

DATABASE DISASTERS RECOVERY PLAN: SISTEM RECOVERY DATABASE MENGUNAKAN ETL (EXTRACTION TRANSFORMATION LOADING)

Joko Prasetyana¹⁾
Sistem Informasi¹⁾
Fakultas Teknologi Informasi¹⁾
Universitas Bina Sarana Informatika¹⁾
Joko.JPA@bsi.ac.id¹⁾

Abstract

Databases Recovery System is made there are basic problems that often arise due to a lot of data in various formats so that it requires a data center to support business processes, disaster events contribute to the formation of this system, securing important data solutions that are currently acceptable, how to handle them also require steps - countermeasures for data that will be stored in the storage center. With this system will be able to share data not only in one part but in the central data so that it can be used in several parts. To make central data does not necessarily carry out system development. If there is cheaper technology to implement the system, it is hoped that companies and agencies can develop the system.

Keywords: *Information Technology, Disasters Recovery Plan, System Recovery Databases*

Abstrak

Sistem Recovery Databases dibuat atas dasar masalah yang sering timbul akibat banyak data dalam berbagai format sehingga memerlukan pusat data sebagai pendukung proses bisnis, kejadian bencana turut andil didalam terbentuknya sistem ini, mengamankan data yang penting solusi yang saat ini bisa diterima, cara penanganannya juga membutuhkan langkah-langkah penanggulangan untuk data-data yang akan disimpan di pusat penyimpanan. Dengan adanya sistem ini akan dapat membagi data tidak hanya pada satu bagian tapi pada central data agar dapat di pakai di beberapa bagian. Untuk membuat central data tidak serta merta melakukan pengembangan sistem. Jika ada teknologi yang lebih murah untuk mengimpelmentasikan sistem maka diharap perusahaan dan instansi dapat mengembangkan sistem tersebut.

Kata kunci: *Informasi, Disasters Recovery Plan, Sistem Recovery Databases*

I. PENDAHULUAN

Suatu organisasi dalam menjalankan kegiatan organisasi ada yang dilakukan dengan bantuan sistem informasi dan ada juga kegiatan yang dilakukan dengan bantuan software pengolah data semisal microsoft office. Pada saat penggunaan sistem informasi penyimpanan data dalam bentuk sistem basis data kadang menggunakan software yang berbeda juga contoh dalam dalam organisasi sistem basis data yang mungkin digunakan menggunakan SQL Server 2000, SQL Server 2008, My SQL, Microsoft Acces dll.

Disaster Recovery Planning adalah bagian dari rangkaian *Business Continuity Planning*. *Disaster*

Recovery Plan bersifat reaktif terhadap suatu bencana, berfokus pada apa yang harus dilakukan untuk mengembalikan fungsi-fungsi yang terganggu oleh bencana, sedangkan bagian-bagian lain dari *Business Continuity Planning* lebih bersifat proaktif/preventif, yaitu berfokus pada apa yang dapat dilakukan untuk mengurangi dampak bencana bila terjadi [1]. Data bila dianggap penting oleh suatu organisasi maka akan disimpan dengan baik, namun penyimpanan yang baik pun dirasa tidak cukup apabila terjadi kejadian di luar jangkauan kita misal terjadi bencana, belum lagi bentuk ancaman pengambilan data secara paksa, maka kegiatan back-up data perlu dilakukan, namun bagaimana apabila kita melakukan kegiatan

tersebut terhadap organisasi yang mempunyai berbagai macam sistem basis data, atau organisasi yang hanya setengah mengimplementasikan sistem informasi dari proses bisnis atau bagaimana kalo misal data tersebut tidak hanya pada sistem basis data namun ada dalam excel, atau yang lebih kacau data tersebut terpencar di masing-masing dibagian sedangkan bagian tersebut tidak terlalu memperhatikan pentingnya sebuah data.

II. LITERATUR DAN METODE

BI atau bisnis intelijen adalah serangkaian kegiatan untuk mengumpulkan dan menganalisis data sehingga dapat digunakan untuk proses pengambilan keputusan yang lebih baik agar dapat digunakan dalam proses pengambilan keputusan bisnis [2].

