PENERAPAN BUSINESS *CONTINUITY PLAN / DISASTER RECOVERY PLAN* (BCP/DRP) PADA BUMN DALAM RANGKA *SUSTAINABILITY*: STUDI KASUS PADA PT.X WILAYAH JAKARTA RAYA

Yulhendri
Fakultas Ilmu Komputer Universitas Esa Unggul
Jalan Arjuna Utara No.9 Kebun Jeruk, Jakarta 11510
yulhendri@esaunggul.ac.id

Abstrak

Lingkungan Teknologi Informasi (TI) yang dimiliki PT. X Wilayah Jakarta dan Tangerang saat ini bersifat heterogen, terpisah-pisah dan terdiri dari gabungan beberapa sistem yang berdiri sendiri dimana disaat awalnya sistem-sistem tersebut dirancang untuk memenuhi kebutuhan spesifik dari tiap-tiap unit/departemen. Lingkungan ini dapat menimbulkan beberapa permasalahan yang semakin rumit seiring dengan perkembangan kebutuhan masing-masing departemen dan meningkatkan biaya pemeliharaan dan operasi bagi masing-masing sistem. Selain itu infrastruktur yang ada tidak memungkinkan untuk mengakomodasi kebutuhan akan manajemen, keamanan, skalabilitas dan *redundancy* yang fleksibel yang dapat memberikan jaminan kelangsungan proses bisnis-proses bisnis di PT. X Wilayah Jakarta Raya dan Tangerang. Tujuan dilakukannya penelitian ini adalah bagaimana penerapan BCP/DRP yang optimal. Metode penelitian yang digunakan adalah studi literatur, dimana studi literatur dilakukan terhadap berbagai macam jenis buku, makalah, dan halaman situs internet.Hasil yang berhasil didapatkan adalah tahapan-tahapan metode pembangunan *Disaster Recovery Planning* yang meliputi *Risk Assessment, Priority Assessment, Recovery Strategy Selection*, dan *Plan Documenting*. Proses pengembangan *Disaster Recovery Planning* pada intinya meliputi dua poin yaitu perencanaan keberlanjutan pemrosesan data dan pemeliharaan rencana pemulihan data. Dengan dilakukannya penelitian ini diharapkan konsep dasar mengenai penerapan DRP dapat dipahami dengan baik dan selanjutnya dapat dikembangkan dengan penyesuaian di lapangan.

Kata kunci: Proses pengembangan, *business continuity plan, disaster recovery planning*

Pendahuluan

Lingkungan Teknologi Informasi (TI) yang dimiliki PT. X Wilayah Jakarta dan Tangerang saat ini bersifat heterogen, terpisah-pisah dan terdiri dari gabungan beberapa sistem yang berdiri sendiri dimana disaat awalnya sistem-sistem tersebut dirancang untuk memenuhi kebutuhan spesifik dari tiap-tiap unit/departemen.

Lingkungan ini dapat menimbulkan beberapa permasalahan yang semakin rumit seiring dengan perkembangan kebutuhan masing-masing departemen dan meningkatkan biaya pemeliharaan dan operasi bagi masing-masing sistem. Selain itu infrastruktur yang ada tidak memungkinkan untuk mengakomodasi kebutuhan akan manajemen, keamanan, skalabilitas dan *redundancy* yang fleksibel *yang dapat memberikan jaminan kelangsungan proses bisnis-proses bisnis di PT. X Wilayah Jakarta Raya dan Tangerang*.

Hal ini akan berdampak pada penurunan tingkat layanan yang dapat diberikan oleh masing-masing sistem dan mengakibatkan operasional perusahaan terganggu karena tidak adanya ketersediaan sistem-sistem tersebut. Untuk menjawab tantangan ini, PT. X Wilayah Jakarta dan Tangerang memutuskan untuk melaksanakan sebuah proyek studi perencanaan yang menyediakan kerangka kerja untuk membuat keputusan investasi TI jangka panjang di bidang *Data Center* dan *Backup* & *Recovery* dengan mempertimbangkan kepentingan perusahaan secara keseluruhan. Inisiatif ini juga harus dapat memenuhi kebutuhan unit-unit pelayanan PT. X Wilayah Jakarta dan Tangerang.

Pelaksanaan operasional perusahaan tidak dapat terhindar dari adanya gangguan/

kerusakan yang disebabkan oleh alam maupun manusia misalnya terjadi gempa bumi, bom, kebakaran, banjir, kesalahan teknis, kelalaian manusia, demo buruh dan huru-hara. Kerusakan yang terjadi tidak hanya berdampak pada kemampuan teknologi yang digunakan perusahaan, tetapi juga berdampak pada kegiatan operasional bisnis perusahaan ter-utama pelayanan kepada pelanggan. Bila tidak ditangani secara serius, selain perusahaan akan menghadapi risiko operasional, juga akan mempengaruhi risiko reputasi dan berdampak pada menurunnya tingkat kepercayaan pe-langgan kepada perusahaan.

Untuk meminimalisasi risiko tersebut, perusahaan diharapkan memiliki *Business Continuity Plan* (BCP) atau Rencana Kelangsungan Bisnis, yaitu suatu kebijakan dan prosedur yang memuat rangkaian kegiatan yang terencana dan terkoordinir mengenai langkah-langkah pencegahan dan pemulihan system pada saat terjadi gangguan/bencana yang disebabkan oleh faktor internal atau eksternal. Tujuan utama BCP ini adalah agar kegiatan operasional perusahaan dan pelayanan kepada pelanggan tetap dapat berjalan. Rencana pemulihan tersebut melibatkan seluruh sumber daya, Teknologi Informatika (TI) termasuk sumber daya manusia yang mendukung fungsi bisnis dan kegiatan operasional yang kritikal bagi perusahaan.

Studi Perencanaan *Data Center* dan *Backup* & *Recovery* merupakan kelanjutan dari perencanaan Arsitektur Informasi Perusahaan (AIP) PT. X Wilayah Jakarta dan Tangerang tahap sebelumnya yang diarahkan untuk dapat memenuhi beberapa hal berikut:

1. Berlandaskan pada arah bisnis strategis dari PT. X Wilayah Jakarta dan Tangerang sebagai sebuah perusahaan.
2. Memungkinkan unit-unit untuk berbagi (*sharing*) komponen infrastruktur TI tanpa mengurangi kemampuan masing-masing unit untuk mengantisipasi perubahan kebutuhan bisnis.
3. Mengurangi waktu yang dibutuhkan TI untuk memenuhi kebutuhan akibat perubahan pada unit bisnis dengan membuat lingkungan TI yang mudah beradaptasi.
4. Menekan biaya TI sepanjang siklus hidup dari setiap sistem.
5. Memiliki proses kendali (*governance process*) yang mendukung evolusi berkelanjutan baik dari AIP maupun dari faktor-faktor pendorongnya.
6. Dapat diimplementasikan dalam jangka waktu yang wajar untuk menghindari tumpulnya analisis (*analysis paralysis*).

Perencanaan arsitektur TI yang telah dilaksanakan menghasilkan Cetak Biru AIP *PT. X Wilayah Jakarta dan Tangerang*, yang mencakup *level* kontekstual, konseptual dan logikal untuk bidang-bidang *CIS*, *Call Center*, *Finance*, *Asset Management*, *Knowledge Management*, GIS/AM/FM, *New Services*, *Pemeliharaan & Operation Management*, *Trouble Management*, dan *interface*-nya ke ERP.

