BAB II

LANDASAN TEORI

2.1 *Information Technology Service Continuity Management* (ITSCM)

Menurut *Information Technology Service Management Forum* (itSMF) (Meijer, 2008), teknologi sebagai komponen inti dalam proses bisnis, kelangsungan atau ketersediaan dari TI adalah hal penting bagi bisnis untuk bertahan secara keseluruhan. Hal ini dapat dicapai dengan memperkenalkan pengukuran pengurangan resiko dan pilihan pemulihan. Pemeliharaan kemampuan pemulihan merupakan hal penting agar proses bisnis dapat berjalan secara efektif.

Menurut itSMF (2007), tujuan ITSCM adalah untuk memelihara kemampuan pemulihan berjalan secara tepat dalam layanan TI untuk mencocokkan kebutuhan yang disetujui, persyaratan dan jadwal dari bisnis. Sedangkan menurut *Information Technology Governance Institute* (ITGI) (2007), ITSCM termasuk kelanjutan dari seluruh aktivitas siklus hidup layanan yang perlu dipastikan. Sekali rencana kelangsungan dan pemulihan layanan dikembangkan, keduanya harus selaras dengan rencana kelangsungan bisnis dan prioritas bisnis. Memeliharan kebijakan strategis ITSCM secara tepat dan rencana ITSCM selaras dengan rencana bisnis merupakan kunci suksesnya proses ITSCM. Hal ini dapat dilakukan dengan secara reguler melakukan analisa dampak bisnis dan latihan manajemen resiko.

2.2 *Information Technology Infrastructure Library (ITIL)*

Menurut Wibowo (2009), ITIL (*Information Technology Infrastructure Library*) adalah suatu kerangka kerja umum yang menggambarkan *best practice* dalam manajemen layanan TI. ITIL menyediakan kerangka kerja bagi tata kelola TI dan berfokus pada pengukuran secara terus-menerus dan perbaikan kualitas layanan TI yang diberikan, baik dari sisi bisnis dan perspektif pelanggan.

Menurut Whittleston (2012), ITIL adalah suatu kerangka kerja yang telah berkembang untuk memenuhi isu organisasi. *Framework* ini lebih ditujukan kepada isu manajemen daripada isu teknis. ITIL dapat memberikan arahan yang tidak bergantung pada teknologi tertentu tetapi tetap dapat memberikan nilai lebih bagi organisasi. Sedangkan menurut Arraj (2010), ITIL adalah sebuah pendekatan untuk manajemen layanan TI. Layanan adalah sesuatu yang memberikan nilai bagi pelanggan.

Menurut *Office of Government Commerce* (OGC) (2007), ITIL merupakan framework untuk mengelola infrastruktur TI di suatu organisasi dan bagaimana memberikan service terbaik bagi pengguna layanan TI.

Menurut (Meijer, 2011), ITIL memberikan arahan untuk menggabungkan manajamen layanan TI dengan konsep dari manajemen informasi bisnis (*business information management / BIS*). ITIL membahas layanan TI dan memungkinkan konsep bisnis memberikan nilai melalui layanan itu kepada pelanggan. Layanan ini didefinisikan sebagai sarana untuk memberikan nilai kepada pelanggan dengan memfasilitasi hasil yang diinginkan pelanggan.

ITIL is a framework of best practice guidance in Information Technology Service Management (ITSM) (Clinch, 2009). ITIL menggambarkan proses, fungsi

dan struktur yang mendukung sebagian besar area ITSM, sebagian besar dari sudut pandang penyedia layanan.

Menurut Jogiyanto dan Abdillah (2010), ITIL adalah seperangkat konsep dan praktik untuk mengelola layanan TI, pengembangan, dan operasi TI. ITIL memberikan deskripsi rinci mengenai sejumlah praktik penting TI dan menyediakan daftar komprehensif mengenai tugas dan prosedur yang setiap organisasi dapat menyesuaikan dengan kebutuhan sendiri. Menurut *Information Technology Government Institute* (ITGI) dan OGC (2007), COBIT dan ISO/IEC 27002 digunakan untuk membantu menentukan apa yang harus dilakukan sedangkan ITIL menyediakan cara aspek manajemen pelayanan.

