MENGEMBANGKAN *BUSINES CONTINUITY PLANNING (BCP)* DENGAN PENDEKATAN KUANTITATIF STUDI KASUS: SIAK –DITJEN ADMINDUK KEMENDAGRI

Muhaemin
Fakultas Teknik Informatika, Universitas Muhammadiyah Jakarta

muhaemin@ftumj.ac.id

ABSTRAK

Sebagaimana kita ketahui, beberapa tahun terakhir bencana alam sering melanda Indonesia dimulai dari yang ringan sampai yang dampaknya sangat menghancurkan. Suatu Bencana (Disaster) bisa terjadi di luar rencana (unplanned) maupun kondisi yang direncanakan (planned), Untuk itu perlu dibuat suatu rencana pencegahan dan pemulihan yang mencakup definisi yang jelas dari data atau record perusahaan yang harus dilindungi. Rencana tersebut lebih dikenal dengan nama Disaster Recovery Plan (DRP) atau Business Continuity Plan (BCP) yang cakupannya lebih luas lagi, dimana di dalamnya terdapat penerapan Disaster Recovery Center (DRC). Sebuah perencanaan penanggulangan bencana (DRP), membutuhkan pemahaman tentang analisa proses bisnis kritikal. Pemahaman ini, selain mencakup aspek teoretis harus juga mencakup aspek praktis dan teknis pengelolaan DRP. Ketersediaan sumber data dan informasi merupakan keharusan bagi proses pemahaman pengelolaan DRP. Sistem Informasi Administrasi Kependudukan (SIAK) yang dikelola oleh Departemen Dalam Negri dalam hal ini dibawah Direktorat Jenderal Administrasi Kependudukan cq Direktorat Informasi Kependudukan. Untuk menghindari resiko dan dampak dari terjadinya bencana terhadap Sistem Informasi Administrasi Kependudukan (SIAK), diperlukan tindakan preventif dan peringanan (mitigation) dengan membuat Pusat Pemulihan Bencana yang selanjutnya disebut Disaster Recovery Center. Disaster Recovery Center merupakan bagian yang integral dari Disater Recovery Plan (DRP) dan yang lebih luas lagi adalah Business Continuity Plan(BCP).

Kata Kunci: BCP, DRP, SIAK

1. PENDAHULUAN

Kegagalan Teknologi Informasi (TI) akan menyebabkan terganggunya kegiatan operasional dan dapat mengancam kelangsungan hidup perusahaan. Penyebab terjadinya bencana atau resiko ini bisa bermacam-macam, meliputi semua kemungkinan yang menyebabkan gagalnya TI dapat terjadi, meskipun kemampuan TI yang mendukung sudah sangat canggih dan dipandang aman. Resiko memiliki tingkat intensitas dan dampak kerugian yang berbeda-beda. Resiko secara umum dapat dibagi menjadi beberapa kategori:

- Bencana alam (bencana tsunami di provinsi Aceh, Gempa di Hokaido tahun 1980-an)
- Kegagalan Sistem (Kegagalan Kelistrikan, Kebakaran)
- Kesalahan Manusia
- Kriminalitas (kasus Klik BCA, pemboman di WTC, Hotel Mariot dan Kedutaan Australia di Jakarta)

Bencana seperti diatas bisa terjadi juga pada pengelola sistem informasi yang sangat

kritikal seperti Sistem Informasi Administrasi Kependudukan (SIAK) yang dikelola oleh Departemen Dalam Negri dalam hal ini dibawah Direktorat Jenderal Administrasi Kependudukan cq Direktorat Informasi Kependudukan. Untuk menghindari resiko dan dampak dari terjadinya bencana terhadap Sistem Informasi Administrasi Kependudukan (SIAK), diperlukan tindakan preventif dan peringanan (*mitigation*) dengan membuat Pusat Pemulihan Bencana yang selanjutnya disebut *Disaster Recovery Center*. Disaster Recovery Center merupakan bagian yang integral dari Disater Recovery Plan (DRP) dan yang lebih luas lagi adalah Business Continuity Plan(BCP).

Dengan demikian, penggunaan TI di suatu organisasi, perlu membangun sebuah Rencana Penanggulangan Bencana (*Disaster Recovery Plan*), DRP mampu memberikan layanan sementara dalam waktu yang cukup panjang dan dirancang untuk menangani kegagalan sistem TI yang diakibatkan oleh resiko yang bersifat besar baik dalam segi dampak dan luas arealnya.

Dampak dari bencana (*disaster*) terhadap pengelola sistem informasi dan komunikasi adalah sebagai berikut :

- Hilangnya kepercayaan atau kredibilitas terhadap pengelola sistem informasi.
- Hilangnya aset seperti data dan informasi yang bersifat kritikal.
- Kerugian berupa materi (financial), waktu dan sumber daya lain, apabila sistem informasi tidak bekerja atau rusak.
- Terhambatnya proses atau kegiatan lain akibat dari hancurnya sistem informasi dan komunikasi yang ada.