Studi Perencanaan *Data Center* dan *Backup* & *Recovery* PT. X Wilayah Jakarta dan Tangerang merupakan tahap selanjutnya dan merupakan bagian tak terpisahkan dari proses perencanaan sebelumnya yang diarahkan untuk dapat memenuhi kriteria-kriteria di atas. Studi Perencanaan *Data Center* dan *Backup & Recovery* difokuskan pada *level* fisik, dengan mempertimbangkan *level* bisnis dan aplikasi.

Tujuan

Tujuan umum dari Studi Perencanaan *Data Center* dan *Backup*&*Recovery* adalah mendefinisikan secara lengkap dan sistematis Arsitektur *Data Center* dan *Backup*&*Recovery* bagi AIP yang dapat mendukung implementasi sistem-sistem yang telah didefinisikan pada tahap-tahap sebelumnya di dalam Cetak Biru AIP PT. X Wilayah Jakarta dan Tangerang.

Studi Perencanaan *Data Center* dan *Backup* & *Recovery* diharapkan dapat mendukung keselarasan antara arah dan strategi perusahaan dengan penerapan sistem informasi yang berbasis komputer dapat terwujud, serta dapat menghemat investasi di bidang TI dalam menggunakan sumber daya perusahaan.

Tujuan umum tersebut dapat dirinci sebagai berikut.

1. Memperoleh hasil kajian yang mendalam mengenai arsitektur infrastruktur TI yang saat ini digunakan.

2. Mendefinisikan secara lengkap dan sistematis arsitektur *Data Center* dan *Backup&Recovery* yang mendukung integrasi dan implementasi sistem-sistem yang ada dan yang akan dikembangkan, dengan mengacu pada IT *MasterPlan* (ITMP) PT. X Wilayah Jakarta dan Tangerang dan Cetak Biru AIP PT. X Wilayah Jakarta dan Tangerang.
3. Meningkatkan efektivitas pengelolaan & konsolidasi TI yang mencakup jaringan, *server*, keamanan, dan *storage* .
4. Mendukung *high availability* & kelangsungan bisnis perusahaan (*business continuity*) melalui perencanaan kebijakan dan teknologi *Backup & Recovery* yang terintegrasi dengan perencanaan dan disain *Data Center*.
5. Meningkatkan perencanaan sistem informasi perusahaan dengan cara meningkatkan efektivitas pengambilan keputusan yang berkaitan dengan pemilihan TI sehingga diperoleh hasil yang optimum bagi perusahaan secara keseluruhan.

Identifikasi Permasalahan

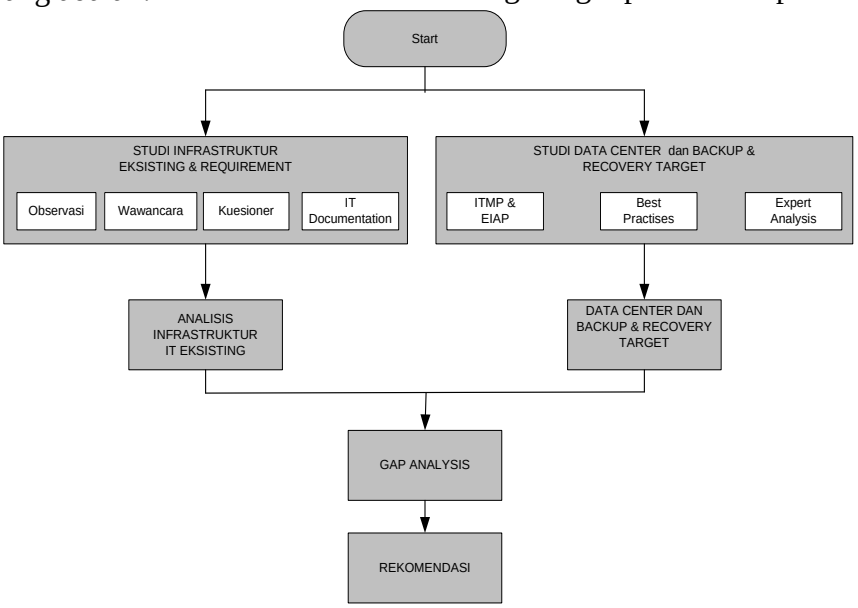
Identifikasi Permasalahan terkait dengan Penerapan BCP/DRP di PT. X Wilayah Jakarta Raya dan Tangerang adalah:

1. *Business Continuity Plan (BCP)* dan *Disaster Recovery Plan (DRP)* adalah dua hal yang sangat penting dalam proses bisnis, jarang menjadi prioritas.
2. Adanya alasan penerapan *BCP/DRP* memerlukan biaya yang mahal dan sulit penerapannya
3. Bencana adalah hal yang umumnya diyakini karena faktor alam yang tak dapat diprediksi dan tak dapat dicegah atau pun dihindari
4. Belum mendapatkan dukungan dari pihak manajemen (Terutama dari manjemen level tertinggi/tingkat direksi)
5. Sudah terlalu sering *BCP/DRP*menempati urutan prioritas terendah, atau proyek ini ditangani staf junior

Metode Penelitian

Studi Perencanaan *Data Center* dan *Backup* & *Recovery* merupakan kelanjutan dari perencanaan tahap sebelumnya yang men-definisikan proses-proses pada perspektif kon-tekstual, konseptual dan logikal AIP PT. X Wilayah Jakarta dan Tangerang.

Secara garis besar, metodologi yang akan dilakukan dalam proses studi perencanaan *Data Center* dan *Backup&Recovery* di lingkungan PT. X Wilayah Jakarta dan Tangerang diperlihatkan pada Gambar 1.



Gambar 1
Metodologi Studi Perencanaan *Data Center* dan *Backup&Recovery*

Data Center

Data Center merupakan suatu fasilitas yang menempatkan sumber daya TI (*computing resources*) perusahaan yang kritis, dalam suatu lingkungan yang terkendali dan dikelola secara terpusat. *Data Center* dapat memberikan kemampuan dan dukungan pada perusahaan untuk beroperasi sepanjang waktu dan sesuai kebutuhan.

Sumber daya TI yang dapat dicakup dalam *Data Center* mencakup *mainframe*, *web server*, *application server*, *file server*, *print server*, *messaging server*, perangkat lunak aplikasi dan operating system, *storage*, dan infrastruktur jaringan.

Aplikasi yang disimpan di dalam *Data Center* dapat bersifat *internal* (misalnya, aplikasi keuangan), maupun eksternal (misalnya, *customer management*). *Data Center* juga mengalokasikan perangkat lunak-perangkat lunak untuk mendukung operasi jaringan maupun aplikasi berbasis jaringan yang mencakup FTP (*File Transfer Protocol*), DNS (*Domain Name System*), DHCP (*Dynamic Host Configuration Protocol*), SNMP (*Simple Network Management Protocol*), NFS (*Network File System*) dan sebagainya. Aplikasi berbasis jaringan dapat mencakup *IP Telephony*, *video streaming*, *IP video conferencing* dan sebagainya.