Menurut Fitriani (2010), ITIL merupakan *best practice* untuk memastikan layanan teknologi informasi berjalan sesuai dengan sebagaimana mestinya. Sedangkan menurut Gilbert, Morse and Lee (2007), dengan menerapkan penggunaan ITIL V-3 akan menciptakan manajemen pengetahuan (*knowledge management*) dari sebuah dokumentasi resolusi manajemen insiden sehingga dapat mempersingkat waktu penyelesaian dari sebuah insiden dan masalah

2.3 Definisi *Disaster* / Bencana

Menurut Whitten (2008), *disaster* (bencana) didefiniskan sebagai kejadian yang waktu terjadinya tidak dapat diprediksi dan bersifat sangat merusak. Pengertian ini mengidentifikasikan sebuah kejadian yang memiliki empat faktor utama, yaitu :

1. Tiba-tiba
2. Tidak diharapkan
3. Bersifat sangat merusak

Dalam istilah lain *disaster* (bencana) didefinisikan sebagai gangguan dari operasi bisnis yang menghentikan organisasi dalam menyediakan pelayanan bisinisnya yang disebabkan oleh ketiadaan faktor-faktor seperti :

1. Tenaga Kerja dan keahlian
2. Fasilitas
3. Komunikasi
4. Power / Daya
5. Akses Informasi

Bencana dapat diakibatkan oleh ulah manusia, maupun akibat alam (*natural disaster*), seringkali tidak dapat diprediksi kapan akan terjadi. Untuk itu perlu dibuat sistem yang dapat mengurangi resiko dan kerugian bila bencana terjadi.

Bencana terjadi dengan frekuensi yang tidak menentu dan akibat yang ditimbulkannya meningkat bagi mereka yang tidak mempersiapkan diri terhadap kemungkinan-kemungkinan timbulnya bencana. Rencana pencegahan dan perbaikan terhadap bencana dapat membantu melindungi semua aset oraganisasi, termasuk sumber daya manusia, pekerjaan, data-data penting, dan fasilitas organisasi.

2.4 Penyebab *Disaster* / Bencana

Menurut Whitten (2008), penyebab suatu kondisi bencana dapat dikategorikan sebagai berikut :

1. Bencana alam, seperti banjir dan gempa bumi.
2. Fasilitas, seperti listrik, air dan komunikasi.
3. Manusia, seperti sabotase, virus, teroris dan kerusuhan.
4. Kegagalan peralatan, seperti sistem informasi, telekomunikasi dan mesin produksi.

2.5 Akibat dari *Disaster* / Bencana

Menurut Whitten (2008), akibat yang ditimbulkan dari suatu bencana dapat dikategorikan sebagai berikut :

1. Sudut pandang keuangan (*Financial perspective*)

   Bencana atau gangguan akan berdampak pada kelancaran finansial dalam sebuah organisasi. Pengeluaran ekstra dan kerugian dari *cash flow* akan berdampak pada modal perusahaan. Pada saat itu waktu akan menjadi musuh utama dalam bisnis.

   a. Beban operasional Normal (*Normal operating expenses*)

      1) Gaji (*Saleries*)

         Dengan adanya bencana atau gangguan yang menyebabkan kelangsungan bisnis berhenti dapat meningkatkan beban gaji.

      2) Sewa (*Rent*)

         Beban sewa akan bertambah besar karena terjadinya *disaster* / bencana.

b. Beban Besar (*Large extraordinary expenses*)

1) Penggantian peralatan (*Equipment replacement*)

2) Fasilitas Sementara (*Temporary facility*)

c. Keuntungan / aliran uang berhenti (*Revenue / cash flow stops*)

d. Nilai *Equity* akan melemah (*Equity position weakened*)

2. Sumber Tenaga kerja (*Human Resources*)

Saat ini perusahaan cenderung hanya memiliki sedikit tenaga kerja, maka hilangnya tenaga kerja pada saat *disaster* / bencana dapat mengakibatkan efek yang besar, seperti :

a. Downsizing

b. Pelatihan ulang (*Re-enginering*)

c. Outsourcing

3. Meningkatnya kompetisi sejalan dengan *Global Economy* (*Increasing Competition in a Global Economy*)

Pada saat terjadi *disaster* / bencana maka kompetisi perusahaan-perusahaan semakin meningkat yaitu dari pelayanan / *service* level yang diberikan, karena setiap perusahaan akan terus meningkatkan pelayanannya. Tentunya perusahaan yang tidak siap dengan keadaan ini dapat kehilangan customernya (*lost costumer don't return*).