Dilihat dari perspektif manajemen, DRP membawa citra positif organisasi, termasuk di dalamnya adalah kepuasan publik yang tinggi dan tingkat kepercayaan *stakeholder* yang tinggi pula, dengan demikian akan meningkatkan pelayanan dan rasa aman dengan stakeholder Direktorat Jenderal Administrasi Kependudukan (Ditjen Adminduk) .

Saat ini Ditjen Adminduk telah menggunakan Teknologi Informasi (TI) untuk menyelesaikan proses bisnis utamanya. Hampir semua unit kerja Ditjen Adminduk telah menggunakan TI sebagai salah satu alat (tools) untuk mendukung proses bisnis mereka. Pada satu sisi, TI memang terbukti meningkatkan efisiensi, efektifitas kerja dan memberi pelayanan yang lebih baik. Namun pada sisi lain penggunaan TI memberikan dampak kerugian bila terjadi kegagalan sistem TI. Semakin tinggi ketergantungan Ditjen Adminduk terhadap TI, maka semakin tinggi pula tingkat resiko kerugian yang dihadapi.

Penerapan TI yang terintegrasi dalam mendukung operasional Ditjen Adminduk yang semakin intensif dewasa ini membawa konsekuensi semakin tergantungnya operasional proses bisnis Ditjen Adminduk terhadap TI, Sehingga jika terjadi suatu bencana yang tidak diperkirakan sebelumnya, maka operasional proses bisnis Ditjen Adminduk dapat terganggu. Menyadari hal yang demikian Ditjen Adminduk merasa perlu melakukan optimalisasi tingkat availability dan reliability dengan membangun DRP.

2. TINJAUAN TEORI

BCP

Bencana (disaster) adalah gangguan yang menyebabkan sumber daya informasi kritikal menjadi tidak beroperasi selama suatu periode waktu tertentu, memiliki dampak membayakan operasi bisnis. Gangguan tersebut dapat terjadi beberapa jam hingga beberapa hari, tergantung pada tingkat kerusakan yang dialami oleh sumberdaya informasi (ISACA 2005).

BCP (Business Continuity Plan) merupakan suatu proses yang didesain untuk mengurangi peningkatan resiko bisnis suatu organisasi dari gangguan yang tidak diharapkan terhadap fungsi/operasi kritikal (manual atau otomasi) yang diperlukan bagi kelanjutan hidup organisasi. BCP adalah program menangani resiko bisnis residual yangn tidak

dapak diatasi oleh manajemen resiko. BCP meliputi prosedur-prosedur DR (*Disaster Recovery*) dan rencana untuk kontinuitas operasi-operasi bisnis. Prosedur DR umumnya berupa rencana yang diikuti unit bisnis untuk pemulihan fasilitas operasional. Pada Domain sistem informasi, prosedur DR menangani langkah-langkah dalam pemulihan fasiltasi pengolahan teknologi informasi.

Laudon dan Laudon (2004) mendefinisikan DRP *(Disaster Recovery Plan)* sebagai rencana untuk menjalankan bisnis dalam kejadian dimana sumberdaya teknologi informasi tidak berfungsi. Rencana ini terdiri dari prosedur-prosedur organisasional dan kemampuan dalam melakukan backup pengolahan, tempat penyimpanan dan basis data. DRP juga mencakup tindakan restorasi pada layanan komputasi dan komunikasi setelah gangguan terjadi. Kontinuitas bisnis mencakup penyediaan lokasi alternatif yang memiliki komputer dan jalur telephon, backup fasilitas teknologi informasi, rencana evakuasi terkini, backup untuk laptop dan server tiap bagian/departemen, dan bantuan kepada karyawan untuk akses komunikasi dalam keadaan bencana (Tucker dalam McNurlin dan Sparague, 2004).

Beberapa area pengolahan informasi kritikal bagi institusi/koorporasi dalam BCP adalah LAN, WAN dan Server, jalur telekomunikasi dan komunikasi data, komputer dan ruang kerja, perangkat lunak dan data, media dan tempat penyimpanan data, dan tugas karyawan dan proses-proses produksi.

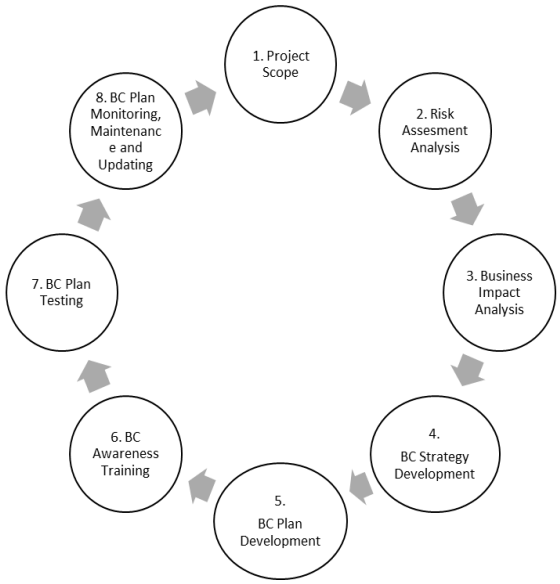
Dalam mengembangkan DRP, korporasi harus menjalankan analisis dampak bisnis untuk mengidentifikasi sistem-sistem paling kritis dan dampak dari terputusnya sistem kritis tersebut pada perusahaan. Manajemen wajib menentukan besaran waktu maksimum operasi bisnis dapat bertahan jika sistem-sistem kritis terhenti dan bagian-bagian mana dari operasi bisnis yang harus pertamakali dipulihkan. Laudon dan Laudon (2004) mengemukakan langkah-langkah berikut:

