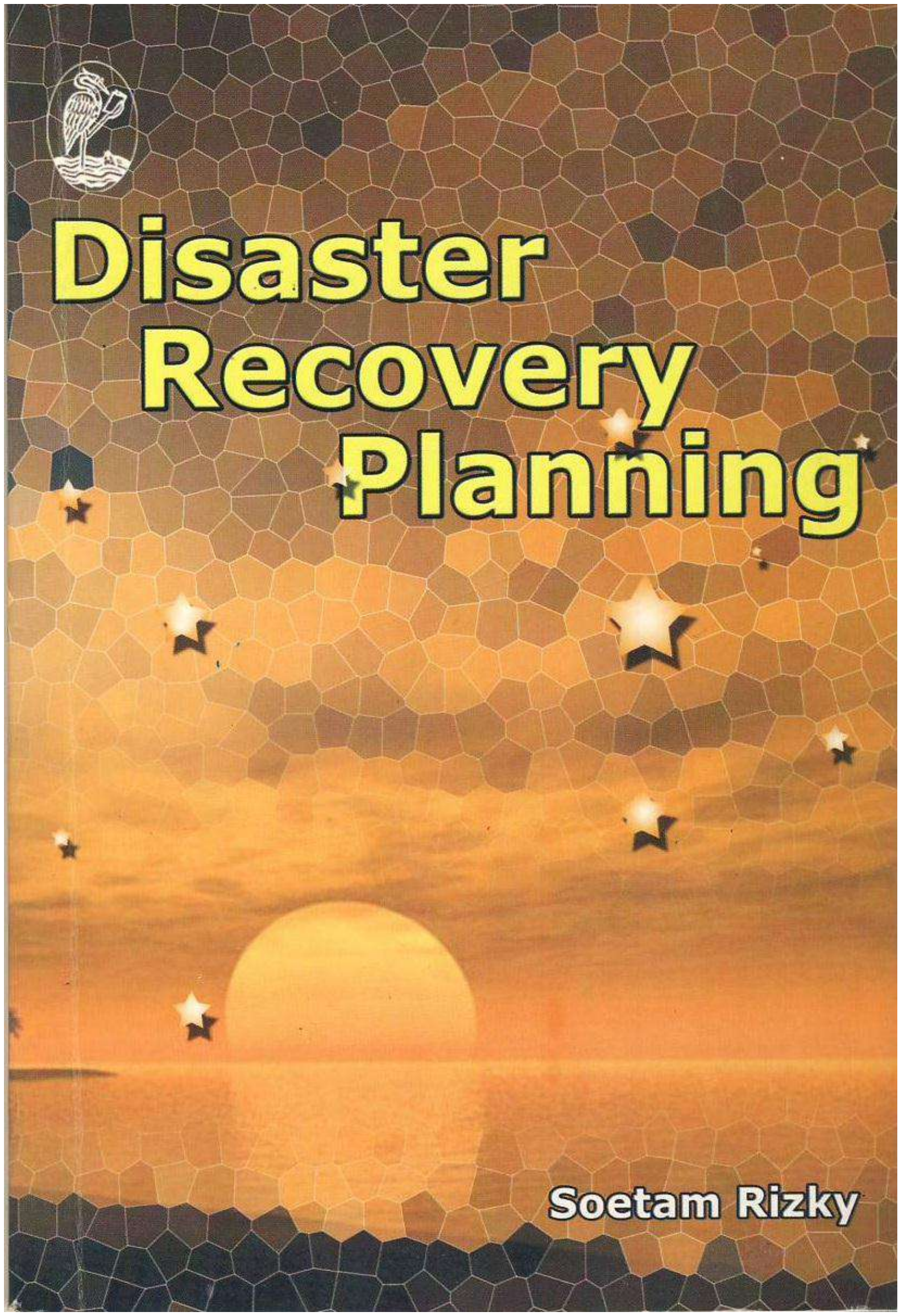

Disaster
Recovery
Planning
Soetam Rizky

PRESTASI PUSTAKA
PUBLISHER
Jakarta

Copyright © Soetam Rizky 2008
DISASTER RECOVERY PLANNING

Penulis : **Soetam Rizky**
Editor: **John Wolor**
Desain Cover: **Soetam Rizky**
Setting: **Tim Prestasi**

Hak penerbitan ada pada Prestasi Pustaka

Hak cipta dilindungi Undang-undang
Dilarang mengutip, memperbanyak dan
menerjemahkan sebagian atau seluruh
isi buku ini tanpa izin tertulis dari Penerbit
Jakarta – Indonesia
2008

Email Penerbit:
pprsby@plasa.com

DISASTER RECOVERY PLANNING

ISBN : **978-602-8117-57-9**

Cetakan Pertama: Agustus 2008

Untuk istri dan putri kecilku, pelipur jiwa di kala lara dan duka

Kekayaan adalah merasa bahagia dan bersyukur dengan apa yang telah kita miliki
Kemiskinan adalah merasa sedih dan mengeluh dengan apa yang telah kita miliki

Kata Pengantar

Alhamdullillah, akhirnya buku yang kesembilan ini telah tuntas diselesaikan. Sebagai buku pertama dari penulis yang membahas sisi lain dari sistem informasi (tidak hanya berkutat pada bahasa pemrograman dan akses database), penyelesaian buku ini memang terasa sangat berat. Konsep-konsep yang dipaparkan tidak hanya sekedar mengambil dari berbagai buku referensi yang ada, tetapi juga disertai dengan paparan konsep hasil analisa dan beberapa kutipan penelitian yang sebelumnya telah dipresentasikan di berbagai call for paper.

Tentu saja, banyak pihak yang secara tidak langsung ikut mendorong dan membantu saat buku ini disusun. Karenanya, penulis sangat berterima kasih kepada para penulis yang tidak pernah bosan membakar semangat dalam menulis buku, Pak Yuswanto, Erwin Sutomo, Slamet Ar Rokhim, Wido

Nugroho, dan juga penulis cilik yang sangat menginspirasi kembali semangat penulis, Adam Pahlevi Baihaqi.

Semoga buku ini tidak hanya memberi wawasan baru kepada para praktisi IT maupun para praktisi manajemen, tetapi juga mampu menjadi bahan referensi yang handal untuk para akademisi, khususnya di bidang sistem informasi dan juga manajemen.

Selamat berkarya !!!

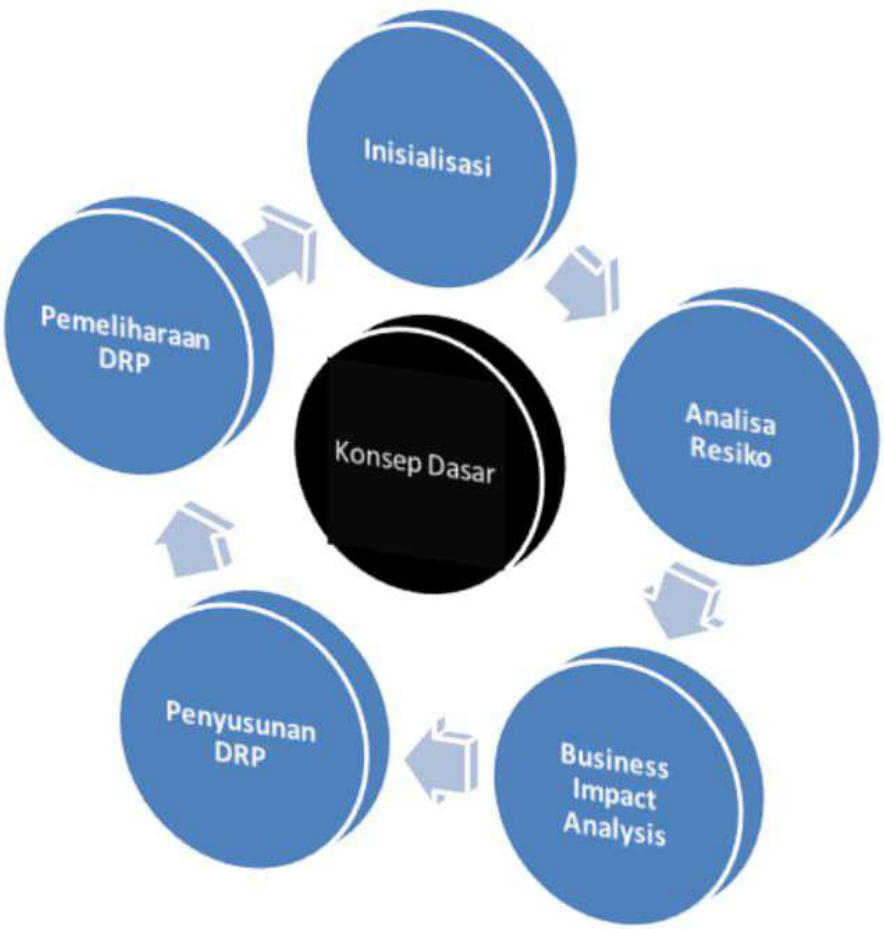
Candi, Sidoarjo

Rajab 1428 H / Juli 2008

Daftar isi

Daftar Gambar

Konsep Dasar



Pengantar

Keberhasilan tidak hanya terjadi karena kebetulan, tetapi ditentukan oleh usaha dan karunia

Masih banyak orang di bidang TI maupun manajemen (baik akademisi ataupun profesional, terutama di Indonesia) yang masih belum mengenal tentang *disaster recovery planning* atau seringkali disingkat sebagai DRP. Mendengar saja pun masih banyak yang mengernyitkan dahi, "apakah itu termasuk ilmu baru ?", "siapa yang mencetuskan ?","apa efeknya bagi lembaga atau perusahaan ?" dan masih banyak pertanyaan lain yang menggelayut di benak para profesional maupun akademisi.

Dan "keawaman" terhadap DRP bukan hanya monopoli di Indonesia, sebab sebuah studi Harris Interactive Inc. pada tahun 2006 mengenai kesiapan para CIO (Chief Information Officer) menghadapi bencana dalam kaitannya dengan DRP, hanya ada 39% yang menyatakan siap dengan DRP yang dimilikinya [1].

DRP sendiri yang nantinya akan menjadi sebuah rangkaian dari *business continuity planning* atau BCP, sesungguhnya bukan hal baru di bidang TI

maupun bidang manajemen. Tetapi meski bukan suatu hal yang baru, DRP sendiri seringkali menjadi "anak tiri" dalam sebuah implementasi sistem informasi di sebuah institusi.

DRP bukanlah sebuah jargon "omong kosong" yang hanya dituliskan dalam sebuah SOP (Standar Operasional Prosedur) untuk kepentingan proses audit.

Bahkan, banyak pihak yang mengklaim bahwa institusinya telah menerapkan DRP, hanya karena sistem informasinya telah dilengkapi fasilitas untuk melakukan backup dan restore data. Tetapi, benarkah DRP (dan juga BCP) hanya sekedar prosedur dan proses backup serta restore data ? Ataukah DRP dan BCP hanya sekedar standar "hiasan" demi kepentingan sebuah proses audit ? Atau mungkin DRP dan BCP hanyalah sebuah jargon yang wajib dipahami pihak manajemen agar tidak

terlihat "ketinggalan jaman" dibanding para pesaingnya ?

Jawabannya, tentu saja tidak !!! DRP bukanlah sebuah jargon "omong kosong" yang hanya dituliskan dalam sebuah SOP (Standar Operasional Prosedur) untuk kepentingan proses audit. DRP juga bukan sebuah "tren" baru (khususnya di Indonesia) yang mewabah sebagai dampak dari maraknya musibah di berbagai tempat di negeri ini. DRP bahkan lebih dari sekedar sebuah form dalam sistem informasi yang didalamnya menyediakan kemampuan untuk melakukan proses backup dan restore data.

Di dalam buku ini, akan dibahas secara ringkas dan sederhana, mengenai teori yang harus dipahami tentang DRP (dan BCP), serta tahapan-tahapan yang harus dilakukan didalamnya. Diharapkan bahwa para pembaca buku ini, jika berasal dari kalangan akademisi di bidang TI, maka dapat menambah wawasan tentang DRP, baik sebagai bagian dari proses audit sistem informasi

maupun sebagai bagian dari manajemen proyek sistem informasi.

Sedangkan dari kalangan akademisi di bidang manajemen, maka dapat menambah wawasan secara lugas mengenai DRP sebagai bagian dari sebuah manajemen strategi modern yang didalamnya selalu mengikutsertakan area sistem informasi didalamnya.

DRP bukan hanya sebagai pelengkap, tetapi menjadi sebuah kewajiban, seperti halnya proses studi kelayakan dari sebuah pengerjaan proyek sistem informasi.

Lalu, bagaimana dengan para profesional ? Untuk para manajer di bidang TI, DRP tentu saja menjadi sebuah prosedur yang mutlak harus diimplementasikan dalam sistem informasi yang diampu olehnya. DRP bukan hanya sebagai pelengkap, tetapi menjadi sebuah kewajiban, seperti

halnya proses studi kelayakan dari sebuah pengerjaan proyek sistem informasi.

Dan untuk para manajer top level, diharapkan dapat lebih memahami bahwa DRP bukan hanya "pekerjaan" para manajer TI, tetapi lebih ke sebuah pengejawantahan komitmen mengenai sebuah prosedur yang dibakukan dan harus dipahami serta dilakukan oleh semua pihak yang ada dalam perusahaan. Sebab DRP bukan hanya tanggung jawab departemen yang berkutat di bidang TI, tetapi juga tanggung jawab dari semua pihak dalam sebuah perusahaan. Terlebih lagi jika perusahaan tersebut telah sepenuhnya "bergantung" kelangsungan hidupnya dari sebuah sistem informasi.

Dengan menggunakan pendekatan tahapan dalam penyusunan DRP, maka buku ini diharapkan dapat menjadi referensi cepat yang mampu menuntun para pembaca dalam memahami serta menerapkan DRP yang sesuai bagi institusinya masing-masing, dan juga sebagai sebuah pembuka

wawasan baru dalam bidang ilmu sistem informasi maupun manajemen.

Selamat berkarya !!!

Konsep Dasar Disaster Recovery Planning

Susu sapi tetaplah putih, tidak peduli dihasilkan oleh sapi berwarna putih atau berwarna hitam

Dalam pemahaman kalangan "awam", disaster recovery planning yang diterjemahkan secara bebas menjadi perencanaan pemulihan bencana, seringkali disalahartikan. Banyak pihak yang masih beranggapan, "mengapa harus berharap akan terjadi bencana ?", "bukankah daerah tempat kita bekerja ini hampir tidak pernah terjadi bencana alam besar seperti gempa bumi ataupun gunung meletus ? Lalu mengapa harus berpikir yang tidak-tidak mengenai bencana ?"

Tentu saja hal tersebut, bukanlah sebuah pemahaman yang sama sekali keliru. Sebab masih banyak yang berasumsi bahwa bencana hanyalah terjadi dari alam seperti gempa bumi, gunung meletus atau tsunami. Tetapi, benarkah bencana hanya ditimbulkan oleh alam ?

Bagaimana dengan bencana yang terjadi karena faktor lain ? Apakah listrik padam secara tiba-tiba dan kemudian mengakibatkan sebuah hard disk server rusak dan *corrupt* sehingga seluruh data hilang dalam sekejap, bukan termasuk kategori

bencana ? Atau kecerobohan seorang pegawai yang tanpa sengaja melakukan penghapusan seluruh data laporan keuangan menjadi lenyap, juga bukan termasuk bencana ? Lalu, bagaimana dengan virus yang sekonyong-konyong menyerang melalui jaringan lokal dan mengakibatkan seluruh aktifitas yang menggunakan sistem informasi terhenti, juga bukan dikategorikan sebuah bencana ?

Dan tentu saja masih sangat banyak contoh kasus yang dapat dikategorikan sebagai bencana (dan akan diterangkan selanjutnya), yang sebenarnya sangat penting untuk dipikirkan ulang. Pastinya pula, tak akan ada seorang pun yang berharap salah satu skenario bencana tadi terjadi di lingkungan tempat kita berada, baik di kantor pemerintahan maupun di institusi swasta.

Karena bencana yang terjadi, baik dari alam maupun tidak dari alam, tidak akan pernah memberi peringatan yang detail mengenai waktu dan tempat terjadinya. Sedangkan pihak manajemen (dan juga

pengguna) malah meremehkan keberadaan ancaman dari bencana itu sendiri.

Padahal, seperti yang kita ketahui bersama, keberadaan data dalam sebuah sistem informasi dan juga infrastruktur sistem informasi merupakan aset yang sangat berharga dari institusi yang bersangkutan. Dan bukankah kita juga lebih peduli untuk mengasuransikan aset lain seperti gedung, mobil ataupun perangkat kantor dibandingkan mengasuransikan data yang kita miliki ?

DRP merupakan bagian penting dalam langkah "mengasuransikan" data serta infrastruktu yang kita miliki agar tetap "hidup" dan berjalan sebagaimana mestinya.

Tetapi, benarkah data serta infrastruktur yang kita miliki tidak layak untuk diasuransikan ? Atau sedemikian remehnya data dan infrastruktur yang kita miliki sehingga tidak ada langkah pasti

dalam mengasuransikan kelangsungan "hidup" dari data dan infrastruktur tersebut ?

Dalam hal tersebut, DRP merupakan bagian penting dalam langkah "mengasuransikan" data serta infrastruktu yang kita miliki agar tetap "hidup" dan berjalan sebagaimana mestinya. Karena dengan menggunakan DRP, maka bencana apapun yang akan terjadi, tetap akan dapat menjamin business continuity atau kelangsungan bisnis yang terjadi dalam sebuah institusi.

Disaster recovery planning merupakan bagian perencanaan dari sebuah institusi untuk melakukan tahapan tertentu yang nantinya akan menjamin kelangsungan pelayanan (khususnya dari segi sistem informasi) yang diberikan tanpa mengurangi kapabilitas serta kinerja dari sebuah sistem jika terjadi sebuah bencana didalamnya.

Disaster recovery planning sendiri sesungguhnya merupakan bagian dari business continuity planning [1]. Definisi resmi dari disaster recovery planning adalah *ability to continue with services in the case of major outages, often with reduced capabilities or performance* atau kemampuan untuk melanjutkan pelayanan jika terjadi kegagalan besar yang seringkali menyebabkan pengurangan kapabilitas atau kinerja dari sebuah sistem [2].

Di referensi yang lain disebutkan bahwa disaster recovery planning merupakan kemampuan organisasi untuk melanjutkan operasional sehari-hari meski terjadi bencana, melalui rangkaian perencanaan aktifitas serta kewaspadaan yang dilakukan oleh pihak manajemen.

Dengan kata lain, bahwa disaster recovery planning merupakan bagian perencanaan dari sebuah institusi untuk melakukan tahapan tertentu yang nantinya akan menjamin kelangsungan pelayanan (khususnya dari segi sistem informasi)

yang diberikan tanpa mengurangi kapabilitas serta kinerja dari sebuah sistem jika terjadi sebuah bencana didalamnya.

Sebuah DRP yang baik, sebagai bagian dari BCP akan selalu menjamin tingginya ketersediaan dari sebuah sistem informasi (*information system high availability*). Ketersedian tinggi disini adalah kemampuan untuk tetap menyediakan layanan dari sistem informasi, baik dalam keadaan normal maupun dalam masa sebuah bencana sedang terjadi tanpa adanya penurunan kinerja dari sistem itu sendiri

Relasi Antara BCP, DRP dan High Availability

Di dalam DRP sendiri, yang paling penting diperhatikan adalah bahwa tiap institusi tidak akan pernah memiliki solusi yang sama mengenai detail dari DRP yang akan diimplementasikan, baik dari segi strategi maupun dari segi perencanaan. Hal tersebut nantinya akan bergantung sepenuhnya terhadap jenis dari organisasi itu sendiri, serta

corporate officer atau orang-orang yang memiliki tanggung jawab serta berinteraksi dalam sebuah sistem informasi di sebuah organisasi.

Dari faktor-faktor tersebut, faktor yang terpenting dalam sebuah DRP tentu saja adalah dari sisi corporate officer.

Corporate officer tidak hanya didominasi oleh orang-orang yang berada di departemen TI, tetapi yang disebut corporate officer adalah seluruh orang yang terlibat dan berinteraksi dalam sebuah sistem informasi di sebuah organisasi. Sebagai contoh adalah seorang kasir di sebuah supermarket merupakan corporate officer dari modul POS (Point of Sales) di sistem informasi.

Faktor Dalam Penyusunan DRP

Dari faktor-faktor tersebut, faktor yang terpenting dalam sebuah DRP tentu saja adalah dari sisi corporate officer. Karakteristik tiap orang, budaya organisasi serta tipe kepemimpinan dari sebuah organisasi sangatlah berpengaruh terhadap penyusunan serta implementasi dari DRP.

Lalu, apa saja sebenarnya yang dimaksud dengan *disaster* atau bencana dalam konteks DRP ? Meski sebagian telah disebut di bagian sebelumnya,

secara umum jenis bencana dapat dibagi menjadi dua bagian, yaitu jenis bencana berdasarkan tingkat kerusakan yang ditimbulkan, serta jenis bencana yang dibagi berdasarkan sumber atau asal bencana itu sendiri.

Terdapat dua jenis bencana yang dibagi berdasarkan tingkat kerusakan yang ditimbulkan, yaitu :

1. *Minor Disaster*

   Bencana kecil (baik dari alam maupun bukan) merupakan bencana yang dampak kerusakannya terhitung kecil dan tidak terlalu dirasakan , sehingga pelayanan dari sistem informasi tidak berhenti secara total. Bencana kecil ini dibagi lagi menjadi beberapa jenis yaitu :

   a. Outage (kerusakan sementara)

      Kerusakan sementara umumnya terjadi karena kerusakan kecil yang mampu diatasi dengan cepat, misalnya : hang pada komputer yang dijadikan sebagai

client, kerusakan hardware kecil seperti keyboard dan mouse.

b. Kategori sistem

Kerusakan dari kategori sistem umumnya terjadi karena ketidaksengajaan dari pengguna, misalnya : kegagalan saat booting karena terdapat boot CD yang masih ada di dalam CD ROM, kegagalan skenario dari uji coba sistem informasi yang baru berjalan.

c. Proteksi otomatis atau recovery system

Bencana kecil dari proteksi otomatis, umumnya terjadi akibat kesalahan dari program proteksi yang dipasang di dalam komputer baik di server maupun di komputer klien. Sebagai contoh adalah kegagalan eksekusi beberapa program akibat dari program anti virus yang melakukan *false detection* atau kegagalan transfer data akibat proteksi dari beberapa program *firewall*. Bencana jenis

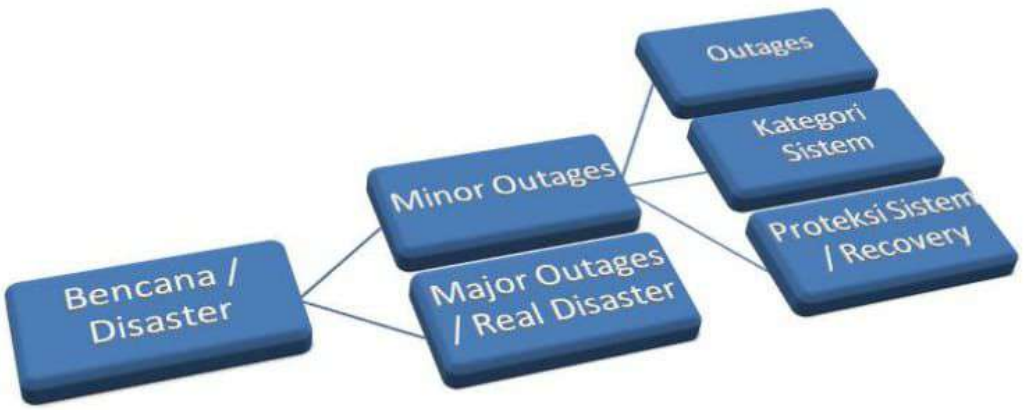
ini juga seringkali terjadi akibat proses recovery yang terjadi karena telah dijadwalkan sebelumnya, misalnya dengan beberapa program *tune up* yang secara otomatis akan mengakibatkan beberapa program mengalami *delay* karena sedang melakukan maintenance otomatis seperti defrag memori ataupun penghapusan file temporer.

Bencana jenis ini (*Major Disaster*) umumnya disinonimkan sebagai "bencana yang sesungguhnya", karena dapat menyebabkan pelayanan dari sistem informasi benar-benar terhenti tanpa toleransi maupun peringatan sebelumnya

2. *Major Disaster*

   Dalam DRP, bencana jenis ini merupakan fokus dari perencanaan yang harus dilakukan. Bencana jenis ini umumnya disinonimkan sebagai "bencana yang sesungguhnya", karena dapat menyebabkan pelayanan dari sistem informasi benar-benar terhenti tanpa toleransi maupun peringatan sebelumnya.

   Beberapa jenis bencana yang masuk dalam kategori ini antara lain seperti gempa bumi, angin topan, tsunami ataupun banjir bandang. Sedangkan contoh lainnya adalah kerusakan hardware server secara total (harddisk mati atau motherboard server yang terbakar), kerusakan jaringan akibat serangan virus maupun karena kerusakan hardware (kabel ataupun wireless).



Jenis Bencana Berdasar Tingkat Kerusakan

Sedangkan untuk jenis bencana jika dilihat dari sumber penyebabnya adalah sebagai berikut :

1. Bencana alam (nature disaster)

   Seperti telah disebutkan sebelumnya, contoh bencana alam adalah seperti gempa bumi, banjir, maupun gangguan dari hewan seperti tikus, kecoa ataupun semut yang mampu menimbulkan kerusakan terhadap kelangsungan hidup sistem informasi.

Unsur kesengajaan bisa terjadi seperti pada kasus persaingan tidak sehat antar perusahaan, ataupun keisengan para hacker untuk mencoba tingkat keamanan sebuah sistem.

2. Bencana dari manusia (human disaster)

   Bencana yang ditimbulkan dari manusia secara umum dibagi menjadi dua jenis yaitu :

   a. Internal

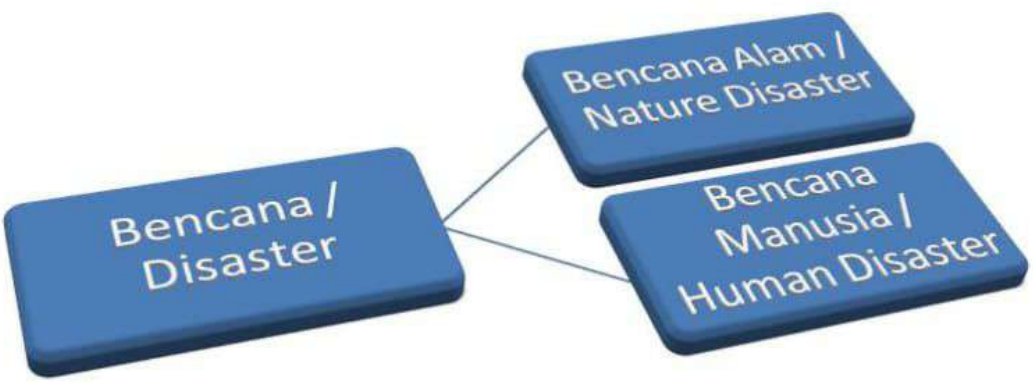
      Bencana dari manusia yang ditimbulkan dari dalam bisa terjadi karena ketidaksengajaan maupun kesengajaan. Bencana yang timbul akibat ketidaksengajaan misalnya : keteledoran pengguna dalam melakukan pengoperasian sistem, atau tingkah laku pengguna yang mengakibatkan sistem tidak berfungsi, seperti kabel yang putus akibat tersandung oleh pengguna maupun

tumpahan makanan / minuman yang mengakibatkan kerusakan komputer. Sedangkan bencana internal akibat kesengajaan bisa terjadi dalam kasus balas dendam yang dilakukan karyawan yang pernah di-PHK ataupun sakit hati.

b. Eksternal

Bencana eksternal dari manusia seringkali timbul akibat interaksi antara pelanggan dengan sistem yang berlebihan. Seperti halnya bencana internal, bencana eksternal juga terbagi menjadi dua yaitu yang sengaja maupun yang tidak sengaja. Unsur kesengajaan bisa terjadi seperti pada kasus persaingan tidak sehat antar perusahaan, ataupun keisengan para hacker untuk mencoba tingkat keamanan sebuah sistem. Sedangkan bencana eksternal akibat ketidaksengajaan bisa timbul jika terjadi penularan virus akibat pengguna luar yang membawa media

yang sudah tertular virus, juga bisa saja terjadi karena kesalahan yang tidak disengaja dari para pekerja perbaikan gedung yang mungkin menyebabkan sistem tidak berfungsi (kabel putus akibat perbaikan, komputer yang terkena reruntuhan perbaikan dan lainnya).