4. Meningkatnya penggunaan teknologi (*Increasing use of technology*)

Perusahaan akan menjadi sangat bergantung pada teknologi, apabila terjadi bencana maka teknologi yang biasa digunakan berubah menjadi manual. Sehingga kebutuhan akan teknologi tersebut dapat menjadi kebutuhan yang luar biasa penting. Teknologi tersebut seperti :

a. Faks (*Fax*)

b. Pesan suara (*Voice mail*)

c. Jaringan lokal dan WAN (*Local and wide area networks*)

d. Sistem pengambilan keputusan (*Decision support systems*)

e. Akses Internet (*Internet Access*)

5. Hutang terhadap ketidaktersedianya produk / pelayanan (*Liabilities Associated with not providing products / services*)

   Manajemen bertanggung jawab dalam memastikan kelangsungan bisnis sehingga pemulihan bencana / gangguan (*disaster recovery*) harus direncanakan dengan matang. Sehingga tidak terjadi adanya penalti dari perusahaan lain atau hal-hal yang tidak diinginkan, seperti :

   a. Penalties associated with notmeeting delivery schedules

   b. Shareholder / Board of directors' new expectations

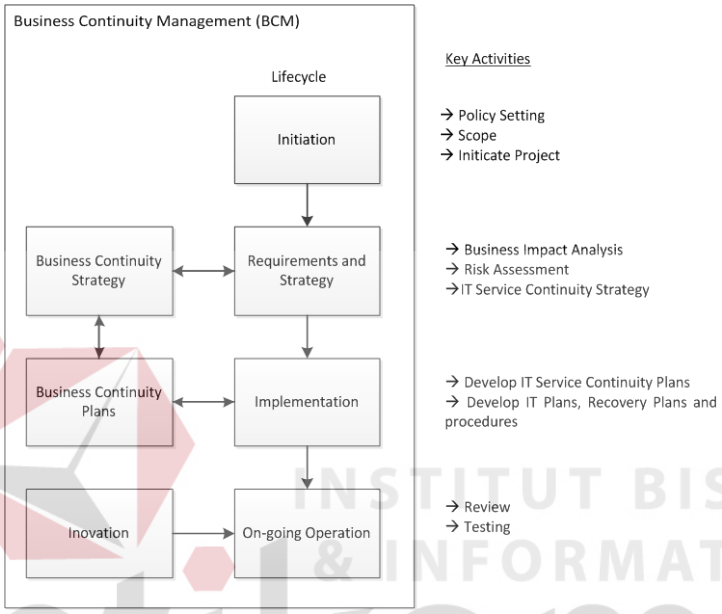
2.6 Rencana Kelangsungan Bisnis (*Business Continuity Plan* / BCP)

Business Continuity Plan (BCP) adalah kebijakan dan prosedur yang memuat rangkaian kegiatan terencana dan terkoordinir mengenai langkah-langkah pengurangan resiko, penanganan dampak gangguan / bencana dan proses pemulihan agar kegiatan operasional dan pelayanan kepada *customer* tetap berjalan.

BCP adalah proses yang dirancang untuk mengurangi resiko dalam sebuah organisasi bisnis. (sumber : ISACA)

BCP adalah sekumpulan prosedur dan sumber informasi yang digunakan untuk memulihkan kegiatan operasional bisnis apabila terjadi gangguan / bencana. (sumber : James C. Barnes, *A Guide to Business Continuity Planning*)

2.7 *Information Technology Service Continuity Management Lifecycle*



Gambar 2.1 *ITSCM Lifecycle*

Penjelasan langkah-langkah dalam *ITSCM* seperti yang tampak pada gambar 2.1 adalah *:*

1. Inisiasi (*Initiation*)

   Fase ini meliputi seluruh organisasi dan mencakup kegiatan-kegiatan berikut :

   a. Mendefinisikan kebijakan

   b. Menentukan ruang lingkup

   c. Mendefinisikan dan memulai proyek

2. Persyaratan dan Strategi (*Requirements and Strategy*)

   Fase ini untuk menentukan kebutuhan bisnisi bagi ITSCM untuk dapat mengetahui sejauh mana organisasi dapat bertahan saat terjadi bencana. Dua

hal penting dalam fase ini adalah kebutuhan dan strategi. Penjabaran kedua hal itu meliputi :

a. Analisa Dampak Bisnis (*Business Impact Analysis*)