1. Melakukan penilaian resiko pada bencana-bencana tertentu yang terjadi khusus pada perusahaan seperti banjir, mati listrik, atau serangan teroris
2. Mengidentifikasi operasi/misi yang paling kritis, file yang digunakan, dan dimana file serta aplikasi tersebut bertempat.
3. Mengembangkan sebuah rencana aksi untuk menangani aplikasi kritikal seperti menggunakan proses manual atau menjalankan aplikasi tersebut di layanan DR atau backup sistem komputer ditempat lain.
4. Menguraikan tanggungjawab para staf dan prosedur-prosedur yang harus diikuti selama bencana, termasuk bagaimana mengatur tempat dan berkomunikasi dengan karyawan.
5. Menguji DRP sekurang-kurangnya sekali dalam setahun
6. Menggunakan proses perencanaan dan metodologi yang konsisten sehingga semua kelompok bisnis memahami aturan-aturan mendasar serta bagaimana pendanaan, perencanaan dan penanganan bencana tersebut.
7. Memastikan bahwa telah dimiliki dukungan penuh dari manajemen untuk memastikan pelaksaaan DR.

3. TAHAPAN PEMBANGUNAN DRP

Terdapat beberapa kerangka penyusunan (IT DRP) yang pada umumnya dapat dibagi kedalam beberapa fase, ISACA (2015) mengurai fase-fase dari siklus hidup proses BCP yaitu Lingkup Proyek, Risk Assesment, analisis dampak bisnis, Strategi pengembangan BC, Perencanaan Pengembangan BC, BC Awareness Training, BC Plan Testing dan monitoring , pemeliharaan dan pembaharuan (updating).

Tahapan Pembanguan BCP yang digunakan dalam studi kasus ini mengacu langkah-langkah BCP life cycle yang bersumber dari ISACA, sebagai berikut:



Gambar 1. Siklum Pengembangan DRP

1. Project Scope
   Pada tahap ini dilakukan ruang lingkup dari proyek, yang didalamnya termasuk menentukan area bisnis kritis yang dituju, sumber daya yang dibutukan serta waktu pengerjaan.
2. Risk Assesment Analysis
   Risk assessment adalah metode yang sistematis untuk menentukan apakah suatu organisasi memiliki resiko yang dapat diterima atau tidak. Risk assessment merupakan kunci dalam perencanan pemulihan bencana Risk assessment mencakup identifikasi risiko, analisis risiko, dan evaluasi risiko.
3. Busines Impact Analysis
   BIA digunakan untuk mengevaluasi proses kritis (dan komponen TI yang mendukungnya) dan untuk menentukan waktu pemulihan, prioritasi, sumber daya dan ketergantungannya.

Pada tahap ini dilakukan :

- Pengumpulan data sekunder berupa dokumen-dokumen awal yang berkaitan dengan Rencana Pemulihan bencana.
- Identifikasi Proses-proses bisnis yang tercakup dalam DRP, meliputi parameter-parameter yang menjadi faktor pertimbangan, kategori proses bisnis, dan identifikasi pelaksanaan proses bisnis.
- Identifikasi Jenis gangguan, mencakup kemungkinan terjadinya ancaman, kemungkinan kejadian yang muncul, dan dampak ancaman yang ditimbulkan terhadap proses-proses bisnis.
- Identifikasi infrastruktur teknologi informasi (Hardware, software, komunikasi data) yang mendukung proses-proses bisnis.
- Identifikasi skala waktu pemulihan , terdiri dari cakupan, kondisi, dan waktu pemulihan proses-proses bisnis.

Skala waktu pemulihan terdiri dari Response Time Objective (RTO) adalah lamanya gangguan yang dapat ditoleransi. Sementara Response Poin Objective (RPO) adalah toleransi banyaknya data yang hilang akibat terjadinya suatu gangguan pada masing-masing proses bisnis. Hubungan RTO dan RPO terhadap toleransi besarnya kerugian yang dapat diterima organisasi

Deliverables dari pekerjaan Tahap 2 Business Impact Analysis ini adalah :

- Confirmed understanding of the Existing IT Infrastructure, IT Processes and Business Operation Process Document

Business Impact Analysis Matrix document yang akan digunakan sebagai dasar untuk menyusun DRP Strategy dan Procedure pada Tahap 3.

4. BC Strategy Development

Mengembangkan alternatif strategi BC berdasarkan hasil dari BIA.