Jenis Bencana Dari Sumber Penyebab

Cost of failure

Selalu berharap untuk yang terbaik dan bersiap untuk menghadapi hal yang terburuk

Setelah memahami jenis dari bencana yang terjadi, maka perlu juga dipahami tentang perhitungan dari dampak bencana tadi. Perhitungan dari dampak bencana tidak akan pernah menemui titik temu yang sama antar organisasi. Hal ini disebabkan tingkat ketergantungan serta besarnya investasi untuk sebuah sistem informasi dari tiap organisasi sangatlah berbeda.

Karenanya sangatlah tidak adil untuk melakukan penilaian sepihak dalam perhitungan biaya kegagalan atau lazim disebut sebagai *cost of failure* (COF) dalam konteks DRP. Untuk melakukan perhitungan dari cost of failure, maka sebuah organisasi harus memperhitungkan hal-hal berikut :

1. Availability (ketersediaan)

   Pengukuran availability adalah pengukuran yang melibatkan berapa banyak waktu yang tersedia saat sebuah sistem melakukan pelayanan dibandingkan dengan total keseluruhan waktu yang tersedia. Karena sesungguhnya tidak pernah ada sebuah sistem (baik dari segi

perangkat lunak maupun perangkat keras) yang mampu menyediakan waktu layanan sebesar 100% tanpa henti.

Pengukuran ketersediaan ini dapat dinyatakan dengan rumus sederhana berikut :

$$\text{Availability} = \frac{\text{Uptime}}{\text{Uptime} + \text{Downtime}}$$

Keterangan :

- Availability = rasio ketersediaan sebuah sistem
- Uptime = satuan waktu saat sistem berjalan normal
- Downtime = satuan waktu saat sistem tidak berjalan normal

Sebagai contoh, sebuah perusahaan "X" memiliki sebuah sistem informasi yang menggunakan sebuah server sebagai penampung data. Server tersebut, dalam satu hari kerja, secara normal akan beroperasi selama 12 jam. Pada saat bulan Maret tahun 2007, server di perusahaan tersebut mengalami

proses penggantian memori yang membutuhkan proses shutdown server selama 3 jam. Maka rasio availability yang dimiliki oleh sistem tersebut pada bulan Maret 2007 (dengan asumsi pada bulan Maret 2007 terdapat 25 hari kerja) adalah :

$$\text{Availability} = \frac{(12 \times 25)}{(12 \times 25) + 3}$$

Maka, availability pada bulan Maret 2007 sebesar 99.009 %.

Pengukuran tingkat kehandalan yang nantinya berpengaruh ke pengukuran *cost of failure* akan menyebabkan resistensi dari pihak pengguna maupun pengembang.

2. Reliability (kehandalan)

   Tingkat kehandalan dalam konteks DRP adalah pengukuran rata-rata waktu yang diperlukan untuk melanjutkan layanan dari sistem, saat

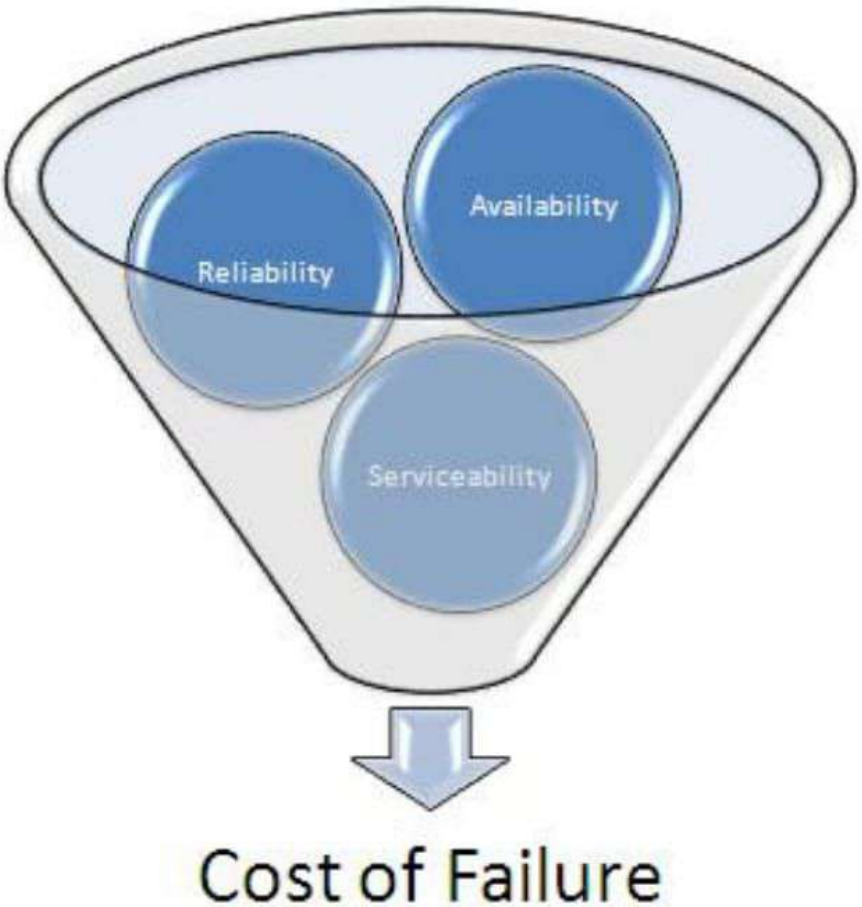
sistem tidak berjalan normal. Sebagai contoh, untuk mengukur tingkat kehandalan suatu sistem terhadap padamnya listrik, secara sederhana dapat diukur dengan lamanya kekuatan dari UPS yang digunakan di server, atau juga lama waktu dari generator (jika ada) untuk menjamin agar data tidak hilang saat listrik padam.

Masalah utama dari pengukuran tingkat kehandalan ini adalah saat tingkat kehandalan harus diukur dari berbagai sudut pandang, baik dari sisi perangkat keras maupun dari sisi perangkat lunak. Karena pengukuran tingkat kehandalan yang nantinya akan berpengaruh ke pengukuran *cost of failure* akan menyebabkan resistensi dari pihak pengguna maupun pengembang. Pihak pengembang akan sebisa mungkin melakukan pengukuran tingkat kehandalan hingga ke level maksimal untuk menunjukkan kinerja sistem yang telah dibuat. Sedangkan pihak pengguna akan berusaha menyatakan tingkat kehandalan ke level yang

paling minimal agar terhindar sebagai "kambing hitam" dari kegagalan sebuah sistem.

3. Serviceability (kemudahan layanan)

   Aspek pengukuran terakhir merupakan aspek pengukuran yang tersulit untuk dilakukan. Tingkat kemudahan layanan merupakan pengukuran yang melibatkan kemudahan sebuah sistem dalam melakukan perbaikan saat sebuah sistem mengalami kerusakan. Tentu saja, pengukuran tingkat kemudahan sangat relatif bagi berbagai pihak. Tetapi sebenarnya terdapat beberapa cara untuk melakukan pengukuran ini, seperti kemudahaan untuk melakukan pelatihan bagi pengguna untuk melakukan *self repair* terhadap kerusakan ringan sistem, kemudahan perbaikan tanpa harus diketahui oleh pelanggan ataupun kemudahan perbaikan yang diukur dari seberapa cepat perbaikan dapat dilakukan.



Komponen Cost of Failuire

Konsep Dasar Business Continuity Planning

Masih banyak orang beranggapan bahwa perencanaan hanya membutuhkan 20% dari proses dan 80% adalah implementasi, padahal sesungguhnya yang terjadi adalah kebalikannya.

Business Continuity Planning Sebagai Tujuan Utama

Seperti telah dijelaskan di sub bab sebelumnya, bahwa tujuan utama dari diadakannya DRP adalah untuk menuju ke arah *business continuity planning.* Business continuity planning (BCP) merupakan perencaaan kelanjutan proses bisnis dan layanan dari sistem informasi pasca terjadinya bencana yang menimpa sistem informasi tersebut.

Recovery atau pemulihan yang diharapkan dari DRP seharusnya langsung berdampak kepada BCP. Hal ini seringkali tidak disadari oleh para konsultan pembuat DRP yang hanya berhenti di tahapan pemulihan, dan tidak memperhitungkan aspek BCP didalamnya.

Segi manusia, tidak hanya menjadi sebuah unsur dalam BCP, tetapi juga menjadi sebuah unsur yang tersulit dalam proses perencanaan.

Di dalam pelaksanaan BCP nantinya, selain melakukan pemulihan dari segi perangkat keras maupun perangkat lunak, salah satu hal terpenting yang harus diperhatikan adalah melakukan pemulihan dari segi *human* atau manusia. Selain sebagai hal terpenting, pemulihan dari segi manusia seringkali terlupakan oleh pihak manajemen.

Dan dalam perencanaannya, segi ini sangat membutuhkan sebuah pemahaman yang menyeluruh serta komitmen manajemen yang kuat didalamnya. Selain itu, perlu juga diperhitungkan mengenai budaya perusahaan serta model DRP yang akan diimplementasikan nantinya (akan dibahas di bab tahapan selanjutnya).

Segi manusia, tidak hanya menjadi sebuah unsur dalam BCP, tetapi juga menjadi sebuah unsur yang tersulit dalam proses perencanaan. Hal ini disebabkan faktor emosional serta stres secara fisik yang dipastikan akan sangat berpengaruh terhadap implementasi DRP.

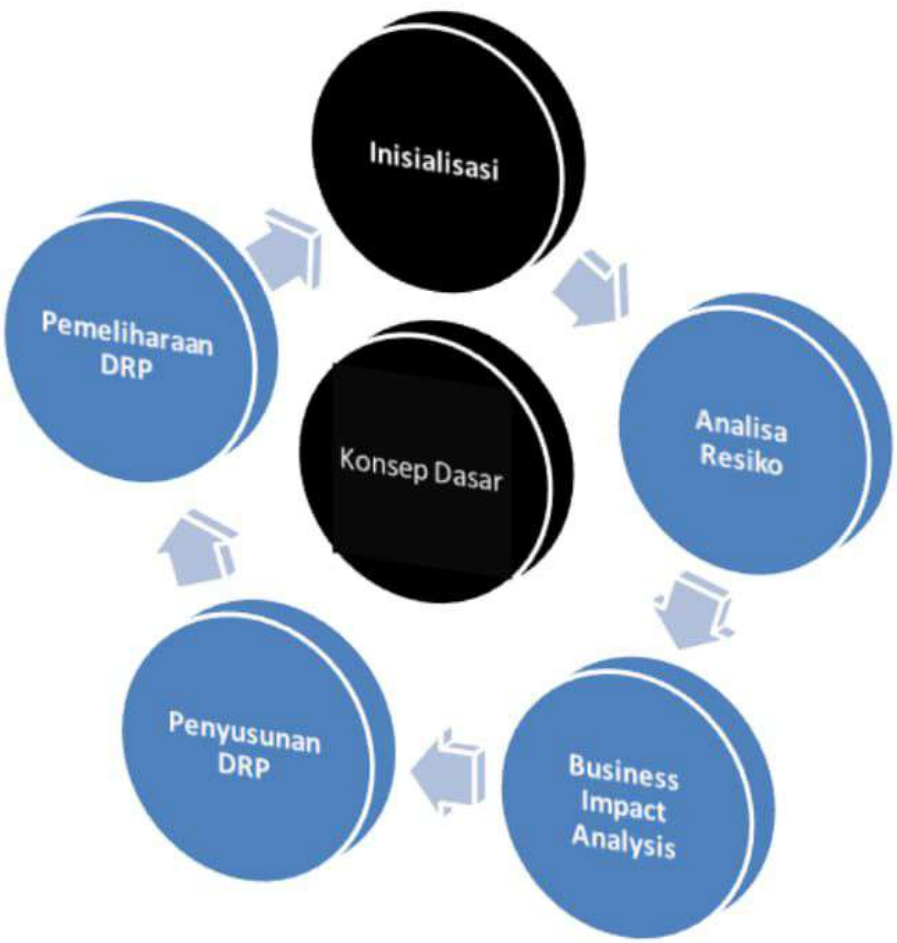
Sebagai contoh sederhana, jika terjadi sebuah kebakaran di suatu gedung dan melenyapkan hampir seluruh perangkat keras dan juga perangkat lunak yang ada didalamnya, maka apa yang akan terjadi ? Meski DRP telah dicanangkan sebelumnya dengan melakukan *remote and separate backup*, tetapi proses recovery bisa jadi akan tidak sepenuhnya berjalan karena faktor

trauma maupun kepanikan yang umumnya terjadi pada para karyawan pasca bencana.

Terlebih lagi jika pada saat bencana terjadi terjadi korban dari sisi manusia, maka nantinya sangat perlu dicadangkan corporate officer yang akan melakukan proses pemulihan. Dan tentu saja pemilhan corporate office ini nantinya memerlukan sebuah kejelian dari pihak manajemen agar implementasi DRP dapat berjalan sebagaimana mestinya.

Dari contoh tersebut, dapat dibayangkan apa yang seharusnya dilakukan oleh pihak manajemen dalam menyusun DRP dengan tujuan untuk mencapai BCP yang sesungguhnya. Perhitungan dari segi perangkat keras, perangkat lunak dan juga segi manusia haruslah diperhitungkan dalam rencana secara detail dan jelas, dan tidak hanya berhitung dari segi hal-hal yang pasti, tetapi juga memperhitungkan sisi kemanusiaan dan juga sisi manajerial didalamnya.

Tahap I : Inisialisasi



Pemahaman Organisasi

Aset paling berharga dari sebuah organisasi adalah karyawan yang memiliki "knowledge" yang tepat guna bagi kemajuan organisasi

Tahapan pertama dalam melakukan DRP untuk menuju ke BCP adalah tahapan inisialisasi. Di dalam tahapan ini terdapat tiga langkah utama yang harus dilakukan yaitu :

1. Pemahaman organisasi
2. Komitmen manajemen
3. Perencanaan awal

Pada bab ini akan dibahas terlebih dulu mengenai pemahaman organisasi yang harus dilakukan sebelum ke langkah perencanaan awal.

Unsur Tahapan Inisialisasi

Yang dimaksud dengan jenis organisasi dalam konteks ini adalah jenis organisasi yang melakukan

implementasi sistem informasi yang didalamnya akan diterapkan DRP. Secara umum, jenis organisasi dalam konteks DRP terbagi menjadi tiga jenis yaitu :

1. Organisasi yang sepenuhnya bergantung terhadap sistem informasi.

   Jenis organisasi ini merupakan jenis organisasi yang paling membutuhkan implementasi DRP didalamnya. Karena berhentinya operasional sistem informasi di dalam organisasi jenis ini akan menyebabkan seluruh proses bisnis akan terhenti dan kerugian yang diderita akan sangat jelas terlihat, baik dari sisi finansial maupun dari sisi kepercayaan pelanggan.

Konsep *zero defect* yaitu konsep yang menafikan kesalahan di dalam proses operasional yang menggunakan sistem informasi didalamnya

Sebagai contoh, sebuah bank yang telah sepenuhnya seluruh proses bisnisnya berjalan dari sebuah sistem informasi, maka dalam konteks DRP, bank ini akan tergolong ke dalam jenis organisasi yang sepenuhnya bergantung terhadap sistem informasi. Dan tentu saja, dengan tergolong ke dalam jenis organisasi ini, maka bank tersebut mutlak membutuhkan DRP didalamnya. DRP yang nantinya akan diimplementasikan juga tidak hanya sebatas DRP dari segi perangkat keras seperti backup dan sejenisnya, tetapi juga harus secara terintegrasi hingga proses BCP benar-benar dapat tercapai dengan baik.

Organisasi jenis ini, pada umumnya wajib menerapkan konsep *zero defect* yaitu konsep yang menafikan kesalahan di dalam proses operasional yang menggunakan sistem informasi didalamnya. Konsep ini selain meminimalkan terjadinya bencana dalam sistem informasi, juga merupakan salah satu unsur yang harus dipenuhi

dalam BCP, khususnya untuk organisasi yang sepenuhnya bergantung terhadap sistem informasi.

2. Organisasi yang tidak bergantung sepenuhnya terhadap sistem informasi

Organisasi yang pihak manajemennya masih belum sepenuhnya percaya terhadap kehandalan sistem informasi, proses DRP akan sangat sulit untuk diimplementasikan

Jenis organisasi yang kedua merupakan jenis organisasi yang dalam proses bisnisnya tidak sepenuhnya menggunakan sistem informasi didalamnya. Jenis organisasi ini umumnya merupakan jenis organisasi yang masih dalam tahapan proses pengembangan sistem informasi, atau juga bisa jadi jenis organisasi yang pihak manajemennya masih belum sepenuhnya

memiliki tingkat kepercayaan terhadap kehandalan sistem informasi.

Untuk jenis organisasi yang masih dalam tahap pengembangan, proses DRP umumnya menjadi tanggung jawab penuh dari pihak pengembang. Karena dalam proses pengembangan, segala bencana yang terjadi akan sangat berpengaruh terhadap tingkat kepercayaan manajamen terhadap sistem informasi yang sedang berjalan. Dalam tahapan ini pihak manajemen seringkali masih menerapkan proses "coba-coba", dengan melakukan berbagai skenario pengujian terhadap kehandalan sistem informasi yang berjalan di dalam perusahaannya.

Corporate officer merupakan karyawan yang memiliki tanggung jawab terhadap aliran data dalam sebuah sistem informasi.

Sedangkan untuk jenis organisasi yang pihak manajemennya masih belum sepenuhnya percaya terhadap kehandalan sistem informasi, proses DRP akan sangat sulit untuk diimplementasikan. Hal ini diakibatkan karena pihak manajemen belum memiliki komitmen yang tinggi mengenai pentingnya melakukan penyelamatan terhadap sistem informasi pasca bencana, dan tetap berasumsi bahwa BCP dapat dijalankan tanpa memiliki sebuah sistem informasi didalam perusahaan.

3. Organisasi yang berasumsi bahwa sistem informasi hanyalah sebagai aksesori.

   Jenis organisasi yang terakhir dalam konteks DRP adalah jenis organisasi yang terlepas dari pembahasan di dalam buku ini. Organisasi ini sesungguhnya memiliki kebutuhan terhadap implementasi sistem informasi, tetapi karena berbagai jenis alasan, maka sistem informasi yang ada hanyalah dianggap sebagai aksesori oleh pihak manajemen. Aksesori yang dimaksud

disini adalah bahwa sistem informasi hanya dianggap sebagai pelengkap dalam organisasi ataupun hanya sebagai alat untuk membentuk citra organisasi sebagai sebuah organisasi yang modern dan mengikuti perkembangan jaman. Dalam jenis organisasi ini dipastikan tidak akan tercipta sebuah komitmen manajemen yang jelas ataupun budaya organisasi yang menganggap bahwa sistem informasi merupakan "anggota keluarga" bagi kelangsungan hidup proses bisnis yang sedang berjalan.

Dari tiap jenis organisasi yang telah dipaparkan tersebut, maka dapat disimpulkan bahwa jenis organisasi yang termasuk dalam lingkup bahasan DRP hanyalah dua jenis organisasi yang pertama, yaitu organisasi yang sepenuhnya bergantung terhadap sistem informasi dan organisasi yang tidak sepenuhnya bergantung terhadap sistem informasi.

Dari kedua jenis organisasi tersebut, langkah selanjutnya adalah melakukan pemetaan terhadap

corporate officer yang akan diikutsertakan dalam proses DRP. Corporate officer merupakan karyawan yang memiliki tanggung jawab terhadap aliran data dalam sebuah sistem informasi. Sehingga pembagian corporate officer bukanlah berdasarkan pada jabatan ataupun pada level kemahiran di bidang sistem informasi pada sebuah perusahaan, tetapi lebih kepada level tanggung jawab dari pihak yang berkepentingan dalam organisasi tersebut.

Sebagai contoh, corporate officer untuk program penjualan (POS : Point Of Sales), bukan hanya kasir yang bertugas mengoperasikan modul POS, tetapi juga termasuk supervisor dari kasir tersebut sebagai penanggungjawab dari aliran data dalam program penjualan. Artinya bahwa pemetaan corporate officer nantinya akan membedakan peranan karyawan dalam sistem informasi dalam menjalankan tugasnya, bukan hanya berdasarkan jabatan.

Karena salah satu faktor penting dalam penyusunan DRP adalah memetakan cadangan tanggung jawab terhadap tugas yang dilakukan oleh corporate officer ke corporate officer lain.

Pemisahan peran karyawan dalam sistem informasi dibagi menjadi empat jenis yaitu [4] :

1. Authorization

   Merupakan corporate officer yang bertugas untuk melakukan verifikasi terhadap sebuah proses yang terjadi dalam sistem informasi.

2. Custody

   Merupakan corporate officer yang bertugas untuk melakukan pemeliharaan data, khususnya data yang berada dalam proses yang tidak boleh diketahui khalayak umum.

3. Record Keeping

   Merupakan corporate officer yang memiliki tanggung jawab terhadap kelancaran aliran data secara umum, umumnya peran ini diambil oleh

operator yang paling rendah tingkatannya dalam sebuah sistem informasi

4. Reconciliation

   Peran dalam corporate officer yang memiliki tugas sebagai pembanding antara sebuah data dengan data yang lain, dan juga memiliki tugas untuk melakukan penggabungan antara satu data dari sebuah proses yang berbeda, dengan data dari proses yang lain.

Pemisahan Tugas Corporate Officer

Dari tiap peran corporate officer tersebut, nantinya akan sangat berpengaruh terhadap inisialisasi penyusunan DRP. Karena salah satu faktor penting dalam penyusunan DRP adalah memetakan cadangan tanggung jawab terhadap tugas yang dilakukan oleh corporate officer ke corporate officer lain. Sehingga dengan pemisahan tugas yang jelas, dapat dilakukan pencadangan PIC (Person in Charge/ orang yang bertanggung jawab) dalam sebuah proses di sistem informasi.

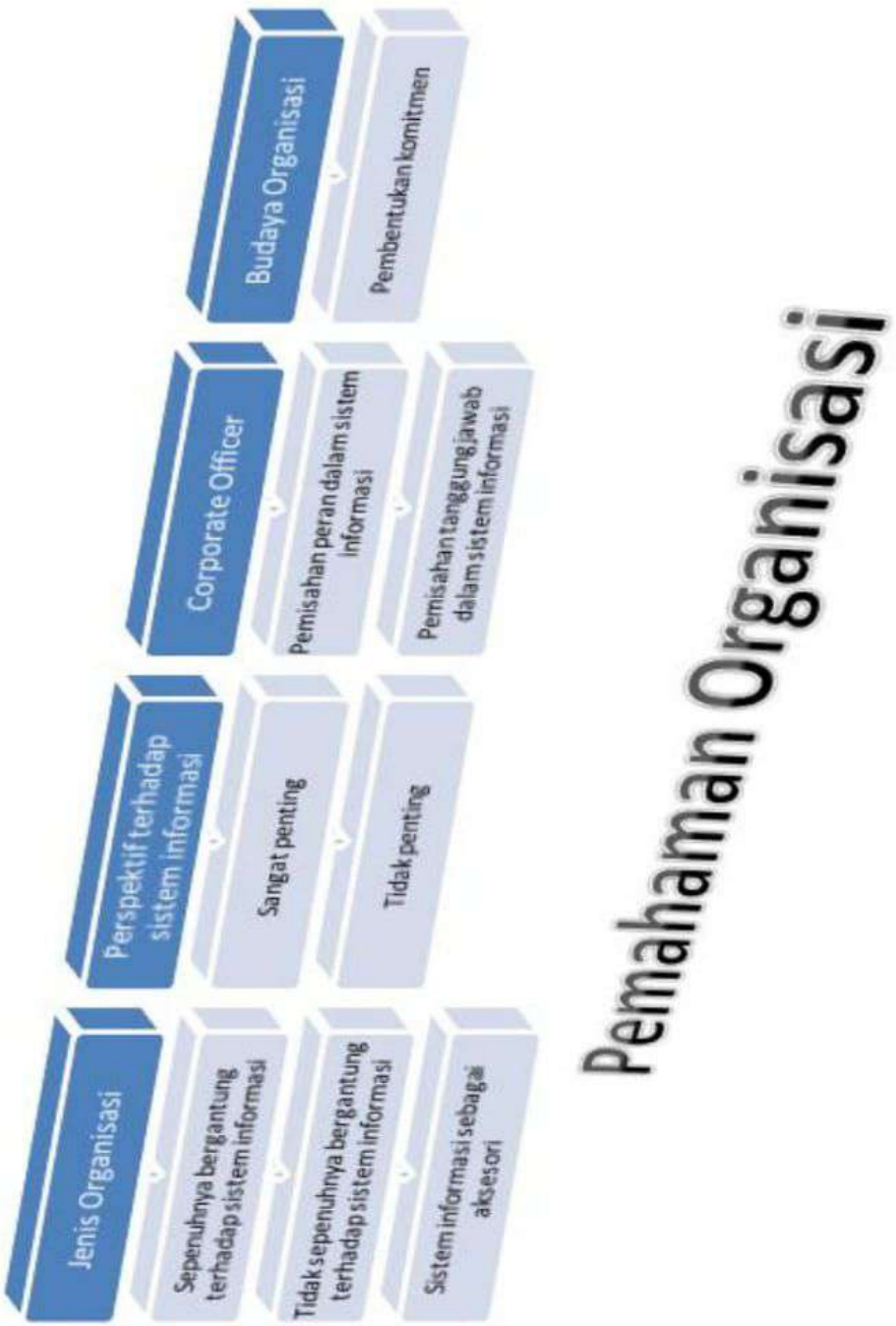
Tahap inisialisasi yang terakhir adalah pemahaman terhadap budaya organisasi yang di tempat yang akan disusun DRP-nya. Budaya organisasi yang dimaksud disini, tentu saja sedikit berbeda dengan budaya organisasi dalam lingkup manajemen sumber daya manusia. Karena budaya organisasi dalam konteks DRP merupakan budaya organisasi yang langsung berpengaruh terhadap kelangsungan proses dalam sistem informasi.

Budaya organisasi merupakan fokus internal dari organisasi itu sendiri, dan nantinya akan

membangun komitmen dari orang-orang yang berada dalam organisasi tersebut untuk mencapai tujuan yang telah ditetapkan [5]. Sehingga pihak manajemen level atas, adalah pihak yang paling bertanggungjawab dalam menetapkan sebuah budaya organisasi.

Pada akhirnya, penentuan budaya organisasi merupakan langkah awal sebelum pihak manajemen mengungkapkan komitmen yang akan dilakukan dalam penyusunan DRP. Sehingga pada saat DRP disosialisasikan, tidak akan terjadi resistensi yang tinggi dari pihak karyawan, yang merupakan komponen penting dalam sebuah penyusunan DRP.

Untuk merangkum seluruh unsur dalam langkah pemahaman organisasi, dapat digambarkan dalam diagram berikut ini :



Rangkuman Pemahaman Organisasi

Komitmen Manajemen

Komitmen ≠ Janji, tetapi sebuah janji dapat menjadi komitmen

Setelah melalui langkah pemahaman terhadap organisasi yang didalamnya akan menerapkan DRP, maka langkah selanjutnya adalah memperoleh komitmen dari pihak manajemen. Komitmen manajemen merupakan faktor yang sangat penting didapat, karena tanpa adanya dukungan dan komitmen dari pihak manajemen, DRP tidak akan pernah dapat terwujudkan.

