PERANCANGAN *DISASTER RECOVERY PLAN* UNTUK TEKNOLOGI DI PERUSAHAAN PT. XYZ

DESIGNING DISASTER RECOVERY PLAN FOR TECHNOLOGY IN PT. XYZ COMPANY

Yasser Sutojoyo Kusumo[1], Rd. Rohmat Saedudin[2], Basuki Rahmat[3]

[1, 2, 3] Program Studi Sistem Informasi, Fakultas Rekayasa Industri, Telkom University

yassersutojoyo@gmail.com, roja2128@gmail.com, basuki@transforma.co.id

Abstrak

PT. XYZ merupakan suatu perusahaan yang bergerak di bidang teknologi, industri, dan infrastruktur. Saat ini PT XYZ Industri mengalami permasalahan pada langkah-langkah menanggulangi bencana yang mungkin dapat terjadi setiap saat. Bencana tersebut dapat mengganggu infrastruktur teknologi PT. XYZ yang mempengaruhi seluruh proses bisnis yang menggunakan infrastruktur tersebut. Oleh karena itu dibuat suatu rancangan Disaster Recovery Plan terkait teknologi yang berguna untuk menanggulangi bencana pada infrastruktur teknologi di PT. XYZ.

Tahap penelitian diawali dengan dengan identifikasi dokumen arsitektur eksisting yang berisi aset infrastruktur teknologi perusahaan PT. XYZ dan hasil business impact analysis yang menentukan RTO dan RPO server-server yang berada di perusahaan. Tahap selanjutnya adalah tahap desain yang berisi perancangan rekomendasi teknologi data, application dan network saat bencana terjadi. Dan tahap terakhir yang dilakukan adalah melakukan analisis untuk menyesuaikan hasil perancangan rekomendasi tersebut.

Dengan menerapkan rancangan Disaster Recovery Plan terkait teknologi, maka perusahaan dapat menanggulangi bencana yang menyebabkan infrastruktur teknologi tersebut terganggu.

Kata Kunci: Disaster Recovery Plan, Infrastruktur Teknologi.

Abstract

PT. XYZ is a company runs in the field of technology, industry, and infrastructure. Currently PT XYZ is experiencing problems on overcoming disaster that may occur at any time. The disaster can disrupt technology infrastructure of PT. XYZ which affects all business processes that use the infrastructure. Therefore, a Disaster Recovery Plan design technology-related has been created for disaster overcoming on technology infrastructure in PT. XYZ.

The research phase begins with the identification of the existing architectural documents containing the technology infrastructure assets of the PT. XYZ company and the result of business impact analysis that determines the RTO and RPO servers in the company. The next stage is the design phase that contains the design of network technology infrastructure, application, and data infrastructure recommendations. And the final step is to do an analysis to adjust the results of the design recommendations.

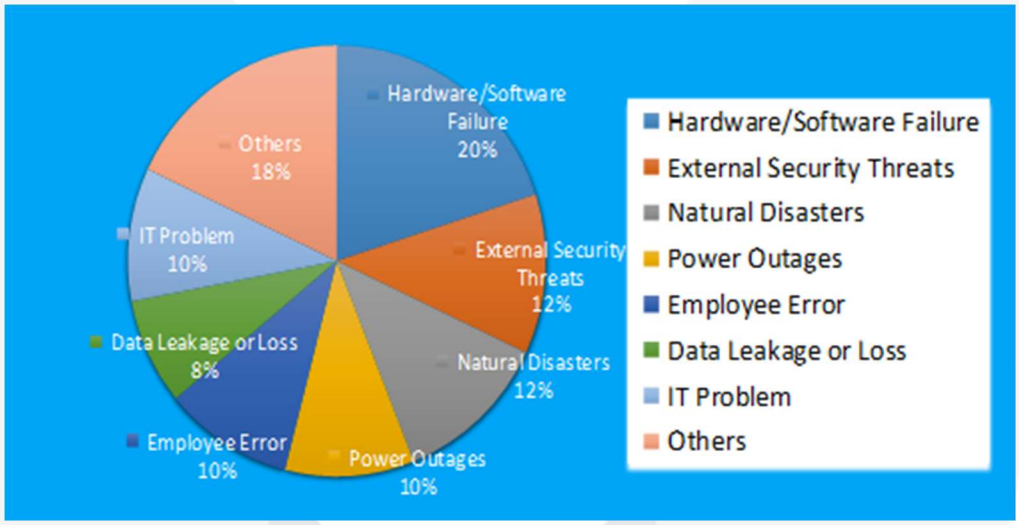
By applying a Disaster Recovery Plan design related to technology, the company can overcome the disaster that caused the technology infrastructure is disrupted.

