UNIVERSITAS INDONESIA

ANALISIS RISIKO KEGAGALAN PADA *CORE NETWORK* PERANGKAT GPRS MENGGUNAKAN METODE FMEA DAN FTA SERTA SKENARIO ALOKASI BIAYA PENANGANANNYA

SKRIPSI

Diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana Teknik

ANISA FITHRASARI
0606043963

FAKULTAS TEKNIK
PROGRAM STUDI TEKNIK INDUSTRI
JAKARTA
DESEMBER 2008

HALAMAN PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya saya sendiri,
dan semua sumber baik yang dikutip maupun dirujuk
telah saya nyatakan dengan benar.

Nama	**: Anisa Fithrasari**
NPM	**: 0606043963**
Tanda Tangan	**:**
Tanggal	**: 24 Desember 2008**

HALAMAN PENGESAHAN

Skripsi ini diajukan oleh	:	
Nama	:	Anisa Fithrasari
NPM	:	0606043963
Program Studi	:	Teknik Industri
Judul Skripsi	:	Analisis Risiko Kegagalan pada *Core Network* Perangkat GPRS Menggunakan Metode FMEA dan FTA serta Skenario Alokasi Biaya Penanganannya

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Teknik pada Program Studi Teknik Industri Fakultas Teknik, Universitas Indonesia

DEWAN PENGUJI

Pembimbing	: Ir. Yadrifil, MSc	(…….)
Penguji	: Ir. Amar Rachman, MEIM	(…….)
Penguji	: Arian Dhini, ST, MT	(…….)
Penguji	: Farizal, Ph.D	(…….)

Ditetapkan di : Jakarta
Tanggal : 24 Desember 2008

KATA PENGANTAR

Puji syukur ke hadirat Allah SWT, atas segala berkah dan rahmat-Nya sehingga penulis dapat menyelesaikan skripsi ini. Penulisan skripsi ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Sarjana Teknik Jurusan Teknik Industri pada Fakultas Teknik Universitas Indonesia. Saya menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan skripsi ini, sangatlah sulit bagi saya untuk menyelesaikan skripsi ini. Oleh karena itu, saya megucapkan terima kasih kepada:

1. Ir. T. Yuri M. Zagloel, MSc, sebagai Ketua Departemen Teknik Industri, yang telah memberikan dukungan selama proses perkuliahan;
2. Ir. Yadrifil, MSc, sebagai Dosen Pembimbing, yang telah menyediakan waktu dan memberikan begitu banyak perhatian, motivasi, dukungan, serta arahan selama penyusunan skripsi ini;
3. Ir.Akhmad Hidayatno MBT, selaku pembimbing akademis, yang telah memberikan masukan dan dukungan selama menjalani perkuliahan;
4. Para dosen Departemen Teknik Industri, selaku fasilitator dan panutan, yang telah memberikan pengetahuan tiada terkira selama menjalani perkuliahan;
5. Para *expert* di perusahaan telekomunikasi yang menjadi objek penelitian, yang telah banyak membantu dalam penyelesaian skripsi ini, dalam usaha untuk memperoleh data yang diperlukan dan berkenan dengan tulus membagi ide serta pengetahuan yang dimiliki;
6. Suami tercinta, Yayat Hidayat, yang telah memberikan dukungan, perhatian, dan pengertian luar biasa selama menjalani proses pendidikan, serta senantiasa mendampingi di saat apapun;
7. Orang tua dan mertua, yang menjadi motivator agar menjadi anak yang lebih baik dan selalu memberi yang terbaik;
8. Om dan Bibi, yang telah memberikan doa dan perhatian selama menjalani proses pendidikan;
9. Teh ita, teh lucy, a'dicky, a'asep, dan seluruh keluarga besar yang telah begitu banyak memberikan dukungan dan perhatian;

10. Ria, Nti, Erika, Uut, dan seluruh sahabat-sahabat Teknik Industri Ekstensi Salemba 2006 atas kekompakan, kebersamaan, keceriaan, canda tawa, serta suka duka;
11. Tika, Lisna, dan Vita, sahabat terbaik, tempat berbagi kisah, yang selalu memberi masukan dan semangat;
12. Teman-teman di Depok yang sama-sama saling mendukung dalam menyelesaikan skripsi ini;
13. Dan semua pihak yang tidak dapat saya sebutkan satu-persatu yang telah banyak membantu dalam menjalankan perkuliahan dan menyelesaikan skripsi ini.

Akhir kata, saya berharap Allah SWT berkenan membalas segala kebaikan semua pihak yang telah membantu. Semoga skripsi ini membawa manfaat bagi pengembangan ilmu dan memperkaya wawasan kita.