Hanya jenis organisasi yang sepenuhnya bergantung pada sistem informasi yang akan mendapatkan komitmen manajemen secara utuh dan relatif mudah.

Secara umum, DRP sesungguhnya melibatkan komitmen seluruh *stakeholder* yang berada dalam organisasi tersebut. Stakeholder disini bisa mencakup pihak manajemen, *shareholder* atau *owner*, karyawan dan juga pelanggan. Artinya, bahwa semua pemegang kepentingan dalam

organisasi harus sama-sama waspada dan mau melakukan seluruh rencana yang telah terkonsep dalam DRP saat bencana terjadi.

Tetapi, dari keseluruhan unsur stakeholder tersebut, pemicu utama dari komitmen pelaksanaan DRP adalah pihak manajemen, khususnya dari pihak manajemen level atas. Dan salah satu hal terpenting untuk mendapatkan komitmen tersebut adalah kesadaran dari pihak manajemen itu sendiri.

Dari penjelasan mengenai langkah pemahaman organisasi di sub bab sebelumnya, dapat dikatakan bahwa hanya jenis organisasi yang sepenuhnya bergantung pada sistem informasi yang akan mendapatkan komitmen manajemen secara utuh dan relatif mudah. Di dalam jenis organisasi ini, secara tidak langsung pihak manajemen (seharusnya) dapat diyakinkan mengenai arti pentingnya DRP dalam menjamin *business continuity planning* (BCP) demi kelangsungan hidup organisasi.

Sedangkan dari jenis organisasi yang tidak sepenuhnya bergantung terhadap sistem informasi,

akan sedikit kesulitan untuk meyakinkan pihak manajemen dalam berkomitmen di pelaksanaan DRP. Karena jenis organisasi ini (umumnya) masih memandang sebelah mata mengenai pentingnya DRP bagi kelangsungan hidup organisasinya.

Implementasi komitmen manajemen dalam DRP dapat berupa :

1. Komitmen untuk mengeluarkan biaya dalam rangkaian DRP.

   Meski biaya yang dikeluarkan untuk DRP sangat variatif, dari mulai yang tinggi hingga sangat rendah, tetap harus dicanangkan dalam kerangka berpikir bahwa DRP bukanlah sesuatu yang bisa secara gratis diterapkan. Biaya yang dikeluarkan, besar ataupun kecil, merupakan sebuah beban tersendiri bagi sebuah organisasi. Pengeluaran biaya dalam proses DRP adalah kendala tersendiri saat akan meyakinkan pihak manajemen untuk melakukan DRP. Pihak pencetus DRP haruslah sangat berhati-hati untuk meyakinkan pihak manajemen bahwa biaya yang

dikeluarkan dalam proses DRP (*cost of planning*) sesungguhnya sangat jauh lebih murah dibandingkan biaya yang harus ditanggung saat terjadi bencana (*cost of failure*).

2. Komitmen untuk melakukan pelatihan bagi seluruh corporate officer tanpa terkecuali.

   Saat DRP telah memasuki tahap pelatihan, maka komitmen manajemen akan diuji kembali. Karena pada tahap ini, seluruh pihak yang terkait, khususnya corporate officer harus sama-sama melalui tahap pelatihan. Dalam tahapan ini, seluruh corporate officer dari segala level jabatan harus mau dan mampu melalui tahapan pelatihan. Dan dengan melibatkan seluruh level jabatan, maka mau tidak mau, pihak manajemen harus berkomitmen untuk "memaksa" seluruh corporate officer agar dapat "turun" menjalani pelatihan dalam DRP.
3. Komitmen untuk melakukan audit internal sebagai tindak lanjut dalam DRP

Dengan adanya komitmen manajemen yang kuat, maka tidak ada lagi alibi ataupun kelalaian dalam menerapkan DRP sejak awal proses pengembangan dilakukan.

Dalam tahap perencanaan (yang akan dijelaskan di sub bab selanjutnya), salah satu langkah yang harus dijalani adalah melakukan audit internal sistem informasi. Dalam proses audit internal ini, kelemahan-kelemahan dalam proses bisnis yang berkaitan dengan sistem informasi akan "dibongkar" dan diselami agar proses pembuatan DRP tidak melenceng jauh dari keadaan yang sedang terjadi. Tentu saja hal tersebut nantinya akan mengakibatkan resistensi dari berbagai pihak yang merasa "terbongkar" kelemahannya. Karenanya, komitmen manajemen sangat diperlukan untuk meyakinkan pihak-pihak yang termasuk dalam golongan yang resisten agar dapat memahami bahwa proses audit internal

bukan hanya proses untuk mencari kelemahan, tetapi juga proses untuk mencari solusi, khususnya dalam konteks DRP.

4. Komitmen untuk menetapkan standar DRP dalam tiap pengembangan sistem informasi

   Dengan adanya DRP, maka akan mengakibatkan seluruh proses pengembangan dalam sistem informasi (yang juga dipastikan merupakan pengembangan baru dalam proses bisnis) harus juga mencakup penerapan DRP didalamnya. Secara umum, hal tersebut akan mengakibatkan penambahan waktu untuk penyusunan DRP serta pertimbangan khusus pada saat proses pengembangan dilakukan. Dengan adanya komitmen manajemen yang kuat, maka tidak ada lagi alibi ataupun kelalaian dalam menerapkan DRP sejak awal proses pengembangan dilakukan.

Dari keseluruhan komitmen tersebut, tidak hanya satu saja yang wajib dipenuhi oleh pihak manajemen, tetapi harus seluruhnya. Dan jika dalam

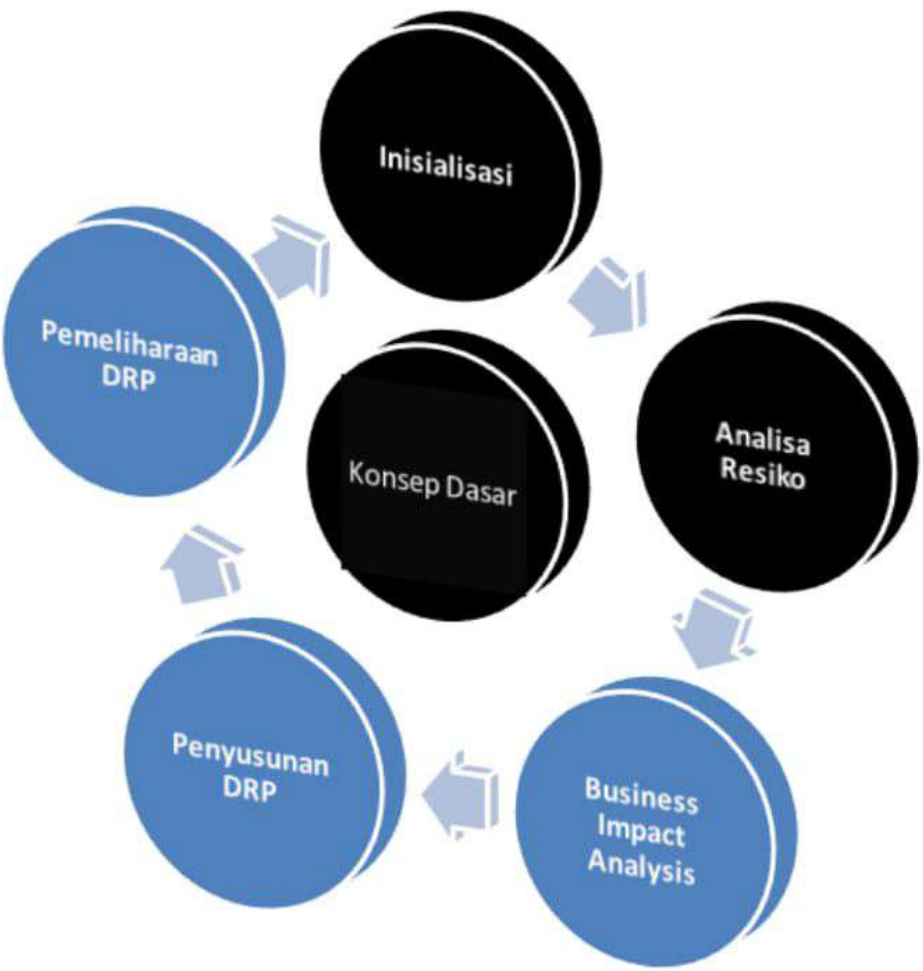
tahapan ini, pihak manajemen tidak mampu diyakinkan agar memiliki komitmen yang tinggi dalam menjalankan DRP, maka bisa dipastikan DRP yang akan dibuat akan gagal di tengah jalan atau tidak berjalan sebagaimana mestinya.

Bukti Komitmen Manajemen Dalam DRP

Hingga sejauh ini.....

Tahap pertama dalam penyusunan DRP adalah melakukan tahapan inisialisasi dalam sebuah organisasi. Tahapan ini mencakup langkah ***pemahaman organisasi*** dan ***komitmen manajemen*** yang harus dilakukan oleh siapapun pelaksana DRP, baik dari pihak internal organisasi ataupun dari konsultan luar organisasi.

Tahap II : Analisa Resiko



Manajemen Resiko

Menjalani usaha tanpa menghitung resiko sama dengan berlayar di samudra dengan menggunakan sekoci tanpa pelampung

Salah satu faktor utama penyebab munculnya teori DRP adalah karena adanya ketakutan akan resiko yang terjadi di kemudian hari akibat hal-hal yang tidak diinginkan. Di dalam bidang ilmu manajemen terdapat sebuah sub bidang yang khusus yang disebut sebagai manajemen resiko.

Definisi dari manajemen resiko sendiri berbeda berdasarkan ruang lingkup yang menyelimuti dari resiko yang akan didefinisikan [6]. Sebagai contoh, definisi manajemen resiko dalam bidang akuntansi sangatlah berbeda dengan manajemen resiko yang terdapat dalam bidang sistem informasi. Begitu juga dengan manajemen resiko yang terdapat dalam konteks DRP.

Resiko juga dapat diartikan sebagai akibat negatif dari hasil kerentanan suatu sistem terhadap kejadian tertentu

Di dalam ruang lingkup DRP, manajemen resiko lebih mengarah kepada pengaturan dan analisa terhadap kejadian yang tidak pasti dan dapat mempengaruhi dari proses bisnis dalam sistem informasi [1]. Tentu saja pengaturan terhadap resiko merupakan inti dari DRP itu sendiri, sedangkan analisa terhadap resiko merupakan salah satu langkah sebelum menuju ke dalam DRP. Di dalam definisi yang lain, manajemen resiko di lingkup sistem informasi adalah proses yang menyeimbangkan antara operasional dan biaya ekonomi untuk hasil perlindungan dalam tujuan untuk melindungi sistem di teknologi informasi dan mendukung tujuan dari organisasi itu sendiri [7].

Sebelum melanjutkan ke tahapan analisa resiko, sangatlah penting untuk memahami resiko itu sendiri. Definisi resiko sendiri juga sangat beragam, tergantung dari ruang lingkup apa yang sedang dihadapi oleh resiko tersebut. Dalam DRP, resiko yang dimaksud adalah resiko bisnis.

Resiko bisnis dalam DRP adalah proses keseluruhan untuk untuk mengidentifikasi, mengendalikan dan menghilangkan atau meminimalkan kejadian-kejadian tidak pasti yang dapat mempengaruhi bisnis. Resiko juga dapat diartikan sebagai akibat negatif dari hasil kerentanan suatu sistem terhadap kejadian tertentu [1].

Dari definisi tersebut, jelas terlihat bahwa resiko bisnis nantinya akan melibatkan proses identifikasi, mitigasi atau pengendalian serta proses untuk menghilangkan atau meminimalkan kejadian tidak pasti yang akan menjadi gangguan. Selain itu, didalamnya juga akan melibatkan proses evaluasi mengenai resiko, khususnya resiko yang dapat muncul di dalam sebuah organisasi, setelah melihat bencana yang terjadi di organisasi atau tempat yang berbeda.

Resiko, di dalam ruang lingkup apapun, merupakan sesuatu yang tak mungkin untuk dihindari oleh sebuah organisasi. Resiko, yang mayoritas dianggap sebagai sesuatu yang negatif

harus dikendalikan agar efek yang terjadi tidak terlalu merugikan.

Agar sebuah resiko mampu dikendalikan, maka perlu dilakukan langkah analisa resiko. Analisa resiko atau *risk analysis* merupakan penggunaan secara sistematis terhadap informasi yang tersedia untuk menentukan kejadian tertentu yang mungkin timbul dan besarnya akibat yang mungkin terjadi [8].

Analisa resiko sangat diperlukan dalam ruang lingkup DRP, karena dengan melakukan analisa resiko yang tepat akan dapat membantu penyusunan langkah-langkah pengendalian sistem informasi pada DRP itu sendiri. Selain itu, dengan analisa resiko yang akurat, tahapan berikutnya dalam penyusunan DRP, yaitu penentuan strategi serta penyusunan respon terhadap krisis dapat dibuat dengan lebih baik dan lebih cepat.

Analisa resiko meliputi tahapan identifikasi resiko serta evaluasi resiko. Kedua tahapan tersebut harus dilakukan secara sekuensial atau berurutan. Di

dalam proses identifikasi (yang akan dijelaskan di sub bab berikutnya) meliputi beberapa proses yang diharapkan mampu mengeluarkan daftar resiko yang potensial terjadi di dalam organisasi tersebut. Sedangkan di dalam evaluasi resiko, akan dikeluarkan daftar yang telah terurut berdasar besarnya akibat yang mungkin terjadi saat resiko tersebut timbul.

Analisa resiko atau *risk analysis* merupakan penggunaan secara sistematis terhadap informasi yang tersedia untuk menentukan kejadian tertentu yang mungkin timbul dan besarnya akibat yang mungkin terjadi

Salah satu kunci utama yang harus diingat dalam melalui tahapan analisa resiko adalah keterbukaan pikiran mengenai resiko yang mungkin terjadi di dalam organisasi tersebut. Bahwa tidak ada satupun sistem informasi yang 100% aman dari

resiko, dan tidak mungkin ada sebuah organisasi yang mampu hidup lancar tanpa gangguan apapun. Tidak peduli apakah organisasi tersebut adalah organisasi profit atau non profit, besar maupun kecil, semuanya akan memiliki resiko didalamnya.

Di dalam proses analisa resiko, secara garis besar, resiko dibagi menjadi tiga jenis berdasarkan sumbernya, yaitu [7] :

1. Berasal dari alam (nature)

   Resiko yang berasal dari alam biasanya dihubungkan dengan lokasi dimana organisasi tersebut berada. Sebagai contoh, sebuah perusahaan yang memiliki letak kantor di daerah sekitar gunung berapi yang sangat aktif akan mendefinisikan resiko jenis ini sebagai resiko nomor satu dalam analisanya. Resiko yang berasal dari alam tidak terbatas pada bencana alam biasa seperti gunung meletus, banjir, gempa bumi, tanah longsor, tsunami ataupun badai. Tetapi juga bisa berasal dari amukan hewan yang tidak bisa dikendalikan seperti

gangguan serangga (kecoa ataupun semut), gangguan hewan peliharaan (misal : kotoran kucing) ataupun gangguan hewan liar (misal : tikus atau sarang burung liar).

2. Berasal dari manusia (human)

   Resiko yang berasal dari manusia dibagi menjadi dua bagian, yaitu kesengajaan dan yang tidak disengaja. Di dalam DRP, melakukan perhitungan resiko yang berasal dari kesengajaan manusia adalah suatu kewajiban. Karena sebuah sistem informasi (betapapun kekuatan keamanan yang dimiliki) sangatlah rentan terhadap gangguan jenis ini. Kesengajaan yang dilakukan manusia bisa saja terjadi karena tingkah laku iseng para *cracker* ataupun perbuatan balas dendam dari karyawan internal ataupun pesaing yang sakit hati terhadap organisasi. Apapun jenis bisnis yang dilakukan oleh sebuah perusahaan, resiko jenis ini tidak mungkin untuk diabaikan begitu saja.

Sedangkan resiko yang berasal dari ketidaksengajaan faktor manusia umumnya berasal dari kesalahan-kesalahan operasional dari dalam organisasi. Salah satu contoh yang seringkali terjadi adalah kesalahan proses input karena ketidaktelitian atau faktor fisik yang lelah dari seorang karyawan. Selain itu, juga bisa terjadi keteledoran karyawan yang menyebabkan peralatan rusak, seperti menumpahkan air minum di atas keyboard atau tersandung oleh kabel secara tidak sengaja.

3. Berasal dari lingkungan (environment)

   Jenis resiko yang terakhir berdasarkan dari asalnya adalah resiko yang berasal dari lingkungan. Lingkungan yang dimaksud di dalam lingkup ini adalah lingkungan secara fisik dari organisasi tersebut. Sebagai contoh adalah sebuah server yang terletak di ruang terbuka akan memiliki resiko yang lebih tinggi dibandingkan sebuah server yang memiliki rak khusus dan tertutup dengan rapi. Server yang

terletak di ruang terbuka dipastikan akan memiliki resiko yang sangat tinggi dibandingkan yang terletak di rak yang tertutup rapi. Selain resiko keamanan, juga resiko yang timbul dari lingkungan yaitu debu serta pengaruh lain seperti tombol power yang bisa tersentuh tanpa sengaja.

Jenis resiko berdasarkan sumber

Threat atau ancaman merupakan resiko potensial yang timbul akibat sebuah kelemahan yang timbul dalam sebuah sistem

Berdasarkan identifikasinya, resiko dibagi menjadi dua jenis yaitu [8] :

1. Threat / ancaman

   Threat atau ancaman merupakan resiko potensial yang timbul akibat sebuah kelemahan yang timbul dalam sebuah sistem [7]. Sebuah threat tidak akan muncul jika tidak terdapat kelemahan yang terekspos oleh sebuah sistem. Ini berarti bahwa sebuah threat hanya akan muncul jika kelemahan dari sebuah sistem diketahui dan diidentifikasi dengan baik oleh pihak luar. Sumber dari ancaman ini bisa berasal dari sebuah ketidaksengajaan yang kemudian memicu sebuah ancaman bagi sistem, misalnya : ketidaksengajaan dalam melakukan input di sebuah proses, sehingga timbul kesalahan

berantai dalam sistem tersebut. Sebagai contoh adalah kesalahan input harga di sebuah data inventory yang kemudian menyebabkan kerugian di dalam proses penjualan. Jika kelemahan tersebut diketahui oleh pihak luar, bukan tidak mungkin akan menjadi sebuah kesengajaan, yaitu dengan berusaha untuk melakukan kesalahan input harga agar pihak tertentu dapat diuntungkan.

2. Vulnerability / kelemahan

   Vulnerability merupakan resiko tidak langsung yang menyebabkan sebuah threat dapat terjadi [7]. Kelemahan ini umumnya terjadi karena ketidaksengajaan ataupun kelalaian dari para pengembang sistem dan juga dari pihak departemen IT yang bertanggungjawab terhadap pemeliharaan sistem itu sendiri.

   Masih banyak pihak yang mengasumsikan bahwa jenis-jenis dari vulnerability lebih kepada arah lalainya setting jaringan komputer, ketidaksengajaan dalam validasi proses input,

kelalaian untuk tidak menghapus data karyawan yang sudah keluar dari perusahaan dan sejenisnya. Padahal vulnerability juga bisa terjadi karena perilaku rutin dari corporate officer yang berada dalam organisasi tersebut. Perilaku rutin tersebut pada akhirnya akan dihapalkan oleh sejumlah pihak dan pada saat-saat tertentu dapat menjadi kelemahan yang akan menjadi sumber ancaman (threat source) bagi sistem.

Resiko berdasarkan identifikasi

Identifikasi Resiko

Takkan pernah ada seorang manajer yang sempurna, karena mengatur manusia bukanlah sebuah pekerjaan sederhana

Langkah pertama yang dilakukan di dalam tahapan analisa resiko adalah melakukan identifikasi resiko yang mungkin terjadi dalam sebuah sistem informasi di dalam organisasi tersebut. Tiap organisasi pasti memiliki jenis resiko yang berbeda dan beragam. Hal tersebut tentu saja bergantung terhadap berbagai faktor seperti jenis organisasi itu sendiri serta lokasi gedung dan juga personil yang terlibat dalam operasional sistem informasi.

Identifikasi resiko atau *risk identification* adalah proses untuk menentukan apa, bagaimana serta mengapa sesuatu atau resiko tersebut dapat terjadi [8]. Di dalam proses identifikasi resiko ini, terdapat beberapa langkah yang harus dikerjakan yaitu :

1. Brainstorming

   Pada langkah pertama ini, perlu dilakukan semacam lokakarya non formal yang dihadiri oleh berbagai elemen dalam organisasi tersebut. Dari hasil lokakarya yang membahas mengenai resiko-resiko yang mungkin terjadi dalam

organisasi, diharapkan akan muncul daftar sementara mengenai resiko di dalam organisasi tersebut.

Tidak ada format khusus di dalam proses brainstorming, tetapi secara umum proses ini dapat dilakukan dengan menyebarkan daftar isian resiko ke tiap individu yang terlibat, kemudian berusaha untuk dibahas secara bersama-sama dalam waktu yang tidak terlalu lama. Hasil dari brainstorming merupakan sesuatu yang penting untuk dibawa ke langkah selanjutnya, karena hasil tersebut nantinya menjadi bahan dasar dalam langkah berikutnya yaitu pemahaman karakteristik sistem.

Identifikasi resiko adalah proses untuk menentukan apa, bagaimana serta mengapa sesuatu atau resiko tersebut dapat terjadi

2. Pemahaman karakteristik sistem

   Dari hasil brainstorming, yaitu daftar resiko non formal yang dibuat oleh berbagai elemen dalam organisasi, maka akan muncul pemahaman terhadap karakteristik sistem yang ada dalam organisasi tersebut. Karakteristik yang dimaksud disini adalah karakter dari unsur yang ada dalam sistem informasi seperti perangkat keras, perangkat lunak, data serta sensitifitas sistem terhadap lingkungan. Karena dengan mengetahui daftar resiko yang mungkin terjadi, pihak manajemen akan tahu titik lemah sekaligus juga keunggulan dari sistem yang dimiliki.

   Pada proses ini, pihak manajemen dari level menengah akan dikumpulkan ulang untuk membahas mengenai hasil brainstorming. Kemudian dari hasil tersebut dikeluarkan daftar baru yaitu mengenai karakteristik sistem yang dimiliki, sifat dari tiap unsur yang ada di dalam sistem informasi, termasuk didalamnya kelemahan serta keunggulan yang dapat

dimanfaatkan untuk kepentingan langkah selanjutnya.

3. Pembuatan daftar resiko

   Langkah yang ketiga adalah mendaftarkan segala jenis resiko yang dapat muncul. Daftar dari resiko atau seringkali disebut *risk checklist* ini disusun berdasarkan proses brainstorming dan kemudian disaring kembali dari proses pemahaman karakteristik sistem.

   Di dalam pembuatan daftar resiko yang ideal, harus dikemukakan mengenai elemen-elemen kunci (key elements) pada daftar tersebut. Hal ini dilakukan supaya daftar resiko yang dibuat tidak terlalu berlebihan dan tidak terlalu sedikit. Daftar resiko yang berlebihan akan mencerminkan ketakutan yang berlebihan dari pihak manajemen mengenai lemahnya sistem yang ada dalam organisasi tersebut. Sedangkan daftar resiko yang terlalu sedikit akan membiaskan kesan arogansi dari organisasi tersebut.

Akibatnya, pembuatan daftar resiko memang harus melibatkan berbagai pihak dan wajib didahului oleh dua langkah sebelumnya (yang seringkali diabaikan oleh pihak manajemen). Karena dua langkah sebelumnya (brainstorming dan pemahaman karakteristik sistem) merupakan langkah yang sangat berpengaruh terhadap keakuratan pembuatan daftar resiko dalam sebuah organisasi.

Control analysis merupakan pengendalian terhadap hal-hal yang telah diimplementasikan atau sedang direncanakan, agar resiko berupa threat yang berasal dari vulnerability dapat diminimalisasi atau bahkan dihilangkan sama sekali.

4. Analisa pengendalian

   Setelah daftar resiko (yang dianggap paling akurat) pada organisasi tersebut selesai dibuat,

maka langkah berikutnya adalah melakukan analisa pengendalian (control analysis) terhadap daftar resiko yang telah dibuat. Control analysis merupakan pengendalian terhadap hal-hal yang telah diimplementasikan atau sedang direncanakan, agar resiko berupa threat yang berasal dari vulnerability dapat diminimalisasi atau bahkan dihilangkan sama sekali.

Salah satu langkah sederhana dalam melakukan analisa pengendalian adalah dengan melakukan *impact analysis* atau analisa terhadap akibat yang mungkin terjadi jika sebuah resiko ternyata menjadi kenyataan. Dengan membayangkan (atau juga mengamati dari akibat yang sudah terjadi, baik dari organisasi lain atau dari internal) mengenai efek negatif yang akan terjadi, dapat dibuat daftar dari hasil analisa pengendalian.

Pembuatan daftar dari analisa pengendalian akan menghasilkan rekomendasi-rekomendasi yang wajib diwaspadai dan juga rekomendasi

pengendalian yang harus dilakukan oleh seluruh corporate officer yang berada dalam organisasi tersebut. Seluruh daftar hasil analisa pengendalian haruslah diketahui oleh seluruh unsur organisasi, baik yang berada dalam posisi sebagai corporate officer ataupun unsur lain yang terlibat secara tidak langsung didalamnya.

5. Dokumentasi

   Langkah terakhir dalam identifikasi resiko adalah melakukan dokumentasi terhadap seluruh hasil identifikasi resiko yang sudah dilakukan. Dokumentasi dalam konteks identifikasi resiko, bukan hanya berupa daftar dari resiko yang mungkin dihadapi oleh organisasi tersebut, tetapi juga rekomendasi dari hasil analisa pengendalian yang sudah ditetapkan sebelumnya.

   Dokumentasi sebaiknya tidak hanya berupa sebuah daftar yang disajikan dalam bentuk tabular, tetapi juga berupa *system flow* atau alur sistem yang akan menggambarkan orang-orang yang terlibat dalam pengendalian resiko serta

tindakan apa yang harus dilakukan jika sebuah resiko menjadi kenyataan dan menimbukan efek yang saling bertautan (chain reaction) dari satu threat ke threat yang lain.

Risk Identification

Departmen :.....

Tanggal : .....

Jenis Resiko	Pengendalian	Person In Charge
1. ..... 2.		
Supervisor		

Contoh Dokumentasi Identifikasi Resiko

Contoh dokumentasi tersebut, bisa saja disusun dengan lebih detail didalamnya. Misalnya dengan menyebutkan sejarah mengenai kemungkinan resiko yang telah terjadi sebelumnya, baik di dalam organisasi itu sendiri, maupun di organisasi lain yang serupa. Selain itu, juga dapat menyebutkan corporate officer yang memiliki resiko tinggi untuk menyebabkan threat ataupun

menyebutkan satu per satu mengenai vulnerability yang dimiliki oleh sistem pada daftar yang berbeda.

Langkah Identifikasi Resiko

Catastrophic merupakan tingkat kerugian terbesar yang mampu meruntuhkan eksistensi dari organisasi.

Di dalam identifikasi resiko, selain menggunakan langkah-langkah yang telah disebutkan, didalamnya juga melibatkan tingkat kerugian dari resiko yang mungkin terjadi. Tingkat kerugian tersebut dapat berupa [8] :

1. Catastrophic

   Merupakan tingkat kerugian terbesar yang mampu meruntuhkan eksistensi dari organisasi. Tingkat kerugian ini umumnya terjadi akibat resiko dari bencana alam yang besar ataupun dari faktor manusia akibat kesengajaan.