Menurut Franklin Fletcher, BIA merupakan dasar dari program bisnis kontinuitas (*business continuity program*). Tujuaanya adalah untuk mengukur dampak yang disebabkan oleh hilangnya layanan. BIA mengidentifikasi layanan yang paling penting bagi organisasi sehingga dapat memberikan masukan penting bagi strategi. Analisis itu mengidentifikasi :

1) Jenis kerusakan (bencana/gangguan)
2) Bagaimana kerusakan bisa meningkat
3) Kompetensi, fasilitas dan layanan yang dibutuhkan untuk melanjutkan proses yang penting
4) Perkiraan penentuan jangka waktu proses pemulihan

Secara umum, langkah-langkah lebih preventif harus diambil untuk proses yang terjadi dengan cepat dan memiliki dampak yang tinggi. Jika dampak rendah dan proses membutuhkan lebih banyak waktu, penekanannya adalah kurang pada pencegahan dan lebih pada tindakan kuratif (recovery).

b. Perkiraan resiko

Menurut Michael Faber (2010), resiko adalah kejadian tak terduga yang memiliki dampak negatif terhadap kinerja maupun profit. Ada berbagai metode dan analisis resiko. Analisis resiko adalah penilaian risiko yang mungkin terjadi. Manajemen resiko mengidentifikasi respon dan tindakan yang dapat diambil. Sebuah metode standar seperti Manajemen Resiko /

Management of Risk (M_o_R) dapat digunakan untuk menyelidiki dan mengelola resiko. Metode ini terdiri dari :

1) Prinsip M_o_R
2) Pendekatan M_o_R (pendekatan organisasi)
3) Proses M_o_R (identifikasi, penilaian, perencanaan, pelaksanaan)
4) Pencocokan dan *review* M_o_R
5) Komunikasi (*up-to-date* dan penyediaan informasi yang memadai)

c. Strategi

Contoh strategi yang dapat diterapkan meliputi :

1) Strategi 1 : langkah-langkah untuk mengurangi resiko

   Langkah-langkah untuk mengurangi resiko harus diimplementasikan dalam kombinasi dengan manajemen ketersediaan karena penurunan kegagalan memiliki dampak pada ketersediaan layanan.

2) Strategi 2 : opsi pemulihan IT

   Strategi kontinuitas harus menitikberatkan pada tindakan penguranngan biaya terhadap langkah-langkah pemulihan untuk mengembalikan proses kritis.

3. Implementasi (*Implementation*)

Rencana ITSCM dapat dibuat setelah strategi disetujui. Anda harus ingat, bagaimanapun, bahwa struktur organisasi (kepemimpinan dan proses pengambilan keputusan) dapat merubah proses pemulihan bencana. Mengatur hal ini pada umumnya bertanggung jawab pada area manajer senior, seperti dengan koordinator di bawahnya dan tim pemulihan di bawah itu.

4. Operasionalisasi (On-going Operation)

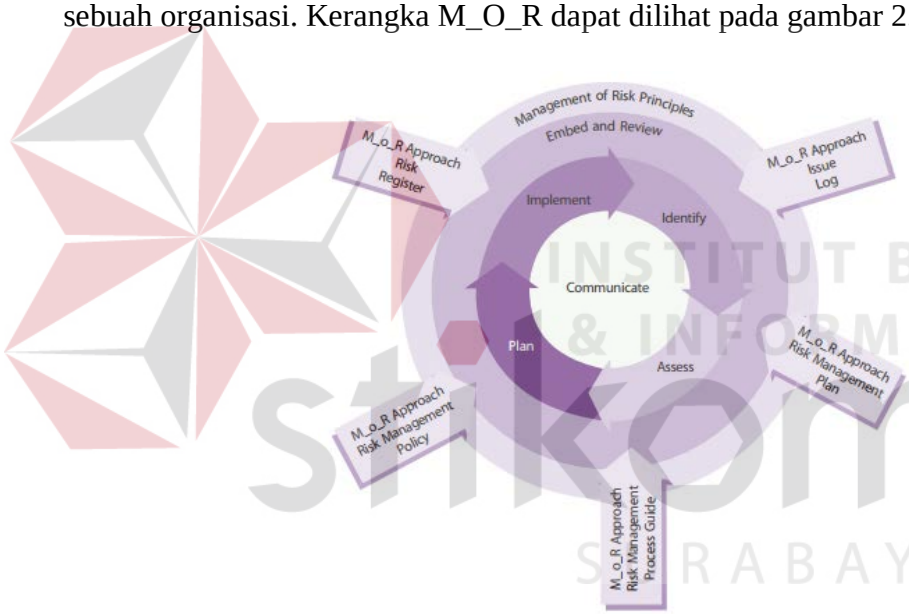
   Fase ini meliputi :