Dalam fase ini termask proses pemilihan sumber daya minimum (untuk proses bisnis berbasis komputer), Pemilihan sumber daya minimum (untuk proses bisnis berbasis non komputer), Strategi-strategi Backup, penentuan Lokasi –lokasi pemulihan dan urutan tindakan.

- Pada tahap ini dilakukan pemilihan sumber daya minimum untuk sumber daya berbasis komputer, proses bisnis yang kritikal didahulukan untuk disediakan perangkat hardware dan

software yang mampu segera beroperasi jika keadaan terjadi bencana.

- Strategi backup dan recovery juga disusun untuk periode harian, mingguan dan bulanan. Pada fase ini juga ditentukan perangkat backup yang pas sesuai dengan perhitungan RTO dan RPO.
- Strategi pemilihan lokasi DRC / Disaster Recovery Site
  Kajian mengenai lokasi disaster recovery site dilakukan dengan mempertimbangkan berbagai faktor seperti : keamanan, kesiapan infrastruktur, kerawanan terhadap bencana alam, regulasi, kemudahan akses dan faktor-faktor lain yang lazim dipergunakan dalam kajian lokasi disaster recovery.

5. BC Plan Development
   Mengembangan perencanaan BC , step by step langkah-langkah yang dilakukan ketika terjadi bencana, termasuk perencanaan mitigasinya.

6. Awareness Training
   Mengkomunikasikan hasil perencanaan BC kepada stakeholder terkait.

7. BC Plan Testing
   Membuat rencana testing BC untuk memastikan dokumen BC dapat diterapkan jika terjadi peristiwa bencana yang sesungguhnya.
   Pada tahap ini berdasarkan skala prioritasnya dan berdasarkan dokumen SOP BCP atau IT DRP dilakukan pengujian dan simulasi untuk memastikan kegiatan pemulihan dapat berjalan dengan berbagai skenario pengujian
8. BC Plan Monitoring, Maintenance and Updating.
   Memastikan termonitor, terpelihara dan terbarukan perencanaan BC.

4. PEMBAHASAN

Hasil Risk Assesment Analysis

Tidak ada batasan jumlah identifikasi resiko dan besarnya parameter-paramenter resiko. Tabel di bawah ini hanya menampilkan beberapa resiko yang dijadikan asumsi untuk memudahkan pembahasan berikutnya.

Tabel 2. Identifikasi bencana dan kemungkinan terjadinya

Kategori Resiko	Nama Resiko	Frekwensi Kejadian Tahunan (ARO)	Persentase Tingkat Kerusakan (EF)
Bencana Alam	Banjir	1,00	0,6
	Kebakaran	0,25	0,5
	Gempa Bumi	0,30	0,6
	Tsunami	0,10	0,8
Kegagalan Sistem	Kegagalan Kelistrikan	1,00	0,25
	Aplikasi Bugs	0,17	0,05
	Kegagalan sistem telekomunikasi	0,33	0,2
Manusia	Kesalahan pemasukan data	1,00	0,02
	Pencurian Data Penting	0,10	0,3
	Serangan Hacker	1,00	0,35
	Serangan Virus	3,00	0,25
	Serangan teroris	1,00	0,22

Hasil Analisa Dampak Bisnis

Setelah mendapatkan hasil analisis risiko , selanjutya menjadi input untuk pelaksanaan Analisis Dampak Bisnis (Business Impact Analysis - BIA) untuk Sistem Informasi Administrasi Kependudukan (SIAK) Direktorat Jenderal Administrasi Kependudukan Departemen Dalam Negeri, berlokasi di Gedung Depnakertrans, Jl.TMP Kalibata 17, Jakarta Selatan. Analsis BIA ini didasarkan pada pandangan kuantitatif dan kualitatif akan risiko dan eksposur atas lingkungan operasi SIAK Ditjen ADMINDUK, termasuk dampak operasioanl dan finansial jika Ditjen ADMINDUK tidak dapat melaksanakan proses bisnisnya dan melayani masyarakat. Tujuan dari BIA ini adalah untuk membantu manajemen dengan:

- Mengidentifikasi kemampuan pemulihan bencana dan kelanjutan operasi yang sekarang dilaksanakan.
- Mengidentifikasi proses bisnis yang kritikal.

- Mengidentifikasi dan mengkuantifisir sumber daya minimum (yang disebut Minimum Operating Requirements atau MOR) yang dibutuhkan untuk melanjutkan operasi bisnis kritikal pada saat terjadi sebuah gangguan.
- Menentukan Recovery Time Objective (RTO) dan Recovery Point Objective (RPO) untuk tiap proses sebelum kepuasan masyarakat dan faktor-faktor kritikasl lain hancur.
- Menyajikan manajemen SIAK Ditjen ADMINDUK dengan informasi yang dibutuhkan untuk keputusan yang handal, dengan memperhatikan persentase berbagai kebutuhan proses bisnis yang akan di back up dan seberapa cepat operasi bisnis seharusnya dilanjutkan untuk mencegah dampak bagi SIAK. Informasi ini akan membantu manajemen SIAK dalam menentukan selera mereka atas risiko – seberapa banyak risiko yang harus diterima atau dicegah dalam lingkungan operasi normal.
- Menyajikan rekomendasi untuk tindakan selanjutnya dalam pengembangan strategi recover yang diperlukan untuk mempertahankan proses bisnis yang kritikal.