2. Major

   Merupakan tingkat kerugian besar dan terjadi pada saat-saat kritis di dalam suatu organisasi, misal : kegagalan penyimpanan pada transaksi kasir di sebuah supermarket.

3. Moderate

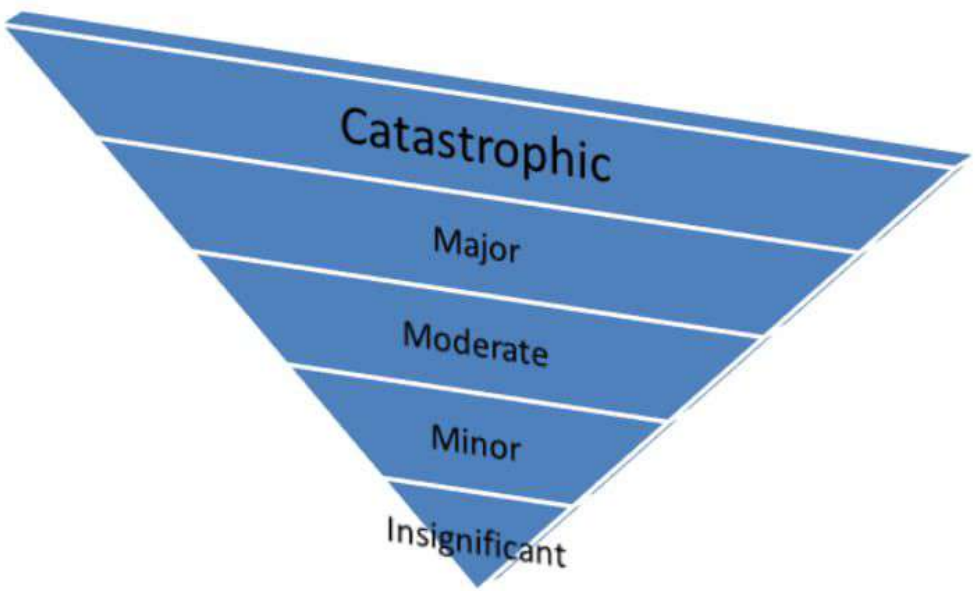
   Merupakan tingkat kerugian yang dianggap sedang, karena masih bisa diatasi dengan cepat menggunakan daftar dari hasil analisa pengendalian.

4. Minor

   Merupakan tingkat kerugian yang kecil dan tidak terlalu mengganggu jalannya operasional sistem. Sehingga seringkali menjadi sebuah ancaman rutin yang mampu diatasi oleh hampir semua orang dalam organisasi.

5. Insignificant

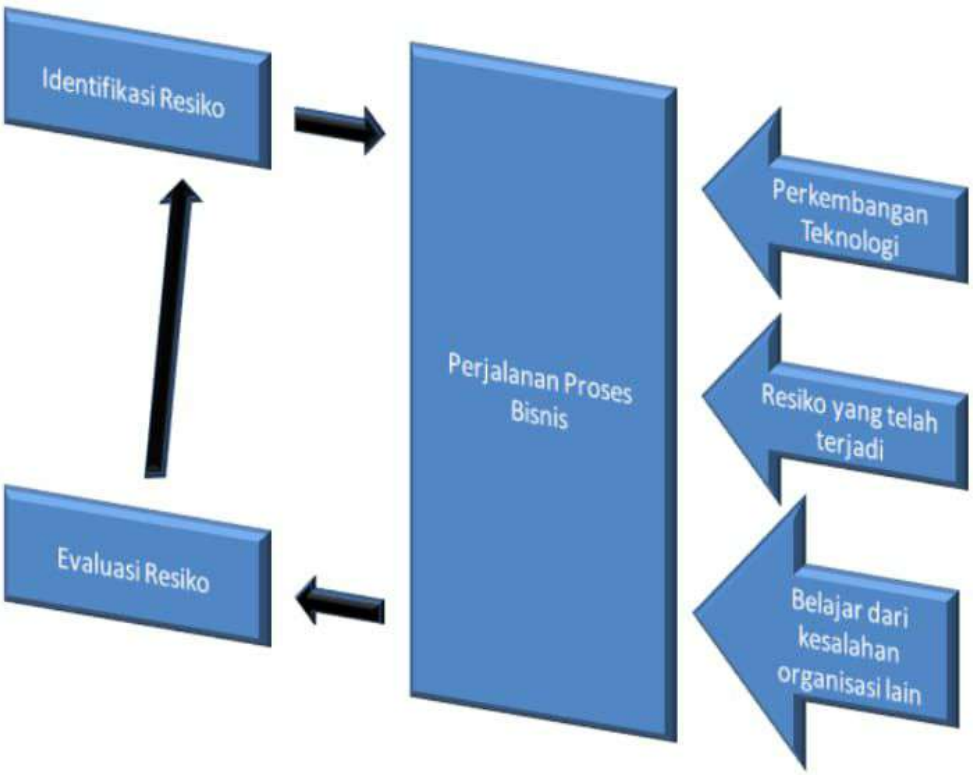
   Merupakan kerugian yang biasanya diabaikan oleh organisasi.



Piramida Tingkat Kerugian

Evaluasi Resiko

Tuhan tidak akan pernah menetapkan sebuah musibah kepada manusia kecuali manusia tersebut mampu mengatasinya



Belajar dari resiko yang sudah ada ?

Evaluasi resiko atau *risk evaluation* dapat didefinisikan sebagai proses menentukan apakah resiko yang terjadi dapat ditoleransi atau tidak, serta mengidentifikasi resiko tertinggi yang mungkin terjadi agar dapat diwaspadai [8]. Evaluasi resiko merupakan kewajiban yang paling sering dilupakan oleh pihak manajemen. Evaluasi resiko juga

didefinisikan sebagai sebuah proses analisa ulang hasil identifikasi resiko yang telah dilakukan, dan melakukan perubahan akibat dari faktor tertentu yang telah terjadi.

Kebutuhan akan evaluasi resiko merupakan dampak dari adanya perkembangan teknologi yang pasti akan menambah pula resiko yang bakal terjadi terhadap sistem dalam sebuah organisasi. Selain itu, organisasi juga harus belajar dari akibat-akibat yang telah muncul dari resiko, baik yang sudah masuk di dalam daftar resiko sebelumnya maupun yang belum ada dari daftar identifikasi resiko.

Evaluasi resiko atau *risk evaluation* dapat didefinisikan sebagai proses menentukan apakah resiko yang terjadi dapat ditoleransi atau tidak, serta mengidentifikasi resiko tertinggi yang mungkin terjadi agar dapat diwaspadai

Perkembangan teknologi tentu saja akan memberi banyak manfaat, tetapi juga harus diperhitungkan mengenai kemungkinan bertambahnya resiko yang harus juga diperhitungkan. Sebagai contoh, adalah perkembangan teknologi di bidang sistem operasi yang tidak hanya menawarkan semakin banyak fasilitas dan kemudahan tetapi juga menawarkan resiko yang semakin banyak. Misalnya, kemunculan versi sistem operasi Windows Vista, ataupun upgrade versi distro Linux yang hampir dipastikan akan muncul secara berkala dari tiap vendor.

Selain disikapi secara positif, dengan mengikuti perkembangan teknologi tersebut, juga harus dipersiapkan dan dikendalikan terlebih dulu resiko yang akan terjadi jika dilakukan upgrade ataupun penyesuaian di dalam sistem.

Sedangkan resiko yang sudah terjadi juga harus diamati dengan seksama oleh pihak manajemen. Ini berlaku untuk resiko yang sebelumnya telah diidentifikasi maupun untuk resiko

yang sama sekali tidak diduga datangnya. Dari segala akibat yang sudah terjadi, hendaknya dilakukan analisa ulang serta catatan-catatan mengenai akibat yang ditimbulkan serta penanganan yang telah dilakukan.

Faktor lain yang melandasi kepentingan evaluasi resiko adalah pentingya belajar dari kesalahan organisasi lain dalam sebuah perjalanan proses bisnis. Baik dari organisasi yang sejenis maupun dari organisasi yang tidak sejenis.

Bahwa resiko, baik berupa threat ataupun vulnerability, bukanlah sebuah aib yang harus ditutupi dan malu untuk diakui bagi sebuah organisasi. Resiko merupakan suatu hal yang akan selalu terjadi di setiap organisasi.

Dari ketiga faktor utama tersebut, maka langkah penting yang harus dilakukan adalah melakukan evaluasi resiko dari hasil identifikasi

resiko yang telah dilakukan sebelumnya. Evaluasi ini dapat dilakukan tepat setelah identifikasi resiko selesai dilakukan oleh pihak manajemen level atas, atau juga dapat dilakukan secara berkala oleh seluruh pihak manajemen.

Evaluasi resiko secara berkala akan bisa berhasil jika di dalam organisasi terdapat orang-orang tertentu yang bertugas untuk melakukan monitoring terhadap resiko. Monitoring tersebut bukan hanya dilakukan sebagai sebuah standard operasional prosedur, tetapi lebih sebagai kesadaran terhadap dampak negatif yang akan terjadi saat resiko menjadi sebuah realita.

Monitoring terhadap resiko yang terjadi, tidak harus melakukan pencatatan terhadap semua kejadian, tetapi cukup mencatat pada resiko dengan tingkat kerugian level moderate ke atas (lihat piramida tingkat kerugian di sub bab sebelumnya). Biasanya hal tersebut disebut dengan *critical incident monitoring* yaitu monitoring terhadap kejadian-

kejadian yang dianggap kritis bagi kelangsungan hidup sebuah sistem di dalam organisasi.

Hal terakhir yang sangat perlu diperhatikan di dalam evaluasi resiko adalah keterbukaan pikiran dari seluruh unsur yang ada di dalam organisasi mengenai resiko. Bahwa resiko, baik berupa threat ataupun vulnerability, bukanlah sebuah aib yang harus ditutupi dan malu untuk diakui bagi sebuah organisasi. Resiko merupakan suatu hal yang akan selalu terjadi di setiap organisasi.

Yang diperlukan bukanlah menganggap bahwa resiko adalah aib, tetapi menetapkan asumsi bahwa resiko adalah sesuatu yang wajib diwaspadai dan direncanakan cara penanganannya. Dan dari titik tolak pemikiran ini, maka evaluasi resiko tidak akan lagi menjadi sebuah kegiatan rutin berkala yang menghasilkan setumpuk kertas dokumentasi biasa, tetapi akan menghasilkan kewaspadaan dan kebijakan baru dalam organisasi untuk lebih berhati-hati dalam menjalani proses bisnis.

Hingga Sejauh Ini .....

Dari hasil analisa resiko yang terdiri dari pemahaman mengenai ***manajemen resiko, identifikasi resiko*** serta ***evaluasi resiko***, akan menghasilkan sebuah daftar resiko beserta rekomendasi mengenai apa yang harus dilakukan untuk menangani resiko tersebut jika suatu saat terjadi.

Dalam tahapan analisa resiko sangat dibutuhkan percobaan yang berulang-ulang serta siklus proses yang mungkin cukup melelahkan dan seringkali dianggap sia-sia bagi banyak pihak.

Hasil dari analisa ini nantinya akan menjadi landasan bagi tahapan berikutnya yaitu melakukan penyusunan analisa pengaruh bisnis atau *business impact analysis*. Karena tanpa adanya analisa resiko

yang akurat, penyusunan business impact analysis tidak akan pernah terwujud dengan baik.

Tentu saja di dalam tahapan analisa resiko sangat dibutuhkan percobaan yang berulang-ulang serta siklus proses yang mungkin cukup melelahkan dan seringkali dianggap sia-sia bagi banyak pihak. Hal ini dikarenakan pada saat melakukan analisa resiko, orang lebih banyak berpikir tentang keunggulan sistem yang dimiliki, bukan kelemahan. Dan umumnya banyak pihak baru akan berpikir dengan baik mengenai analisa resiko saat sebuah bencana sudah terjadi dalam organisasi tersebut, yang tentu saja akan menjadi sebuah proses yang sangat terlambat untuk dilakukan.

Siklus Analisa Resiko

Tahap III : Business Impact Analysis

Penyusunan Business Impact Analysis

Setiap organisasi memiliki faktor kunci yang menjadi urat nadi dari proses bisnis didalamnya, dan yang wajib dilakukan adalah memahami serta memelihara faktor tersebut sebaik mungkin

Di dalam setiap organisasi, akan selalu terdapat beberapa faktor kunci atau *key factors* yang akan menjadi elemen terpenting dalam kelangsungan hidup organisasi tersebut. Sebagai contoh di sebuah perusahaan distributor, maka salah satu faktor kuncinya adalah di bagian pemasaran yang menjadi ujung tombak dari perusahaan. Karena tanpa adanya bagian pemasaran dalam sebuah perusahaan distributor, maka perusahaan tersebut akan terhenti.

Contoh lain lagi adalah pada sebuah perusahaan manufaktur yang salah satu faktor kuncinya adalah operasional mesin di dalam pabrik. Inti dari contoh-contoh tersebut adalah bahwa faktor-faktor kunci yang menjadi penentu dalam sebuah organisasi haruslah teridentifikasi dengan baik oleh pihak manajemen, khususnya dalam hubungannya dengan disaster recovery planning.

Identifikasi faktor-faktor ini sepintas terlihat sangat mudah bagi pihak manajemen ataupun bagi pihak penyusun DRP. Tetapi sesungguhnya

identifikasi dari faktor-faktor tersebut seringkali tidaklah akurat. Hal ini disebabkan pihak manajemen lebih memandang faktor-faktor kunci hanya dari satu sudut pandang. Padahal, faktor kunci harus dilihat dari berbagai sudut pandang dan dianalisa dengan sangat cermat.

Departemen atau bagian yang memiliki resiko terbesar jika dilihat dari tingkat kerugian yang bisa dihasilkan, maka didalamnya akan terdapat faktor-faktor kunci yang perlu lebih lanjut ditelaah oleh pihak penyusun DRP.

Salah satu metode terbaik untuk mengidentifikasi faktor kunci yang berpengaruh dalam proses bisnis adalah dengan menggunakan analisa resiko seperti yang telah dijelaskan di bab sebelumnya. Dari hasil analisa resiko tersebut, nantinya akan muncul peringkat resiko dengan

berdasarkan pada tingkat kerugian yang mungkin muncul dari resiko tersebut.

Selanjutnya, dari peringkat resiko tersebut barulah dapat ditentukan faktor-faktor kunci yang menjadi urat nadi dalam suatu organisasi. Karena, departemen atau bagian yang memiliki resiko terbesar jika dilihat dari tingkat kerugian yang bisa dihasilkan, maka didalamnya akan terdapat faktor-faktor kunci yang perlu lebih lanjut ditelaah oleh pihak penyusun DRP.

Business impact analysis bertujuan untuk menghubungkan antara komponen sistem secara spesifik terhadap layanan kritis yang disediakan, serta menyatakan karakteristik dari akibat yang mungkin muncul terhadap gangguan pada komponen sistem tersebut

Saat faktor-faktor penting tadi telah disusun, maka secara tidak langsung pihak penyusun DRP juga telah melaksanakan sebagian dari tahapan business impact analysis, yaitu analisa mengenai pengaruh bencana terhadap sebuah organisasi.

Di dalam ruang lingkup DRP, business impact analysis bertujuan untuk menghubungkan antara komponen sistem secara spesifik terhadap layanan kritis yang disediakan, serta menyatakan karakteristik dari akibat yang mungkin muncul terhadap gangguan pada komponen sistem tersebut [1]. Sehingga, business impact analysis dapat dikatakan sebagai lanjutan dari tahapan analisa resiko.

Di dalam lingkup DRP, business impact analysis dilakukan dengan mengikuti langkah-langkah berikut :

1. Identifikasi faktor kunci

   Seperti telah dijelaskan sebelumnya bahwa identifikasi faktor kunci merupakan langkah

terpenting dalam memulai proses business impact analysis.

2. Menetapkan kebutuhan untuk pemulihan proses bisnis

   Pada saat analisa resiko dilakukan, selain memunculkan peringkat resiko berdasarkan tingkat kerugian, juga menampilkan rekomendasi yang harus dilakukan oleh corporate officer dalam mengatasi resiko tersebut. Di dalam business impact analysis, ditambahkan kolom baru yang menjelaskan kebutuhan apa saja yang harus dilakukan agar proses bisnis dan layanan sistem informasi dapat berjalan normal kembali setelah sebuah bencana terjadi.

   Kebutuhan yang dimaksud dalam konteks ini bisa berupa kebutuhan biaya, kebutuhan peralatan dan juga kebutuhan personil didalamnya. Kebutuhan biaya, seperti telah dijelaskan pada bab sebelumnya membutuhkan komitmen manajemen yang sangat tinggi. Karena dengan mengungkapkan kebutuhan

biaya, berarti pihak manajemen harus menyediakan dana cadangan yang diikutsertakan dalam anggaran rutin. Akibatnya, bila tanpa komitmen dari pihak manajemen (khususnya level atas), tidak akan mungkin terjadi tahapan-tahapan yang harus dilakukan dalam DRP.

Kebutuhan peralatan juga harus diinventarisasi sebagai sebuah cadangan jika peralatan yang tersedia pada suatu saat tidak berjalan sebagaimana mestinya. Sebagai contoh, jika pada suatu saat sebuah server mengalami gangguan, maka perlu diinventarisasi komputer yang akan dijadikan sebagai cadangan server.

Penetapan PIC cadangan haruslah dari personil inti yang tidak terlibat dalam pengembangan sistem informasi.

Komputer cadangan tersebut bukan berarti harus memiliki spesifikasi yang sama dengan server,

tetapi minimal harus mampu menjadi server sementara selama server utama tidak berfungsi dengan baik. Bahkan seringkali komputer cadangan tersebut hanya berasal dari salah satu komputer workstation yang dianggap memiliki kapabilitas cukup sebagai server temporer.

Sedangkan untuk kebutuhan personil yang sering disebut sebagai PIC (person in charge) atau orang yang bertanggungjawab terhadap suatu tugas, merupakan salah satu proses dalam business impact analysis yang dianggap tersulit untuk dilakukan. Hal ini dikarenakan penetapan PIC cadangan haruslah dari personil inti yang tidak terlibat dalam pengembangan sistem informasi. Sebagai contoh, pemilihan PIC untuk admin server cadangan yang berasal dari karyawan yang posisinya berada di luar departemen IT. Pemilihan personil untuk posisi tersebut tentu saja tidak semudah yang dibayangkan, karena pada umumnya personil yang berada di luar departemen IT bukanlah

orang yang memiliki latar belakang pendidikan IT. Akibatnya, pihak manajemen harus jeli untuk melakukan pemilihan personil yang tepat.

Selain kesulitan dalam memilih orang yang tepat dan dianggap bisa melakukan tugasnya, dengan melakukan pelatihan-pelatihan tertentu, PIC yang dipilih juga harus memiliki integritas yang tinggi terhadap organisasi. Sebab dengan menjadi PIC cadangan berarti juga memegang beberapa faktor kunci yang jika disalahgunakan akan berakibat sangat fatal bagi organisasi itu sendiri. Misalnya, PIC yang ditunjuk sebagai cadangan admin server, apabila menyalahgunakan penggunaan password server maka dapat menyebabkan layanan sistem informasi berhenti atau bahkan menyebabkan resiko jenis threat yang berasal dari human factor menjadi realita.

Dalam penyusunan *chain reaction*, tiap PIC maupun corporate officer harus melakukan langkah yang mirip dengan langkah yang dilakukan pada proses identifikasi resiko.

Kebutuhan Pemulihan Proses Bisnis

3. Menentukan tingkat ketergantungan antar faktor kunci

   Setelah proses identifikasi beserta penetapan kebutuhan dalam business impact analysis dilaksanakan, maka langkah berikutnya adalah mencari keterkaitan antar faktor kunci beserta kebutuhan yang ada. Pencarian keterkaitan antara satu faktor dengan faktor yang lain sangatlah penting untuk menyusun rantai tingkat ketergantungan antar faktor kunci. Rantai reaksi atau *chain reaction* tersebut haruslah benar-benar sangat dipahami oleh para PIC yang telah ditunjuk pada langkah sebelumnya. Dalam penyusunan chain reaction tersebut, tiap PIC maupun corporate officer harus melakukan langkah yang mirip dengan langkah yang dilakukan pada proses identifikasi resiko.

   Langkah tersebut adalah melakukan brainstorming pada saat pertama kali, yaitu setiap PIC dan corporate officer diwajibkan untuk memberikan keterkaitan antara pekerjaan yang

dilakukannya dengan bagian lain dalam organisasi tersebut. Dari hasil brainstorming ini, akan disusun sebuah daftar sementara mengenai tingkat ketergantungan dari departemen atau bagian ke departemen atau bagian yang lain.

Selanjutnya dari hasil brainstorming tersebut, maka pihak penyusun DRP wajib menyusun alur sistem dari daftar ketergantungan di tiap departemen. Alur sistem yang dimulai dari daftar-daftar kecil, selanjutnya dirangkum menjadi sebuah alur sistem besar (grand system flow) yang menggambarkan chain reaction secara utuh dari organisasi tersebut. Tentu saja chain reaction yang disusun juga harus diurutkan berdasarkan skala prioritas tingkat kerugian yang didapat pada saat analisa resiko.

Diharapkan dari gambaran umum chain reaction ini akan dapat dihasilkan sebuah pemikiran baru bagi pihak manajemen dan juga penyusun DRP, agar dapat menetapkan prosedur yang tepat jika satu saat terjadi bencana yang tidak diinginkan.

Selain itu, hasil dari penyusunan chain reaction tersebut juga dapat disosialisasikan kepada seluruh corporate officer dan juga PIC, sehingga tiap personil dapat memahami langkah-langkah penanggulangan resiko, khususnya yang berhubungan dengan antar departemen atau bagian.

Fungsi inti yang bersifat vital umumnya diperlakukan sebagai fungsi sistem yang dalam masa pemulihannya sangat sulit untuk digantikan dengan peralatan lain.

Diagram Alir Penyusunan Chain Reaction

4. Menetapkan prioritas dan klasifikasi proses

   Langkah keempat dalam business impact analysis adalah melakukan penetapan prioritas serta klasifikasi proses dari hasil daftar resiko dan rekomendasi serta alur sistem chain reaction. Jika pada penyusunan chain reaction telah disusun prioritas secara global, maka pada langkah ini, prioritas kembali disempitkan ruang lingkupnya menjadi prioritas untuk tiap proses.

   Klasifikasi proses dibagi berdasarkan kategori kritis dari tiap proses tersebut. Klasifikasi yang dihasilkan tidak akan mungkin sama antara satu organisasi dengan organisasi yang lain, tetapi secara garis besar kategori yang dihasilkan tetap sama. Kategori-kategori kritis tersebut antara lain :

   a. Fungsi kritis yang berkaitan dengan tujuan perusahaan (Critical Function)

      Kategori ini serupa dengan faktor kunci, tetapi yang lebih ditekankan adalah fungsi dari sebuah proses, bukan faktor keterkaitan

dalam resiko. Selain itu, waktu yang diperlukan nantinya pada saat pemulihan sangat lama. Fungsi kritis ini ditetapkan sebagai klasifikasi proses yang tidak bisa ditoleransi lagi resiko yang ada didalamnya.

b. Fungsi inti yang bersifat vital (Vital Function)

   Banyak organisasi yang nantinya tidak memiliki kategori kritis ini. Hal ini disebabkan fungsi inti seringkali dikategorikan sama dengan fungsi kritis dalam suatu organisasi. Tetapi di sebuah organisasi yang beragam departemen dengan fungsi yang bervariasi, bisa jadi kategori kritis ini muncul.

   Fungsi inti yang bersifat vital umumnya diperlakukan sebagai fungsi sistem yang dalam masa pemulihannya sangat sulit untuk digantikan dengan peralatan lain.

c. Fungsi penting yang sangat diperlukan

   Kategori ini juga disebut sebagai *moderate function*. Pada fungsi ini umumnya merupakan fungsi yang bertindak sebagai

syarat utama dalam operasional sehari-hari. Tetapi meski menjadi syarat utama dalam sebuah fungsi operasional rutin, pada saat terjadi bencana atau gangguan masih dapat digantikan dengan peralatan lainnya.

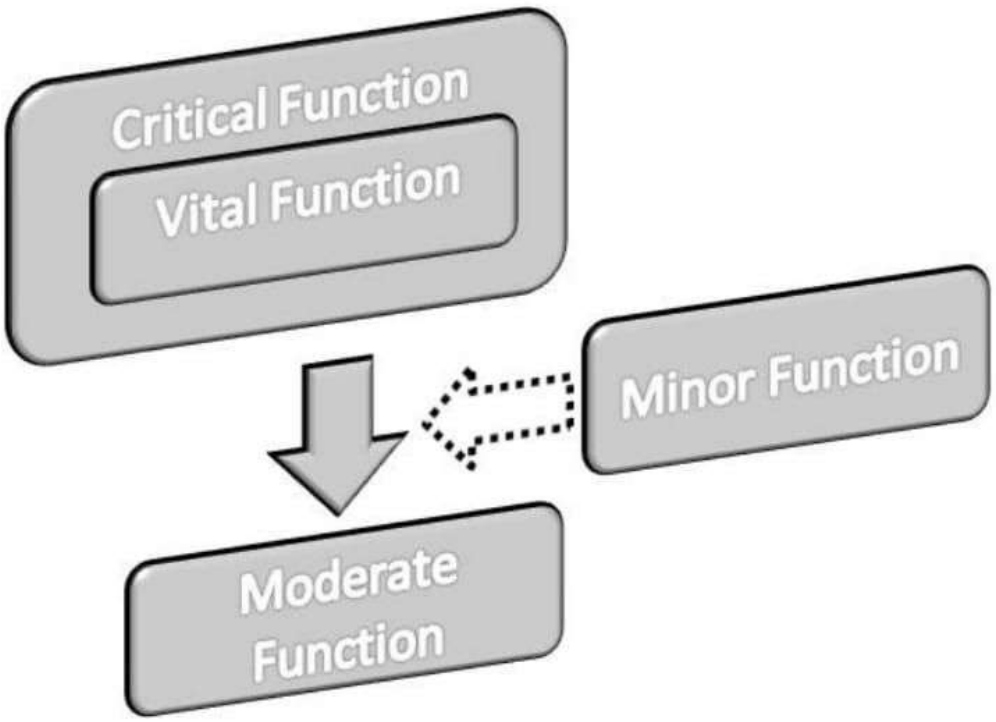
Fungsi dalam kategori ini umumnya waktu pemulihannya memakan waktu yang tidak bisa dibilang singkat, tetapi pada saat terjadi proses pemulihan layanan sistem informasi masih bisa dilakukan dengan baik meski tidak dengan sempurna. Sebagai contoh adalah kerusakan yang terjadi pada UPS yang berada di sebuah lingkup sistem. Meski perbaikan pada UPS tidak akan terjadi dalam waktu satu hari, tetapi sistem masih akan tetap berjalan normal seakan-akan tidak pernah ada gangguan. Begitu pula jika terjadi kerusakan pada modul penggajian di sebuah sistem informasi. Meski pengerjaan perbaikan dapat memakan waktu lebih dari satu minggu, asalkan modul tersebut sudah dapat

diselesaikan perbaikannya pada saat tanggal penggajian, maka kerusakannya tidak akan terlalu banyak dirasakan akibatnya oleh perusahaan.

d. Fungsi minor yang tidak diinginkan (Minor Function)

   Kategori terakhir adalah fungsi minor atau fungsi yang sebenarnya cukup berpengaruh di dalam sebuah sistem, tetapi pada saat terjadi kerusakan semua pihak masih dapat bertoleransi terhadap kerusakan tersebut. Bahkan untuk beberapa kasus, kerusakan dalam kategori ini seringkali diabaikan karena dianggap tidak terlalu penting efeknya dalam sebuah sistem.