Keywords: Disaster Recovery Plan. Infrastructure Technology.

1. Pendahuluan

Di era saat ini, pemanfaatan TI sudah menjadi bagian yang sangat penting didalam perusahaan untuk menunjang proses bisnis perusahaan tersebut. Dengan persaingan bisnis yang semakin ketat, perusahaan pun dituntut untuk memperbaharui sistem maupun infrastruktur TI yang menunjang proses bisnis tersebut. Teknologi informasi merupakan sumber daya teknologi yang menyediakan sistem informasi yang meliputi perangkat keras dan perangkat lunak di perusahaan. Teknologi informasi ini mendukung bisnis perusahaan dan strategi sistem informasinya. Oleh dari itu, teknologi informasi mempunyai dampak yang besar terhadap proses bisnis perusahaan agar seluruh aspek dan proses bisnis tersebut dapat berjalan sebagaimana mestinya. Sesuai dengan pengertian penerapan TI dan infrastruktur dapat disimpulkan bahwa penerapan TI mempunyai andil penting dan sangat krusial, teknologi informasi tidak boleh mengalami kegagalan yang membuat rantai proses bisnis hancur. Hal tersebut dapat dicegah jika sudah ada perencanaan TI yang melindungi teknologi informasi dari gangguan-gangguan untuk memungkinkan proses bisnis terus berlangsung. PT. XYZ harus memastikan bahwa teknologi informasi tetap berjalan dari gangguan yang dapat mengganggu proses bisnis perusahaan. PT. XYZ merupakan suatu perusahaan yang bergerak di bidang teknologi, industri, dan infrastruktur dan berada di bawah koordinasi Kementrian Negara BUMN dengan kepemilikan saham 100% oleh Pemerintah Republik Indonesia. Dalam menunjang proses bisnis perusahaan, PT. XYZ mempunyai aset infrastruktur teknologi berupa server data center yang berisi data dan aplikasi serta jaringan komputer yang menghubungkan semua entitas-entitas teknologi informasi yang berada di PT. XYZ. Dalam melakukan proses bisnis PT. XYZ terdapat permasalahan yang mungkin terjadi seperti kegagalan media penyimpanan, server data center rusak, jaringan terputus oleh bencana alam maupun sabotase dan lain sebagainya.

Perusahaan Symantec selaku perusahaan keamanan sistem informasi merilis sebuah chart berupa gambar hasil audit yang berisi kemungkinan presentase penyebab-penyebab gangguan terhadap infrastruktur teknologi di perusahaan yang terjadi di tahun 2017, berikut merupakan gambar chart tersebut.



Gambar 1. DRP Drivers

(Sumber: Symantec Annual IT Reports, 2017)

Hal-hal tersebut berpotensi infrastruktur teknologi tersebut terganggu. Untuk memulihkan infrastruktur teknologi yang terganggu tersebut dibutuhkan perancangan Disaster Recovery Plan terkait teknologi sebagai perencanaan TI untuk memulihkan aset-aset teknologi informasi perusahaan agar terus berjalan saat terkena gangguan. Disaster Recovery Plan, dibuat dan dirancang untuk segera menangani teknologi informasi yang mengalami down yang menyebabkan proses bisnis tersebut gagal agar dapat terus berjalan pasca terjadinya keadaan darurat (Barnes, 2001). Pada dasarnya DRP dirancang untuk menyediakan kemampuan dan sumberdaya untuk memulihkan teknologi informasi ke suatu lokasi cadangan untuk sementara yang disebut Disaster Recovery Center dimana bencana dapat timbul sewaktu-waktu di lokasi utama sehingga proses bisnis akan berjalan diluar normal. Dibutuhkan perencanaan yang matang dalam pemilihan lokasi cadangan tersebut, dikarenakan data dan informasi penting perusahaan akan disimpan di lokasi tersebut serta biaya yang akan digunakan dalam implementasi DRP oleh perusahaan PT. XYZ.

Pada saat ini PT. XYZ belum memiliki rancangan Disaster Recovery Plan untuk perusahaannya, dan dengan hal ini PT. XYZ hendaknya mengimplementasikan Disaster Recovery Plan agar dapat menghindari kegagalan aset teknologi

informasi tersebut. Terkait dengan itu didalam penelitian ini akan menghasilkan perancangan Disaster Recovery Plan terkait teknologi yang disusun dengan identifikasi teknologi informasi eksisting dan akan dirancang sesuai dengan kebutuhan infrastruktur teknologi informasi tersebut untuk dapat melakukan tugasnya dalam mendukung proses bisnis perusahaan. Diharapkan rancangan tersebut dapat memenuhi strategi PT. XYZ dalam keadaan recovering disaster.Dari masalah yang telah dijelaskan, pada tugas akhir ini DRP terkait teknologi dirancang untuk mencegah proses bisnis PT XYZ dari gangguan bencana yang akan mengganggu keberlangsungan proses bisnis PT XYZ tersebut.