Selain itu, *Data Center* mendukung implementasi komunikasi elektronik seperti *Internet* dan perdagangan *Digital* (*Digital Commerce*) yang handal melalui konsolidasi pemanfaatan data dan informasi perusahaan, agar dapat digunakan bersama-sama sesuai dengan wewenangnya secara efektif.

Dewasa ini berbagai perusahaan dapat memiliki satu atau lebih *Data Center* yang berkembang dengan sangat cepat untuk mengakomodasi berbagai sistem informasi perusahaan. *Data Center-Data Center* tersebut terdiri dari sejumlah *server farm* yang umumnya menggunakan sistem operasi dan *platform* yang berbeda. Kondisi ini berdampak pada biaya pemeliharaan dan pengelolaan yang besar karena kompleksitas masing-masing *Data Center*.

Tujuan implementasi *Data Center* tergantung pada kebutuhan perusahaan, namun sebagian diantaranya dapat dinyatakan sebagai berikut.

1. Kelangsungan bisnis (*business continuance / resiliency*)
2. Mengurangi biaya operasi dan pemeliharaan untuk menopang fungsi-fungsi bisnis perusahaan
3. Meningkatkan keamanan sistem informasi
4. Pengembangan aplikasi yang cepat
5. Konsolidasi sumber daya TI
6. Menunjang proses integrasi dan rekonsiliasi aplikasi

Untuk mendukung pencapaian tujuan-tujuan diatas, terdapat lima prinsip yang harus diperhatikan dalam perencanaan dan disain arsitektur *Data Center* yaitu:

1. *Availability*
2. Skalabilitas
3. Keamanan
4. Kinerja
5. *Manageability*

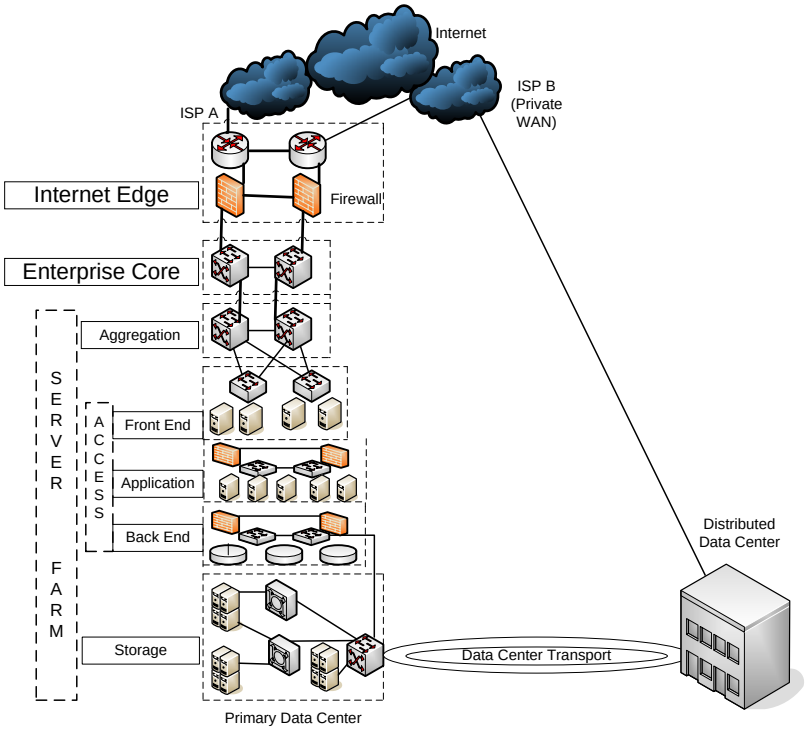
Kriteria disain di atas diterapkan pada bidang fungsional jaringan *Data Center*:

1. Layanan infrastruktur yang digunakan sebagai pendukung layanan-layanan yang bias diberikan oleh *Data Center*. Infra-struktur IP secara umum dikelompok-kan ke dalam tiga lapisan yaitu L2, L3, dan *Intelligent Network* (*QoS* dan *Multicast*)
2. Layanan aplikasi mencakup sejumlah fitur yang dapat mengoptimalkan kemampuan-kemampuan aplikasi melalui jaringan dengan meningkatkan waktu respon *server*, dan lain-lain. Beberapa fitur yang dapat digunakan antara lain: *load balancing*, *Secure Socket Layer* (SSL) *offloading*, dan *caching*
3. Layanan keamanan–mencakup fitur dan teknologi yang digunakan untuk meng-amankan infrastruktur *Data Center* dan lingkungan aplikasi. Beberapa fitur dan teknologi yang digunakan antara lain; *packet filtering* & *inspection*, *Intrusion Detection System (IDS)*, *Intrusion Prevention System (IPS)*, *firewall*, dll.
4. Layanan *storage* – memberikan kapabilitas untuk melakukan konsolidasi *storage* dengan menggunakan *Diskarray* yang ter-hubung ke jaringan, diantaranya: arsitektur

Storage Area Network (*SAN*), *Fiber Channel* (*FC*) *switching.*

5. Kelangsungan bisnis layanan yang memberikan *Availability* aplikasi pada tingkat tertinggi melalui pemanfaatan teknologi jaringan. Beberapa area yang terdapat di dalamnya antara lain: site selection, SAN *extension* dan *Data Center Interconnectivity.*

Secara umum topologi arsitektur *Data Center* dapat diperlihatkan pada Gambar 2.



Gambar 2
Arsitektur *Data Center*

Arsitektur *Data Center* pada Gambar II.2 merupakan arsitektur yang *fully redundant* dimana tidak terdapat *single point of failures* di dalamnya dan memiliki beberapa koneksi ke sistem-sistem lainnya.

Arsitektur ini juga dibagi dalam beberapa lapisan yang terdiri dari:

1. Lapisan *aggregation*, perangkat-perangkat yang umumnya terdapat di lapisan ini antara lain: *multi layer switch* L2-L3, *firewall*, *cache*, *load balancer*, *SSL offloader*, dan IDS
2. lapisan akses, perangkat-perangkat yang umumnya terdapat di lapisan ini antara lain: *switch* L2, IDS &*Host* IDS, yang dibagi dalam beberapa segmen sebagai berikut:
   a. Segmen *front-end* (*switch* L2, IDS, *Host* IDS, *WebServer*, *Server internal* pendukung; *internal* DNS, DHCP, WINS, dll)
   b. Segmen aplikasi (*firewall*, *switch* L2, IDS, *Server* Aplikasi)
   c. Segmen *Back-End* (*firewall*, *switch* L2, IDS, *Server* basis data)
3. Lapisan *storage*
4. Lapisan *Data Centertransport*

Selain itu, mengacu pada arsitektur *Data Center* di atas dan prinsip-prinsip disain dimana sumber daya TI diletakkan pada suatu atau beberapa lingkungan yang terkendali dan dikelola secara terpusat, serta tingkat kekritisan aplikasi, maka diperlukan perhatian khusus terhadap fasilitas-fasilitas yang akan disediakan termasuk personil yang akan mengoperasikan dan memelihara selama 24 jam sehari dan tujuh hari dalam seminggu.