   Tetapi, meski seringkali diabaikan, seluruh kerusakan tetaplah harus dipikirkan cara menanggulanginya dan juga waktu yang dibutuhkan pada saat perbaikan dilakukan oleh PIC.



Kategori Proses Kritis

5. Menetapkan waktu pemulihan yang dibutuhkan

   Langkah selanjutnya setelah melakukan klasifikasi proses yang sudah dilakukan, adalah menentukan waktu pemulihan yang dibutuhkan. Penetapan waktu pemulihan tidak lagi didasarkan pada tiap kategori proses, karena pada penetapan waktu lebih mengarah kepada kerangka ukuran saat layanan sebuah sistem

informasi telah berjalan sebagaimana mestinya seperti pada saat operasional rutin.

Waktu pemulihan yang dibutuhkan atau *recovery time* merupakan total waktu yang dibutuhkan untuk kembali ke keadaan normal dari saat bencana terjadi. Dalam perhitungan waktu pemulihan, seluruh satuan yang digunakan haruslah sama, misalnya menggunakan satuan jam atau satuan menit. Sehingga pada saat terjadi sebuah bencana, perkiraan waktu pemulihan tidak akan mengalami bias antara satu personil dengan personil lainnya. Selain itu, dengan satuan waktu yang pasti, maka pihak pelanggan layanan sistem informasi dapat memperkirakan kapan layanan dapat digunakan kembali.

Waktu pemulihan akan berakhir pada saat operasional rutin dapat dilakukan kembali. Hal ini tentu saja dianggap selesai jika telah terjadi verifikasi terhadap integritas data, bahwa data

yang akan diproses merupakan data di saat keadaan normal berlangsung.

Waktu pemulihan yang dibutuhkan atau *recovery time* merupakan total waktu yang dibutuhkan untuk kembali ke keadaan normal dari saat bencana terjadi.

Di dalam konteks business impact analysis, waktu pemulihan terbagi menjadi beberapa bagian yaitu [1] :

a. RPO (Recovery Point Objective)

   RPO merupakan waktu toleransi yang dibutuhkan untuk kembali ke keadaaan normal. Sebagai contoh untuk menghitung RPO adalah periode backup yang ditetapkan dalam sebuah sistem. Seperti jamak diketahui, bahwa periode backup tiap sistem selalui bervariasi. Sebuah sistem bisa saja mengalami periode backup mingguan,

bulanan, harian atau bahkan dua kali dalam sehari. Misalkan sebuah sistem memiliki periode backup harian, maka pada saat terjadi sebuah gangguan atau bencana dalam sistem tersebut, data yang hilang secara kasar perhitungannya maksimal adalah data pada hari tersebut. Dalam kasus ini, RPO dari sistem tersebut adalah satu hari.

b. RTO (Recovery Time Objective)

RTO merupakan waktu yang dibutuhkan untuk mengembalikan sistem ke dalam posisi operasional. Posisi operasional bukan berarti bahwa sistem telah pulih seperti sediakala, tetapi lebih ditekankan kepada pulihnya fungsi kritis (lihat di item sebelumnya mengenai klasifikasi proses) dari sebuah sistem. Sebagai contoh, pada saat sebuah server mengalami kerusakan, dan telah dianalisa bahwa sistem dapat kembali ke operasional rutin dalam tiga hari lengkap dengan fitur verifikasi data. Tetapi server

dapat digunakan kembali dan sistem informasi dapat dijalankan hanya dalam waktu satu hari. Maka dalam contoh tersebut, RTO yang dicatat adalah satu hari, tetapi dalam RTO tersebut tidak mencakup proses pengecekan ulang atau verifikasi data serta pulihnya seluruh workstation.

Integrasi dan verifikasi data lebih mengarah kepada kegiatan pengecekan ulang, titik terhentinya proses saat terjadi bencana kemudian melakukan pengecekan ulang dari titik pada saat posisi operasional pertama.

c. WRT (Work Recovery Time)

WRT adalah waktu yang yang dibutuhkan dalam masa pemulihan sebagai lanjutan dari RTO. Di dalam perhitungan WRT hanya melibatkan proses verifikasi serta integrasi data ataupun perangkat keras, sehingga pada

masa ini benar-benar dilakukan pengecekan secara detail hingga seluruh keadaan kembali ke posisi operasional rutin, baik dari fungsi kritis hinga ke fungsi minor.

Proses integrasi dan verifikasi data bukan hanya sekedar untuk memastikan bahwa data telah siap dioperasionalkan kembali setelah terjadi bencana. Integrasi dan verifikasi data lebih mengarah kepada kegiatan pengecekan ulang, titik terhentinya proses saat terjadi bencana kemudian melakukan pengecekan ulang dari titik pada saat posisi operasional pertama. Sehingga hasil dari proses ini adalah memastikan bahwa tidak ada lagi data yang hilang ataupun tertinggal pada saat pemulihan dilakukan.

d. MTD (Maximum Tolerable Downtime)

MTD adalah gabungan dari RTO dan WRT dalam sebuah proses pemulihan. Seringkali dalam perhitungan MTD ditambahkan waktu yang dibutuhkan untuk transisi dari sebuah

perangkat atau sistem lama ke sistem atau perangkat baru yang dibutuhkan untuk kembali ke dalam keadaan operasional rutin.

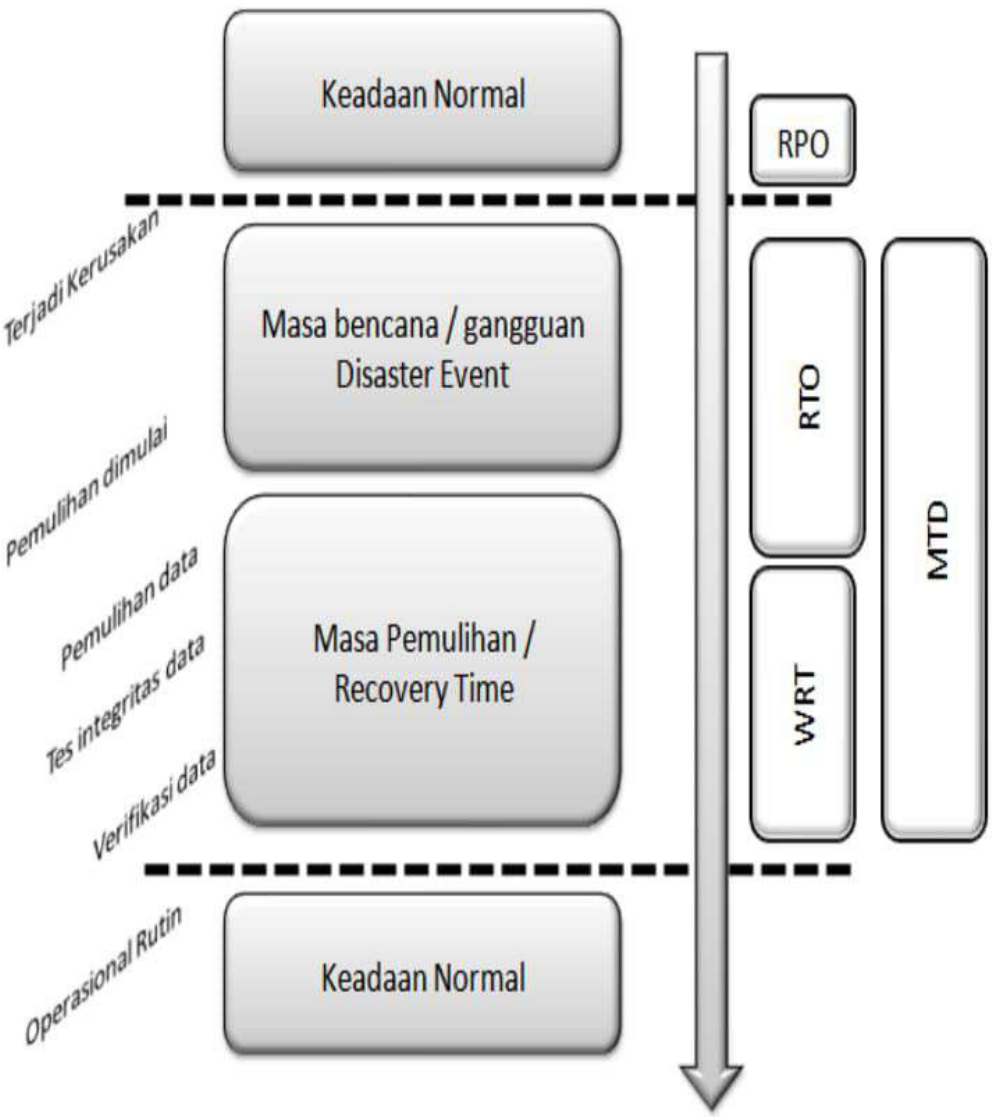


Diagram Waktu Pemulihan

e. Menentukan kerugian secara finansial, operasional dan layanan yang diakibatkan oleh resiko yang mungkin terjadi.

   Di dalam langkah terakhir pada business impact analysis ini seluruh hasil analisa dikuantisasi agar kerugian yang terjadi akibat sebuah bencana dapat dihitung. Perhitungan mengenai kerugian ini sangatlah subyektif berdasarkan tim penyusun DRP yang terlibat didalamnya. Hal ini diakibatkan bahwa perhitungan kerugian dilakukan sebelum sebuah bencana terjadi, sehingga besar kerugian yang sesungguhnya sebenarnya tidak pernah diketahui.

   Pada jenis bisnis yang berkutat di area perdagangan atau jual beli, kerugian finansial dapat didasarkan pada omzet rata-rata yang kemudian dikalikan dengan MTD (maximum tolerable downtime) atau waktu yang hilang akibat proses pemulihan. Tetapi pada beberapa bidang jasa, seringkali perhitungan

tersebut menjadi sulit untuk dilakukan. Sebagai contoh perbandingan, jika sebuah supermarket mengalami bencana gangguan sistem informasi selama tiga hari, maka perhitungan kerugian secara finansial adalah omzet rata-rata dalam sehari dikalikan tiga. Tetapi untuk sebuah perguruan tinggi misalkan, kerugian tersebut bisa bersifat relatif, karena tidak ada omzet yang bisa dikalikan dengan satuan hari.

Kerugian lain yang seharusnya juga ikut dihitung (tetapi seringkali dilupakan) adalah kerugian operasional dan layanan. Kerugian jenis ini sesungguhnya lebih bersifat abstrak karena secara finansial tidak terlalu terlihat dengan jelas. Tetapi, dampak dari kerugian ini adalah menurunnya kepercayaan dari pengguna sistem informasi (dalam hal ini adalah personil organisasi) serta pelanggan terhadap reliabilitas dari sistem informasi itu sendiri. Sehingga kerugian ini juga harus

diperhitungkan untuk membangkitkan kembali *trust* dari pelanggan maupun dari pengguna sistem informasi itu sendiri.

Bisa dibayangkan, seandainya sistem informasi di sebuah supermarket mengalami gangguan di saat *peak time*, maka pelanggan akan langsung mengutarakan komentar negatif, dan bahkan mungkin akan meninggalkan supermarket tersebut. Meski pada akhirnya sistem dapat berjalan normal kembali, tetapi pengguna sistem informasi (sebagai contoh yang terlibat langsung adalah kasir) akan mengalami tingkat stress yang cukup tinggi selama masa pemulihan dilakukan.

Diagram Business Impact Analysis

Respon Krisis

'Perubahan pada dasarnya bukanlah menerapkan teknologi, metode, struktur, atau manajer-manajer baru. Perubahan pada dasarnya adalah mengubah cara manusia dalam berpikir dan berperilaku.' (Rhenald Kasali, dari buku "Re-code your change DNA)

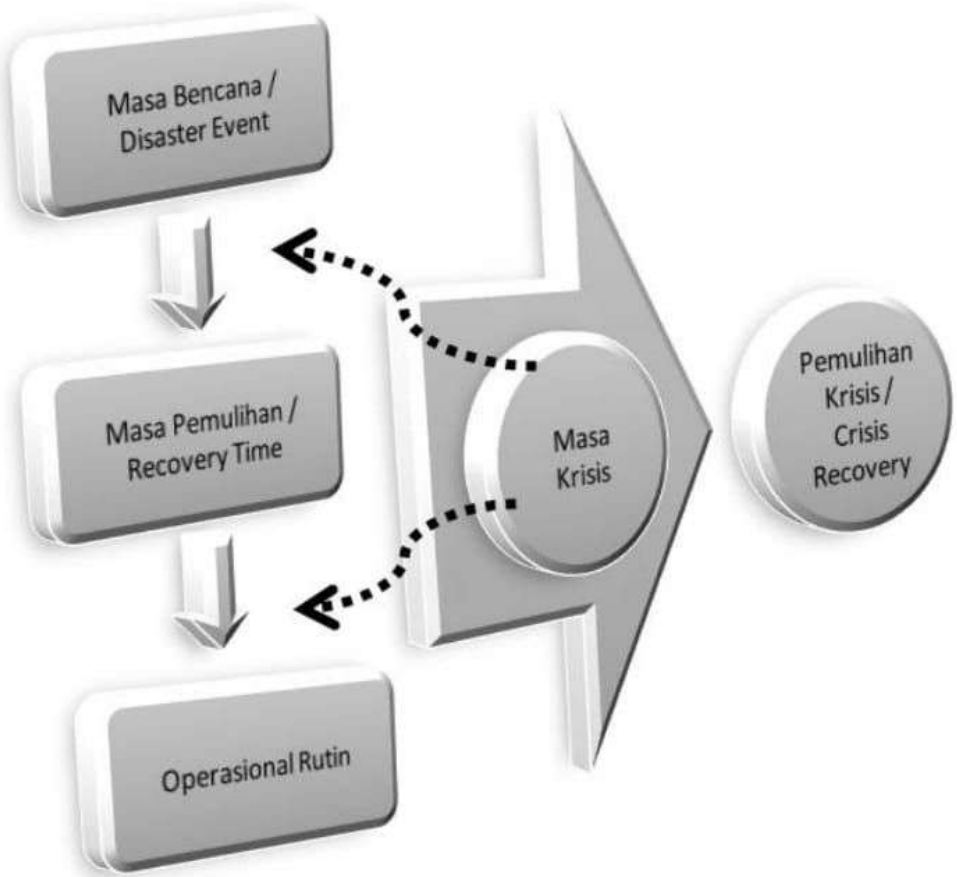


Diagram Pemulihan Krisis

Saat terjadi sebuah bencana dalam sebuah sistem informasi, baik yang berjenis *major outage* ataupun *minor outage*, maka dipastikan akan terjadi sebuah krisis di dalam organisasi tersebut. Krisis, merupakan hal yang selalu terjadi baik pada saat

bencana terjadi maupun pada pasca bencana, terlebih jika bencana tersebut telah memiliki level major.

Krisis adalah keadaan yang genting [10], atau keadaan kritis yang jika tidak ditangani dengan layak akan dapat mempengaruhi keuntungan, reputasi serta kemampuan sebuah organisasi untuk beroperasi [9]. Sehingga sebuah krisis dalam ruang lingkup DRP merupakan keadaan yang dapat mematikan fungsi kritis dari sebuah organisasi.

Di dalam business impact analysis, respon organisasi terhadap suatu krisis merupakan fokus utama setelah analisa awal telah selesai dilakukan. Respon krisis sesungguhnya lebih mengarah kepada reaksi para personil yang ada di dalam suatu organisasi untuk menghadapi keadaan yang mematikan fungsi kritis sebuah sistem.

Apa yang terjadi pada proses bisnis saat terjadi krisis ? Salah satu pertanyaan utama yang selalu menghantui setiap pihak manajemen tersebut, seharusnya telah terjawab pada saat proses analisa

awal (seperti yang sudah dijelaskan di sub bab sebelumnya). Tetapi jika pertanyaannya berubah, "Apa yang direspon oleh pihak organisasi saat krisis terjadi ?". Maka jawabannya bergantung pada masing-masing organisasi tersebut.

Krisis adalah keadaan yang genting , atau keadaan kritis yang jika tidak ditangani dengan layak akan dapat mempengaruhi keuntungan, reputasi serta kemampuan sebuah organisasi untuk beroperasi

Salah satu kejadian umum yang dipastikan terjadi adalah kepanikan. Krisis = panik, panik = tidak terkendali. Rumus sederhana yang selalu ditakutkan oleh berbagai pihak, baik oleh pihak manajemen, para personil atau karyawan maupun oleh para pelanggan.

Kepanikan yang sering menjadikan keadaan tidak terkendali, bukan hanya menambah rumit

bencana yang sedang terjadi, tetapi juga dapat menimbulkan kerugian yang lebih besar. Bahkan dengan adanya kepanikan tersebut dapat menyebabkan runtuhnya sebuah organisasi hanya dalam waktu sekejap.

Krisis = panik, panik = tidak terkendali.

Karenanya diperlukan sebuah strategi khusus dalam mengatasi masa krisis tersebut. Strategi tersebut seringkali dirangkum dalam sebuah rangkaian proses yang disebut sebagai manajemen krisis. Manajemen krisis juga didefinisikan sebagai kemampuan organisasi dalam melaksanakan respon krisis dalam waktu yang sudah ditentukan untuk menghindari kerugian yang lebih besar [9].

Dan yang pasti, di dalam manajemen krisis, fokus utama tetap pada sisi manusia, dibandingkan pada sisi peralatan. Karena dari sisi peralatan, seharusnya telah ditangani pada bagian business

impact analysis, tetapi respon krisis lebih pada sisi manusia.

Di dalam masa krisis, terdapat beberapa langkah awal yang harus dilakukan untuk melaksanakan respon krisis, yaitu [11] :

1. Definisikan status komponen organisasi

   Pada saat awal terjadi krisis, baik oleh bencana dari alam, non alam ataupun lainnya, pihak manajemen harus sesegera mungkin menyatakan status dari tiap komponen organisasi. Pernyataan status ini selain untuk menenangkan personil dari organisasi maupun pelanggan, juga berfungsi untuk menentukan prioritas inisial yang harus dipenuhi terlebih dulu. Untuk kepentingan khalayak umum, harus ditunjuk seseorang secara resmi untuk mengumumkan status tersebut (umumnya dari pihak public relation atau humas), sehingga tidak ada lagi kerancuan dari pihak luar mengenai status organisasi pasca bencana.

Bagaimanapun beratnya bencana yang ditanggung oleh organisasi, aset utama yang wajib diproteksi pertama kali adalah personil organisasi itu sendiri.

Status komponen organisasi meliputi :

a. Status karyawan

Di dalam teori DRP, hal utama yang wajib diselamatkan terlebih dulu adalah unsur manusia. Bagaimanapun beratnya bencana yang ditanggung oleh organisasi, aset utama yang wajib diproteksi pertama kali adalah personil organisasi itu sendiri. Karena aset terpenting dari suatu organisasi adalah para personilnya. Status karyawan tidak hanya didefinisikan dari keselamatan jiwa dan sisi fisik, tetapi juga dari kestabilan mental para karyawan pasca bencana. Sebab, meski para karyawan yang ada telah dinyatakan selamat dari bencana tanpa ada luka secara fisik,

tetapi trauma dan kondisi mental yang labil pasca bencana juga harus tetap diperhitungkan. Sehingga respon krisis dapat dilalui dengan lebih baik dan lancar.

b. Status bangunan

Status berikutnya yang wajib didefinisikan adalah status dari bangunan tempat organisasi tersebut beroperasi. Seberapa parah tingkat kerusakan yang dialami, dan jika kerusakan yang terjadi ternyata benar-benar melumpuhkan bangunan yang dimiliki, maka harus didefinisikan pula apakah terdapat lokasi cadangan tempat operasional sementara. Pada bidang bisnis tertentu yang mengutamakan pelayanan publik, pernyataan perusahaan mengenai status bangunan sangatlah penting. Hal ini dikarenakan dalam bangunan umumnya diasumsikan juga sebagai tempat penampung data yang dimiliki oleh pelanggan. Sebagai contoh, kantor pemerintahan, bank ataupun

perusahaan finansial yang pada saat terjadi bencana akan menyebabkan para pelanggan menjadi ikut panik akibat kekhawatiran akan kehilangan data yang ada.

c. Status area inti

Area inti merupakan area dari lingkungan organisasi, baik berupa bangunan ataupun lahan yang memiliki pengaruh paling besar dalam fungsi kritis. Status area inti harus dinyatakan khususnya bagi para personil dalam proses respon terhadap krisis, agar fungsi kritis dapat dijalankan kembali. Contoh dari area inti adalah ruang server, ruang customer service atau ruang penyimpanan berkas dan backup.

Sebisa mungkin status sistem harus dinyatakan sejujurnya tetapi dalam pernyataan yang tidak membuat panik para personil maupun para pelanggan.

d. Status sistem

Jika kondisi karyawan telah dipastikan dalam keadaan baik, begitu pula dengan keadaan gedung dan area inti, maka status selanjutnya yang harus dipastikan adalah status dari sistem itu sendiri. Seberapa parah kerusakan yang terjadi, dan seberapa mungkin sistem dapat dioperasionalkan kembali dalam waktu yang ditentukan dalam MTD (maximum tolerable downtime). Sebisa mungkin status sistem harus dinyatakan sejujurnya tetapi dalam pernyataan yang tidak membuat panik para personil maupun para pelanggan.

Status dari sistem harus didefinisikan berdasarkan analisa awal di dalam business impact analysis, sehingga kerugian yang diderita juga dapat diperkirakan dengan lebih akurat.

e. Status listrik dan air

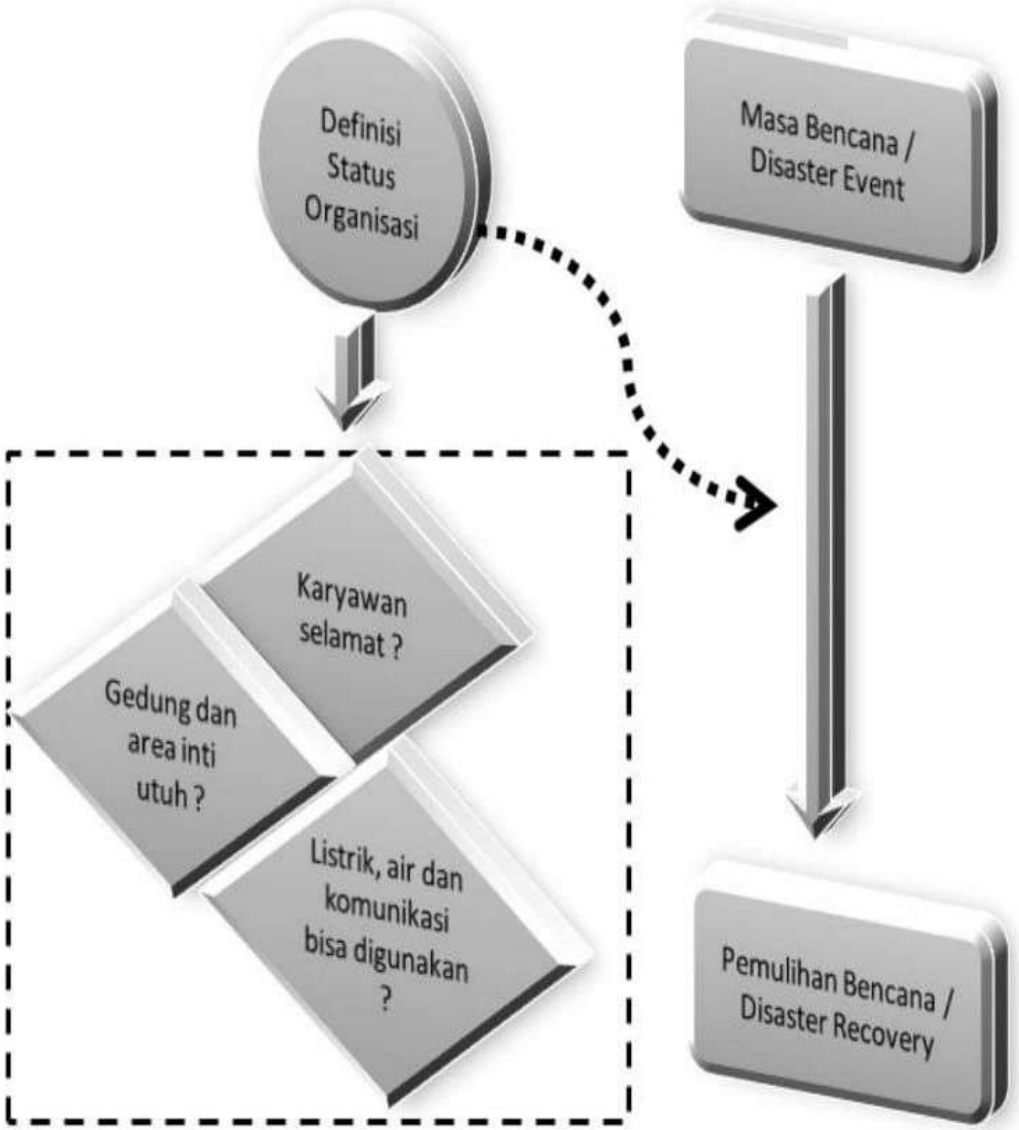
Dalam kelangsungan proses sebuah sistem informasi, hal pertama yang dibutuhkan adalah tenaga listrik. Darimanapun sumber tenaga listrik tersebut, dari pihak penyedia (PLN) ataupun dari generator, statusnya harus ditetapkan oleh pihak manajemen. Baik status durasi ketahanan tenaga ataupun status sumber listrik yang digunakan.

Sedangkan untuk kelancaran proses, status air dalam gedung juga harus diperhitungkan. Karena tanpa sirkulasi air yang baik, tentu saja kenyamanan para personil dalam mengatasi krisis akan terganggu. Bahkan di beberapa kasus sirkulasi air dalam gedung sangat berpengaruh dalam proses pemulihan sistem.

f. Status proses komunikasi

Komunikasi dalam konteks ini bukan hanya komunikasi melalui jaringan telepon, baik kabel maupun selular. Tetapi juga komunikasi

lain seperti jaringan internet ataupun jaringan lokal dalam gedung (LAN). Sebagai contoh, jika server telah dinyatakan dapat berfungsi tetapi jaringan lokal yang mendukung didalamnya tidak dapat digunakan, maka secara umum status dari sistem informasi masih belum dapat dikatakan pulih ke titik operasional.



Status Organisasi dalam Respon Krisis

2. Definisikan kewenangan dan tim krisis

   Pada saat krisis terjadi, maka adalah kewajiban bagi pihak manajemen, khususnya pihak manajemen tingkat atas untuk membentuk sebuah tim penanggulangan krisis lengkap dengan kewenangan yang dimiliki dalam lingkup waktu masa krisis berlangsung. Tim krisis yang dibentuk bisa saja terdiri dari gabungan personil dari berbagai departemen dengan level jabatan yang berbeda-beda.

   Pembentukan tim krisis bukanlah pembentukan tim yang terdiri dari level manajemen menengah ke atas, karena personil dari tim ini haruslah terdiri dari orang-orang yang memiliki mentalitas kuat dalam menghadapi bencana serta kondisi fisik yang prima pasca bencana. Seharusnya tim krisis telah dibentuk terlebih dulu oleh pihak manajemen sebagai bagian dari DRP. Karena efektifitas dari tim krisis tidak hanya bergantung pada kondisi fisik dan mental saat bencana terjadi, tetapi juga harus melalui sebuah proses

pelatihan atau simulasi agar krisis dapat secepat mungkin dilalui oleh organisasi tersebut.

3. Menentukan prioritas inisial

   Langkah terakhir dalam respon krisis ini adalah menentukan prioritas inisial yang harus ditangani pertama kali. Penentuan prioritas inisial harus mengikuti penentuan fungsi kritis yang telah dilakukan di dalam business impact analysis.