Rumusan masalah pada penelitian ini adalah bagaimana perancangan *Disaster Recovery Plan* terkait teknologi pada PT. XYZ dalam hal jaringan, aplikasi, dan *database* serta *fileserver* serta bagaimana penentuan jenis *Disaster Recovery center* untuk PT. XYZ?

Tujuan dari penelitian ini adalah memberikan perancangan *Disaster Recovery Plan* pada teknologi terkait jaringan, aplikasi, dan *database* serta *fileserver* di PT. XYZ serta memberikan rekomendasi jenis *Disaster Recovery Center* untuk PT. XYZ.

2. Tinjauan Pustaka

1. *Disaster Recovery Plan*

Disaster Recovery Plan adalah bagian dari Business Continuity Plan yang merupakan suatu acuan berisikan prosedur untuk merespon kejadian yang mengakibatkan hilangnya sumber daya sistem informasi oleh bencana, menyediakan operasi cadangan selama sistem terhenti, dan mengelola proses pemulihan serta penyelamatan sehingga mampu meminimalisir kerugian yang dialami oleh perusahaan. Tujuan utama dari Disaster Recovery Plan adalah menyediakan sumber daya untuk mejalankan proses vital dan untuk meminimalisir kerugian perusahaan. Karena bertindak sebagai pegangan saat terjadinya keadaan darurat, Disaster Recovery Plan tidak dapat disusun secara sembarangan, Disaster Recovery Plan yang tidak sesuai dapat berakibat lebih buruk bagi keberlangsungan organisasi daripada bencana itu sendiri. Disaster Recovery Plan menyediakan kemampuan dalam menerapkan proses kritis di lokasi lain dan mengembalikannya ke lokasi dan kondisi semula dalam suatu batasan waktu yang memperkecil kerugian kepada organisasi, dengan pelaksanaan prosedur recovery yang cepat.

2. Recovery Time Objective (RTO)

RTO didefinisikan sebagai waktu maksimum sebuah sistem untuk down sebelum adanya dampak yang tidak diinginkan dari rangkaian sistem lainnya yang mendukung proses bisnis perusahaan tersebut.

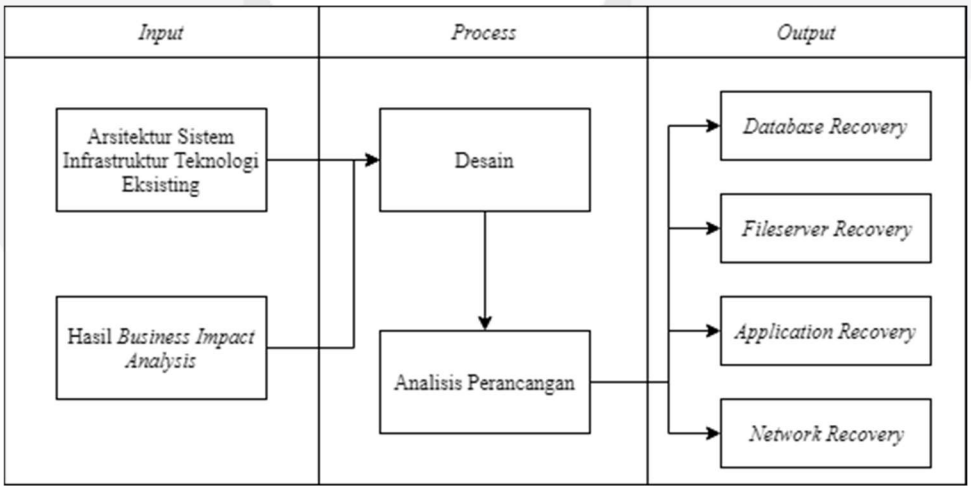
3. Recovery Point Objective (RPO)

RPO didefinisikan tentang jumlah toleransi minimum data dari sebuah sistem yang bisa direstorasi dari proses pemulihan yang akan dilakukan.