Beberapa fasilitas *Data Center* yang harus diperhatikan antara lain:

1. Kapasitas catu daya
2. Sistem perkabelan
3. Pengendalian temperature dan kelembaban ruangan.
4. Sistem pendeteksi dan pemadam kebakaran

5. Pembatasan akses dan sistem pengawasan area *Data Center*
6. Kapasitas rak, dan lain-lain.

Untuk meningkatkan kehandalan *Data Center*, umumnya diterapkan pula topologi *distributed Data Center* yang dapat memberikan solusi bagi *Backup & Recovery* yang dikenal dengan *Disaster Recovery Plan* (DRP). *Data Center* dapat terdiri dari beberapa lokasi yang terpisah secara geografis.

Persyaratan fungsional *Data Center* antara lain:

1. Menyimpan komputer, *storage*, dan perangkat jaringan dengan aman
2. Menyediakan sumber daya yang dibutuhkan untuk memelihara perangkat-perangkat diatas.
3. Menyediakan lingkungan yang memiliki temperatur udara terkendali dengan paramater-parameter yang sesuai dengan kebutuhan perangkat.
4. Menyediakan konektivitas dengan perangkat lain di dalam maupun di luar *Data Center*.

Backup & *Recovery*

Backup adalah langkah-langkah yang dilakukan untuk menyalin data ke media yang lain untuk disimpan dan dipergunakan bila terjadi kerusakan data pada sistem komputer. Sementara *recovery* adalah mekanisme yang dilakukan untuk memulihkan data ketika terjadi kerusakan data. Pemulihan data tersebut dilakukan dengan mengaktifkan kembali data-data yang telah di-*backup* dalam media yang lain.

Proses *Backup & Recovery* akan memakan waktu tergantung pada jumlah data yang harus dilindungi. Terdapat beberapa metode yang dapat digunakan. Secara umum *Backup & Recovery* dapat dibagi menjadi tiga jenis:

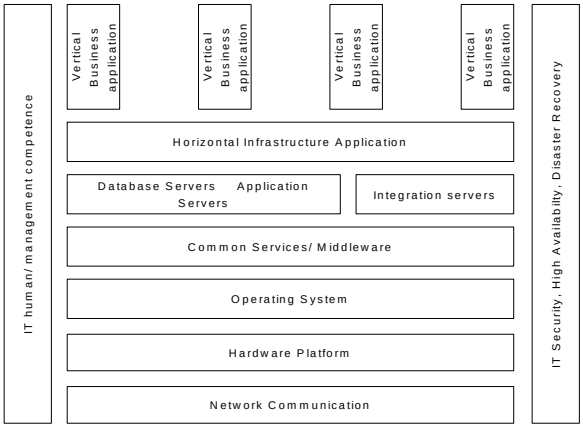
1. *Full backup*; adalah metode yang mem-*backup* semua file, folder atau data. Metode ini membutuhkan waktu yang cukup lama dibandingkan dengan metode lainnya. Namun diperlukan setidaknnya ketika memulai penerapan strategi *backup*.
2. *Incremental backup*; Metode ini hanya mem-*backup* data yang telah berubah semenjak *backup* terakhir. Metode ini lebih efisien dalam menggunakan media *backup* dan waktu *backup* relatif lebih cepat.
3. *Differential backup*; metode ini dimulai dengan *full backup*, lalu *subsequence backup* hanya menyimpan data yang telah berubah semenjak *full backup* terakhir. Metode ini relatif lebih lambat dibandingkan dengan *incremental backup*.

Analisis Infrastruktur TI dan Spesifikasi Kebutuhan *Data Center*

Studi infrastruktur TI merupakan suatu proses penilaian dan evaluasi terhadap infrastruktur TI yang telah ada. Hasil-hasil studi ini selanjutnya akan digunakan sebagai acuan untuk melakukan perencanaan *Data Center* dan *Backup* & *Recovery*.

Studi terdiri dari identifikasi terhadap arsitektur kontekstual, arsitektur konseptual dan arsitektur logikal yang telah didefinisikan di dalam cetak biru AIP PT. X Wilayah Jakarta dan Tangerang pada tahap sebelumnya dan ITMP PT. X Wilayah Jakarta dan Tangerang serta identifikasi terhadap infrastruktur TI yang telah ada. Studi terhadap Cetak Biru AIP PT. X Wilayah Jakarta dan Tangerang pada Studi Perencanaan *Data Center* dan *Backup* & Recovery, difokuskan pada upaya menentukan aplikasi yang kritis bagi bisnis perusahaan dan kebutuhan integrasi data/aplikasi dan *shared* basis data.

Identifikasi Infrastruktur TI yang ada di masing-masing unit kerja dilakukan untuk melihat kuantitas, kualitas dan kemampuan infrastruktur tersebut dalam mendukung implementasi arsitektur *Data Center* target yang telah didefinisikan. Untuk itu, perlu dilakukan proses pendataan/inventarisir perangkat/infrastruktur TI yang telah ada dan menyimpannya dalam bentuk basis data.



Gambar 3
Kerangka Kerja Infrastruktur TI

Analisis Dampak Usaha (*Business Impact Analysis*)

PT. X Wilayah Jakarta dan Tangerang memiliki banyak aplikasi untuk mendukung operasional perusahaan. Kompleksitas aplikasi membutuhkan usaha yang besar dalam pengelolaannya dan membutuhkan biaya perlindungan yang tinggi. Dengan keterbatasan alokasi sumber daya yang ada, baik sumber dana dan manusia, PT. X Wilayah Jakarta dan Tangerang perlu memprioritaskan aplikasi-aplikasi yang kritis untuk dilindungi dan dijamin ketersediaan layanannya, agar proses bisnis utama PT. X Wilayah Jakarta dan Tangerang tidak terganggu. Untuk menentukan data-data dan aplikasi yang kritis tersebut dilakukan dengan *Business Impact Analysis* (BIA) atau Analisis Dampak Usaha.

Tujuan *Business Impact Analysis*

Business Impact Analysis umumnya dilakukan dengan tujuan sebagai berikut.

1. Mengidentifikasi dan mengklasifikasikan proses bisnis utama atau proses bisnis yang berkaitan erat dengan keberhasilan misi perusahaan.
2. Mengidentifikasi semua *asset* TI perusahaan
3. Memetakan dukungan *asset* TI terhadap proses bisnis utama.
4. Melakukan perhitungan biaya yang ditimbulkan bila terjadi kegagalan TI terhadap proses bisnis utama.
5. Menentukan toleransi kerugian (biaya).
6. Menentukan *Response Time Objective* (RTO) dan *Response Point Objective* (RPO) untuk setiap proses bisnis.

Pengumpulan Data

Pengumpulan data dilakukan dengan menyebar kuesioner, wawancara dan observasi lapangan. Responden yang melakukan pengisian data adalah sebagai berikut:

1. Manajer Bidang dan staf Bidang TI PT. X Wilayah Jakarta dan Tangerang
2. Manajer-Manajer Bidang PT. X Wilayah Jakarta dan Tangerang
3. General Manajer PT. X Wilayah Jakarta dan Tangerang

Setiap responden diminta untuk menjawab pertanyaan-pertanyaan yang berbeda, sesuai dengan ruang lingkup masing-masing. *Business Impact Analysis*PT. X Wilayah Jakarta dan Tangerang dilakukan dengan menggunakan dua metode, yaitu metode kualitatif dan metode kuantitatif. Metode kualitatif dilakukan untuk identifikasi awal aplikasi kritis perusahaan. Selanjutnya metode kuantitatif digunakan untuk mempertajam analisis kualitatif terhadap besarnya dampak kerugian akibat suatu gangguan dan menentukan RTO dan RPO.