   Dalam penentuan prioritas ini, setiap personil dari tim penanggulangan krisis harus memiliki satu kata sepakat, sehingga tidak terjadi tumpang tindih dalam pelaksanaannya. Prioritas inisial mungkin saja berubah dari penentuan fungsi kritis awal, karena bencana yang terjadi bisa saja tidak pernah diprediksi sebelumnya dari mana datangnya ataupun jenis apa yang datang. Tetapi, sebuah proses yang dianggap prioritas inisial haruslah tetap menjadi pangkal dari *chain reaction* yang terjadi dalam sebuah sistem.

Langkah Awal Respon Krisis

Hingga Sejauh Ini.....

Business Impact Analysis dan Respon Krisis

Dalam bab ini telah dibahas berbagai langkah yang melibatkan dua tahapan yaitu ***business impact analysis*** dan ***respon krisis***. Dalam kedua tahapan tersebut, selain terdapat langkah-langkah yang menghasilkan keputusan yang bersifat

kuantitatif, juga terdapat hasil keputusan yang bersifat kualitatif.

Dalam hasil yang bersifat kuantitatif diantaranya adalah perhitungan waktu pemulihan baik berupa RPO (Recovery Point Objective), RTO (Recovery Time Objective), WTR (Work Time Recovery) maupun MTD (Maximum Tolerable Downtime). Seluruh perhitungan waktu tersebut harus ditetapkan dan juga harus disepakati oleh seluruh unsur dalam organisasi.

Hasil kuantitatif lainnya adalah pada perhitungan kerugian yang seharusnya tidak diputuskan sepihak oleh manajemen level atas, tetapi juga harus melibatkan personil yang terlibat di dalam proses tersebut. Sehingga pada saat terjadi bencana dapat melakukan perhitungan dengan lebih akurat mengenai segala jenis kerugian, baik secara finansial maupun layanan operasional.

Di sisi lain, hasil kualitatif yang berupa definisi fungsi yang bersifat kritis atau vital dan juga yang bersifat sedang, harus benar-benar dihasilkan

berdasarkan proses yang matang. Baik dari langkah awal brainstorming, pengumpulan ide hingga ke pendefinisian.

Sedangkan dalam respon krisis, fokus utama tetap harus berpusat ke unsur manusia sebagai personil dari organisasi. Karena karyawan adalah aset terpenting dalam suatu organisasi yang harus pertama kali dilindungi saat terjadi bencana. Dan di sisi lain, unsur manusia umumnya memiliki ketidakstabilan, baik fisik maupun mental saat terjadi atau setelah bencana.

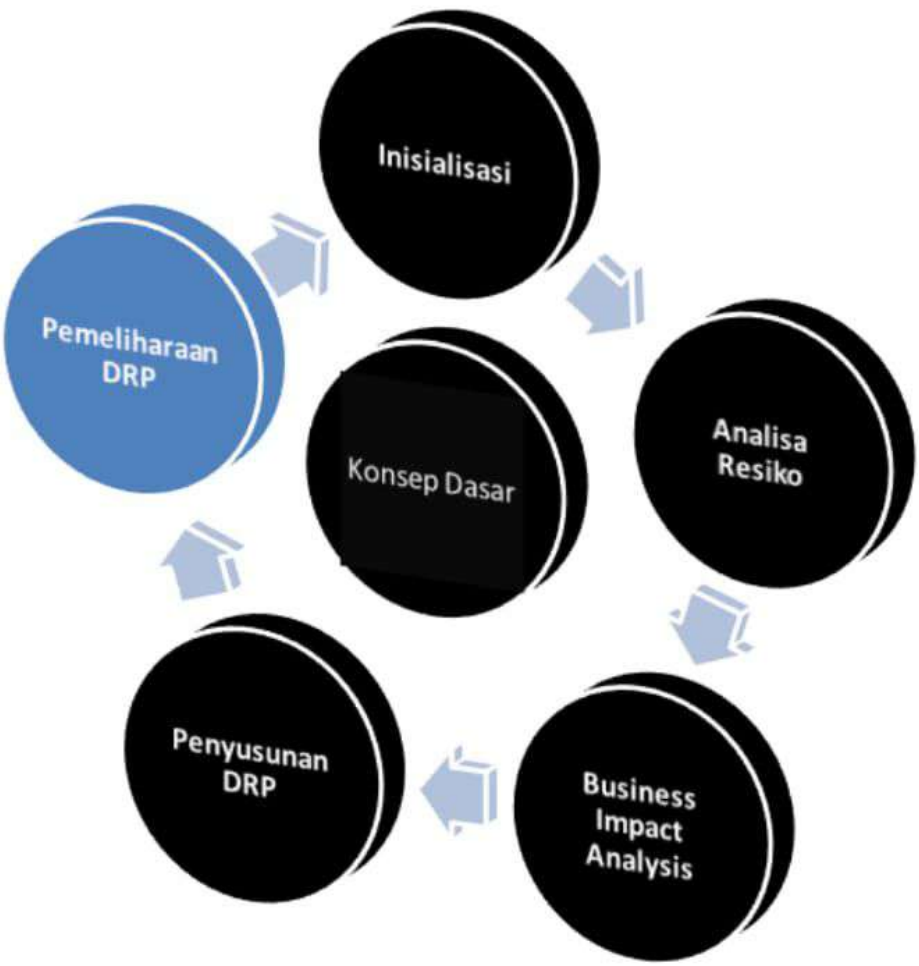
Kedua tahapan tersebut, baik business impact analysis dan juga respon krisis, merupakan tahapan terakhir dari langkah pendahuluan sebelum menuju ke implementasi disaster recovery planning yang sesungguhnya.

Dan hal terpenting lain dalam respon krisis adalah adanya tim penanggulangan yang diharapkan

dapat sigap dan siap dalam menangani bencana. Sehingga pihak yang tidak terlibat didalamnya dapat sesegera mungkin menyelesaikan masa pemulihan tanpa ada kerugian.

Kedua tahapan tersebut, baik business impact analysis dan juga respon krisis, merupakan tahapan terakhir dari langkah pendahuluan sebelum menuju ke implementasi disaster recovery planning yang sesungguhnya. Selain itu, hasil dari kedua tahapan tersebut akan menjadi salah satu komponen penting dalam penyusunan DRP yang baik. Karena tanpa melalui kedua tahapan tersebut, penyusunan DRP akan menjadi lebih lama, akibat terlalu banyaknya proses yang beriterasi atau berulang dan harus ditelaah berkali-kali.

Tahap IV : Penyusunan Disaster Recovery Planning

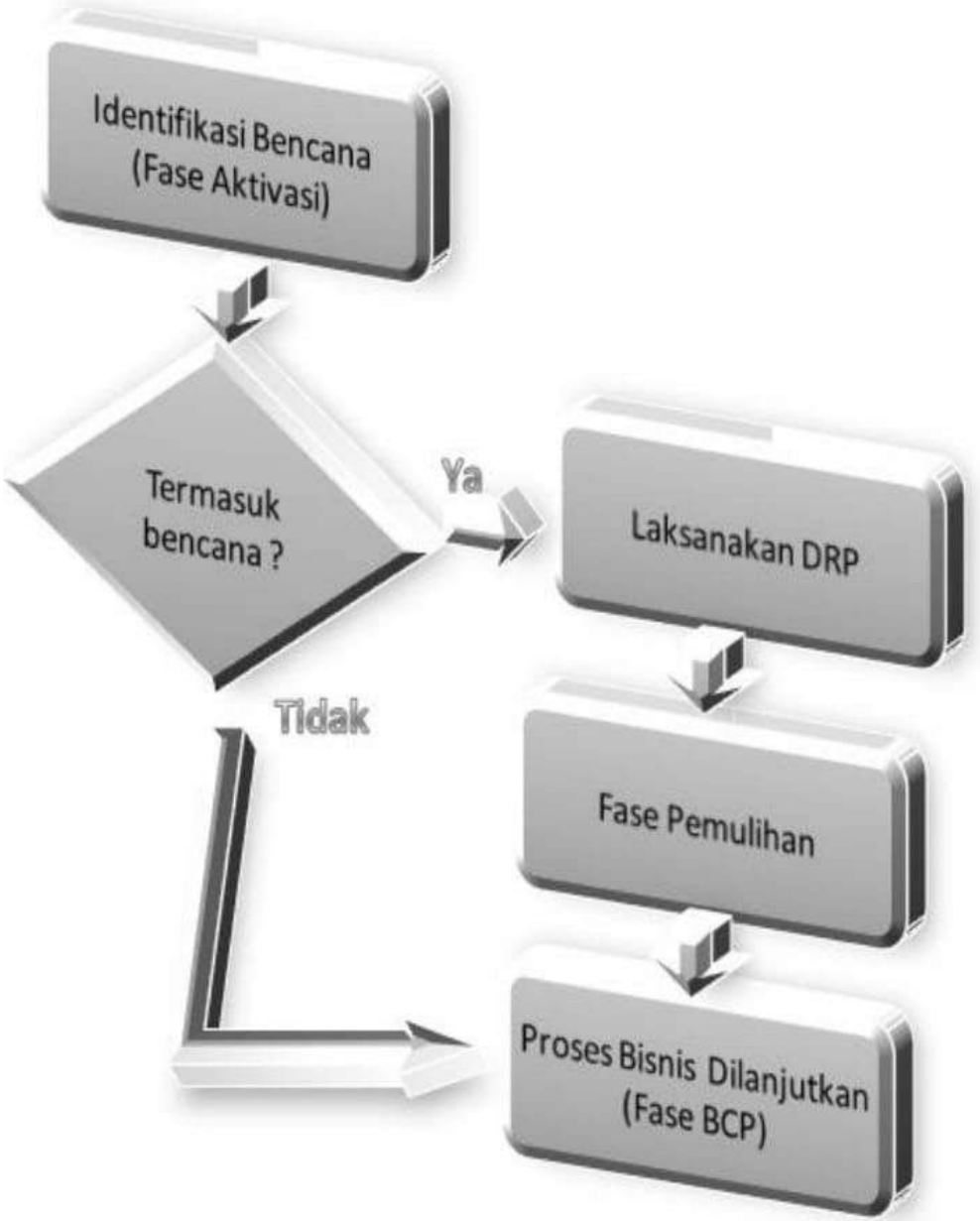


Penetapan Disaster Recovery Planning

Sebuah bencana tidak akan pernah hanya membawa masalah, tetapi juga pasti ada hikmah dibaliknya

Setelah melalui tahapan- tahapan yang telah dijelaskan di bab-bab sebelumnya, maka cukuplah bekal untuk melakukan penyusunan DRP dalam sebuah perusahaan. Di dalam penyusunan DRP, selain memperhatikan tahapan pendahuluan yang sudah dilakukan yaitu inisialisasi, analisa resiko dan business impact analysis, juga perlu diperhatikan tahapan sesungguhnya yaitu penyusunan atau perencanaan, strategi penanganan resiko serta pemeliharaan dari DRP itu sendiri.

Dalam implementasinya, tahapan pendahuluan yaitu inisialisasi, analisa resiko dan business impact analysis seringkali dianggap proses yang membuang waktu dan tenaga karena banyak orang yang cenderung mementingkan implementasi dibanding perencanaan yang matang



Fase Dalam DRP

Penyusunan DRP sendiri terdiri dari empat fase yaitu [1] :

1. Fase Aktivasi

   Pada fase ini, ditarik kembali data-data serta laporan yang sudah dihasilkan di dalam tahapan inisialisasi, analisa resiko serta business impact analysis. Yang pertama kali dilakukan dari hasil ketiga tahapan sebelumnya tersebut adalah melakukan analisa ulang dan menyesuaikan dengan fase aktifasi.

   Dalam fase ini disusun, bencana jenis apa yang nantinya akan dianggap sebagai *major disaster* ataupun *minor disaster* bagi perusahaan. Tentu saja penentuan ini juga melibatkan pemahaman yang kuat terhadap organisasi itu sendiri. Karena tidak akan pernah ada jenis bencana yang sama untuk organisasi yang berbeda.

   Dari penentuan bencana tersebut, kemudian disusun resiko yang akan dihadapi oleh organisasi dari tiap bencana tersebut. Sekaligus

pula ditentukan business impact analysis dari bencana yang telah terdapat dalam daftar.

Penentuan bencana ini tentu saja merupakan fase terpenting dalam penyusunan DRP. Karena selain didahului oleh berbagai jenis tahapan pendahuluan yang panjang dan melelahkan, fase ini pula yang nantinya akan menentukan *trigger* atau pemicu kapan implementasi DRP harus dilaksanakan oleh seluruh pihak yang telah ditunjuk sebelumnya.

Dalam implementasinya, tahapan pendahuluan yaitu inisialisasi, analisa resiko dan business impact analysis seringkali dianggap proses yang membuang waktu dan tenaga karena banyak orang yang cenderung mementingkan implementasi dibanding perencanaan yang matang. Padahal di dalam tahapan pendahuluan tersebut akan terkumpul segala jenis data yang dibutuhkan dalam fase ini.

Pada fase ini, selain ditentukan jenis bencana yang akan dianggap sebagai pemicu pelaksanaan

DRP, juga disusun ruang lingkup DRP dalam organisasi tersebut.

Dan satu hal yang lebih penting lagi adalah bahwa para corporate officer yang terpilih juga harus memiliki ketersediaan mental yang kuat untuk menghadapi segala jenis tekanan pada saat bencana benar-benar terjadi.

Dalam penentuan ruang lingkup DRP, maka akan ditarik kembali data teknis dari organisasi untuk kemudian diolah ulang dalam penyusunan DRP, yaitu :

a. Corporate officer

   Siapa saja para karyawan yang terlibat di dalam *disaster team* pada saat bencana terjadi. Pembentukan tim penanganan bencana bisa jadi akan redundan dan saling tumpang tindih antara satu jenis tim dengan tim yang lain (akan dijelaskan selanjutnya

mengenai jenis dari tim penanganan bencana). Tetapi satu hal yang patut diperhatikan bahwa corporate officer yang telah dianalisa sebelumnya benar-benar merupakan para karyawan yang memiliki tugas serta tanggung jawab dibidangnya masing-masing, dan juga memiliki kemampuan serta ketrampilan yang mumpuni untuk dilibatkan dalam tim penanganan bencana. Dan satu hal yang lebih penting lagi adalah bahwa para corporate officer yang terpilih juga harus memiliki ketersediaan mental yang kuat untuk menghadapi segala jenis tekanan pada saat bencana benar-benar terjadi.

b. Budaya organisasi

Hasil pemahaman terhadap budaya organisasi juga sangat patut untuk diperhitungkan dalam penyusunan DRP, khususnya dalam fase aktivasi saat terjadi bencana. Budaya organisasi yang cenderung didominasi oleh

kepanikan dari para karyawannya akan membutuhkan sebuah penanganan yang lebih intensif dibandingkan sebuah organisasi yang didalamnya telah kuat tertanam budaya untuk tetap tenang dalam menghadapi berbagai jenis situasi.

c. Hasil analisa resiko

Seperti telah dibahas di bab sebelumnya, hasil dari analisa resiko akan menetapkan daftar dari jenis-jenis resiko yang potensial dari organisasi tersebut. Sehingga pada saat bencana terjadi, tim penanganan bencana telah mengambil tindakan yang diperlukan sebelum resiko tersebut benar-benar terjadi.

d. Hasil business impact analysis

Data terakhir yang tidak boleh luput dari fase ini adalah hasil dari business impact analysis. Dari hasil analisa tersebut, segala jenis tingkat kerugian beserta rangking kerusakan yang bakal terjadi dalam sebuah bencana akan menjadi dasar utama dalam

penyusunan daftar periksa atau *checklist* di dalam DRP.

Setelah data-data yang diperlukan telah selesai dianalisa ulang, maka selanjutnya langkah yang harus dilakukan adalah melakukan penyusunan *disaster team* atau tim penanganan bencana. Tim tersebut nantinya akan dibagi menjadi beberapa jenis, dan di dalam tiap organisasi, tidak seluruh jenis harus diimplementasikan. Karena hal tersebut bergantung sepenuhnya terhadap situasi serta kondisi yang harus dihadapi. Jenis tim penanganan bencana tersebut antara lain :

a. Incident Response Team

   Tim ini merupakan tim yang pertama kali bertindak saat terjadi bencana, ataupun pada saat terjadi tanda-tanda akan terjadi suatu bencana. Tim ini pula yang nantinya akan menjadi menganalisa terlebih dulu, apakah sebuah kejadian dapat dikategorikan sebagai sebuah bencana dan perlu penanganan lebih

lanjut berdasarkan prosedur yang telah ditetapkan.

b. Disaster Team

Merupakan sebuah tim yang bertugas langsung saat sebuah kejadian telah dikategorikan sebagai sebuah bencana. Tim ini seringkali menjadi satu dengan *incident response team*, mengingat tugas yang dilakukan tim ini merupakan kelanjutan dari tim tersebut. Tim inilah yang nantinya akan menjalankan seluruh prosedur dari DRP secara detail. Di sisi lain, tim ini merupakan tim yang memiliki tanggung jawab terbesar serta dituntut untuk memiliki ketenangan yang luar biasa dalam menghadapi situasi yang terjadi.

c. Recovery Team

Tim ini seringkali juga diberi nama *cleaning up team* yang tugasnya lebih ditekankan pada penanganan pasca terjadinya bencana. Tim ini akan bertindak saat kondisi bencana

telah dinyatakan usai dan disaster team telah dianggap usai melakukan tugasnya. Anggota dari tim ini biasanya adalah corporate officer yang sesungguhnya di dalam sebuah organisasi. Karena tugas utama dari tim ini adalah memastikan bahwa proses bisnis yang terjadi akan kembali lagi seperti sedia kala.

d. Maintenance Team

Anggota dari jenis tim yang terakhir ini seharusnya berasal pihak manajemen level menengah ataupun dari pihak auditor internal yang memiliki tugas untuk memantau serta memastikan bahwa DRP tetap sesuai dengan kondisi yang ada dan juga mengikuti perkembangan dari organisasi itu sendiri.

Setelah proses penarikan dan pengolahan ulang data dan pembentukan tim telah selesai dilakukan, maka langkah selanjutnya adalah melakukan penyusunan prosedur dan perencanaan yang sesungguhnya dalam penanganan bencana alias penyusunan dari DRP

itu sendiri. Tentu saja dari hasil pengolahan ulang data tersebut, dengan sedikit penyusunan dan perapian format, sudah menjadi sebuah DRP yang utuh. Dan jika dirangkum dalam sebuah proses kegiatan, maka fase aktivasi sekaligus fase penyusunan DRP ini akan tampak sebagai berikut :

Tabel Penyusunan DRP di fase aktivasi

Tahapan	Deskripsi
1. Pengumpulan Data	Pengumpulan ulang data berupa : 1. Corporate officer Untuk menentukan anggota tim penanganan bencana 2. Budaya organisasi Menentukan level tindakan yang harus dilakukan pada saat bencana terjadi 3. Hasil analisa resiko Menentukan rangking resiko yang harus diperhatikan terlebih dulu 4. Hasil business impact analysis

Tahapan	Deskripsi
	Menentukan daftar periksa (checklist) dari DRP berdasarkan tingkat kerugian
2. Penyusunan tim penanganan bencana	Jenis dari tim penanganan bencana : 1. Incident response team 2. Disaster team 3. Recovery team 4. Maintenance team
3. Penyusunan prosedur DRP	Menyusun standard prosedur operasional dari DRP, yang berisikan : 1. Kategori kejadian yang digolongkan sebagai bencana 2. Peringkat resiko dari tiap bencana 3. Tingkat kerugian dari tiap bencana 4. Tim penanganan dari tiap bencana 5. Hal-hal penting yang dilakukan dalam penanganan bencana.

Pada tahapan yang terakhir, yaitu penyusunan prosedur DRP, format dan skema yang

digunakan untuk tiap organisasi bisa saja berbeda. Tetapi secara umum gambaran dari susunan tersebut adalah sebagai berikut :

Contoh Standar Prosedur DRP

Disaster Recovery Planning

Departemen : .....
Kategori bencana :
1. .....
2. .....

Tim penanganan :
1. ..... jabatan : .....
2. ..... jabatan : .....

Estimasi waktu : .....

Resiko	Tingkat kerugian	Penanganan
1.	.....	.....
2.	.....	.....

Di dalam sebuah departemen, bisa saja terdapat lebih dari satu standar prosedur DRP, jika memang departemen tersebut memiliki ragam bencana yang dirasa terlalu banyak untuk ditampung dalam sebuah tabel standar prosedur. Hal tersebut juga bisa saja terjadi apabila

terdapat sebuah bencana yang nantinya akan melibatkan lintas departemen dalam sebuah perusahaan, sehingga dibutuhkan sebuah standar prosedur yang lebih kompleks.

Format dari standard prosedur tersebut hanyalah sebagai contoh dari standard prosedur dari DRP yang sesungguhnya. Di tiap organisasi, dipastikan akan memiliki format yang berbeda, baik berupa penambahan maupun pengurangan dari contoh tersebut. Tetapi poin penting yang harus ditampilkan dalam standard tersebut haruslah tetap ada.

Disaster team merupakan tim yang memiliki tanggung jawab terbesar serta dituntut untuk memiliki ketenangan yang luar biasa dalam menghadapi situasi yang terjadi.

Implementasi DRP di Fase Aktivasi

2. Fase Pemulihan / Recovery

   Penyusunan standard prosedur di dalam fase pemulihan lebih berkonsentrasi terhadap penanganan pasca bencana. Ini berarti, pada fase ini data yang paling utama dibutuhkan adalah data dari hasil business impact analysis. Terutama dari sisi *chain reaction* yang dapat terjadi jika bencana terjadi di sebuah departemen dapat mempengaruhi kinerja dari departemen yang lain. Seperti telah disebutkan pada bahasan di bab sebelumnya, chain reaction

merupakan rantai reaksi yang terjadi karena keterkaitan antara satu faktor dengan faktor yang lain dalam sebuah organisasi.

Di dalam penyusunan standard prosedur operasional untuk fase pemulihan ini, pemahaman terhadap chain reaction akan membantu tahapan yang harus dilakukan dalam pemulihan sistem pasca bencana. Selain itu, juga harus diperhitungkan mengenai cost of failure yang terjadi selama masa pemulihan terjadi, termasuk didalamnya adalah reaksi dari para konsumen perusahaan maupun pengguna sistem informasi baik internal maupun eksternal.

Sebagai contoh, pada saat penyusunan *recovery procedure* di departemen purchasing, maka pemulihan sistem informasi yang dilakukan tidak hanya menyangkut kepentingan di dalam departemen tersebut. Karena umumnya departemen purchasing berhubungan dengan stok dan inventori, maka secara tidak langsung segala macam bencana dalam sistem informasi

tersebut akan juga berpengaruh ke semua departemen yang didalamnya membutuhkan pasokan stok dan inventori. Misalnya, departemen penjualan pastinya harus dimasukkan ke dalam daftar departemen yang tercantum di chain reaction yang akan terjadi. Sebab pasokan stok yang terhambat akibat bencana di departemen purchasing juga dipastikan akan mempengaruhi kinerja di departemen penjualan tersebut.

Pada fase ini juga dibentuk tim penanganan bencana untuk jenis *recovery team*. Seperti disebutkan di poin sebelumnya, anggota tim ini umumnya merupakan corporate officer yang sesungguhnya, karena lebih banyak bertindak sebagai pengguna internal dari sistem informasi. Tetapi didalamnya juga harus melibatkan pihak manajemen level menengah sebagai pengawas dan pengendali dari fase pemulihan agar tetap berjalan sesuai dengan rencana.

Contoh Formulir recovery Procedure

Recovery Procedure

Departemen : .....
Jenis bencana :
1. .....
2. .....

Tim penanganan :
1. ..... jabatan : .....
2. ..... jabatan : .....

Estimasi waktu : .....

Akibat	Rencana Pemulihan	Keterkaitan
1.	.....	.....
2.	.....	.....

Hal penting lain yang tidak boleh dilewatkan dalam fase ini adalah kendali terhadap fase pemulihan atau *recovery control*. Di dalam unsur ini, kendali masa pemulihan sebenarnya ditentukan oleh pelanggan dan pengguna sistem informasi itu sendiri. Artinya, sebuah sistem telah dapat dikatakan pulih jika pelanggan telah merasa bahwa layanan telah kembali normal seperti keaadan sebelum bencana terjadi. Dan

pengguna sistem informasi juga mampu menggunakan kembali sistem informasi dengan normal dan baik.

Unsur Penting Fase Recovery

3. Fase *Business Continuity*

   Fase ketiga dalam penetapan DRP adalah melakukan penyusunan rencana untuk menjaga

kelangsungan proses bisnis atau *business continuity*. Business continuity sebagai tujuan utama dari DRP sesungguhnya merupakan gabungan dari fase aktivasi serta fase recovery. Tujuan utama penyusunan DRP di fase ini adalah memastikan bahwa proses bisnis tetap berjalan dengan baik (dan tidak harus berjalan dengan normal atau dalam keadaan tanpa bencana) apapun yang sedang dilakukan oleh tim penanganan bencana, baik pada masa penanganan kejadian kritis (critical incident response) atau pada masa pemulihan.

Salah satu unsur terpenting pada fase ini adalah melakukan pelatihan terhadap seluruh unsur organisasi agar tidak panik pada saat sebuah bencana terjadi. Tentu saja pelatihan ini tidaklah semudah yang dibayangkan. Karena dalam kenyataannya, faktor kepanikan membutuhkan banyak latihan dalam mode simulasi, sehingga pada saat bencana benar-benar terjadi tidak ada lagi kecanggungan atau bahkan kepanikan dari

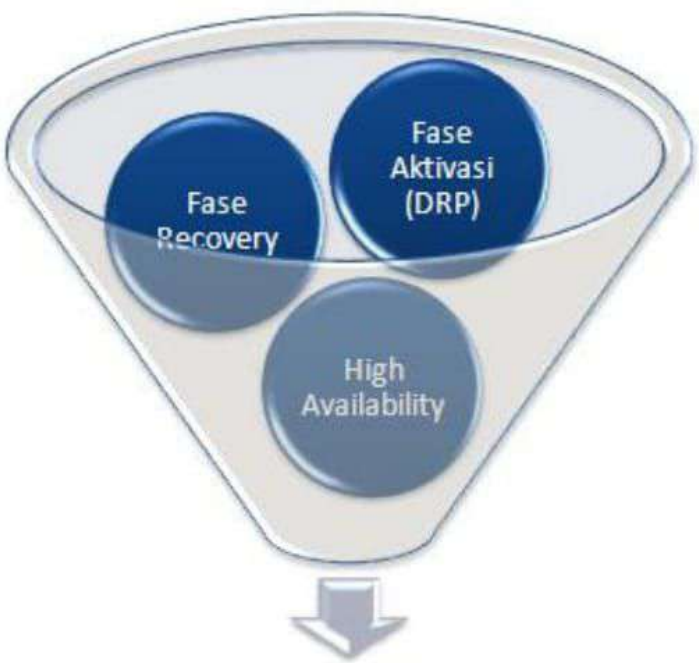
seluruh unsur yang ada dalam organisasi. Terlebih bagi para corporate officer yang terlibat di dalam tim penanganan bencana.

Dalam pelatihan yang dilakukan ini, tidak akan memakan waktu serta biaya yang sedikit jumlahnya. Karenanya, (seperti telah dijelaskan di dalam bab pertama), dibutuhkan komitmen manajemen yang kuat serta konsisten agar segala jenis prosedur yang telah dirancang dapat dengan baik diimplementasikan.

Salah satu unsur terpenting pada fase ini adalah melakukan pelatihan terhadap seluruh unsur organisasi agar tidak panik pada saat sebuah bencana terjadi.

Dari sisi teknis (yang akan dijelaskan lebih detail di sub bab berikutnya), keadaan proses bisnis yang tetap berjalan normal merupakan sebuah tantangan tersendiri bagi seluruh pihak,

khususnya bagi pihak yang terkait langsung dengan teknologi informasi di dalam organisasi tersebut. Konsep *high availability* yang harus diterapkan untuk meminimalkan cost of failure harus diimbangi dengan dokumentasi prosedur yang baik sehingga proses bisnis tidak akan pernah terlihat timpang dalam keadaan apapun.