4. Disaster Recovery Center

Data center merupakan denyut nadi bisnis suatu perusahaan, bila suatu saat terjadi gangguan atau bencana alam yang tidak dapat diprediksi sebelumnya maka dijamin akan terjadi kelumpuhan pada beberapa sector bisnis atau mungkin keseluruhan sektor bisnis yang dimiliki perusahaan. Oleh karenanya, aspek penting yang harus dimiliki oleh semua data center adalah manajemen bencana yang baik dan telah teruji sehingga sewaktu-waktu hal tersebut terjadi tidak menimbulkan dampak yang terlalu merugikan perusahaan.

3. Metodologi Penelitian



Gambar 2. Model konseptual

Gambar 2 menjelaskan tentang bagaimana mendapatkan data-data organisasi perusahaan dengan melakukan penelitian. Tahap penelitian dimulai dengan mendapatkan dokumen-dokumen organisasi, seperti Arsitektur Sistem Eksisting dan Hasil Business Impact Analysis. Dokumen-dokumen tersebut akan digunakan pada tahapan rancangan disaster recovery plan terkait teknologi yang akan menjadi tiga atas kebutuhan perusahaan tersebut yaitu teknologi data. Hasil penelitian tersebut akan dianalisis dan menghasilkan rekomendasi DRP terkait teknologi..

4. Pengumpulan dan Identifikasi data

4.1 Identifikasi Aset PT XYZ

Pada tahap ini adalah mengidentifikasi aset infrastruktur teknologi yang terdapat di PT XYZ. Identifikasi aset infrastruktur teknologi dapat memberikan informasi terkait perancangan data dan database recovery serta network recovery. Tabel dibawah ini menujukkan daftar aset perusahaan tersebut..

Tabel 1. Aset PT XYZ

ID	Aset	Kategori	Contoh
A	Server	*Main System* Server	• Server Email (Zimbra CS 8.0.4) • Server Active Directory + DNS Internal • Server Proxy Internet
		Development Server	• Server Web • Server Web Aplikasi Proxy (WAP)
		Additional Server	• Windows System Update Server (WSUS) • Server Network Access Storage (NAS) • Server DNS Public • Server Nagios Network Monitoring System (NMS) • Server Media dan FTP Internal
		Application Server	• Server E-procurement • Server ERP Agresso • Server Aplikasi Perusahaan (aplikasi SIM (aplikasi HRIS, aplikasi monitoring proyek, aplikasi monitoring marketing)) • Server Aplikasi Pengadaan • Server Aplikasi Cash Flow • Server aplikasi monitoring Pengadaan

4.2 Identifikasi RTO dan RPO Server

Berikut ini merupakan tabel RTO dan RPO dari hasil rancangan Business Impact Analisys di server aplikasi PT XYZ yang akan jadi acuan frekuensi backup dan recovery.

Tabel 2. Tabel RTO dan RPO

No	Nama Aplikasi	Server	RTO	RPO
1	ERP Agresso	ERP Agresso	4 Jam	1 Jam
2	Aplikasi Cash Flow	AppServer-2	4 Jam	1 jam
3	Aplikasi Pengadaan	SISFO-intern2	4 Jam	1 jam
4	Aplikasi *e-Procurement*	e-Procurement	4 Jam	1 jam
5	Aplikasi Monitor Pengadaan	SISFO-intern2	4 Jam	1 jam
6	Aplikasi SIM	SISFO-intern2	4 Jam	1 jam
7.	Jaringan Data Center		4 jam	

4.3 Identifikasi Aplikasi

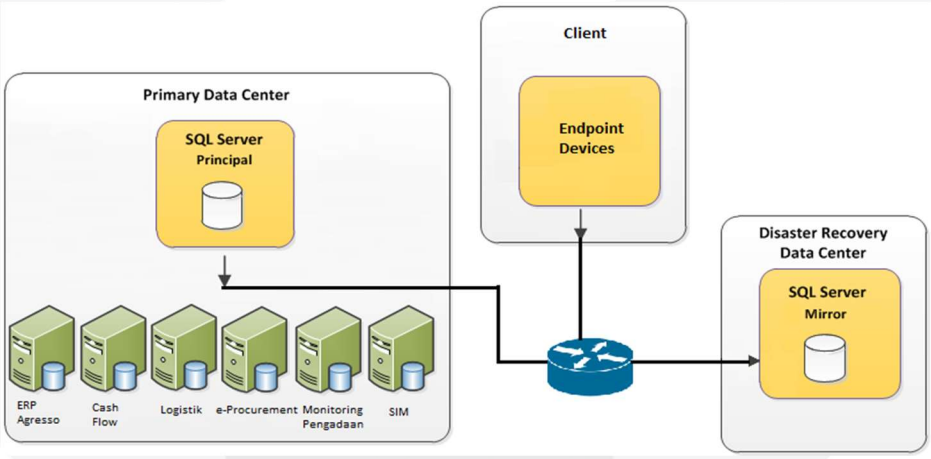
Pada tahap ini adalah mengidentifikasi aplikasi yang berjalan di sistem operasi Microsoft Windows yang terdapat pada PT XYZ. Berikut ini merupakan daftar dan penjelasan aplikasi-aplikasi tersebut.