Jakarta, 24 Desember 2008

Penulis

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Universitas Indonesia, saya yang bertanda tangan di bawah ini:

Nama	: Anisa Fithrasari
NPM	: 0606043963
Program Studi	: Teknik Industri
Departemen	: Teknik Industri
Fakultas	: Teknik
Jenis Karya	: Skripsi

demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Indonesia **Hak Bebas Royalti Noneksklusif (*Non-exclusive Royalty Free Right*)** atas karya ilmiah saya yang berjudul:

Analisis Risiko Kegagalan pada *Core Network* Perangkat GPRS Menggunakan Metode FMEA dan FTA serta Skenario Alokasi Biaya Penanganannya

beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini Universitas Indonesia berhak menyimpan, mengalihmedia/format-kan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.
Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta
Pada tanggal : 24 Desember 2008

Yang menyatakan

(Anisa Fithrasari**)**

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

ABSTRAK

Nama : Anisa Fithrasari
Program Studi : Teknik Industri

Judul : Analisis Risiko Kegagalan pada *Core Network* Perangkat GPRS Menggunakan Metode FMEA dan FTA serta Skenario Alokasi Biaya Penanganannya

Seiring dengan terus meningkatnya perkembangan teknologi, muncul tuntutan bagi perusahaan telekomunikasi untuk memberikan layanan data lebih efisien dan pada laju data yang lebih tinggi maupun memperkenalkan layanan-layanan baru. Di sinilah GPRS menawarkan solusi bagi tuntutan teknologi seperti yang disebut di atas. Ditambah dengan semakin meluasnya pemanfaatan teknologi GPRS yang memberikan banyak kemudahan bagi penggunanya, maka perusahaan telekomunikasi memanfaatkan GPRS untuk meningkatkan *value added services*. Namun, pada perangkat GPRS yang digunakan tidak lepas dari munculnya risiko kegagalan. Untuk menghindari maupun meminimalisir terjadinya risiko tersebut maka perlu dilakukan analisis risiko. Analisis risiko yang dilakukan pada penelitian ini bertujuan untuk memperoleh usulan penanganan risiko kegagalan pada *core network* perangkat GPRS serta skenario alokasi biaya penanganannya. Dengan menggunakan metode FMEA, diperoleh risiko kritis yang kemudian dianalisis lebih lanjut menggunakan FTA untuk memperoleh *basic event* sehingga dapat diusulkan tindakan penanganan risikonya. Risiko kritis juga disimulasikan dengan simulasi optimasi OptQuest-Crystal Ball untuk memperoleh alokasi biaya penanganan risiko yang optimal.

Kata kunci :
GPRS, analisis risiko, FMEA, FTA, simulasi OptQuest-Crystal Ball.

ABSTRACT

Name	:	Anisa Fithrasari
Study Program	:	Industrial Engineering
Title	:	Failure Risk Analysis on Core Network of GPRS Equipment using FMEA & FTA Method and Scenario of Treatment Cost Allocation

Due to increasing of technology development, telecommunication corporate must provide more efficient data services on higher traffic data, and also introduce new services. GPRS can be a solution to achieve that things. Now application of GPRS technology is more developing and give a lot of advantages for user. That's why corporate telecommunication use GPRS to increase their value added services. But, there is potential failure risk on GPRS equipment, so risk analysis need to be done. Objectives of risk analysis in this research are to get idea of risk treatment action on GPRS equipment and scenario of treatment cost allocation. By using FMEA method, be able to have critical risk which will be further analysed using FTA to have basic event from those critical risk. And also by using OptQuest-Crystal Ball simulation can have optimal treatment cost allocation.

Key words :
GPRS, risk analysis, FMEA, FTA, OptQuest-Crystal Ball simulation.