Proses Bisnis Kritikal

Tabel di bawah ini dapat dijadikan rujukan untuk proses bisnis yang menjadi dasar analisis dalam mengidentifikasi proses bisnis yang kritikal untuk kemudian dijadikan sebagai bagian dari perencanan pemulihan bencana. Proses bisnis umum (seperti pengelolaan kelahiran) terdiri dari proses bisnis khusus yang sifatnya spesifik terhadap suatu produk. Sehingga dengan mengasumsikan bahwa proses pengelolaan kelahiran memiliki tiga (3) proses khusus, total transaksi yang akan terjadi adalah 3 dikali 2 transaksi (jumlah minimal transaksi yang mungkin terlibat dalam satu proses bisnis). Dikalikan lagi dengan jumlah penduduk akan diperoleh dasar total transaksi dalam satu tahun atau satu hari.

Dari hasil analisis terhadap masing-masing risiko di tiap proses bisnis, maka dapat diturunkan profil proses bisnis yang dapat dikategorikan sebagai proses bisnis kritikal. Proses bisnis tersebut adalah:

1. Pencatatan Biodata Kependudukan
2. Perpindahan Penduduk
3. Pencatatan Kelahiran
4. Pencatatan Kematian
5. Pencatatan Pernikahan/Perceraian

Dasar atau batas kritikalitas proses bisnis berdasarkan pengukuran kualitatif dan teknik pengumpulan data diperoleh angka sekitar 65. Sehingga, hasil observasi dan pengumpulan data atas proses bisnis yang didefinisikan dalam Perpres 25 Tahun 2008 dan UU No.23 Tahun 2006 akan mengarah pada proses bisnis kritikal dengan nilai risiko total melebihi 65. Indikator 65 diperoleh melalui penggunaan asumsi bahwa probabilita dari sistem akan rusak, kerentanan data center atas musibah, dampak musibah terhadap keuangan dan operasional dan kemampuan manajemen Ditjen Adminduk dalam mengelola musibah berada pada kondisi paling minimal bila nilai yang diperoleh sekitar 65. Lebih jauh lagi, kondisi proses bisnis yang berada di bawah 65 mengindikasikan bahwa manajemen menempatkan prioritas yang kurang utama dalam pengelolaan datanya.

Tabel berikut ini menggambarkan Analisis Risiko atas Proses Bisnis Kritikal.

Tabel 1. Hasil Analisis Risiko atas Proses Bisnis Kritikal

PROSES BISNIS	Probabilitas (1)	Kerentanan (2)	Dampak (3)	Bobot Risiko (4)	Kemampuan Manajemen (5)	Nilai Risiko (6)
Pencatatan Biodata Kependudukan	5	5	4.8	120	3	96
Perubahan biodata penduduk	4.5	4.7	5	105.75	2.5	70.5
Peristiwa Kependudukan	3.7	5	4.8	88.8	3	71.04
Pendaftaran Pindah datang antar negara	4.1	4	5	82	2.8	61.23
Pencatatan Kelahiran	4.5	4.6	4.8	99.36	3	79.488
Pencatatan Perkawinan	4.6	4.9	5	112.7	2.4	72.128
Pencatatan Perceraian	4.8	4.5	4.8	103.68	3	82.944
Pencatatan Kematian	5	5	4.8	120	2.5	80
Pencatatan Pengangkatan anak, pengakuan anak, dan pengesahaan anak	4.5	4.7	4.8	101.52	2	54.144
Pencatatan Perubahan nama	2.5	4.7	4.8	56.4	3	45.12
Pencatatan Peristiwa penting lainnya	3	4.7	5	70.5	2.7	50.76

Perhitungan RTO dan RPO

Recovery Time Objective (RTO, RTO adalah waktu yang dibutuhkan untuk melakukan recovery secara keseluruhan hingga sistem berjalan lagi. *Recovery Point Objective (RPO)* RPO adalah jumlah data yang boleh hilang atau yang dapat ditoleransi akibat bencana yang terjadi. Setelah menemukan proses bisnis yang kritis dan menentukan RTO dari proses bisnis tersebut hasilnya akan dijadikan dasar bagi manajemen dalam mengambil keputusan tentang banyaknya orang, proses, sistem dan sumberdaya yang diperlukan pada saat bencana terjadi. RTO didefenisikan sebagai jangka waktu setelah bencana terjadi dan sebelum proses pemulihan selesai dilaksanakan untuk menghindari kerugian yang signifikan terhadap bisnis. RTO bisa dipengaruhi oleh bulan, hari, jam pada saat bencana terjadi. Berikut formula-formula baku yang digunakan dalam pendekatan kuantitatif:

• ***Exposure Factor (EF)***

adalah Persentase kehilangan asset yang disebabkan resiko yang terindentifikasi; nilainya berada diantara 0% sampai 100%

• ***Annualized Rate of Occurrence (ARO)***

adalah estimasi frekwensi kejadian sebuah resiko dalam setahun. Resiko yang terjadi 10 tahun sekali dituliskan dengan 1/10, resiko yang terjadi 2 kali dalam 8 tahun dituliskan dengan 2/8

• ***Asset Value (AV)***

adalah nilai asset TI yang dapat berupa nilai tangible dan intangible.

