media jika itu dibutuhkan.

- Sebagai juru bicara dalam melakukan komunikasi di saat darurat.
- Mengomunikasikan kepada karyawan PT XXX bahwa telah terjadi bencana.
- Mengomunikasikan terjadinya bencana dan dampak dari bencana tersebut kepada klien, mitra kerja,vendor.

**4. Recovery team**

Terdapat beberapa recovery team dalam struktur organisasi *disaster recovery plan* ini diantaranya:

- Network Recovery team (Jika beberapa layanan infrastruktur jaringan terkena dampak, tim akan memprioritaskan pemulihan layanan dengan cara dan urutan yang memiliki dampak bisnis paling tinggi.)
- Application Recovery team (Jika ada aplikasi yang terkena dampak dari bencana maka tim akan memprioritaskan pemulihan aplikasi dengan cara mengurutkan dari yang memiliki dampak bisnis paling tinggi.)
- Server Recovery Team (Jika beberapa server terkena dampak dari bencana maka prioritas utama perbaikan adalah server yang memiliki dampak pada proses bisnis yang besar.)
- Data Recovery Team ( Memastikan bahwa fasilitas *backup* dipelihara dalam rangka kerja, dan melakukan *backup* harian pada DRC)

C. Prosedur Pada penelitian prosedur yang direkomendasikan dibagi menjadi 5 bagian diantaranya:
1. Identifikasi dan deklarasi bencana

Untuk mengetahui akan terjadinya bencana dapat diatasi dengan cara berikut:

- Observasi yang dilakukan oleh *IT operation team*
- Sistem alarm dan monitor jaringan
- Sistem alarm lingkungan jika terjadi bencana yang disebabkan faktor alam
- Keamanan pada fasilitas utama
- Staff keamanan pada lingkungan organisasi

*Disaster recovery lead* akan menginstruksikan *communication team* untuk mulai menghubungi pihak berwenang dan semua karyawan yang tidak terkena dampak bahwa sebuah bencana telah terjadi. Serta menghubungi *recovery team* maupun *vendor* untuk melakukan pemulihan terhadap aset yang terkena dampak bencana.

2. Communication plan
*Communication plan* merupakan tahapan yang dijalankan ketika perusahaan mengalami situasi darurat. Tahap ini dilakukan setelah gangguan yang terjadi pada perusahaan sudah di deklarasikan sebagai bencana. Pada tahap ini dijelaskan bagaimana *communication team* melakukan alur komunikasi dengan *vendor* dan *user*.

3. Recovery secara parsial

*Recovery* secara parsial merupakan proses pemulihan yang berfokus pada aset terkena dampak dari bencana. Selama proses pemulihan dilakukan, fasilitas alternatif (DRC) akan diubah status fungsional dari pasif menjadi aktif. Selama aktivasi sistem fasilitas alternatif (DRC), tim jaringan, server, data, dan aplikasi perlu memastikan bahwa tanggung jawab mereka dijalankan, seperti yang dijelaskan di bagian "*Disaster Recovery Team and Responsibilities*" dari dokumen ini dilakukan dengan cepat dan efisien agar tidak adanya kerusakan yang lebih lanjut. Pada perancangan ini diberikan dua rekomendasi prosedur recovery yaitu:

- Prosedur *recovery* sistem informasi (aplikasi, data, dan server)
- Prosedur *recovery* infrastruktur jaringan

Prosedur recovery catastrophic
Prosedur ini dijalankan ketika bencana yang terjadi menyerang fisik dari aset di fasilitas utama perusahaan. Pada kategori bencana ini kerusakan yang berdampak pada aset TI perusahaan menyebabkan fasilitas utama (DC) tidak dapat menunjang proses bisnis perusahaan sehingga, berhentinya layanan perusahaan secara keseluruhan.