1. ERP Agresso
   Merupakan aplikasi yang digunakan perusahaan sebagai pengolah dan menjalankan ERP. Aplikasi ini digunakan di seluruh proses bisnis dan digunakan oleh semua divisi.
2. Aplikasi Cash Flow
   Aplikasi ini merupakan salah satu aplikasi yang dibuat dan dikembangkan sendiri oleh perusahaan, aplikasi ini digunakan oleh bagian keuangan perusahaan sebagai pengolah alur keuangan.
3. Aplikasi Logistik
   Aplikasi ini juga merupakan salah satu aplikasi yang dibuat dan dikembangkan sendiri oleh perusahaan, aplikasi ini digunakan sebagai pengelola logistik perusahaan yang mempunyai fungsi untuk melakukan proses pengadaan.
4. Aplikasi e-Procurement
   Aplikasi yang seluruh permintaan pengadaan diberikan melalui aplikasi web (brosur, dokumen, dsb).
5. Aplikasi Monitoring Pengadaan
   Aplikasi ini juga termasuk aplikasi yang dibuat sendiri oleh perusahaan untuk dapat memudahkan dalam melakukan pemantauan pengadaan, baik itu bahan baku, barang jadi, maupun produk perusahaan yang mempunyai fungsi untuk melacak barang.
6. Aplikasi SIM
   Merupakan pengembangan dari beberapa aplikasi yang dibuat dan digunakan oleh perusahaan ini, terdiri dari: (a) Aplikasi Monitoring Proyek; (b) Aplikasi Human Resource Information System, dan; (c) Aplikasi Monitoring Marketing / Perolehan Kontrak.

5. Perancangan

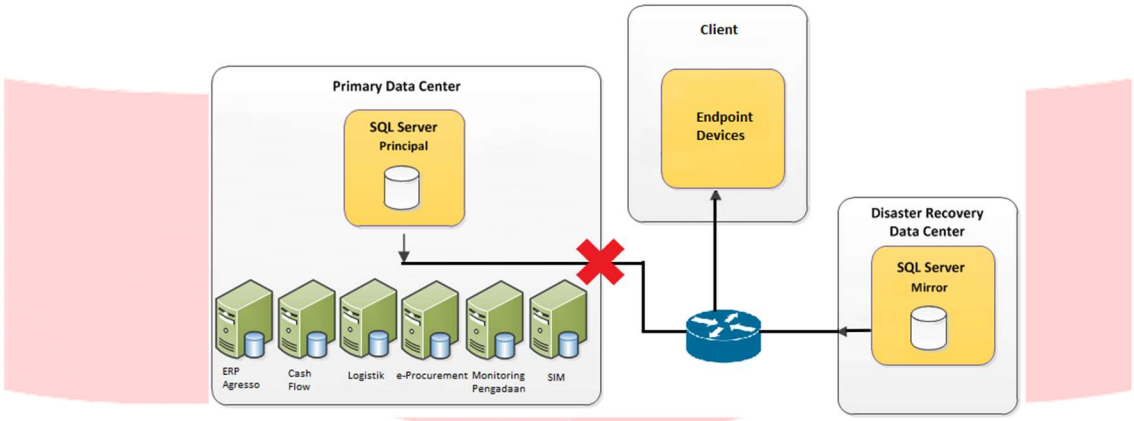
5.1 Backup dan Recovery Database

Dalam melakukan Disaster Recovery Plan terkait teknologi database, terdapat alternatif yaitu database mirroring SQL Server yang akan disimpan disaster recovery center, alternatif ini mempunyai dua jenis yaitu database mirroring high-safety dan database mirroring high-perfomance. Server utama dalam database mirroring biasa disebut sebagai server principal, sedangkan server cadangan biasa disebut server mirror. Dalam kondisi normal, client akan mengakses database ke server principal. Ketika terjadi update transaksi database pada server principal, duplikasi database dan log akan terjadi secara otomatis terjadi di server mirror. Proses duplikasi transaksi tersebut melibatkan setiap adanya operasi insert, update, dan delete yang berubah. Gambar V.1 berikut merupakan ilustrasi proses database mirroring dalam kondisi normal.