   a. *Review*

   b. *Testing*

2.8 Metode M_O_R (*Management of Risk*)

Menurut Graham Williams (2007:2011), M_O_R merupakan sebuah metodologi *standard* yang digunakan untuk menilai dan mengelola resiko dalam sebuah organisasi. Kerangka M_O_R dapat dilihat pada gambar 2.2 di bawah ini :



Gambar 2.2 *Kerangka M_O_R (Management of Risk)*

Pendekatan M_O_R seperti yang tampak pada gambar 2 terdiri dari :

1. M_O_R *Principles* (Prinsip M_O_R)

   Prinsip-prinsip merupakan hal penting untuk pengembangan praktek manajemen resiko yang baik, prinsip-prinsip itu berasal dari kebijakan perusahaan.

2. M_O_R *Approach* (Pendekatan M_O_R)

   Prinsip-prinsip dalam pendekatan dengan perusahaan perlu disepakati dan ditetapkan dalam dokumen seperti :

   a. Risk Management Policy
   b. Process Guide
   c. Plans
   d. Etc

3. M_O_R *Proccesses* (Proses-proses M_O_R)

   Empat langkah utama yang menggambarkan input, proses dan output dari kegiatan yang memastikan bahwa resiko dikontrol :

   a. *Identify* : ancaman dan peluang dalam kegiatan yang dapat mempengaruhi kemampuan untuk mencapai tujuan.
   b. *Assess* : pemahaman tentang efek ancaman dan peluang yang diidentifikasi terkait dengan kegiatan ketika kedua hal itu dikumpulkan bersama-sama.
   c. *Plan* : untuk mempersiapkan sebuah manajemen respon tertentu yang akan mengurangi ancaman dan memaksimalkan peluang.
   d. *Implement* : tindakan manajemen risiko yang direncanakan untuk memantau efektivitas dan mengambil tindakan korektif mengenai respon yang tidak sesuai harapan.

4. *Embedding* and *reviewing* M_O_R (Pencocokan dan me-*review* M_O_R)

   Menempatkan prinsip-prinsip, pendekatan dan proses di satu tempat, semua hal itu harus terus dikaji dan ditingkatkan untuk memastikan semuanya tetap efektif.

5. *Communication*

   Memiliki kegiatan komunikasi yang tepat di suatu tempat untuk memastikan bahwa semua orang terus *up-to-date* dengan perubahan-perubahan dalam ancaman, kesempatan dan aspek-aspek lain dari manajemen risiko.

2.9 Aktivitas pada ITSCM

Aktivitas-aktivitas yang dapat dilakukan dalam lingkup *ITSCM* adalah analisa dampak bisnis, rencana pemulihan IT, IT *service continuity plan*, ITSCM *strategy*, identifikasi dan analisa resiko, uji dan tinjau resiko.

2.9.1 Analisa Dampak Bisnis (*Business Impact Analysis*)

Business Impact Analysis (BIA) adalah landasan awal dalam proses penyusunan BCP melalui proses identifikasi dampak bisnis, identifikasi aktivitas yang penting, penentuan target waktu pemulihan, dan pengukuran standar operasi minimal yang dibutuhkan. Menurut Franklin Fletcher, BIA landasan dari setiap program kelangsungan bisnis dalam sebuah organissai. Tujuan dari Analisis dampak bisnis (*business impact analysis*) ini adalah untuk mendapatkan :

1. Informasi yang menyeluruh mengenai fungsi organisasi dan business process
2. Informasi kepada manajemen mengenai *Recovery Time Objective*
3. Informasi mengenai kebutuhan minimal dalam penyelenggaraan organisasi (*minimum resources*)

2.9.2 Rencana Pemulihan IT (*IT Recovery Plan*)

Strategi pemulihan harus dikembangkan untuk teknologi informasi (TI) seperti sistem, aplikasi dan data. Ini termasuk jaringan, *server*, *desktop*, laptop, perangkat nirkabel, data dan konektivitas.