Disaster recovery plan adalah proses, kebijakan dan prosedur yang berkaitan dengan persiapan pemulihan atau keberlangsungan infrastruktur teknologi yang kritis bagi organisasi setelah terjadinya bencana, baik bencana yang disebabkan oleh tindakan manusia ataupun bencana alam. *Disaster recovery* merupakan bagian dari *business continuity*. Sedangkan *business continuity* sendiri merupakan aktivitas yang dilakukan oleh organisasi untuk menjamin bahwa fungsi bisnis kritis dapat tetap tersedia bagi konsumen, supplier dan pihak-pihak lainnya yang berkepentingan. Perencanaan *disaster recovery* mengacu pada persiapan untuk menghadapi bencana dan respon yang harus diberikan ketika bencana terjadi. tujuan DRP adalah keberlangsungan (*continuity*) atau kemampuan organisasi untuk bertahan (*survival*) dalam menghadapi bencana (Proses penyusunan DRP meliputi analisis, perencanaan, pembuatan DRP, pengujian dan revisi periodik berdasarkan kondisi bisnis terkini. Beberapa jenis bencana yang dapat mengancam bisnis dapat dikelompokkan berdasarkan penyebab sebagai berikut: bencana alam, bencana akibat kegagalan alat-alat, akibat kegagalan aspek keamanan, dan situasi lingkungan seperti demonstrasi, terorisme, perang, sabotase dan lain-lain. Berbagai macam penyebab kejadian bencana di atas, dapat berpotensi menyebabkan kerusakan pada gedung, peralatan dan sistem teknologi informasi. Dampak bencana terhadap organisasi dapat berupa *direct damage* (kerusakan langsung alat-alat dan gedung), *inaccessibility* (fasilitas tidak dapat diakses), *utility outage* (tidak tersedianya infrastruktur pendukung seperti listrik, air dan sebagainya), *transportation disruption*, *communication disruption*, *evacuation* dan *worker absenteeism*. Dampak tersebut dapat menghentikan

bisnis baik untuk sementara atau hingga jangka waktu tertentu. Jika terhentinya bisnis ini terus berlanjut, dapat mengakibatkan pindahannya para konsumen ke pelaku bisnis lainnya [3].

III. METODE

Pengembangan Sistem Databases Disasters Recovery Plan bertahap sebagai berikut:

1. Risk Assessment

Risk Assessment adalah proses identifikasi ancaman-ancaman yang mungkin terjadi, baik yang berasal dari dalam, maupun dari luar. Bencana yang dianalisa termasuk bencana alam, bencana kegagalan teknis, maupun ancaman-ancaman faktor manusia.

2. Priority Assessment

Saat suatu bencana terjadi dan mengganggu berbagai macam proses bisnis dan operasi, sangatlah penting untuk memiliki urutan prioritas proses yang jelas. Prioritas dapat diurutkan berdasarkan banyak hal. Dari segi arsitektur misalnya, server/ router manakah yang menjadi prioritas dalam dipulihkan? Data mana yang harus lebih dahulu diselamatkan? Begitu juga dengan proses, prioritas pemulihan harus terurut dengan jelas. Proses yang dianggap paling vital untuk keberlangsungan sistem nantinya akan mendapatkan alokasi perhatian paling besar untuk dipulihkan kembali sebelum proses-proses lainnya. Dengan demikian tujuan dari pembangunan *Disaster Recovery Plan*, yaitu untuk memastikan sistem dapat berfungsi sebaik mungkin secepat mungkin setelah gangguan suatu bencana, dapat terlaksana *Recovery Strategy Selection*

3. Recovery Strategy

Hasil yang didapatkan dari tahap *risk assessment* dan *priority assessment* kemudian akan digunakan sebagai masukan untuk menentukan strategi pemulihan seperti apa yang sebaiknya disusun. Strategi pemulihan akan mencakup isu seperti lokasi cadangan dan metode pemulihan yang akan dilakukan.