1. Metode Kualitatif; Metode ini menggunakan asumsi-asumsi dan penilaian responden untuk menentukan tingkat kebutuhan proses bisnis dan *asset* TI pendukungnya dalam beberapa kategori. Selain digunakan untuk identifikasi awal aplikasi kritis di PT. X Wilayah Jakarta dan Tangerang, metode ini digunakan secara lebih intensif pada proses-proses bisnis yang nilai produksinya sangat sulit diukur karena bersifat tidak langsung, seperti pelayanan *Call Center*. Pengukuran dengan metode ini dilakukan dengan menilai tingkat kebutuhan suatu proses bisnis dan *asset* TI yang terkait. Tingkat kebutuhan tersebut dibagi dalam beberapa kategori yang merujuk pada kriteria perancangan sebuah *Data Center*. Adapun kriteria tersebut adalah sebagai berikut:
   a. Keamanan; tingkat keamanan aplikasi dari hal-hal yang akan mengakibatkan kegagalan operasi aplikasi.
   b. Skalabilitas; kemudahan untuk pengembangan berikutnya.

c. *Availability*;keterdiaan data dan informasi yang diatur dengan mekanisme akses data dan informasi
d. *Manageability*; kemudahan dalam pengelolaan aplikasi yang diatur dengan SOP (*standard operating procedure*).
e. *Integrity*; jaminan integritas data dan informasi yang dapat menjamintingkat minimasi kesalahan operasi aplikasi dan adanya dukungan *feed back correction.*
f. Kinerja; kepastian berjalannya operasi aplikasi dengan tingkat performansi yang tinggi pada saat diakses dan tingkat toleransi *idle* dan kesalahan yang rendah.

Setiap kategori dinilai dengan peringkat penilaian sebagai berikut:

1. *High*, untuk penilaian tingkat kebutuhan yang tinggi, dengan nilai 3.
2. *Medium*, untuk penilaian tingkat kebutuhan yang menengah, dengan nilai 2
3. *Low*, untuk penilaian tingkat kebutuhan yang rendah, dengan nilai 1.

Untuk mengukur kualitatif data, dilakukan dengan dua sumber pembobotan dengan bobot nilai yang ditentukan sebagai berikut:

a. *Departemen TI* sebagai penyedia layanan TI, dengan bobot 60%
b. Pengguna / Bidang sebagai pengguna layanan TI dengan bobot 40%

Nilai-nilai setiap kategori diakumulasi untuk setiap proses bisnis dan *asset* TI pendukungnya, dan dijadikan dasar penilaiaan proses bisnis dan *asset* TI yang kritis untuk segera lindungi dalam *Data Center*PT. X Wilayah Jakarta dan Tangerang.

2. Metode Kuantitatif; metode ini menggunakan pendekatan secara finansial. Metode kuantitatif digunakan untuk mempertajam analisis kualitatif. Metode kuantitatif diterapkan secara lebih intensif pada proses bisnis dan *asset* TI yang memiliki keterkaitan erat dengan proses-proses yang bersifat finansial, seperti penerimaan pembayaran dari pelanggan, penagihan piutang dan lain-lain. Metode kuantitatif yang diterapkan menggunakan pendekatan *Total of Cost Down time*, dimana pendekatan ini melakukan perhitungan-perhitungan besarnya kerugian finansial akibat kegagalan layanan TI di PT. X Wilayah Jakarta dan Tangerang. Kerugian-kerugian tersebut dapat dinilai dari besarnya kontribusi secara finansial suatu proses bisnis atau *asset* TI terhadap perusahaan.

   Pengukuran dilakukan dengan beberapa asumsi-asumsi yang disepakati dan data-data transaksi yang ada. Berikut adalah parameter yang digunakan dalam menghitung *Total of Cost Down Time*:

   a. Rata-Rata Nilai Transaksi; adalah rata-rata nilai finansial yang diperoleh suatu proses bisnis dan *asset* TI yang terkait.
   b. Rata-Rata Jumlah Transaksi; adalah rata-rata jumlah transaksi yang dilayani suatu proses bisnis dan *asset* TI yang terkait.
   c. Nilai Produktifitas; adalah nilai yang menunjukkan kontribusi suatu proses bisnis dan *asset* TI terkait terhadap PT. X Wilayah Jakarta dan Tangerang. Nilai tersebut diperoleh dengan menggunakan formula matematis sebagai berikut:

Rata-Rata Nilai Transaksi x Rata-Rata Jumlah Transaksi = Nilai Produksi

Kegagalan suatu *asset* TI akan menyebabkan gangguan terhadap proses-proses bisnis yang terkait, dan gangguan terhadap proses bisnis tersebut secara langsung menyebabkan penurunan atau hilangnya kontribusi suatu proses bisnis pada perusahaan yang sebanding dengan nilai produksi proses bisnis yang bersangkutan. Besarnya nilai produksi dijadikan dasar untuk menentukan proses bisnis dan *asset* TI kritis untuk segera dilindungi dalam *Data Center*PT. X Wilayah Jakarta dan Tangerang. Perbandingan toleransi kerugian yang ditetapkan oleh general Manajer terhadap nilai produksi masing-masing proses bisnis dan sistem TI pendukungnya digunakan untuk memperoleh nilai RTO dan RPO. Nilai RTO dan dan RPO dijadikan dasar untuk menentukan teknologi dan strategi *Backup & Recovery Data Center*PT. X Wilayah Jakarta dan Tangerang.

Hasil *Business Impact Analysis*

Langkah pertama dalam melakukan BIA adalah melakukan identifikasi *asset* TI yang dikelola Bidang TI PT. X Wilayah Jakarta dan Tangerang. Identifikasi dilakukan pada Nama Sistem Informasi, *asset* TI (spesifikasi umum Perangkat keras dan perangkat lunak), Nilai Finansial *asset* yang bersangkutan (*Asset* Value –AV) dan Nama *vendor* atau *outsourcing* setiap *asset* yang ada. Nilai *asset* value tidak dijadikan pertimbangan dalam pembangunan *Data Center*PT. X Wilayah Jakarta dan Tangerang, tetapi akan digunakan pada manajemen resiko (*Risk Management*) dan pembangunan Rencana Penanganan Darurat TI (*IT Contingency Plan*) yang terkait pada pembangunan Rencana Kelangsungan Usaha Dan Rencana Penanggulangan Bencana (*Business Continuity Plan* – BCP dan *Disaster Recovery Plan* – DRP.

Secara umum *asset* TI PT. X Wilayah Jakarta dan Tangerang dapat dibagi menjadi:

1. Aplikasi dan basis data
2. *Server* dan perangkat keras
3. Jaringan komputer.

Analisis Aspek *Backup*&*Recovery*

Semua aplikasi di lingkungan PT. X Wilayah Jakarta dan Tangerang menggunakan strategi *Backup & Recovery* sebagai berikut:

1. Strategi *backup* pada *server farm* menggunakan *fullbackup* pada setiap awal bulan dengan media penyimpanan berupa *tape*
2. *Increment backup* tidak dilakukan secara berkala, hanya dilakukan bila dipandang perlu untuk pengamanan pada kondisi tertentu.
3. Data-data yang terdistribusi di AP dan unit-unit lain di *backup full* secara *offline*, kemudian di kirim ke PT. X Wilayah Jakarta dan Tangerang pada setiap awal bulan dengan menggunakan kurir.
4. Strategi *backup* data pada *server farmvendor* dilakukan secara mandiri oleh masing masing *vendor*. Namun *backupfull* dilakukan pada awal bulan oleh masing-masing *vendor* tersebut.