Gambar 3. Database Mirroring SQL Server Kondisi Normal

Di kondisi bencana, server principal akan mengalami gangguan sehingga tidak dapat diakses, server mirror akan mengambil peran server principal untuk client dalam pengaksesan database. Gambar V.2 berikut ini merupakan gambar kondisi bencana pada database mirroring.



Gambar 4. Database Mirroring SQL Server Kondisi Bencana

Dalam menentukan metode database recovery yang akan dipilih untuk memenuhi target RPO, akan dilihat dari tabel perbandingan berikut.

Tabel 3. Perbandingan Jenis Database Mirroring SQL Server

Disaster Recovery SQL Server	RPO	(RTO)
Database Mirroring - High-safety with automatic failover	*Zero*	*Seconds*
Database Mirroring - High-safety with manual failover (forced service)	*Zero*	*Minutes*
Database Mirroring - High-performance with manual failover (forced service)	*Seconds*	*Minutes*

(Sumber: LeRoy Tuttle, Jr., 2012)

Menganut pada acuan RPO yang dimiliki oleh server yang berhubungan dengan aplikasi memiliki waktu maksimal satu jam RPO yaitu terdapat satu jam tingkat konsistensi data di server cadangan yang dapat telat dari server utama, yang mempunyai arti bahwa ketiga tipe database mirroring dapat dilakukan. Jika mengacu pada acuan budget, jenis mirroring high-safety dengan automatic failover membutuhkan budget yang lebih mahal karena diharuskan menambah server witness untuk melakukan failover. Dilain pihak mirroring high-safety membutuhkan budget yang lebih besar karena bandwidth yang digunakan pun lebih besar. Server mirror membutuhkan proses pencatatan transaksi dan informasi pencatatan transaksi tersebut akan dikirim kembali ke server principal tidak seperti metode mirroring high-performance yang pencatatannya hanya terjadi di server. Dikarenakan keterangan diatas, maka database mirroring high-performance yang akan dipilih dalam kasus PT. XYZ karena penggunaan sumberdaya koneksi bandwidth dan budget akan lebih efisien, dan jenis database mirroring ini tetap dapat memenuhi RPO server maksimal 1 jam yang dimiliki oleh perusahaan. Berikut ini merupakan tabel analisis kelebihan dan kekurangan untuk rekomendasi database recovery.

5.2 Backup dan Recovery Fileserver

Dalam menentukan metode fileserver recovery yang akan dipilih untuk memenuhi target RPO, akan dilihat dari tabel perbandingan berikut.

Tabel 3. Perbandingan Jenis Fileserver Recovery

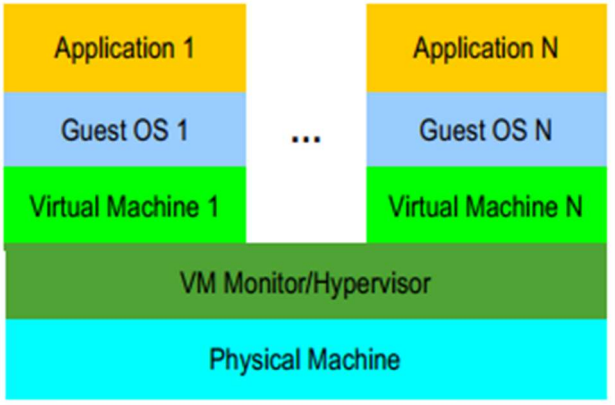
Tipe *Replication*	Jarak	Bandwidth	RPO
SnapMirror Synchronous	Sampai dengan 150km	*Bandwidth* yang dibutuhkan tinggi	*Zero* RPO (replikanya identik setiap waktu)
SnapMirror Asynchronous	Tidak terpengaruh jarak.	*Bandwidth* lebih rendah	RPO lebih dari 0 sampai 30 menit.