Prioritas pemulihan TI harus konsisten dengan prioritas untuk pemulihan fungsi bisnis dan proses yang dikembangkan selama analisis dampak bisnis. Sumber daya TI yang diperlukan untuk mendukung fungsi bisnis terhadap waktu dan proses juga harus diidentifikasi. Waktu pemulihan untuk sumber daya TI harus sesuai dengan tujuan waktu pemulihan untuk fungsi bisnis atau proses yang bergantung pada sumber daya TI.

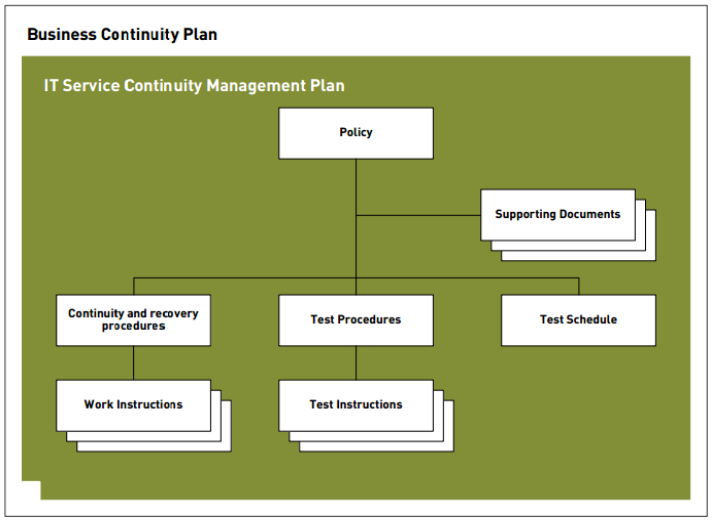
Sistem teknologi informasi memerlukan perangkat keras, perangkat lunak, data dan konektivitas. Tanpa salah satu komponen dari sistem itu maka bisa saja sistem tidak dapat berjalan. Oleh karena itu, strategi pemulihan harus dikembangkan untuk mengantisipasi hilangnya satu atau lebih komponen sistem seperti berikut :

1. Ruang komputer lingkungan (ruang komputer aman dengan kontrol iklim, *power supply*, AC dan cadangan, dll)
2. *Hardware* (jaringan, *server*, komputer desktop dan laptop, perangkat nirkabel dan periferal)
3. Konektivitas ke penyedia layanan (fiber, kabel, nirkabel, dll)
4. *Software* aplikasi (*electronic data interchange*, surat elektronik, manajemen sumber daya perusahaan, produktivitas kantor, dll)
5. Data dan restorasi

Sejumlah pilihan pemulihan yang mungkin :

1. *Manual workarounds* : solusi manual sementara dengan untuk jangka waktu yang terbatas
2. *Reciprocal arrangements* : dukungan perjanjian antara pihak-pihak terkait (tidak sering digunakan hari ini)
3. *Gradual recovery* (Pemulihan Bertahap) : Metode yang membuat fasilitas dasar seperti akomodasi dan ruang komputer menjadi tersedia dengan biaya yang terbatas dalam beberapa hari (empat atau lebih).
4. *Intermediate recovery* (Pemulihan Menengah) : pemulihan dalam waktu dua sampai tiga hari, umumnya didasarkan pada fasilitas yang disiapkan sering berbagi dengan beberapa pihak lain
5. *Fast recovery* (Pemulihan Cepat): pemulihan dalam waktu 24 jam yang berfokus pada layanan utama, yang melibatkan fasilitas yang bisa melakukan operasional sangat cepat dan dengan kehilangan data yang sangat rendah
6. *Immediate recovery* (Pemulihan Segera). pilihan untuk pemulihan segera terutama layanan bisnis penting dengan bantuan teknik *mirroring* dan solusi redundansi lainnya, tidak ada data yang rendah yang terlibat

2.9.3 *IT Service Continuity Plan*



Gambar 2.3 *IT Service Continuity Plan*

Berikut adalah penjelasan mengenai setiap bagian pada gambar 2.3 diatas :

1. *Policy*

   Kebijakan kelangsungan pelayanan adalah pernyataan keseluruhan kesiapan. Ini mendefinisikan konteks kesinambungan layanan untuk organisasi, mengidentifikasi langkah-langkah yang akan diambil untuk memberikan kontinuitas dalam kasus gangguan, dan menyediakan kerangka kerja untuk penyusunan dan pemeliharaan rencana ITSCM.