Hanya aplikasi CIS dan GIS yang menerapkan metode rotasi *bakup tape Grandfather, Father, Child* (GFC) dalam melakukan *backup* dan *recover*y. Metode GFC dilakukan dengan menggunakan 10 *backup tape*. Siklus *backup* berakhir pada setiap akhir bulan. Siklus *Backup* dimulai pada awal bulan dengan *backup full*, dilanjutkan dengan *backup* secara *Full* pada setiap awal minggu dan *backup increment* setiap harinya. *Backup* dilakukan terhadap data-data yang berada pada *server* setiap aplikasi, maupun data-data CIS dan GIS yang tersebar pada masing-masing unit.

Pemilihan teknologi *Backup & Recovery*

Pemilihan teknologi *Backup & Recovery* PT. X Wilayah Jakarta dan Tangerang didasarkan pada hasil *Business Impact Analisys*. Salah satu dari hasil BIA adalah toleransi waktu dan kehilangan data (*RTO* dan *RPO*) pada masing-masing *asset* TI atau aplikasi kritis yang ada.

Strategi dan teknologi *backup-recovery* yang diterapkan harus dapat memenuhi toleransi tersebut. Bila terjadi gangguan pada sistem TI, kegagalan fungsi *Backup & Recovery* akan menyebabkan terganggunya operasional PT. X Wilayah Jakarta dan Tangerang yang pada akhirnya akan menyebabkan kerugian secara berkelanjutan seiring dengan bertambah lamanya gangguan yang terjadi.

Hasil BIA PT. X Wilayah Jakarta dan Tangerang menunjukkan rata-rata RTO aplikasi kritis berada pada orde waktu detik hingga orde waktu menit. RPO rata-rata setiap aplikasi kritis berdasarkan dari rata-rata jumlah transaksi yang terjadi, berada pada orde waktu detik sampai dengan orde waktu menit.

Secara umum teknologi *Backup & Recovery* yang diterapkan pada *Data Center*PT. X Wilayah Jakarta dan Tangerang menggunakan teknologi *Syncronous Replication* dan *Clustering*. Selain menggunakan teknologi tersebut beberapa teknologi *Backup & Recovery* diterapkan untuk memberi perlindungan secara berlapis pada setiap segmen aplikasi dalam lingkungan *multitier*, antara lain:

1. Perlindungan kegagalan mesin.
2. Perlindungan kegagalan *Harddisk.*
3. Perlindungan kehilangan data.

Arsitektur *Backup* & *Recovery PT*. X Wilayah Jakarta dan Tangerang

Metodologi Strategi *Backup & Recovery*

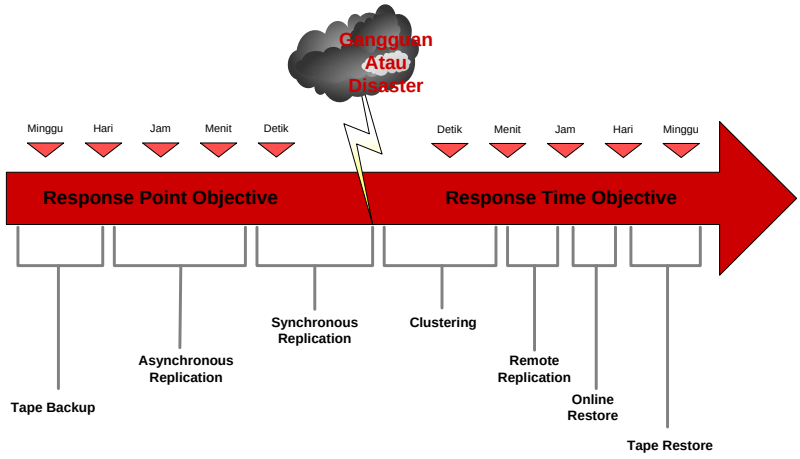
Dewasa ini *Backup & Recovery* tidak hanya terbatas pada penerapan media *backup* dan metode-metode diatas dalam strategi *Backup & Recovery*. *Backup & Recovery* dihubungkan dengan kerugian tidak beroperasi-nya proses bisnis perusahaan. Pendekatan ini dikenal dengan *Total of Cost Down Time*. Strategi *Backup & Recovery* sebaiknya juga dikaitkan dengan Rencana Penanggulangan Bencana (*Disaster Recovery Plan*) dan Rencana Kelangsungan Usaha (*Business Continuity Plan*), dua hal yang secara eksplisit disebut dalam ITMP – PLN.

Melalui Analisis Dampak Usaha (*Business Impact Analysis*) dapat diperoleh RTO dan RPO, yang selanjutnya akan digunakan sebagai dasar menentukan strategi *Backup & Recovery*. RTO adalah toleransi lamanya sebuah proses bisnis berada dalam gangguan. RPO adalah toleransi jumlah data yang hilang bila terjadi suatu gangguan.

Disain Arsitektur *Data Center* dan *Backup & Recovery* PT. X Wilayah Jakarta dan Tangerang juga akan disesuaikan dengan AIP dalam konteks integrasi aplikasi di lingkungan *internal* dan eksternal.

Teknologi *Backup & Recovery*

Gambar V.1 memperlihatkan beberapa teknologi *Backup & Recovery*, dikaitkan dengan waktu *recovery* (RTO) dan dampak bisnis perusahaan(toleransi kehilangan data – RPO). Semakin besar dampak bisnis yang ditimbulkan, diperlukan waktu *recovery* yang semakin cepat.



Gambar 4
Pemilihan teknologi *Backup* &*Recovery*

Teknologi dan prinsip kerja masing-masing teknologi *Backup & Recovery* yang diterapkan dalam *Data Center*PT. X Wilayah Jakarta dan Tangerang adalah sebagai berikut:

SAN

Data Center PT. X Wilayah Jakarta dan Tangerang dirancang menggunakan *SAN*. Secara umum SAN dapat didefinisikan sebagai jaringan yang digunakan oleh perangkat-perangkat *storage* dan di dalam lingkungan *Data Center*, umumnya menggunakan *Fiber Channel* untuk menghubungkan *server-server* ke *storagedevice* dan berkomunikasi dengan mengirimkan perintah-perintah SCSI. *Storagenetwork* menyediakan komunikasi SCSI melalui jaringan baik dengan FCIP maupun iSCSI.

Data Center PT. X Wilayah Jakarta dan Tangerang menggunakan sebuah *SAN* dengan teknologi *Enterprise Storage*. Teknologi tersebut mampu mengumpulkan data di dalam sebuah media besar yang memiliki *Availability* mencapai 99,999%.

Cluster

Mekanisme *Clustering* menggunakan beberapa *server* yang dapat beroperasi sebagai suatu perangkat tunggal dengan tujuan menyediakan *high availability* dan pendistribusian beban. Aplikasi-aplikasi bisnis yang kritis PT. X Wilayah Jakarta dan

Tangerang di*deploy* pada *server-server* yang di*cluster*.