Fase Business Continuity

4. Fase Pemeliharaan DRP

   Pada saat seluruh prosedur dalam DRP selesai dibentuk dan dilatihkan kepada seluruh unsur dalam organisasi, fase terakhir dalam penyusunannya adalah melakukan proses *maintenance* atau pemeliharaan terhadap DRP itu sendiri. Fase terakhir ini yang seringkali terabaikan dan juga dianggap tidak penting oleh kebanyakan orang. Masih banyak pihak manajemen (khususnya level atas) yang berasumsi bahwa jika sebuah DRP telah selesai dibentuk dalam perusahaan, maka tugas untuk DRP telah selesai. Terlebih jika telah terjadi suatu bencana, dan prosedur DRP telah dapat dilaksanakan dengan sukses serta keberlanjutan proses bisnis atau *business continuity* dapat tercapai. Maka pihak manajemen umumnya merasa puas dan berpendapat bahwa DRP yang ada harus tetap dipertahankan.

   Padahal, di dalam sebuah DRP sangat penting diadakan proses maintenance atau pemeliharaan

DRP dengan melihat perkembangan situasi serta evaluasi dari DRP yang sudah ada berdasarkan hasil testing dan simulasi dari DRP itu sendiri. Untuk keterangan lebih lanjut mengenai fase ini akan dibahas di bab selanjutnya.

Sisi Teknis DRP

Hidup bukan hanya sebuah perbuatan, tetapi juga berani menerima resiko atas segala perbuatan

Setelah terdeskripsikan langkah-langkah manajerial dalam penyusunan dan penetapan DRP hingga ke fase business continuity, maka langkah berikutnyayang tak kalah pentingnya adalah melakukan peninjauan sisi teknis dari DRP itu sendiri. Para praktisi IT sendiri, seringkali memperkirakan bahwa proses teknis DRP hanya akan berkutat pada prosedur mengenai backup dan recovery dari data di dalam sebuah sistem informasi.

Padahal yang terjadi sesungguhnya tidaklah demikian. Proses DRP bukan hanya sekedar proses backup yang secara rutin dilakukan oleh departemen IT dan kemudian jika terjadi kegagalan didalamnya akan dapat dilakukan proses recovery atau pemulihan dengan cepat dan aman. Proses DRP juga membutuhkan dokumentasi yang rapi dan tertata, serta ketersediaan proses yang "aman dan terencana". Sekaligus juga membutuhkan penataan sistem informasi yang didalamnya tercakup teknik pemrograman yang "baik dan benar" untuk meminimalkan kemungkinan terjadinya bencana.

Sisi teknis DRP melibatkan beberapa unsur diantaranya :

1. Unsur Perencanaan (Planning)

   Unsur ini merupakan unsur yang terpenting dalam sisi teknis DRP. Dan salah satu kelemahan utama dalam implementasi DRP adalah peniadaan dari unsur perencanaan itu sendiri. Perencanaan dalam DRP bukan berarti hanya berlaku pada sebuah sistem informasi yang belum diimplementasikan. Dalam konteks ini, perencanaan yang dimaksud adalah perencanaan untuk melakukan perubahan ataupun modifikasi dalam sebuah sistem informasi, baik dari segi perangkat lunak dan perangkat keras, agar dapat mendukung pelaksanaan DRP.

   Dari segi perangkat lunak, perencanaan DRP dapat meliputi beberapa hal, yakni :

   a. Penanganan kesalahan dari sisi penyusunan aplikasi

      Penanganan kesalahan atau lazim disebut sebagai validasi, harus masuk dalam tahap

perencanaan pada sebuah penyusunan aplikasi. Bagi aplikasi yang masih sedang dalam proses pengerjaan, adanya validasi yang lebih kompleks dan kuat akan sangat membantu dalam proses DRP, terutama dari segi bencana yang ditimbulkan oleh manusia, baik secara sengaja maupun tidak sengaja.

Sebagai contoh adalah validasi inputan, di dalam proses input yang didalamnya mengandung unsur inputan dengan jenis data tipe tanggal (date), harus dicek keberadaan dari proses bisnis yang sedang dijalankan. Apabila proses bisnis yang sedang dijalankan tidak memperbolehkan adanya transaksi yang berjalan mundur, maka dalam proses isian tanggal, harus ditangani agar pada saat isian tanggal kurang dari tanggal sistem (tanggal berjalan) harus diberikan pesan kesalahan.

Contoh validasi sederhana tersebut, jika dilewati dapat saja berakibat fatal terhadap jalannya sistem secara keseluruhan, sehingga

pada saat terjadi kesalahan entri tanggal (sengaja ataupun tidak), akan sangat sulit dicari proses pemulihan sistem yang sesungguhnya.

b. Rencana backup dan recovery secara otomatis.

Backup dan recovery, secara teknis, tidak hanya sekedar melakukan proses copy data dari sebuah database dan menyimpannya di sebuah media penyimpan yang dianggap aman seperti tape backup ataupun CD/DVD. Tetapi didalamnya juga mencakup proses-proses penting yang harus diperhatikan sebelumnya. Sebagai contoh, untuk sebuah sistem yang memiliki data yang dirasa cukup besar, dan didalamnya memiliki proses backup otomatis dengan menggunakan media harddisk ataupun tape backup. Maka perlu dipertimbangkan berapa besar kapasitas harddisk ataupun tape backup tersebut, dibandingkan dengan besar data yang harus

dibackup dalam periode tertentu. Sehingga pada saat implementasi, tidak akan terjadi kegagalan backup hanya karena media penyimpan yang dibutuhkan telah tidak mencukupi kapasitasnya. Selain itu, juga wajib diperhatikan pada saat kapan backup harus ditindih ulang (overwrite) sehingga hanya backup pada periode yang terbaru yang menjadi landasan dalam masa pemulihan. Dan juga harus diperhitungkan pada periode mana, data backup harus dipertahankan, misalkan : tahunan, bulanan atau mingguan.

Perencanaan tersebut, tidak hanya dipikirkan oleh pihak manajemen di departemen IT, tetapi seharusnya juga dipertimbangkan dari segi perangkat lunak yang digunakan. Baik dari engine server database server yang digunakan, misal : SQL Server, Oracle ataupun MySQL. Dan juga kemampuan dari tiap database server itu sendiri dalam

menangani proses backup, sehingga jika terjadi kegagalan pada aplikasi, tidak akan terjadi pemulihan yang lambat.

c. Pengembangan sistem yang sekuensial dan berbasis obyek.

Salah satu bencana lain yang sumbernya berasal dari campuran kesengajaan dan ketidaksengajaan adalah bencana yang berasal dari kegagalan pengembangan sistem. Pengembangan sistem yang tidak terencana, baik dari internal (pihak departemen IT) ataupun eksternal (pihak software house), seringkali menyebabkan kegagalan dalam operasional sistem informasi. Kegagalan tersebut umumnya terjadi karena karena pengembangan sistem yang bersifat sekuensial, atau berdasarkan urutan waktu serta kebutuhan yang ada. Sehingga terkesan tidak ada sebuah *blueprint* atau perencanaan yang matang dari awal. Selain itu, jarang terdapat sebuah sistem

yang benar-benar berbasis obyek dalam implementasinya, sehingga pengembangan sistem terkesan seperti sebuah proses tambal sulam yang mengakibatkan sistem memiliki resiko kegagalan yang sangat tinggi.

Tentu saja resiko tersebut bisa diatasi atau minimal dicegah dengan adanya pengembangan sistem yang menganut asas blueprint (sehingga tidak tergantung pada bahasa pemrograman maupun engine database yang digunakan), serta teknik pemrograman yang berbasis obyek agar pengembangan sistem dapat lebih mudah beradaptasi dengan lingkungan di organisasi tersebut.

Dan salah satu kelemahan utama dalam implementasi DRP adalah peniadaan dari unsur perencanaan itu sendiri.

Software Planning Dalam DRP

Dari segi perangkat keras, perencanaan juga mencakup beberapa hal diantaranya :

a. Upgrade perangkat keras

Salah satu dilema terbesar dari sebuah organisasi yang sebagian besar proses bisnisnya bergantung pada sistem informasi adalah menentukan kapan dan bagaimana upgrade dari perangkat keras yang dimilikinya. Seringkali pihak perusahaan (terutama yang berkaitan dengan pelayanan publik) melakukan upgrade perangkat keras yang tidak terencana, dan hanya bergantung pada trend sesaat yang sedang berkembang. Upgrade tersebut tidak hanya terbatas pada server, tetapi juga pada perangkat keras yang terdapat di klien.

Tentu saja hal tersebut akan sangat merugikan bagi pihak perusahaan, baik dari segi biaya, maupun dari segi DRP. Karena belum tentu upgrade perangkat keras yang dilakukan akan dapat memenuhi kompatibilitas dari sistem informasi yang sedang berjalan. Akibatnya, upgrade yang

dilakukan juga dapat menimbulkan kegagalan dari operasional yang sedang berlangsung.

b. Penataan jaringan

Penataan dari jaringan komputer yang ada, juga seringkali menimbulkan bencana yang tidak terduga akibatnya. Penataan ini seringkali mengalami kesalahan yang tidak disengaja, baik karena kesalahan dalam pemasangan ataupun kesalahan dalam memperkirakan kapasitas yang harus ditampung dalam sebuah jaringan. Jika sebuah perusahaan memiliki gedung sendiri, maka harus dipertimbangkan dengan matang, model jaringan serta penataan yang rapi agar alur data dalam sistem tetap dapat berjalan dengan baik tanpa memperdulikan berapa besar aliran data yang ada.

Selain itu, juga perlu dipikirkan lebih lanjut mengenai topologi jaringan yang akan digunakan di dalam sebuah organisasi berdasarkan sebuah rencana jangka panjang

yang nantinya harus disesuaikan dengan perkembangan dan kebutuhan organisasi. Sebagai contoh, jika sebuah organisasi memiliki rencana pengembangan yang akan melebar ke lokasi yang berbeda atau berjauhan, maka topologi yang digunakan tidak akan sama dengan sebuah organisasi yang nantinya memiliki rencana pengembangan hanya dalam sebuah gedung. Tentu saja hal tersebut juga akan sangat berpengaruh dalam penyusunan DRP khususnya dari sisi teknis.

c. Perkembangan kuantitas pengguna

Unsur terakhir dalam segi perangkat keras adalah perkembangan kuantitas pengguna. Unsur ini tidak terjadi pada semua jenis organisasi, karena hanya terdapat organisasi yang memiliki perkembangan kuantitas pengguna secara cepat. Umumnya, dengan perkembangan yang cepat tersebut, maka perangkat keras yang tersedia tidak lagi

mumpuni untuk menampung data ataupun lalu lintas aliran data dalam jaringan. Akibatnya, bencana yang terjadi karena kegagalan penyimpanan dalam server maupun ketidakmampuan jaringan dalam menerima data sering terjadi.

Perlu dipikirkan lebih lanjut mengenai topologi jaringan yang akan digunakan di dalam sebuah organisasi berdasarkan sebuah rencana jangka panjang yang nantinya harus disesuaikan dengan perkembangan dan kebutuhan organisasi.

Supaya hal tersebut tidak terjadi, organisasi yang memiliki tipikal perkembangan kuantitas pengguna yang cepat harus terlebih dulu melakukan perencanaan yang akurat dalam

penyediaan perangkat keras, agar tidak terjadi hal-hal yang tidak diinginkan.

Hardware Planning Dalam DRP

2. Unsur Implementasi (Implementation)

Unsur kedua dalam sisi teknis DRP adalah mengenai implementasi. Sangat banyak hal yang perlu diperhatikan dalam unsur ini, dan tidak semua organisasi memiliki fokus yang sama dalam DRP, khususnya di unsur implementasi. Tetapi, dari sekian banyak jenis fokus tersebut, terdapat beberapa fokus utama yang secara umum sama dan sangat penting serta memiliki keterkaitan antara satu dengan yang lain, yaitu :

a. Konsistensi

   Pada saat implementasi, pihak pengembang (baik departemen IT ataupun konsultan yang ditunjuk) harus memiliki konsistensi baik dari sisi perangkat lunak maupun perangkat keras yang dipilih. Konsistensi memang tidak sepenuhnya menjamin hilangnya kegagalan dalam sistem yang diimplementasikan, tetapi paling tidak akan meminimalkan resiko sehingga bencana tidak akan memiliki kuantitas yang tinggi.

Salah satu contoh dari konsistensi di sisi perangkat lunak adalah tidak adanya migrasi yang revolusioner dalam pengembangan dan implementasi yang dilakukan oleh perusahaan tersebut. Misalkan, jika pada satu saat perusahaan tersebut sudah menggunakan database engine SQL Server, kemudian pada satu saat ingin melakukan migrasi seluruh databasenya sekaligus ke Oracle. Meski tidak ada landasan teori yang mengatakan bahwa migrasi akan mengakibatkan sebuah kegagalan sistem, tetapi dalam kenyataan, migrasi secara total seperti pada contoh tersebut sangatlah rentan dan memiliki kuantifikasi resiko yang sangat tinggi. Terutama jika dilakukan tanpa perencanaan yang matang.

Konsistensi di perangkat keras juga harus dipatuhi oleh tiap organisasi. Sebagai contoh, jika pada instalasi jaringan telah menggunakan kabel UTP sebagai struktur

utama dari jaringan, kemudian pihak manajemen ingin migrasi total ke jaringan nirkabel (wireless network), maka perpindahan tersebut harus dipertimbangkan dengan baik dan benar, tidak hanya sekedar mengikuti tren sesaat. Jika tidak, maka resiko akan terjadinya bencana akibat kegagalan koneksi sangatlah rentan untuk terjadi.

b. Komitmen

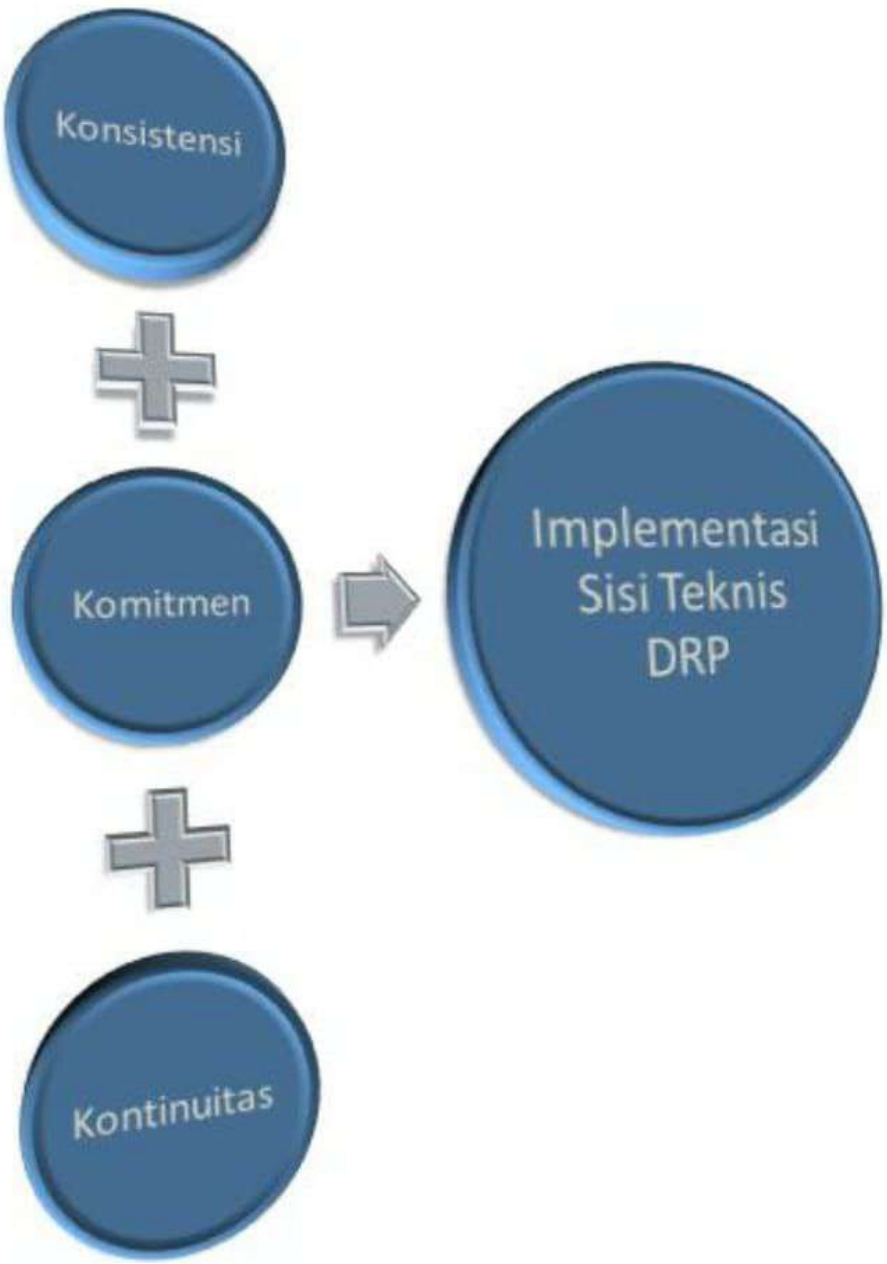
Pada saat implementasi sistem informasi, seluruh pihak (tanpa terkecuali) yang terlibat didalamnya harus memiliki komitmen yang kuat bahwa sistem informasi merupakan unsur penting dan harus dijaga dari segala kemungkinan yang menyebabkan terjadinya bencana. Seperti yang telah disebutkan di bab mengenai awal mengenai inisialisasi, bahwa komitmen yang kuat harus diawali dari pihak manajemen, khususnya dari pihak manajemen level atas.

c. Kontinuitas

Yang dimaksud dengan kontinuitas dalam lingkup ini adalah keberlangsungan perawatan dari tiap sisi teknis perangkat yang ada, baik perangkat keras maupun perangkat lunak. Kontinuitas tersebut, dapat juga diartikan bahwa pengembangan sistem informasi tidak boleh berhenti pada satu level tertentu, tetapi harus tetap berkembang sesuai dengan kebutuhan dari organisasi itu sendiri, dan juga ancaman-ancaman yang dipastikan akan terus berkembang di tiap masa.

Seringkali pihak manajemen, khususnya level atas tidak peduli dengan pengembangan sistem ini. Dan malah menganggap bahwa pengembangan sistem (baik berupa upgrade perangkat keras atau penambahan modul dalam sistem informasi) hanyalah kegiatan yang membuang biaya dan waktu. Padahal, pengembangan tersebut juga merupakan salah satu faktor penting untuk menghindari

bencana, sekaligus merupakan perencanaan yang penting sehingga jika terjadi sebuah bencana dapat langsung teratasi dan diminimalkan akibatnya.



Implementasi Sisi Teknis Dalam DRP

Pada saat fase recovery atau pemulihan dilakukan, yang paling penting diperhatikan adalah kesiapan mental dari tiap personil yang terlibat didalamnya.

3. Unsur Pemulihan (Recovery)

   Pada saat fase recovery atau pemulihan dilakukan, yang paling penting diperhatikan adalah kesiapan mental dari tiap personil yang terlibat didalamnya. Karena tanpa kesiapan mental yang baik, sebagus apapun perencanaan yang disusun dan sesempurna apapun implementasi yang dilakukan, pemulihan tidak akan pernah tercapai dengan baik.

   Mengapa harus kesiapan mental yang dijadikan faktor utama ? Bukankah perencanaan juga memegang peranan yang penting ?

   Saat bencana terjadi, secara umum sangatlah sulit untuk mencari seseorang yang tegar dan mampu untuk bekerja tanpa kepanikan di saat

seperti itu. Dan kepanikan tersebut sangatlah berpengaruh terhadap implementasi dari rencana yang telah disusun dengan rapi dan memenuhi segala syarat yang telah dijelaskan di sub bab sebelumnya. Karenanya, agar kesiapan mental dapat lebih fokus, sangatlah perlu dilakukan pelatihan mengenai DRP, terutama dari sis teknis. Pelatihan tidak hanya mencakup prosedur yang harus dilakukan oleh tiap personil, tetapi juga harus mencakup pelatihan dari sisi teknis dari personil tersebut.

Sebagai contoh, para personil dari tim penanganan bencana tidaklah harus berasal dari departemen IT secara keseluruhan. Akibatnya, para personil non IT tersebut, harus (minimal) mengetahui alur sistem serta penanganan ringan terhadap perangkat keras maupun perangkat lunak saat bencana terjadi.

Pelatihan tersebut, bukanlah sebuah hal yang mudah untuk dilaksanakan. Mengingat bahwa daya tangkap serta kesigapan tiap personil

sangat mempengaruhi proses pelatihan yang sesungguhnya. Tetapi, dengan alasan apapun, pelatihan harus tetap dilakukan sehingga pada saat fase pemulihan dilakukan, seluruh DRP yang telah disusun dapat berjalan sebagaimana mestinya.

4. Unsur Pemeliharaan (Maintenance)

   Unsur terakhir dari sisi teknis DRP adalah unsur pemeliharaan atau maintenance. Pemeliharaan di lingkup ini lebih mengarah ke pemeliharaan dari seluruh sistem dalam kaitannya dengan DRP. Tentu saja ini juga berkaitan dengan sub unsur komitmen yang telah disebutkan di poin kedua yaitu mengenai implementasi.

   Dengan adanya komitmen yang tinggi dari seluruh personil yang terlibat, proses pemeliharaan dan juga perawatan bukanlah suatu hal yang sulit untuk dilakukan. Terlebih jika tiap personil ikut berpartisipasi didalamnya. Contoh kecil yang bisa diambil adalah pemeliharaan yang melibatkan kebersihan dari

perangkat keras yang digunakan. Jika tiap personil waspada terhadap resiko akan bencana yang dapat timbul dari kurang bersihnya perangkat keras, maka tidak akan ada lagi bencana yang sumbernya dari perangkat keras yang kotor. Karena tiap personil telah mampu menjaga kebersihan dari tiap perangkat keras yang digunakannya sendiri, ataupun menghindari adanya makanan atau minuman yang berserakan di tiap perangkat keras.

Perilaku-perilaku sederhana seperti pada contoh tersebut, sangatlah penting untuk dijadikan budaya dari organisasi yang bersangkutan. Bukan hanya sebagai sebuah peraturan yang mengikat dengan segala sanksi yang diterapkan, tetapi lebih menjadi sebuah tindakan yang ditujukan untuk menjaga kelangsungan hidup organisasi dengan menghindari bencana yang mungkin terjadi.

Sisi Teknis DRP

Hingga Sejauh Ini.....

Di dalam bab ini, sebagai bab inti dari keseluruhan isi buku, merupakan pengejawantahan dari tiap rangkuman di bab-bab sebelumnya. Tetapi bukan berarti bahwa hanya bab ini yang harus diperhatikan dan ditelaah lebih dalam dan mengabaikan bab-bab lainnya.

Di dalam penyusunan dan penetapan DRP, setelah fase aktifasi disusun, maka penataan organisasi (yang sesungguhnya merupakan poin terpenting di bagian inisialisasi) menjadi kunci pembuka utama sebelum melangkah ke tahapan berikutnya. Dan kemudian disusul oleh hasil-hasil dari analisa selanjutnya yaitu hasil analisa resiko dan hasil dari business impact analysis.

Hal penting lainnya adalah pada saat melakukan penyusunan tim penanganan bencana yang harus dilakukan secermat mungkin oleh pihak manajemen sebagai pihak yang paling tahu karakteristik secara detail dari tiap personilnya.

Sehingga tidak akan ada kejadian yang natinya akan saling melemparkan tanggung jawab antar anggota tim pada saat terjadi bencana.

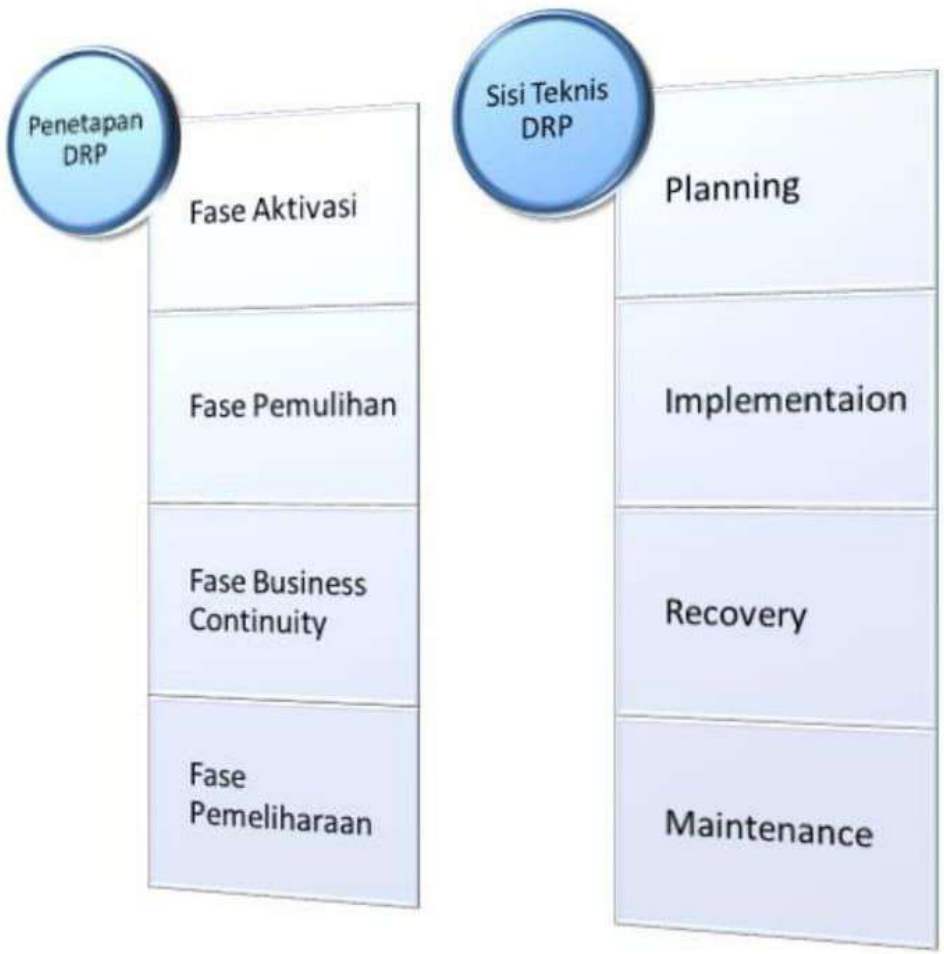
Dan pada langkah utama utama dalam DRP, yaitu penyusunan dari DRP itu sendiri yang melibatkan penetapan prosedur dan daftar periksa (checklist) yang harus dilakukan pada saat bencana. Kemudian, langkah yang tidak boleh terlewatkan adalah penetapan fase business continuity dan fase recovery yang harus juga diselesaikan didalamnya.

Dan meski hingga sejauh ini, proses DRP telah selesai dibahas dengan ringkas, tetapi bukan berarti proses DRP telah berjalan tuntas.