4. Plan Documenting

Hasil analisa dan rancangan strategi yang sudah dihasilkan dari tahapan-tahapan sebelumnya tidak akan berarti apa-apa jika tidak terdokumentasi dengan baik. Saat terjadi bencana, personel-personel yang mengerti benar akan *Disaster Recovery Plan* yang sudah dirancang mungkin tidak akan sepenuhnya tersedia, atau bahkan sudah tidak aktif di organisasi tersebut. Karena itu *Disaster Recovery Plan* haruslah didokumentasikan dengan terstruktur sehingga mudah dipahami saat dibutuhkan.

IV. HASIL DAN PEMBAHASAN

Langkah pertama dalam membuat Databases Disasters Recovery Plan adalah risk assessment.

1. Risk Assesmen

Setiap bencana memiliki atribut-atribut yang dapat diboboti untuk menentukan nilai ancam, atribut bencana yang akan digunakan dalam pembahasan ini adalah *Likelihood, Restoration Time, Predictability*. Pembobotan dilakukan dengan cara wawancara, observasi. Wawancara dilakukan dengan pihak-pihak yang terkait di institusi tersebut antara lain dengan pihak biro layanan teknologi informasi, pihak biro ketenagaan, keuangan dan asset. Dari hasil wawancara tersebut dapat dilihat dalam tabel berikut:

No	Ancaman	Likelihood (0-10)	Restoration Time (0-10)	Predictability (0-3)	Score
1	Mati Listrik	6	4	2	48
2	Kebakaran	3	4	2	24
3	Kerusakan Alat	5	5	2	50
4	Kerusakan Perangkat Lunak	5	4	1	20
5	Banjir	5	6	1	30
6	Gempa (Ringan)	6	7	1	42
7	Kerusakan gedung	3	6	2	36
8	Kerusakan Jaringan	6	4	2	48

2. Priority Assessment

Sistem informasi yang digunakan di perguruan tinggi ini meliputi perangkat keras, perangkat lunak, jaringan dan data. Jika bencana terjadi dan mengakibatkan komponen sistem tersebut terancam, manakah urutan prioritas yang di utamakan di kembalikan, untuk mengetahui hal tersebut tentu menggunakan beberapa atribut untuk meninjau hal tersebut, atribut-atribut antara lain: *necessity, recoverability, dan replaceability*.

Tabel skala attribute prioritas

No	Necessity	Recoverability	Replaceability
1	Sistem tetap dapat berfungsi sempurna walaupun elemen tidak ada.	Elemen dapat dengan mudah diperbaiki, tenaga ahli sangat mudah ditemui, dengan waktu perbaikan sangat singkat.	Elemen dapat digantikan dengan mudah tanpa biaya maupun usaha yang berarti
2	Sistem mengalami hambatan/delay dalam menjalankan fungsinya jika	Elemen dapat dengan mudah diperbaiki, tenaga ahli sangat mudah ditemui, namun dengan waktu perbaikan yang	Elemen dapat digantikan dengan yang lain namun tetap membutuhkan biaya dan atau

	elemen tidak ada.	berdampak pada sistem	usaha yang cukup besar.
3	Sistem hanya dapat menjalankan fungsi-fungsi vital jika elemen tidak ada.	Elemen cukup sulit diperbaiki, tenaga ahli cukup sulit ditemui, dan dengan waktu perbaikan yang dapat mengganggu sistem.	Elemen dapat digantikan dengan yang lain namun tetap membutuhkan biaya dan atau usaha yang cukup besar.
4	Sistem hanya dapat menjalankan fungsi-fungsi vital jika elemen tidak ada.	Elemen sangat sulit diperbaiki, tenaga ahli sangat sulit ditemui, dan membutuhkan waktu perbaikan yang sangat panjang.	Elemen dapat digantikan dengan yang lain namun tetap membutuhkan biaya dan atau usaha yang cukup besar.
5	Sistem tidak dapat berfungsi sama sekali jika elemen tidak ada.	Elemen hampir tidak mungkin untuk diperbaiki	Elemen bersifat unik dan tidak dapat digantikan dengan apapun.