Metode yang digunakan adalah *active/active shared everything*. Arsitektur ini terdiri dari *server-server* yang terhubung pada system *storage* yang sama dimana *server-server* dapat mengakses file-file yang sama. Suatu mekanisme *locking* disediakan oleh Perangkat Lunak *cluster* untuk mencegah pengaksesan sebuah file secara bersama-sama. Arsitektur ini umumnya menggunakan *Fiber Channel*.

Clustering dapat juga dilakukan terhadap *server-server* yang berbeda lokasi secara geografis sehingga memungkinkan untuk menempatkan aplikasi-aplikasi dan data-data yang sama pada beberapa *Data Center*. Kebutuhan utama *geographical clustering* adalah data yang tersedia pada salah satu *Data Center* harus direplikasi dan tersedia pada *remoteData Center*.

Syncronous Replication

Mekanisme Replikasi sinkronous mengirimkan data ke dua media *storage* dalam waktu yang bersamaan, namun mekanisme tersebut memerlukan mekanisme *acknowledgement* apabila berhasil melakukan proses penyimpanan sedangkan replikasi *asynchronous* tidak memerlukan mekanisme tersebut. *Syncronous replication* sering digunakan untuk *Backup & Recovery* pada lingkungan SAN, pembangunan DRP dan memperluas jaringan replikasi data.

Perluas jangkauan SAN secara geographis dapat menggunakan teknologi-teknologi berikut:

1. *Internet* SCSI (iSCSI).
2. SAN *Extension* via CWDM atau DWDM.
3. *Fiber Channelover* IP (FCIP); merupakan teknik *tunneling Fiber Channel* melalui jaringan IP dengan menggunakan *router-router* yang memiliki *Fiber ChannelPort Adapter* atau *Fiber ChannelSwitch*/*director* dengan *Gigabit Ethernet Port* dan kapabilitas FCIP. Perangkat yang mendukung implementasi FCIP antara lain: Cisco MDS9000 *Family*.

Aplikasi *Syncronous Replication* yang direkomendasikan adalah :

1. RAC Oracle
2. Veritas *Storage* Replicator
3. Veritas R*link*
4. Veritas Flashsnap
5. Double Take

RAID

Redundant Array Inexpensive Disks (RAID) merupakan metode yang menggabungkan beberapa *harddisk* ke dalam sebuah *logical unit* agar diperoleh kecepatan yang tinggi (RAID 0), *redundancy* (RAID 1) atau kedua-duanya (RAID 5). Penggunaan RAID umumnya diperuntukkan sebagai *fault tolerant* terhadap media menyimpanan data (*harddisk*).

Seperti pada umumnya perangkat keras yang lain, *harddisk* dapat mengalami kerusakan dan hilang (*corruption* dan *lost*) akibat faktor usia (*life time*) ataupun faktor-faktor gangguan yang lain, seperti gangguan kelistrikan dan *overhead* kerja *harddisk*. Kerusakan *harddisk* akan menyebabkan hilangnya data yang tersimpan pada media tersebut. Cara sederhana untuk mengatasi permasalahan tersebut adalah menyalin data-data yang ada kebeberapa *harddisk*. Mekanisme RAID menyamarkan pengaturan distribusi data, sehingga beberapa *harddisk* yang ada dapat diperlakukan sebagai sebuah media *storage* atau *volume* atau *drive* atau partisi.

Struktur dasar dari RAID adalah *array*, yaitu sekumpulan media *storage* yang diatur untuk meningkatkan keefektifan fungsi yang diharapkan. Jumlah media *storage* dan cara pemisahan *controllerharddisk* mempengaruhi keefektifan suatu *Array*.

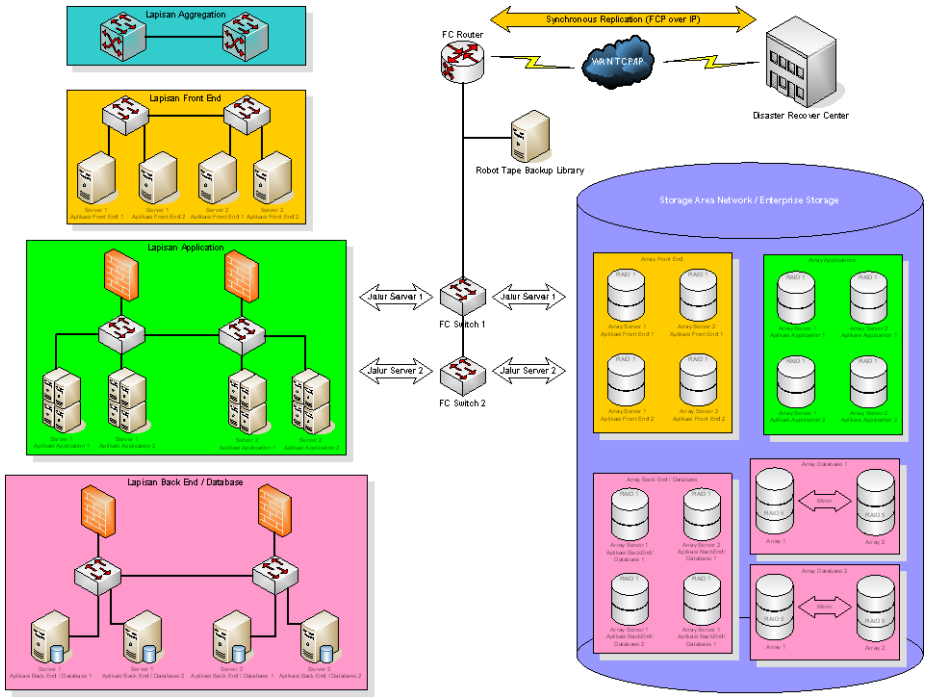
Strategi dan Arsitektur *Backup & Recovery*

Data Center PT. X Wilayah Jakarta dan Tangerang dibangun dalam beberapa segmen sebagai berikut:

1. Lapisan *Aggregation Data Center*
2. Lapisan Akses *Data Center*
   a. Segmen *Front-end*
   b. Segmen *Application*
   c. Segmen *Back-End*/Basis data

Pada setiap segmen terdapat *server-server* yang memiliki fungsi tersendiri. Setiap

server membutuhkan media penyimpanan (*storage*) untuk sistem operasi, aplikasi dan basis data. Media penyimpanan tersebut dikumpulkan dalam sebuah SAN dengan teknologi *EnterpriseStorage*. Pengumpulan ini dilakukan untuk mempermudah pengelolaan *storage* dan memberikan tingkat *availibility* yang tinggi dengan mekanisme tertentu.