   Kebijakan ini perlu dibaca dan dipahami oleh semua staf dalam organisasi, sehingga menjaganya agar tetap singkat dan "*to the point*" sangat penting untuk keberhasilannya.

2. *Procedures*

Prosedur menggambarkan kegiatan yang akan dilakukan sebagai bagian dari kontinuitas dan pemulihan, dan mengidentifikasi tugas (instruksi kerja) yang diperlukan untuk menyelesaikan kegiatan.

3. *Work instructions*

   Instruksi kerja menggambarkan langkah yang diperlukan untuk menyelesaikan tugas yang telah dilakukan sebagai bagian dari suatu kegiatan (prosedur).

4. *Test procedures*

   Prosedur pengujian mengidentifikasi pemeriksaan spesifik dan tes yang akan dilakukan untuk memastikan kemampuan lanjutan, kelangsungan hidup dan keandalan rencana ITSCM, dan jika berlaku, bisnis fasilitas kelangsungan organisasi Anda.

5. *Test instructions*

   Instruksi Uji menjelaskan langkah-langkah yang diperlukan untuk menyelesaikan kelangsungan individu dan tes pemulihan.

6. *Test schedule*

   Jadwal Tes mengidentifikasi tanggal dan waktu untuk pelaksanaan pemeriksaan dan tes.

7. *Supporting documents*

Rencana ITSCM dilengkapi dengan satu set dokumen teknis dan bisnis yang berisi informasi untuk mendukung kelangsungan pelayanan dan pemulihan. Dokumen - seperti daftar komponen - mungkin sudah ada atau mungkin perlu disusun untuk referensi oleh, atau dimasukkan ke dalam rencana.

2.9.4 *ITSCM Strategy*

ITSCM Strategy harus menitikberatkan pada tindakan pengurangan biaya terhadap langkah-langkah pemulihan untuk mengembalikan beberapa proses kritis. Sejumlah pilihan pemulihan yang mungkin :

1. *Manual workarounds* : solusi manual sementara dengan untuk jangka waktu yang terbatas
2. *Reciprocal arrangements* : dukungan perjanjian antara pihak-pihak terkait (tidak sering digunakan hari ini)
3. *Gradual recovery* (Pemulihan Bertahap) : metode yang membuat fasilitas dasar seperti akomodasi dan ruang komputer menjadi tersedia dengan biaya yang terbatas dalam beberapa hari (empat atau lebih).
4. *Intermediate recovery* (Pemulihan Menengah) : pemulihan dalam waktu dua sampai tiga hari, umumnya didasarkan pada fasilitas yang disiapkan sering berbagi dengan beberapa pihak lain
5. *Fast recovery* (Pemulihan Cepat) : pemulihan dalam waktu 24 jam yang berfokus pada layanan utama, yang melibatkan fasilitas yang bisa melakukan operasional sangat cepat dan dengan kehilangan data yang sangat rendah

6. *Immediate recovery* (Pemulihan Segera) : pilihan untuk pemulihan segera terutama untuk layanan bisnis yang penting dengan bantuan teknik *mirroring* dan solusi redundansi lainnya, tidak ada data yang rendah yang terlibat

2.9.5 Identifikasi dan Analisa Resiko (*Risk Assessment and Analysis*)

Maksud dari identifikasi resiko adalah proses identifikasi resiko yang dihadapi suatu organisasi, identifikasi terhadap fungsi kritikal untuk menjamin kelangsungan operasional bisnis, serta memperoleh gambaran dalam pengendalian bisnis fungsi untuk mengurangi resiko kerugian apabila terjadi gangguan. Resiko Operasional adalah potensi seluruh gangguan dalam proses operasional suatu organisasi atau perusahaan yang menyebabkan kerugian dimasa yang akan datang (*future losses*) atau terjadi fluktuasi pendapatan dimasa yang akan datang.

Tujuan dilakukannya *risk assessment* adalah sebagai berikut :

1. Menentukan tingkat resiko dari berbagai jenis resiko.
2. Menentukan pengendalian dari jenis resiko.
3. Mengukur dampak dan kuantitas berbagai jenis resiko.
4. Menentukan kebjakan dalam rangka mengambil keputusan terhadap resiko yang berdampak besar.