4. Resumption
Resumption merupakan pengembalian proses bisnis yang sebelumnya telah berhenti dikarenakan bencana yang menimpa. Proses ini merupakan pengembalian fungsi DC dari DRC menjadi fasilitas utama kembali. Fokus pada proses ini adalah pemulihan pada fasilitas utama atau DC, ketika bencana telah di deklarasikan maka proses ini akan dijalankan untuk mengembalikan fungsi aset pada DC menjadi fungsional kembali.
Ada beberapa rekomendasi prosedur yang diberikan diantaranya:

- *Resumption* sistem informasi
- *Resumption* infrastruktur jaringan
- *Resumption* untuk level *catastrophic*

5. Testing
Pada *Disaster Recovery Plan (DRP)* rencana pengujian ini sangatlah penting. *Disaster Recovery Plan (DRP)* memiliki banyak elemen yang berupa teori sehingga benar-benar diuji dan di validasi. *Testing Disaster Recovery Plan (DRP)* harus sesuai dengan urutannya, mengikuti standar yang telah ditetapkan, dan harus disesuaikan dengan keadaan sebenarnya. *Testing Disaster Recovery Plan (DRP)* dapat dilakukan tidak hanya pada saat bencana terjadi, tetapi *testing* dapat dilakukan sebelum bencana terjadi. Dengan tujuan bahwa semua karyawan perusahaan sudah siap khususnya pada unit kerja sistem informasi perusahaan jika ada kejadian bencana.
Pada pelaksanaan testing ini diberikan dua rekomendasi testing yang dapat dijalankan yaitu:

- Simulation test
- Parallel Test

## IV. Kesimpulan

Berdasarkan keseluruhan proses yang telah dilakukan pada penelitian ini menghasilkan rancangan dokumen Disaster Recovery Plan untuk prosedur dan organisasi yang dapat dijadikan rekomendasi untuk menjaga berlangsungnya proses bisnis yang dijalankan pada PT XXX, dapat disimpulkan bahwa:

a. Hasil perancangan DRP dihasilkan prosedur untuk:

1. Identifikasi dan deklarasi bencana
2. *Communication plan*
3. *Recovery* dan aktivasi fasilitas *backup*
4. Untuk *recovery* dihasilkan tiga prosedur *recovery* diantaranya:

- Prosedur *recovery* sistem informasi
- Prosedur *recovery* infrastruktur jaringan
- Prosedur *recovery catastrophic*

5. *Resumption*
   - *Resumption* sistem informasi
   - *Resumption* infrastruktur jaringan
   - *Resumption catastrophic*
6. *Testing disaster recovery plan*

   Pada pelaksanaan *testing* diberikan rekomendasi jenis *testing* yang dapat dijalankan dan beserta dengan prosedur
   - Prosedur *simulation test*
   - Prosedur *parallel test*

b. Struktur Organisasi pada penelitian ini adalah tim yang bertanggung jawab dalam menghadapi bencana pada PT XXX pada penelitian ini ditetapkan pihak yang bertanggung jawab dalam menghadapi bencana yaitu:

1. *Disaster Recovery lead*
2. *IT Operation Team*
3. *Communication Team*
4. *Recovery team*
   - *Application Recovery Team*
   - *Server Recovery Team*
   - *Network Recovery Team*
5. *Vendor*

Marianne. S, P. B. (2010). *Contingency Planning Guide for Federal Information Systems.* NIST.

McAndrew, C. (2013). *Business Continuity Management Framework.* [5] Amatillah, Z., Yanuar, A., & Santosa, B. (2016). Design of Drive-In Racking System for Lubricant Warehouse Using Heuristic Approach with Class Based Storage. *JRSI*.

Pama, C. B. (2014). *PERANCANGAN STRATEGI & PROSEDUR CONTINUITY PLAN PADA LAYANAN AKADEMIK, KEUANGAN DAN KEPEGAWAIAN (STUDI KASUS: UNIVERSITAS TELKOM).*

Prazeres. A, L. E. (2013). Disaster Recovery – a project planning case study in Portugal. Procedia Technology.

Snedaker, S. (2007). *Business Continuity & Disaster Recovery for IT Professionals.*

Solehudin, U. (2005). Business Continuity and Disaster Recovery Plan. UNIVERSITAS INDONESIA, Magister Teknologi Informasi.

Yunita Caroline Manurung, K. S. (2008). *Pengembangan Rencana Penanggulangan Bencana (Disaster Recovery Planning) untuk Data Center ITB*