Gambar 5
Arsitektur *Backup & Recovery*

SAN *Data Center* PT. X Wilayah Jakarta dan Tangerang dibagi menjadi beberapa *array* yang digunakan untuk menyimpan data, sistem operasi, aplikasi dan basis data yang ada pada masing-masing segmen *Data Center*. Secara umum *array-array* tersebut dapat dibedakan menjadi:

1. *Array* OS & Aplikasi; adalah *array* dalam *EnterpriseStorage* yang dialokasikan untuk menyimpan sistem operasi, aplikasi dan aplikasi basis data yang ada pada setiap *server* di masing-masing segmen. Proses *booting server* dan proses komputasi dasar setiap *server* dilakukan pada masing-masing *array* ini. *Array* OS & Aplikasi ini diberi *label* dengan *format* :
   ArrayServer[NoServer]-[NamaAplikasi]-Segmen [NamaSegmen]
   Contoh :
   Array Server 1 - SIMKeu – Segmen Application
   Array Server 2 - SIMKeu – Segmen Application.
2. *Array* basis data; adalah *array* yang berada pada segmen *back-End*/basis data dengan fungsi menyimpan data dari basis data tertentu. Aplikasi-aplikasi yang terkait akan mengakses *array-array* ini untuk mengambil data yang diperlukan. *Array* ini di beri *label* dengan *format*:
   basis data[Namabasis data]-Array[NoArray]
   Contoh :
   basis data-SIMKEU-Array 1
   basis data-SIMKEU-Array 2

Protokol yang digunakan untuk komunikasi dalam lingkungan SAN adalah FC. Pada SAN *Data Center* terdapat dua buah *switch* FC yang menghubungkan *server-server* dengan *array* yang bersesuaian (dalam *EnterpriseStorage*) dimana OS, aplikasi, basis data dan data dari basis data setiap *server* tersebut disimpan. Pemasangan dua buah *switch* tersebut digunakan sebagai *redundancy* apabila terjadi gangguan pada sebuah *switch*.

Sebuah *Robot backup Tape Array* digunakan untuk melakukan *backup* masing-

masing data dari basis data pada segmen *Back-End*/basis data melalui *media tape backup*. *Backup* dengan menggunakan *tape backup* di dalam SAN menggunakan teknologi *server free*. *Syncronous replication* digunakan untuk melakukan replikasi secara *real time* di dalam SAN *Data Center*. *Synconous Replication* juga digunakan untuk melakukan replikasi secara *real time* melalui jaringan WAN TCP/IP ke *Disaster Recovery Center* (DRC) dengan memasang sebuah *router* FCIP.

Syncronous replication membutuhkan *bandwitdh yang besar*. *Asyncronous replication* dapat digunakan bila tidak tersedia bandwitdh yang memadai. Hal ini akan menyebabkan RPO yang diperoleh sedikit lebih besar dari nilai RPO hasil BIA (dalam orde menit sampai dengan jam).

Implementasi ERP berpotensi untuk menggantikan SIMMAT, SIMKeu, dan SIPeg. Oleh karena itu jika implementasi ERP sudah dapat dipastikan, ketiga aplikasi tersebut tidak perlu lagi di *host* ke dalam *Data Center*.

Disaster Recovery Plan

Disaster Recovery Plan (DRP) bukan merupakan salah satu pembahasan pada dokumen ini. Diperlukan studi khusus untuk membangun sebuah DRP yang dikaitkan dengan manajemen resiko, BIA dan *Data Center*. Mekanisme replikasi sinkronous digunakan untuk mengirim data secara *real time* ke DRC melalui jaringan WAN (protokol TCP/IP) yang didukung dengan pemanfaatan FCIP *router*. Teknologi *FC* over IP memungkinkan pengiriman data pada jarak hampir 100 Km.

Rekomendasi *Backup & Recovery*

1. Pengumpulan data di dalam *Data Center* memerlukan pengawakkan/Staf khusus yang bertanggung jawab terhadap manajemen dan operasional *Backup & Recovery* (*Storage* dan *Backup Administrator*).
2. Jumlah basis data yang banyak dalam *Data Center* memerlukan dokumentasi, standarisasi *label* dan penamaan komponen-komponen dalam *storage*, *backup* & *recovery*. Seperti Penamaan *Array* dalam SAN, Penamaan perangkat jaringan SAN, *Backup Tape* dan penjadwalan *backup*.
3. Jumlah basis data yang banyak dan lingkungan penyimpanan data dalam SAN membutuhkan perangkat dan Perangkat Lunak manajemen *backup* untuk mempermudah operasional, terutama pada lingkungan SAN. Seperti *Robot Tape Library, Backup Asisst*.
4. Perlu disusun sebuah SOP penangananan *Backup & Recovery*.
5. Simulasi dan latihan proses *recovery* data perlu dilakukan untuk menguji sistem dan kemampuan staf *backup* dalam mencapai RTO dan RPO.
6. Perlu diterapkan rotasi *backup tape* yang disesuaikan dengan jumlah data dan efisiensi penggunaan *tape backup*.
7. Setelah pembangunan *Data Center* direkomendasikan untuk dilanjutkan dengan pembangunan Rencana Penang-gulangan Bencana (*Disaster Recovery Planning* / DRP)

Masalah yang sering dihadapi dalam *Backup & Recovery* adalah staf TI terbiasa dengan proses *backup* tetapi tidak terlatih dalam proses *recovery* data. Hal ini memerlukan latihan, dokumentasi dan standar langkah-langkah kerja (*Standard Operating Procedure*) untuk mengatur *Backup & Recovery*. Permasalahan lainnya adalah waktu yang digunakan untuk proses *recovery* yang terkadang tidak dapat diperkirakan dan mengganggu operasional proses bisnis perusahaan.

Kesimpulan

Dengan adanya *Disaster Recovery Planning* yang baik, maka segala kemungkinan ancaman-ancaman yang mungkin muncul dalam pelaksanaan bisnis dan industry dapat diatasi dengan baik. Kontinuitas bisnis dapat dijaga dan segala bentuk kerugian dapat diminimalisir sehingga perusahaan dapat bangkit kembali dari keadaan darurat yang mungkin terjadi. Disaster Recovery Planning harus disesuaikan dengan situasi dan kondisi perusahaan agar perencanaan yang dilakukan tidak salah dan dapat menangani masalah secara tepat.

Daftar Pustaka

Kusmayadi. (2010). Perancangan Business Continuity Plan: Studi Kasus PT. X. *Laporan Proyek Akhir Program Magister Teknologi Informasi* (Tidak diterbitkan). Fasilkom Universitas Indonesia.

Novianto, Sandra. (2006). Kajian dan Analisis Business Continuity Plan pada Bank XYZ. *Laporan Proyek Akhir Program Magister Teknologi Informasi* (Tidak diterbitkan). Fasilkom Universitas Indonesia.

Putri, Sila Wiyanti. (2008). *Pembangunan Disaster Recovery Plan Untuk Sistem Informasi Manajemen Terintegrasi ITB*.

Slamet, K. (2004). Pembentukan Kerangka Kerja Business Continuity Plan pada Bank Ritel X. *Laporan Proyek Akhir Program Magister Teknologi Informasi* (Tidak diterbitkan). Fasilkom Universitas Indonesia.

Sharing Vision. (2008). Business Continuity and Disaster Recovery Trend and Issue in Indonesia 2008. *Workshop SharingVision*. Bandung. Diakses dari http://www.sharingvision.biz

Solehudin, Usep. (2005). *Business Continuity and Disaster Recovery Plan*.

Weblog]. Diakses dari *http://s.itb.ac.id/home/jayidoans@students.itb.ac.id/Magister%20Informatika%20ITB/TA051Studi%20kasus.pdf.*

Weblog]. Diakses dari *http://bebas.vlsm.org/v06/Kuliah/MTIKeamanan-Sistem-Informasi/2005/128/128P-08final2.0business-continuity-and-disaster recovery-plan.pdf.*