Di tahapan berikutnya, adalah pengalihan fokus DRP, dari segi prosedural dan manajerial ke sisi teknis yang juga sangat penting dan tidak boleh terlewatkan. Sisi teknis yang tidak mungkin sama di

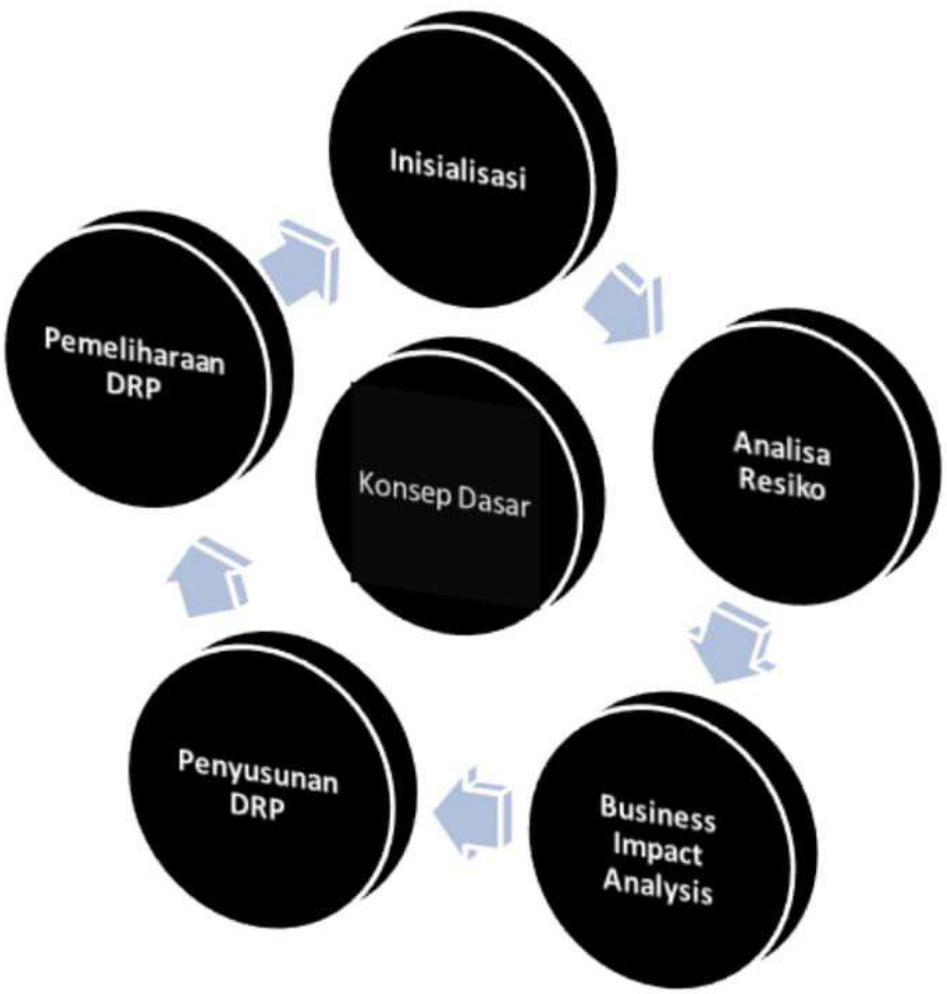
tiap organisasi, mengakibatkan DRP juga tidak akan pernah sama pula dilihat dari sisi yang satu ini. Meski demikian, masih terdapat beberapa unsur yang harus diperhatikan dengan seksama oleh tiap organisasi, yaitu unsur perencanaan, implementasi, pemulihan dan juga pemeliharaan.

Dan meski hingga sejauh ini, proses DRP telah selesai dibahas dengan ringkas, tetapi bukan berarti proses DRP telah berjalan tuntas. Karena masih ada satu tahapan lagi yang juga tidak kalah pentingnya, tetapi juga sangat sering dilupakan yaitu pemeliharaan dari DRP itu sendiri yang akan dibahas pada bagian terakhir dari buku ini.



Penetapan dan Sisi Teknis DRP

Tahap V : Pemeliharaan Disaster Recovery Planning



Testing DRP

Mengharapkan kesuksesan tanpa perencanaan sama dengan mendaki sebuah gunung yang kita tidak pernah tahu dimana letak puncak gunung tersebut

Pertanyaan pertama yang selalu muncul saat DRP telah selesai disusun dan ditetapkan oleh pihak manajemen adalah, "Kini, apa langkah selanjutnya dari DRP ini ?". Apakah DRP hanya akan menjadi sebuah tumpukan berkas dokumentasi berdebu yang tersimpan di lemari besi, ataukah DRP hanyalah sebuah formalitas dari sebuah rangkaian proses audit sistem informasi, atau mungkin DRP hanya sebagai alat untuk menyakinkan para pelanggan, bahwa sistem informasi di organisasi tersebut telah memiliki sebuah prosedur yang baku ?

Tentu saja jawabannya adalah tidak. DRP bukan hanya sekumpulan prosedur yang terbentuk dari sebuah proses yang tidak mudah untuk dijalankan. Tetapi DRP juga berarti sebuah pengawas dari pelaksanaan operasional sehari-hari yang nantinya mampu menghindarkan diri dari segala bencana. Dan dari hal tersebut akan muncul sebuah pertanyaan baru, "Apakah DRP yang telah disusun telah benar adanya ?".

Jika ditanya mengenai sebuah DRP yang telah berhasil disusun tersebut benar atau tidak, maka jawabannya sangatlah subyektif. Bagi pihak penyusun, dengan segala jerih payah yang telah dilakukan, maka DRP tentu saja menjadi sebuah prosedur yang benar. Tetapi bagi pihak auditor ataupun pihak manajemen level atas, DRP bisa saja menjadi salah dan tidak memenuhi standar dari organisasi tersebut.

Tetapi kebenaran yang sering bersifat subyektif tersebut bisa ditetapkan dengan jalan melakukan testing terhadap DRP itu sendiri.

Lalu, bagaimana menentukan bahwa DRP yang telah disusun tersebut sudah berhasil dikatakan benar ? Apakah ada sebuah standard baku mengenai tingkat kebenaran sebuah DRP ?

Kebenaran dari sebuah DRP secara teoritis memang tidak pernah disebutkan secara gamblang. Tetapi kebenaran yang sering bersifat subyektif tersebut bisa ditetapkan dengan jalan melakukan testing terhadap DRP itu sendiri. Tetapi jangan pernah berpikir bahwa untuk melakukan testing dari sebuah DRP diperlukan waktu untuk menunggu sebuah bencana terjadi. Karena tidak mungkin ada sebuah organisasi yang mengharapkan bencana terjadi hanya sekedar untuk melakukan testing terhadap DRP yang telah disusun.

Testing dari DRP sendiri sesungguhnya dapat dilakukan dengan berbagai cara sesuai dengan keadaan dan kebutuhan dari organisasi tersebut. Beberapa cara yang mungkin bisa dilakukan dalam ruang lingkup testing DRP antara lain :

1. Role play

   Melakukan proses testing dengan jalan role play (bermain peran) merupakan cara testing yang dianggap paling efisien. Dalam melakukan testing dengan menggunakan role play, tiap

pihak yang terlibat dalam penyusunan DRP akan saling bertukar peran demi mendapatkan skenario terburuk yang mungkin terjadi dari tiap penanganan bencana.

Proses role play ini pada awalnya harus melalui tahapan *brainstorming* yang matang, sehingga tiap anggota tim penyusun serta tiap personil yang akan terlibat mampu menjalankan perannya dengan obyektif. Obyektifitas yang dimaksud di dalam lingkup ini adalah cara pandang yang tidak "pilih kasih" dalam melaksanakan peran di role play, yang akibatnya dirasa dapat merevisi DRP yang telah disusun.

Di dalam pelaksanaannya, role play juga dapat dikombinasikan dengan metode lainnya yaitu :

a. Simulasi

   Dengan mengadakan simulasi penanganan bencana, maka diharapkan role play menjadi lebih "hidup" dan segala prosedur yang ada dalam DRP dapat lebih memahami jika ada kekurangan yang harus dibenahi didalamnya.

Meski demikian, role play yang dikombinasikan dengan simulasi umumnya sangat terbatas karena adanya kendala biaya serta waktu yang dibutuhkan dalam melakukan simulasi tersebut.

Sebagai contoh sederhana, adalah simulasi penanganan bencana kebakaran yang bisa melibatkan seluruh personil dalam organisasi. Meski hanya bersifat permainan, tapi simulasi semacam ini sangatlah efektif untuk menguji DRP yang telah disusun sebelumnya. Tetapi di sisi lain, proses simulasi tersebut juga akan memakan waktu dan biaya yang tidak sedikit. Sehingga menyebabkan role play yang dikombinasikan dengan simulasi menjadi pilihan terakhir bagi pihak manajemen dalam melakukan testing sebuah DRP.

b. Pelatihan

Cara efektif lainnya dalam melaksanakan role play adalah menempatkan role play dalam

sebuah pelatihan implementasi DRP. Dengan mengadakan sebuah pelatihan dengan model role play didalamnya, maka tim penyusun DRP akan mendapatkan dua manfaat sekaligus, yaitu mendapatkan umpan balik mengenai DRP yang telah disusun dari peserta pelatihan yang notabene juga merupakan personil dari tim penanganan bencana, serta mendapatkan testing yang obyektif berdasarkan hasil pelatihan yang didapat.

Pada saat pelatihan dilaksanakan, tim penyusun DRP, seharusnya turun langsung sebagai instruktur dari pelatihan tersebut. Hal ini ditujukan agar pada saat pelatihan berlangsung, tim penyusun dapat segera mengetahui dimana letak kekurangan dari DRP yang sudah disusun. Tetapi sebelumnya harus ditekankan terlebih dulu, bahwa DRP bukanlah sesuatu yang bersifat konstan dan kaku, tetapi DRP merupakan sebuah prosedur

yang sangat fleksibel berdasarkan kebutuhan dan perkembangan teknologi. Dan juga harus diungkapkan kepada para tim penyusun, bahwa hasil dari testing tersebut, bukan berarti menghakimi pihak penyusun dan juga bukan untuk mencari kesalahan dari DRP yang telah susah payah ditetapkan. Tetapi lebih bersifat mencari kebenaran dan memperbaiki kekurangan dari DRP yang ada. Sehingga di dalam pelaksanaannya nanti, pelatihan akan bersifat dua arah, dari peserta dan instruktur untuk mencari solusi terbaik jika terdapat kekurangan dalam sebuah DRP.

Proses audit hanya melakukan perbaikan jika memang terdapat bukti yang mendukung bahwa DRP yang telah disusun memiliki kelemahan atau kekurangan

2. Audit DRP

   Metode testing yang dianggap paling efektif hingga saat ini adalah dengan melakukan audit dari DRP itu sendiri. Pada saat audit dilakukan, diharapkan akan muncul pertanyaan-pertanyaan baru yang lebih obyektif, sehingga jika terdapat kekurangan dari DRP, maka perbaikan dapat segera dilakukan.

   Pada saat proses audit dilakukan, terdapat beberapa prinsip yang harus dipegang oleh pihak auditor yaitu :

   a. Evidence Only

      Proses audit hanya melakukan perbaikan jika memang terdapat bukti yang mendukung bahwa DRP yang telah disusun memiliki kelemahan atau kekurangan. Bukti atau evidence tersebut bisa berupa hasil dari pelatihan atau simulasi yang telah dilakukan, atau hasil evaluasi tertulis yang telah dilakukan secara seksama. Dengan kata lain, bahwa perbaikan atau penemuan akan suatu

kelemahan hanya bisa dilakukan jika terdapat bukti yang dianggap valid. Sehingga tidak akan ada debat kusir yang berkepanjangan pada saat terjadi perbaikan antara pihak auditor dan pihak yang diaudit. Bukti yang diajukan bisa berupa bukti langsung (direct) atau bukti tidak langsung (indirect). Bukti langsung atau juga sering disebut sebagai bukti forensik merupakan bukti yang terlihat oleh mata telanjang. Sebagai contoh, dalam konteks DRP adalah kesalahan penulisan prosedur, kesalahan perhitungan dalam analisa resiko atau business impact analysis. Sedangkan contoh bukti tidak langsung adalah mentahnya logika berpikir dalam menyusun prosedur pemulihan.

b. Objectivity

Obyektifitas yang dimaksud dalam proses audit adalah peniadaan segregasi dalam proses audit. Segregasi adalah masuknya unsur subyektifitas akibat hubungan

pertemanan, keluarga atau hubungan lainnya yang dapat menyebabkan proses audit tidak lagi berjalan sebagaimana mestinya.

c. Repair strategy

Di dalam proses audit, segala jenis kelemahan dan kekurangan yang berhasil ditemukan dari bukti yang ada harus diungkapkan demi tercapainya sebuah perbaikan dari pihak yang sedang diaudit. Ini juga berarti bahwa pihak auditor bukan bertujuan sebagai pihak agressor, tetapi lebih sebagai pihak yang memiliki niatan baik agar DRP yang telah disusun dapat menjadi sebuah DRP yang sesempurna mungkin.

Prinsip Audit DRP

Di dalam proses audit DRP, dapat dilakukan dengan dua macam cara yaitu :

a. Audit internal

   Yang dimaksud dengan audit internal adalah proses audit DRP yang dilakukan oleh tim yang telah dibentuk oleh pihak manajemen yang seluruh personilnya merupakan anggota dari organisasi tersebut, baik dari level

manajemen tingkat atas ataupun dari level karyawan biasa.

Proses audit internal seringkali dipilih karena dianggap sebagai proses audit yang tidak terlalu memakan banyak biaya dan waktu. Hal ini disebabkan para pelaku audit, baik auditor maupun yang diaudit, sama-sama berasal dari tempat yang sama. Selain itu, dengan menggunakan cara internal ini, diharapkan para auditor telah benar-benar memahami kondisi yang sesungguhnya terjadi sehingga ruang lingkup audit tidak akan melebar ke ruang lingkup lain yang sesungguhnya tidak perlu diperhatikan.

Tetapi di sisi lain, proses audit internal juga memiliki resiko kegagalan yang sangat tinggi. Hal ini disebabkan kemungkinan terjadinya segregasi (segregation) di saat proses audit dilakukan. Segregasi merupakan subyektifitas yang diakibatkan oleh adanya pencampuran perasaan oleh auditor dalam melakukan

proses audit. Sebagai contoh dari segregasi adalah, pada saat pihak auditor merasa mengenal dengan baik pihak yang diaudit (baik sebagai sesama rekan kerja ataupun hubungan keluarga), maka hasil audit akan cenderung baik, dibandingkan jika mengaudit bagian yang sama sekali belum dikenal. Contoh lainnya adalah rasa *sungkan* dari pihak auditor jika pihak yang diaudit ternyata dalam struktur organisasi lebih tinggi dari pihak auditor itu sendiri.

Salah satu solusi untuk mencegah segregasi adalah menetapkan tim auditor agar langsung bertanggungjawab ke pihak manajemen level teratas, dan juga pemilihan personil tim auditor dari orang-orang yang relatif baru di dalam perusahaan sehingga perasaan yang ada tidak terlalu terlibat didalamnya.

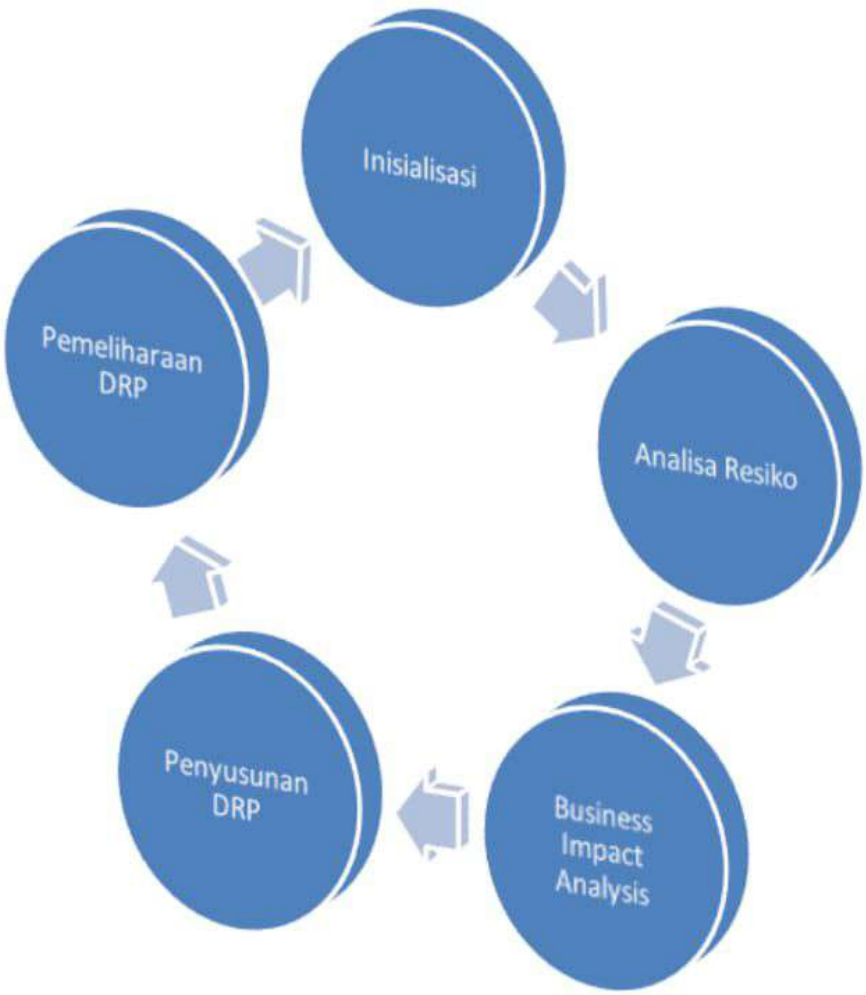
b. Audit eksternal

Proses audit eksternal seringkali dianggap lebih efektif dibanding dari proses audit

internal karena proses audit dipandang lebih obyektif. Tetapi, dengan menggunakan proses audit eksternal yang melibatkan pihak luar didalamnya (umumnya dari biro jasa konsultan), maka biaya yang dikeluarkan untuk proses testing akan bertambah. Selain itu, dengan menggunakan bantuan pihak luar yang notabene harus belajar lagi mengenai situasi dan kondisi yang terjadi organisasi tersebut, akan menambah rancu dari DRP yang telah disusun sebelumnya.

Evaluasi

Mengevaluasi tidak hanya bertujuan untuk mencari kelemahan, tetapi juga mencari solusi dari kelemahan tersebut



Siklus DRP

Dalam sebuah DRP, tidak akan pernah ada istilah bahwa DRP akan menjadi sebuah prosedur yang bertahan untuk selamanya di dalam suatu organisasi. Karenanya setelah DRP selesai disusun,

bahkan hingga ke level testing, proses evaluasi tetap harus dilakukan. Evaluasi tidak hanya dilakukan pada saat- saat tertentu, misalkan pada saat terjadi perubahan struktur manajemen, pergantian pimpinan atau pergantian pemilik perusahaan. Evaluasi selayaknya harus dilakukan secara periodik, misalkan satu tahun sekali atau dua tahun sekali.

Dalam sebuah DRP, tidak akan pernah ada istilah bahwa DRP akan menjadi sebuah prosedur yang bertahan untuk selamanya di dalam suatu organisasi.

Mengapa harus secara periodik ? Bukankah bencana besar atau major disaster tidak datang secara periodik ?

Memang bencana tidak datang secara periodik, tetapi secara periodik organisasi yang ditempati dipastikan akan berkembang, baik dari segi sumber daya manusia maupun sumber daya

lainnya. Begitu pula dengan teknologi informasi yang digunakan. Tak pelak lagi, dengan perkembangan tersebut, bisa dipastikan DRP yang disusun bisa saja mengalami perubahan, atau juga tidak mengalami perubahan.

Di dalam melakukan evaluasi tersebut, tahapan evaluasi yang bisa dilakukan antara lain :

1. Evaluasi kelebihan dan kekurangan

   Evaluasi yang dilakukan tidak hanya terbatas pada evaluasi terhadap kekurangan yang ada, tetapi juga mengevaluasi kelebihan dari DRP yang telah disusun. Kelebihan dari DRP yang telah disusun, selain sebagai alat untuk mendapatkan *competitive advantage* dari pihak pesaing juga merupakan sebuah bahan evaluasi terhadap kelemahan yang ditemukan. Tidak seluruh kelemahan nantinya mampu untuk diperbaiki dengan sekejap, tetapi dengan memanfaatkan kelebihan yang ada, diharapkan mampu untuk menutupi kelemahan tersebut.

Tetapi di sisi lain, evaluasi kelemahan juga harus memperhitungkan perkembangan teknologi yang sedang berjalan. Sebagai contoh adalah perkembangan teknologi remote backup yang memudahkan proses backup ke sebuah server dengan lokasi yang terpisah jauh dari lokasi kantor. Jika sebuah organisasi ingin mengimplementasikan teknologi ini dalam DRP yang akan disusun ulang, juga harus memperhitungkan kelemahan yang mungkin malah bisa menjadi bencana baru pada saat proses berlangsung.

2. Evaluasi pemahaman proses

   Pemahaman akan sebuah proses bisnis akan berkembang sesuai dengan perkembangan dari organisasi serta perkembangan pengetahuan dari para personil di dalam organisasi tersebut. Semakin banyak masalah yang terjadi atau semakin seringnya *minor disaster* yang muncul, juga memicu perkembangan pemahaman proses dari para personil tersebut.

Dari perkembangan pemahaman tersebut, secara periodik DRP yang telah disusun seharusnya juga akan berkembang. Tentu saja ada syarat yang harus diikuti, yaitu melakukan pencatatan dari setiap perkembangan pemahaman tersebut sehingga evaluasi yang dilakukan dapat lebih terstruktur. Selain itu, pasca evaluasi nantinya juga harus mengikuti tahapan yang ada sebelumnya ada di dalam penyusunan DRP yaitu analisa resiko serta business impact analysis.

Sebagai contoh adalah pemahaman mengenai proses penjualan di sebuah perusahaan distributor. Setelah dilakukan evaluasi, ternyata muncul resiko baru dari pelanggan yang melakukan transaksi melalui internet, akibatnya muncul resiko baru dari jenis transaksi tersebut. Dalam kasus ini, DRP yang telah disusun (jika sebelumnya tidak melibatkan resiko dari internet), harus dievaluasi.

3. Recode strategy

   Tahapan terakhir dari evaluasi adalah melakukan pengkodean ulang strategi. Yang perlu diingat adalah bahwa strategi bukanlah rencana, tetapi rencana merupakan bagian dari sebuah strategi. Sehingga saat evaluasi dari DRP terjadi dan menimbulkan susunan prosedur baru tentang perencanaan maka strategi yang dijalankan dalam sistem informasi juga wajib berubah.

   Strategi implementasi sistem informasi yang sedang berlangsung memang harus berlaku secara dinamis dalam sebuah perusahaan. Tetapi, bagaimana jika sebuah perusahaan merasa belum memiliki strategi implementasi sistem informasi ? Dalam kasus seperti ini, bisa jadi DRP dijadikan pemicu untuk membuat strategi implementasi sistem informasi. Meski DRP bukanlah dasar utama dari strategi tersebut, tetapi diharapkan dengan adanya DRP maka pihak manajemen dapat lebih paham akan

pentingnya strategi dalam implementasi sistem informasi.

Tahapan Evaluasi DRP

Daftar Pustaka

[1]. Snedaker, Susan, 2007, *Business Continuity and Disaster Recovery Planning for IT Professionals*, Syngress

[2]. Schmidt, Klaus, 2006, *High Availability and Disaster Recovery*, Springer

[3]. Bates, Regis J., 1992, *Disaster Recovery Planning,* Mc Graw Hill

[4]. Keele, Allen & Keith Mortier, 2005, *Exam Cram 2 CISA*, Que

[5]. Barker, Carolyn & Robyn Coy, 2004, *The Power of Culture : Driving Today's Organization*, Mc Graw Hill

[6]. Condamin, Laurent et all, 2006, *Risk Quantification – management, diagnosis and hedging*, John Wiley & Sons

[7]. Stoneburner, Gary et all, 2001, *Risk Management Guide for Information Technology Systems,* NIST

[8]. Cooper, Dale et all, 2005, *Managing Risk in Large Projects and Complex Procurements,* John Wiley & Sons

[9]. Fulmer, Kenneth .L, 2005, *Business Continuity Planning: A Step-by-Step Guide with Planning Forms*, Rothstein Associates

[10]. Purwadarminta, W.J.S, 1976, *Kamus Umum Bahasa Indonesia*, Balai Pustaka

[11]. Maiwald, Eric & William Sieglein, 2002, *Security Planning and Disaster Recovery*, Osborne

Daftar Istilah

Disaster Recovery Planning	Bagian perencanaan dari sebuah institusi untuk melakukan tahapan tertentu yang nantinya akan menjamin kelangsungan pelayanan (khususnya dari segi sistem informasi) yang diberikan tanpa mengurangi kapabilitas serta kinerja dari sebuah sistem jika terjadi sebuah bencana didalamnya.
Information system high availability	Kemampuan untuk tetap menyediakan layanan dari sistem informasi, baik dalam keadaan normal maupun dalam masa sebuah bencana sedang terjadi tanpa adanya penurunan kinerja dari sistem itu sendiri
Corporate officer	Orang-orang yang memiliki tanggung jawab serta berinteraksi dalam sebuah sistem informasi di sebuah organisasi.

Minor Disaster	Bencana kecil (baik dari alam maupun bukan) merupakan bencana yang dampak kerusakannya terhitung kecil dan tidak terlalu dirasakan , sehingga pelayanan dari sistem informasi tidak berhenti secara total.
Major Disaster	Bencana yang dapat menyebabkan pelayanan dari sistem informasi benar-benar terhenti tanpa toleransi maupun peringatan sebelumnya.
Cost of failure	Biaya yang harus ditanggung saat terjadi bencana
Business continuity planning	Perencaaan kelanjutan proses bisnis dan layanan dari sistem informasi pasca terjadinya bencana yang menimpa sistem informasi tersebut.
Zero defect	Konsep yang menafikan kesalahan di dalam proses operasional yang menggunakan sistem informasi didalamnya.

Resiko	Akibat negatif dari hasil kerentanan suatu sistem terhadap kejadian tertentu
Manajemen Resiko	Proses yang menyeimbangkan antara operasional dan biaya ekonomi untuk hasil perlindungan dalam tujuan untuk melindungi sistem di teknologi informasi dan mendukung tujuan dari organisasi itu sendiri
Analisa resiko	Penggunaan secara sistematis terhadap informasi yang tersedia untuk menentukan kejadian tertentu yang mungkin timbul dan besarnya akibat yang mungkin terjadi
Threat	Resiko potensial yang timbul akibat sebuah kelemahan yang timbul dalam sebuah sistem
Vulnerability	Resiko tidak langsung yang menyebabkan sebuah threat dapat terjadi

Identifikasi resiko	Proses untuk menentukan apa, bagaimana serta mengapa sesuatu atau resiko tersebut dapat terjadi
Analisa pengendalian	Pengendalian terhadap hal-hal yang telah diimplementasikan atau sedang direncanakan, agar resiko berupa threat yang berasal dari vulnerability dapat diminimalisasi atau bahkan dihilangkan sama sekali.
Catastrophic	Tingkat kerugian terbesar yang mampu meruntuhkan eksistensi dari organisasi
Evaluasi resiko	Proses menentukan apakah resiko yang terjadi dapat ditoleransi atau tidak, serta mengidentifikasi resiko tertinggi yang mungkin terjadi agar dapat diwaspadai
Critical incident monitoring	Monitoring terhadap kejadian-kejadian yang dianggap kritis bagi kelangsungan hidup sebuah sistem di dalam organisasi.

Business impact analysis	Analisa mengenai pengaruh bencana terhadap sebuah organisasi.
Chain reaction	Keterkaitan antara satu faktor dengan faktor yang lain
Recovery time	Total waktu yang dibutuhkan untuk kembali ke keadaan normal dari saat bencana terjadi.
Recovery Point Objective	Waktu toleransi yang dibutuhkan untuk kembali ke keadaaan normal.
Recovery Time Objective	Waktu yang dibutuhkan untuk mengembalikan sistem ke dalam posisi operasional.
Work Recovery Time	Waktu yang yang dibutuhkan dalam masa pemulihan sebagai lanjutan dari RTO.
Maximum Tolerable Downtime	Gabungan dari RTO dan WRT dalam sebuah proses pemulihan.
Krisis	Keadaan kritis yang jika tidak ditangani dengan layak akan

Seribu Bintang

www.SeribuBintang.co.id
info@SeribuBintang.co.id
fb.com/cv.seribu.bintang