• ***Single Loss Expectancy (SLE)***

adalah nilai kerugian terhadap asset bila sebuah resiko yang teridentifikasi terjadi.

SLE = AV x EF

• ***Annualized Loss Expectancy (ALE)***

adalah nilai estimasi kerugian pertahun terhadap asset bila sebuah resiko yang teridentifikasi terjadi.

ALE = SLE x ARO

• ***Safeguards Cost/Benefit Analysis***

adalah analisa cost/benefit terhadap langkah-langkah penanganan resiko yang telah dimiliki bagi setiap resiko yang teridentifikasi.

(ALE Sebelum Pembuatan Safeguards) – (ALE Setelah Pembuatan Safeguards) – (Biaya Tahunan Safeguards) = Nilai Safeguards Terhadap Organisasi.

Prinsip-prinsip dasar pendekatan Cost And Benefit memberikan batasan etimasi besarnya investasi pembangunan DRP agar tidak lebih besar dari besarnya kerugian yang mungkin terjadi. Asumsi nilai investasi DRP yang optimal adalah rata-rata ALE dari potensi kerugian tinggi (ALEHigh). Nilai (ALErata-rata) sebesar Rp. 10.718.000.000 akan menjadi dasar perhitungan RTO dan RPO pada Analisa Dampak Bisnis (BIA). Berikut ini perhitungan tingkat besarnya kerugian dengan metode kuantitatif.

Tabel 3 Perhitungan Tingkatan Besarnya Kerugian

Bencana	ARO	EF	SLE	ALE
Banjir	1.00	0.6	28,800,000,000	28,800,000,000
Kebakaran	0.25	0.5	24,000,000,000	6,000,000,000
Gempa Bumi	0.30	0.6	28,800,000,000	8,640,000,000
Tsunami	0.10	0.8	38,400,000,000	3,840,000,000
Kegagalan Kelistrikan	1.00	0.25	12,000,000,000	12,000,000,000
Aplikasi Bugs	0.17	0.05	2,400,000,000	408,000,000
Kegagalan Sistem Telekomunikasi	0.33	0.2	9,600,000,000	3,168,000,000
Kesalahan Pemasukan Data	1.00	0.02	960,000,000	960,000,000
Pencurian Data Penting	0.10	0.3	14,400,000,000	1,440,000,000
Serangan Hacker	1.00	0.35	16,800,000,000	16,800,000,000
Serangan Virus	3.00	0.25	12,000,000,000	36,000,000,000
Serangan Teroris	1.00	0.22	10,560,000,000	10,560,000,000

Sumber: Surya Lesmana dan Suhardi, 2005 (dimodifikasi):

Identifikasi Kemungkinan Bencana

Tabel 4 Perhitungan RTO dan RPO

Critical Business Process	Toleransi Kerugian	Jam Kerja/Hari	RTO(hari)	RTO(jam)	RPO (Transactio
PENDAFTARAN PENDUDUK					
Pencatatan Biodata Penduduk	10,718,000,000	8	3.4699313	27.7594506	572,011.8
Perubahan biodata penduduk	10,718,000,000	8	7.6338489	61.07079131	5,720,118.1
Peristiwa Kependudukan	10,718,000,000	8	19.084622	152.6769783	1,521,487.8
Pengelolaan Perpindahan	10,718,000,000	8	12.723082	101.7846522	1,014,325.2
Pendaftaran Pindah datang antar negara	10,718,000,000	8	38.169245	305.3539566	9,128,927.2
CATATAN SIPIL					
Pencatatan Kelahiran	10,718,000,000	8	9.5423111	76.33848914	2,282,231.8
Pencatatan perkawinan	10,718,000,000	8	19.084622	152.6769783	9,128,927.2
Pencatatan Perceraian	10,718,000,000	8	19.084622	152.6769783	22,822,318.1
Pencatatan Kematian	10,718,000,000	8	19.084622	152.6769783	4,564,463.6
Pencatatan Pengangkatan anak, pengakuan anak, pengesahaan anak	10,718,000,000	8	38.169245	305.3539566	30,429,757.5
Pencatatan Perubahan nama	10,718,000,000	8	38.169245	305.3539566	30,429,757.5
Pencatatan Peristiwa penting lainnya	10,718,000,000	8	38.169245	305.3539566	9,128,927.2

Strategi untuk Recovery System

Dasar Penentuan Recovery System.