Hasil dari *Priority Assessment* dapat dilihat dalam tabel berikut:

No	Elemen	Necessity	Recoverability	Replaceability	Priority Value
1	Perangkat Keras	5	2	2	20
2	Perangkat Lunak	5	3	4	60
3	Jaringan	5	2	4	40
4	Data	5	4	5	100

3. Strategy Selection

Pada tahap *Risk Assessment* telah didapatkan daftar berbagai macam jenis ancaman terhadap ISTA berikut dengan nilai atribut-atribut bencana tersebut. Selanjutnya pada tahap *Priority Assessment* didapatkan dua jenis lokasi penting bagi yaitu Gedung Utama dan lingkungan Kampus Institut Sains Dan Teknologi Al-Kamal (ISTA). Untuk menentukan strategi pemulihan yang sebaiknya dilakukan, akan dilakukan klasifikasi tambahan terhadap bencana-bencana dengan mempertimbangkan lingkup kerusakan yang dapat disebabkan olehnya. Di bawah ini adalah istilah yang akan digunakan untuk melakukan klasifikasi tersebut.

Lingkup A: digunakan untuk menandai ancaman bencana yang jika terjadi hanya akan mempengaruhi salah satu lokasi vital ISTA (baik sebagian maupun seluruh lokasi tersebut).

Lingkup B: digunakan untuk menandai ancaman bencana yang jika terjadi akan mempengaruhi kedua lokasi vital ISTA dan lingkungan sekitarnya.

Apabila sebagian besar ancaman yang telah didaftar merupakan ancaman dengan lingkup A, maka kebutuhan ISTA akan dibuat *mirror site* (lokasi cadangan) dengan menggunakan metode ETL. Jika diinginkan pun, *mirror site* dapat diletakkan di bagian yang berbeda dari lokasi tersebut, misalnya, meletakkan *server repository* cadangan di lantai 1 yang berbeda dengan *repository* utamanya.

A. Strategi Pemulihan Bencana Lingkup A

Bencana-bencana yang tergolong dalam lingkup A umumnya merupakan bencana yang mendapatkan nilai cukup tinggi dalam *Risk Assessment*, dengan demikian dapat disimpulkan paling mengancam. Kerusakan alat dan pencurian alat misalnya, tidak memerlukan keberadaan sebuah *mirror site* untuk menangani pemulihannya, sesuai dengan deskripsi bencana lingkup A. Kedua bencana di atas dapat ditanggulangi dengan perbaikan ataupun penggantian komponen. Untuk menekan waktu pemulihan yang dibutuhkan, dapat diadakan pencadangan perangkat keras yang rawan rusak atau dicuri, seperti *router*, *access point*, dan lain lain. Cadangan ini dapat disimpan di tempat yang tidak jauh (masih dalam lokasi yang sama), maupun dicadangkan pada pihak ketiga selaku supplier.

B. Strategi Pemulihan Bencana Lingkup B

Bencana-bencana yang tergolong dalam Lingkup B merupakan bencana yang bersifat destruktif dan memiliki lingkup luas. Bencana-bencana semacam ini umumnya ditanggulangi dengan alternatif pembuatan *mirror site* di lokasi yang berada di luar area lokasi vital. Diharapkan dengan demikian, saat lokasi-lokasi vital terpengaruh oleh terjadinya bencana dan mengalami kerusakan/ gangguan operasi, lokasi cadangan yang diletakkan di luar area akan tetap aman, lebih baik lagi jika lokasi cadangan juga dapat mengambil alih tanggung jawab yang harus dilakukan oleh lokasi vital.

a. Lokasi Mirror Site

Untuk lokasi, yang harus diperhatikan adalah jarak dari lokasi utama, ketersediaan sumber daya yang dibutuhkan, dan terlindung atau tidaknya lokasi cadangan tersebut dari bencana yang mengancam lokasi utama (keduanya tidak boleh terganggu oleh bencana yang sama dalam satu waktu). Selain hal tersebut, jarak juga harus diperhatikan, karena jarak yang jauh dari lokasi utama berarti tambahan alokasi dana untuk melakukan perawatan. Jarak yang terlalu jauh juga akan menyulitkan jika suatu saat lokasi tersebut dibutuhkan untuk menjadi lokasi operasional

pengganti sementara saat lokasi utama mengalami gangguan bencana. Terdapat alternatif untuk menyewa pihak ketiga yang berpengalaman untuk mengelola dan menjaga lokasi cadangan. Bagi organisasi yang hanya memiliki lokasi induk yang terpusat, alternatif ini jauh lebih murah dan terjamin dibandingkan dengan mencari lokasi baru, membeli/ menyewa tempat tersebut, membangun infrastruktur yang dibutuhkan disana, mengalokasikan sumber daya manusia yang diperlukan untuk mengelolanya, dan banyak lagi.