Cakupan resiko *risk assesment* :

1. Operasional Proses
2. Operasional Sumber Daya Manusia
3. Operasional Sistem Teknologi Informasi
4. Faktor Eksternal

Proses dan prosedur *risk assessment* :

1. Identifikasi resiko :

a. Mengetahui dimana saja resiko berada

b. Mengetahui penyebab timbulnya resiko

c. Mengetahui metode yang digunakan untuk mengidentifikasi keberadaan dan penyebab resiko

d. Mengetahui pengendalian yang ada bila resiko itu terjadi

2. Pengukuran resiko

a. Kuantitatif : "Analisis berdasarkan angka-angka nyata (nilai finansial) terhadap biaya dan besarnya kerugian yang terjadi"

b. Kualitatif : "Sebuah analisis yang menentukan resiko tantangan organisasi dimana penilaian tersebut dilakukan berdasarkan institusi, tingkat keahlian dalam menilai jumlah resiko yang mungkin terjadi dan potensi kerusakannya"

Hal-hal yang harus diperhatikan dalam *risk assessment* :

1. Membuat prioritisasi kemungkinan gangguan yang terjadi berdasarkan tingkat kerusakan dan kemungkinan terjadinya.
2. Membuat suatu *gap analysis* dengan membandingkan BCP atau DRP atau *Contingency Plan* yang dimiliki saat ini dengan hasil *Risk Assessment.*
3. Melakukan analisis resiko yang akantimbul bagi perusahaan dan stakeholders akibat adanya gangguan atau bencana.

2.9.6 Uji dan Tinjau Resiko (*Risk Monitoring and Testing*)

Risk monitoring and testing adalah langkah terahkir dalam proses rencana kelangsungan bisnis (*business continuity plan*). *Risk monitoring and*

testing memastikan bahwa BCP dalam sebuah perusahaan dapat berjalan dengan baik melalui :

1. Penggabungan BIA and ke *risk assessment* dalam BCP dan *testing program.*
2. Pengembangan program *testing* perusahaan.
3. Penetapan dari aturan dan tanggung jawab dalam implementasi *testing program*
4. Evaluasi dari *testing program* dan hasil *test* oleh menejemen senior dan unit kerja.
5. Penilaian dari testing program dan hasil testing oleh pihak *independent*.
6. Revisi dari BCP dan testing program berdasarkan perubahan operasi bisnis, audit, dan rekomendasi dari pemeriksaan dan hasil test

2.10 PT. Telkom MSC Area V Jawa Timur

PT. Telekomunikasi Indonesia, Tbk atau yang bisa disebut sebagai PT. Telkom merupakan perusahaan yang bergerak dibidang telekomunikasi, informasi, media dan *edutainment* (TIME). PT Telkom mempunyai beberapa divisi sebagai unit bisnisnya diantaranya adalah Divisi Akses, Divisi Infratel, Divisi Telkom Flexi, Divisi Multimedia, Telkom MSC dan lain-lain.

Telkom MSC (*Maintenance Service Center*) merupakan salah satu divisi dari PT. Telekomunkasi Indonesia, Tbk yang fungsi utamanya yaitu melakukan maintenance management infrastruktur perangkat telekomunikasi yang dimiliki oleh Telkom. Untuk melakukan *maintenance management*, Telkom MSC membagi area pengelolaannya menjadi tujuh, yaitu Area I Sumatra, Area II DKI

Jakarta, Area III Jawa Barat, Area IV Jawa Tengah dan DIY, Area V Jawa Timur, Area VI Kalimantan dan Area VII Kawasan Timur Indonesia (KTI).

Seiring berkembangnya teknologi telekomunikasi dan banyaknya unit bisnis yang dimiliki oleh PT. Telkom, maka Telkom MSC juga harus bisa melakukan *maintenance management* pada setiap divisi yang dimiliki oleh PT. Telkom dan mendukung kegiatan operasional pada setiap divisi diantaranya melakukan perbaikan dan pemeliharaan perangkat telekomunikasi pada infrastruktur yang dimiliki oleh Divisi Akses, Divisi Infratel, Divisi Multimedia, dan Divisi Telkom Flexi.