Mengacu pada RPO yang dimiliki oleh server yang mempunyai hubungan dengan aplikasi yaitu semua server tersebut memiliki waktu 1 jam RPO yaitu terdapat 1 jam tingkat konsistensi data di server cadangan yang dapat telat dari server

utama, yang mempunyai bahwa kedua tipe replikasi dapat memenuhi RPO tersebut. SnapMirror synchronous replication menggunakan bandwidth yang lebih besar daripada asynchronous karena jika data center utama mengalami update data fileserver maka harus secara real-time untuk disaster recovery center melakukan update fileserver juga, bandwidth yang semakin besar mempunyai arti biaya yang digunakan juga besar. Jika dilihat dari faktor jarak, snapmirror replication synchronous tidak boleh berjarak lebih dari 150km karena akan menimbulkan latency yang tinggi yang tidak dapat ditolerir oleh jenis replikasi ini, sedangkan untuk tipe snapmirror replication asynchronous tidak terperanguh jarak karena tipe replikasi ini tidak harus secara real-time dalam melakukan replikasi, yang menjadikan latency yang tinggi masih bisa ditolerir. Maka dalam fileserver recovery, tipe replikasi snapmirror asynchronous akan dipilih karena tipe ini lebih efisien dalam penggunaan sumber daya tanpa mengorbankan kebutuhan RPO server yang dimiliki perusahaan PT. XYZ. Berikut ini merupakan tabel analisis kelebihan dan kekurangan dari metode fileserver recovery yang telah dipilih.

5.3 Backup dan Recovery Application

Dalam menentukan metode mana yang akan dipilih, akan melihat pada acuan RTO. Kondisi RTO server tersebut memiliki waktu 4 jam yang berarti karyawan perusahaan memiliki waktu maksimal 4 jam untuk tidak bisa mengakses aplikasi yang berakibat proses bisnis tidak akan berjalan sebagaimana mestinya. Dilihat dari kedua metode, kedua metode tersebut dapat memenuhi target 4 jam RTO karena jika diasumsikan RTO tersebut dihitung dari berapa lama aplikasi di server cadangan tersebut untuk siap diakses. Tetapi jika mengacu pada keefisienan yang dipakai untuk menggunakan kedua metode tersebut, metode P2P merupakan metode yang paling tidak efisien dalam segi sumberdaya maupun biaya, karena metode P2P diharuskan mempunyai konfigurasi perangkat keras maupun perangkat lunak yang identik. Seperti pada kasus di PT. XYZ, perusahaan ini mempunyai konfigurasi tujuh server aplikasi yang berjalan untuk menunjang proses bisnis perusahaan. Jika metode P2P yang dipilih, maka server cadangan pun harus mempunyai konfigurasi tujuh server juga. Sedangkan metode P2V memanfaatkan teknologi virtualisasi yang memungkinkan beberapa server berjalan diatas satu server fisik, maka dalam rekomendasi application recovery, metode yang dipilih yaitu P2V. Berikut ini merupakan tabel analisis kelebihan dan kekurangan atas metode application recoery yang dipilih.



Gambar 5. Virtualisasi
(Sumber: Jim Metzler, 2011)

5.4 Backup dan Recovery Network

Perbedaan dari proses failover tersebut adalah dimana router public mengirimkan paket PING untuk pengecekan. Jika dalam simple failover, pengiriman paket PING hanya di kirim ke router DC1 dan router DC2, selama keadaan router tersebut masih up, simple failover tidak dapat mendeteksi komponen jaringan setelah router DC1 dan router DC2 sehingga failover tidak akan berjalan. Sedangkan dalam recursive failover, pengiriman PING akan dikirim sampai ke server, jika paket PING tidak sampai dikirim ke server yang dikarenakan akses menuju server mengalami kegagalan ataupun server tersebut mengalami kegagalan, maka proses failover akan langsung berjalan.

Kedua proses failover ini akan berjalan secara otomatis. Saat kondisi bencana, DRC akan mengambil peran utama DC lalu semua data-data yang sudah terbackup di DRC akan dilakukan proses recovery agar proses bisnis yang menggunakan data-data tersebut tetap bisa diakses oleh client saat link menuju DC tidak dapat diakses. Kondisi eksisting jaringan PT. XYZ mempunyai RTO 4 jam yang berarti waktu maksimal data center untuk tidak bisa diakses selama 4 jam. Dalam RTO, semakin kecil waktu RTO semakin baik karena waktu downtime jaringan tersebut semakin kecil. Kedua failover tersebut mempunyai RTO nyaris nol dikarenakan jalur pengaksesan data tetap terjamin dengan adanya proses otomatis yang diberikan jika RTO tersebut dihitung dari berapa lama link utama dapat berpindah ke link cadangan. Tetapi jika dalam faktor reliability, maka recursive failover akan dipilih karena proses pengiriman PING terjadi sampai ke server. Berikut ini merupakan tabel analisis kelebihan dan kekurangan dari metode network recovery yang dipilih.