b. Infrastruktur Mirror Site

Infrastruktur yang dapat dikatakan primer untuk diadakan di lokasi cadangan adalah *server* basis data, *server repository* perangkat lunak, dan perangkat keras pendukung jaringan yang memungkinkan terjadi lalu lintas data dari lokasi utama ke lokasi cadangan. Untuk infrastruktur lain seperti meja, bangku, dan alat-alat fasilitas operasional, tidak perlu diadakan karena lokasi cadangan ini hanya akan diperuntukkan untuk menyimpan *server* basis data dan *repository* perangkat lunak. Jika nantinya terjadi hal yang membuat suatu lokasi operasi harus diadakan, pengadaan perlengkapan kantor juga tidak akan terlalu sulit meninjau letak dari lokasi cadangan.

c. Pengambilan Data Mirror Site

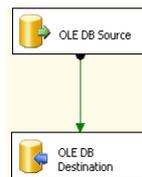
Pengambilan data yang penting atau tidak melalui tahapan wawancara sehingga sistem mengetahui data mana yang akan di cadangkan, sebagian contoh data penting pihak PMB yang akan di ambil meliputi

Tabel 4.1 pada Data PMB

No.	Tabel Name	Description
1	sekolah	Menyimpan data sekolah SMU dan SMK
2	Karyawan dan dosen	Menyimpan data dosen dan karyawan ista
3	Promosi	Menyimpan data promosi
4	Realisasi anggaran	Jumlah realisasi anggaran yang sudah di keluarkan untuk PMB

5	Rencana Kerja	Menyimpan data rencana kerja
6	Pendaftar Regular	Menyimpan data calon mahasiswa yang mendaftar
7	Pendaftar Karyawan	Menyimpan data calon mahasiswa yang melakukan registrasi ulang

Salah satu tampilan ETL dari *Data* cadangan terhadap table-table yang telah ditentukan, berikut gambar yang menunjukkan proses ETL.



Gambar 4.1. Proses ETL

4. *Plan Documenting*

Segala hal yang sudah didapatkan pada analisis dan tahapan-tahapan pembangunan selanjutnya akan dituangkan dalam sebuah *Disaster Recovery Plan*. Dokumentasi *Disaster Recovery Plan* yang akan disusun akan terdiri dari bagian:

1. Lingkup Dokumen dan Penjabaran Aset
2. Penilaian dan Penjelasan Risiko
3. Penilaian Prioritas
4. Langkah Pemulihan

V. KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan, maka dapat disimpulkan sebagai berikut:

1. Untuk mengidentifikasi bencana yang sering terjadi menggunakan wawancara terhadap pihak-pihak yang langsung berada di satu perguruan tinggi.
2. Pengimplementasian sistem ini menghasilkan dokumen *recovery plan* yang berguna untuk menghadapi bencana yang tak terduga, selain itu sistem ini dapat melakukan mirror side (pecadangan data) dengan menggunakan metode ETL

REFERENSI

- [1] Rachmaningrum, Nila dan Falahah, Studi Kelayakan Disaster Recovery Plan Pada Infrastruktur Jaringan Komputer (Studi Kasus Jaringan Komputer Universitas Widyatama). Seminar Nasional Informatika 2011, 30-36.
- [2] Noviandi, Rizki. Microsoft Business Intelligence dengan SQL Server 2008 R2 dan Sharepoint 2010. Microsoft SQL Server MVP, Jakarta. 2010.
- [3] Bahroni, Isa. (2010). Rancang Bangun *Data Warehouse* (Studi Kasus) Di PDAM Kabupaten Cilacap. Infotekmesin Volume 1 Edisi Juli 2010.