Berdasarkan perhitungan Analisa Dampak Bisnis, diperoleh informasi bahwa proses bisnis yang dianggap paling kritis adalah proses bisnis pencatatan biodata penduduk karena memiliki intensitas kegiatan paling tinggi, dengan nilai Recovery Time Objective sebesar 3,8 hari atau 27 jam kerja (asumsi waktu kerja 8 jam per hari) , yang berarti bahwa apabila terjadi kegagalan operasional Data Center utama, maka toleransi waktu yang dapat diterima agar proses bisnis tersebut bisa tetap berjalan adalah selama 3,8 hari atau 27 jam kerja, dan untuk menanggulangi kegegalan operasional tersebut maka Data Center yang berfungsi sebagai backup harus sudah siap menggantikan data center utama sebelum waktu toleransi habis yaitu 3,8 hari..

Recovery Point Objective yaitu toleransi banyak data/transaksi yang boleh hilang akibat terjadinya gangguan pada sistem dari transaksi proses bisnis pencatatan biodata penduduk karena memiliki intensitas kegiatan paling tinggi sebesar 572,011 (lihat Tabel 4.5 Analisis Perhitungan RTO dan RPO).

Strategi recovery yang baik merupakan kombinasi dari tindakan preventif dan

tindakan korektif. Strategi yang efektif adalah :

- Menghilangkan keseluruhan ancaman dari setiap kategori resiko.
- Meminimasi tingkat kejadian bencana tahunan
- Meminimasi dampak tahunan akibat bencana

Menghilangkan ancaman bencana dan meminimasi tingkat kejadian bencana dapat dilakukan dengan membangun lokasi recovery site ditempat lain, sedangkan meminimasi dampak dapat dilakukan dengan membangun sistem yang redudancy. Karena pada rancangan ini mengambil asumsi total lost pada Data Center, maka hanya dengan membuat sistem yang redudancy saja tidak cukup, tetap harus dikombinasi dengan membangun recovery site ditempat lain.

Berikut ini dibahas beberapa alternatif pilihan strategi untuk melakukan recovery dari sistem Teknologi Informasi Ditjen Adminduk.

1. "Next Box off The Line"

Strategi "Next Box Off The Line" adalah strategi dengan melakukan backup sistem pemrosesan data yang menerima dampak bencana apa adanya sampai sistem yang baru dapat dibeli dan diinstal untuk menggantikan mesin/CPU yang hilang/rusak. Sementara itu, sampai sistem yang baru siap, Ditjen Adminduk akan berjalan dengan melakukan prosedur manual, sambil mencari dan mempersiapkan fasilitas yang baru karena fasilitas lama rusak. Setelah ada mesin yang baru, tahap berikutnya adalah mengambil backup sistem aplikasi dan file dari tempat penyimpanan tape lalu personil TI akan melakukan loading tape tersebut ke sistem. Selanjutnya user mulai melakukan input data interim sampai file-file dan record-record terbaharui dan up to date.

Kelemahan dari strategi ini ada beberapa, pertama rencana hanya dapat berjalan di dalam lingkungan dimana tidak ada sistem yang kritis. Yaitu alternatif manual tersedia untuk semua komputer yang diperuntukkan bagi fungsi-fungsi bisnis, tidak ada aplikasi komputer yang diasumsikan kritis terhadap business survival. Kedua, strategi ini tidak mempersiapkan adanya fasilitas site yang telah dipersiapkan sebelumnya untuk dapat menginstalasi sistem yang baru. Pada kenyataannya memperoleh fasilitas site yang sesuai tidak merupakan pekerjaan yang sulit, akan tetapi mempersiapkan fasilitas seperti membuat raised floor, instalasi AC, instalasi UPS, pemasangan kabel-kabel Listrik, instalasi sistem keamanan, pengamanan kebakaran dan lain-lain merupakan pekerjaan yang membutuhkan waktu.

Hal yang perlu diketahui oleh manajemen Ditjen Adminduk adalah melakukan strategi recovery yang realistis memang diperlukan adanya biaya tambahan. Sedangkan melakukan bisnis kembali/recovery menjadi sistem yang manual, setelah membelanjakan biaya yang banyak untuk sistem aplikasi dan komputer sebelum disaster adalah tidak realistis. Didalam menjalankan proses yang manualpun dapat terjadi hambatan-hambatan, seperti misalnya staff yang berpengalaman untuk melakukan kegiatan manual sudah tidak ada terkena bencana. Form-form yang ada untuk pekerjaan manual sudah tidak cocok lagi dan tidak dipergunakan lagi selama bertahun-tahun.

2. Cold Site

Strategi cold site (shell site) mirip dengan strategi "Next Box Off The Line" dimana recovery sistem untuk operasional baru dapat dilakukan sampai dengan hardware yang baru telah diperoleh/dibeli (Server dibeli setelah terjadi bencana). Perbedaannya adalah pada strategi cold site ini fasilitas site telah dipersiapkan sebelumnya dimana seluruh fasilitas AC, listrik, raised floor telah tersedia. Fasilitas site ini juga dapat dipergunakan untuk kegiatan lain seperti misalnya tempat pelatihan karyawan dan sebagai tempat menyimpan off site.