5.5 Disaster Recovery Center

Dalam menentukan jenis disaster recovery center mana yang akan dipilih oleh PT. XYZ, akan dilihat dari faktor security data, biaya operasional maupun kompleksitas dari jenis DRC tersebut. Jenis DRC in-house mempunyai tingkat security

data yang paling baik dari jenis DRC yang lain, tetapi mempunyai biaya operasional dan kompleksitas yang paling tinggi diantara DRC yang lain. Sedangkan jenis DRC colocation dan private cloud adalah jenis DRC yang mempunyai tingkat security data dibawah jenis DRC ¬in-house tetapi mempunyai biaya operasional dan kompleksitas yang lebih rendah dari jenis DRC ¬in-house, sedangkan untuk jenis DRC public cloud merupakan jenis DRC yang mempunyai tingkat security data yang paling rendah dari jenis DRC yang lain, sedangkan untuk biaya operasional DRC ini paling kecil dan mempunyai kompleksitas yang paling rendah.

Dikarenakan semua jenis DRC dapat memenuhi kebutuhan PT. XYZ dalam kebutuhan recovering disaster, maka jenis DRC yang akan dipilih adalah jenis public cloud. Meskipun public cloud mempunyai tingkat security data yang paling rendah, tetapi jenis DRC tetap dapat memberikan tingkat sekuritas data yang baik karena pihak ketiga yang menyediakan public cloud tersebut memberikan Service Level Agreement yang disetujui oleh PT. XYZ saat penyetujuan kontrak kerjasama. Dilain pihak, biaya operasional dan kompleksitas yang paling rendah merupakan nilai tambah mengapa jenis DRC ini yang direkomendasikan untuk dipilih oleh perusahaan PT. XYZ.

6. Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan, maka dapat disimpulkan bahwa:

1. Perancangan Disaster Recovery Plan terkait teknologi pada perusahaan PT. XYZ antara lain
   a. Untuk DRP terkait teknologi recovery data database akan menggunakan database mirroring high-perfomance agar proses recovering disaster untuk teknologi data database dapat dilakukan dan menggunakan sumberdaya yang efisien.
   b. Untuk DRP terkait teknologi recovery data fileserver akan menggunakan snapmirror asynchronous replication untuk proses recovering disaster terkait teknologi data fileserver.
   c. Untuk DRP terkait teknologi recovery aplikasi akan menggunakan metode P2V untuk mengefisiensikan sumberdaya yang digunakan oleh perusahaan.
   d. Untuk DRP terkait teknologi recovery jaringan akan menambah link jaringan untuk diinterkoneksikan dengan disaster recovery center dan memanfaatkan teknologi di perangkat mikrotik dengan metode recursive failover agar proses failover dilakukan secara otomatis jika link utama tidak bisa diakses karena gangguan.
2. Rekomendasi jenis disaster recovery center yang akan digunakan oleh PT. XYZ adalah public cloud untuk mengefisiensikan sumber daya yang digunakan oleh perusahaan tanpa mengesampingkan faktor security data yang dibutuhkan oleh PT. XYZ dalam melakukan proses disaster recovery plan.

Referensi:

Swanson, M., Bowen, P., Wohl, A.P., Gallup, D., & Lynes, D. (2010): Contingency Planning Guide for Federal Information Systems., National Institute of Standards of Technology, Gaithersburg.

Freddy, A.S., Firmansyah, G., Mukarom., M. (2005): Business Continuity Planning and Disaster Recovery Planning., MTI UI., Depok

Brouwer. P. (2011): The Art of Replication., Oracle Corporation., USA.

Tuttle, L.J. (2012): Microsoft SQL Server AlwaysOn Solutions Guide

for High Availability and Disaster Recovery., Microsoft., USA

Vivek, Kumar, (2012): Using AlwaysOn Availability Groups for High Availability and Disaster Recovery of Data Quality Services., Microsoft., USA.

Dewiyanti, Rachmi. (2011): Perencanaan dan Perancangan Data Center dan Disaster Recovery Center di PT. Pos Indonesia., Universitas Telkom., Bandung

Pawana, I.G.N.A. (2016): Perancangan Server Dengan Menggunakan Virtualisasi, Load Balancer, Failover, dan Database Replication (Studi Kasus: IKIP PGRI BALI)., Universitas Telkom., Bandung

Alapati, S. (2011): Back to Basics: SnapMirror., NetApp.

Mirzoev, Timur. (2009): Synchronous replication of remote storage., Georgia Southern University., USA

Wood, T., Cecchet, E., Ramakhrishnan, K.k., Shenoy, P., Merwe, J.v.D., Venkataramani, A. (2012): Disaster Recovery as a Cloud Service: Economic Benefits & Deployment Challenges., University of Massachusetts Amherst., U