3. Commercial Cold Site (Sewa Site)

Strategi ini identik dengan strategi cold site diatas, perbedaannya adalah commercial cold

site adalah fasilitas yang disediakan oleh pihak ketiga untuk disewakan. Biasanya lokasinya terletak di kantor provider. Dengan banyaknya perusahaan-perusahaan yang melakukan sharing cost dengan cara menyewa fasilitas tersebut, biaya sewa tentunya dapat dipertimbangkan lebih murah dari pada menyiapkan fasilitas site sendiri. Seperti kedua strategi lainnya, pendekatan terhadap recovery sistem diasumsikan bahwa perusahaan menerima dampak dari bencana apa adanya sampai dengan sistem yang baru diperoleh dari vendor atau dari penyedia jasa sewa. Kelemahannya sama dengan strategi cold site dan juga tidak dapat melakukan test untuk memperkirakan waktu efektif recovery.

4. Hot-Site

Hot site adalah recovery site yang terdiri dari mesin yang kompatibel dengan mesin utama pada data center, yang juga dapat menjalankan semua aplikasi-aplikasi yang sifatnya kritis, dan sudah dilengkapi dengan fasilitas pendukung lainnya seperti AC, UPS, Security System, Raise Floor dan lain-lain. Keuntungan yang diperoleh adalah recovery time yang cepat sehingga perusahaan tidak perlu melakukan proses bisnis secara manual, testing recovery dapat dilakukan sesuai jadwal dengan adanya mesin yang kompatibel dengan mesin pada DRC. Kerugiannya adalah biaya yang dikeluarkan untuk penyediaan mesin, dimana mesin tersebut hanya dipergunakan sebagai cadangan/ backup mesin utama pada DRC.

Berikut ini adalah butir-butir yang menjadi pertimbangan didalam pemilihan site strategies sebagai bagian dari DRP:

- Employee Comfort; Krisis/Bencana terhadap lingkungan kerja, dapat berdampak terhadap lingkungan tempat tinggal pegawai. Lebih jauh lagi penugasan pegawai dengan merelokasikannya ke tempat fasilitas site recovery yang jauh dapat menyebabkan trauma yang lebih parah lagi.
- Lokasi Site; Jarak tempuh recovery site yang jauh menyebabkan biaya perjalanan dan akomodasi yang cukup signifikan. Terlebih lagi Tim Recovery yang jumlahnya cukup banyak perlu mencapai site recovery dalam waktu singkat, tentunya perlu diperhitungkan biayanya dibandingkan dengan nilai/value yang diperoleh perusahaan. Jarak recovery site terdekat yang diperbolehkan oleh Peraturan Bank Indonesia adalah 80KM.
- Waktu recovery yang cepat dengan anggaran yang masuk akal dan diperbolehkan oleh perusahaan; Bisnis menginginkan recovery system mereka sesegera mungkin setelah terjadi bencana, akan tetapi semakin cepat waktu yang diinginkan, semakin besar pula biaya yang dikeluarkan untuk membeli teknologinya.

Berdasarkan butir-butir kriteria diatas ditambah dengan hasil perhitungan Business Impact Analysis strategi Next Box Off The Line kurang dapat diterima karena RPO yang diperlukan maksimum 3 hari, sedangkan pengadaan mesin dengan persiapan/perbaikan fasilitas pendukungnya dapat memakan waktu sampai 2 minggu.

Strategi Cold Site juga kurang dapat diterima, walaupun site sudah disiapkan, fasilitas pendukung juga sudah dipersiapkan tetapi pengadaan mesin membutuhkan waktu lebih dari 3 hari. Strategi Comercial Cold Site juga kurang dapat diterima, karena tetap harus menyediakan mesin, dimana pengadaannya akan memakan waktu yang lebih dari 3 hari. Akhirnya pilihan tinggal pada strategi Hot-Site. Untuk strategi Hot-Site ini perlu dilakukan survey lokasi fisik nya.

5. KESIMPULAN

1. SIAK merupakan sistem Informasi yang mengelola data kependudukan dimana cukup krusial data-data yang dikelola, membutuhkan DRP untuk menjamin kelangsungan pengelolaannya.
2. Dengan metode kuantitatif dapat ditentukan RTO dan RPO nya serta alternatif strategi implementasi DRP nya.
3. Dibutuhkan dukungan semua pihak dalam penyusunan DRP.

DAFTAR PUSTAKA

Business Savvy – IT Smart, "Disaster Recovery Planning – Process and Options, White Paper", Comprehensive Consulting Solutions, Inc, United State, 2001.

IT Governance Institute, "CISA Review Manual 2005", ISACA, 2005.

Micki Krause, Harold F, "Handbook of Information Security Management", CRC Press LLC, United State, 1993.

National Institute of Standards and Technology, "Contingency Planning Guide for Information Technology Systems", NIST, United State, 2002.

Price Waterhouse Disaster Recovery Plan Methodology 1996 (PWSMM-1996)

.