BAB I
PENDAHULUAN

1.1 Latar Belakang Permasalahan

GPRS merupakan teknologi yang memungkinkan para operator jaringan komunikasi bergerak menawarkan layanan data dengan laju bit yang lebih tinggi dengan tarif rendah, sehingga membuat layanan data menjadi menarik bagi pasar massal. Para operator jaringan komunikasi bergerak melihat GPRS sebagai kunci untuk mengembangkan pasar komunikasi bergerak menjadi pesaing baru di lahan yang pernah menjadi milik jaringan kabel, yakni layanan internet. Perkembangan yang pesat bagi komunikasi bergerak mendorong para operator layanan berlomba untuk memperkaya macam layanannya guna menambah pemasukan bagi perusahaannya sambil tetap mempertahankan pelanggan yang dimilikinya. Komunikasi data bergerak, teristimewa untuk akses internet, nampaknya kini menjadi pendorong utamanya. Di sinilah GPRS menawarkan solusi bagi tuntutan teknologi seperti yang disebut di atas, yakni dapat memberikan kepada para operator kesempatan untuk memberikan layanan data lebih efisien dan pada laju data yang lebih tinggi maupun memperkenalkan layanan-layanan baru untuk mengkompensasi penurunan biaya komunikasi per menit. Jelasnya, GPRS memungkinkan para pelanggan dapat menciptakan fasa hubungan lebih cepat, tetap terhubung secara permanen, menggunakan kecepatan data lebih tinggi dan hanya membayar biaya tiap bit yang ditransfer saja. Pertimbangannya jelas, bahwa kecenderungan pasar pastilah tidak menuju kepada setiap teknologi yang sifatnya justru menaikkan biaya atau tarif langganan.

Teknologi GPRS kini juga memberikan *corporate solution.* Penyediaan jasa link untuk perbankan pada mesin ATM (*Automatic Teller* Machine) yang semula menggunakan teknologi satelit sekarang sudah menggunakan teknologi GPRS, sehingga manfaat yang diambil adalah efisiensi biaya oleh perbankan dengan sewa bandwidth yang lebih efisien. Teknologi GPRS juga dapat digunakan pada teknologi EDC (*Electronic Data Capture*), untuk mempermudah teknologi EDC sehingga dapat

memudahkan customer dalam melakukan pembayaran dimana pun, diantara yang dapat memanfaatkan teknologi EDC adalah transaksi yang dilakukan di hypermarket dan transaksi dalam penggunaan taksi sehingga penumpang bisa membayar taksi menggunakan kartu kredit. Dan yang sedang *booming* saat ini adalah aplikasi Blackberry yang juga menggunakan teknologi GPRS. Dengan adanya Blackberry maka memudahkan para praktisi bisnis dalam menjalankan pekerjaan mereka sehingga layanan ini telah memiliki banyak pelanggan dan akan senantiasa terus bertambah seiring dengan tuntutan kemajuan teknologi.

Operator telekomunikasi yang telah memanfaatkan GPRS untuk meningkatkan *Value Added Services* haruslah menaruh perhatian terhadap perangkat GPRS yang digunakan. Perangkat GPRS harus di*maintain* untuk mempertahankan kinerja yang diinginkan. Sehingga masalah yang mungkin timbul dapat dihindari ataupun diminimalisir dan tuntutan pencapaian tujuan perusahaan dapat terpenuhi. Yang lebih utama adalah pelanggan dapat memberikan loyalitasnya bahkan jumlah pelanggan semakin bertambah karena adanya *excellent service*.

Untuk mencapai *excellent services*, maka ditetapkan *Key Performance Indicator* (KPI), dalam hal ini adalah KPI dari bagian/divisi yang bertanggung jawab terhadap operasional dan pemeliharaan perangkat GPRS. Pada perusahaan yang menjadi objek penelitian penulis, ditetapkan KPI yang terdiri dari 2 faktor utama yaitu *Attach Success Rate* dan *PDP Context Success Rate. Attach Success Rate* mengindikasikan tingkat keberhasilan pelanggan dalam mendapatkan sinyal, adapun *PDP Context Success Rate* mengindikasikan tingkat keberhasilan pelanggan untuk bisa *connect* ke jaringan internet. Permasalahan yang sering timbul adalah gagal sinyal dan gagal *connect* yang diantaranya disebabkan oleh *transmission problem, capacity issue, configuration links issue,* dan *equipment GPRS reliability*. Dengan timbulnya masalah tersebut, perusahaan tersebut berpotensi untuk kehilangan pendapatan dan muncul ketidakpuasan pelanggan. Selain 2 faktor KPI tersebut, ada faktor lain yang menjadi perhatian operator yaitu *Attack Security* terhadap jaringan GPRS yang bisa merugikan atau bisa membuat *fraud* dalam sistem GPRS.

Permasalahan yang pernah terjadi ataupun belum pernah terjadi namun memiliki peluang untuk terjadi akan menjadi potensi risiko. Oleh karenanya, analisis risiko perlu dilakukan untuk mengidentifikasi, mengukur, dan kemudian menyusun strategi sebagai dasar untuk membangun sistem manajemen risiko yang utuh. Manajemen risiko adalah sebuah proses untuk mengukur atau menilai risiko, dan kemudian mengembangkan strategi untuk mengelola risiko tersebut[1]. Dengan melihat latar belakang tersebut, maka penulis menyusun penelitian dengan mengambil judul 'Analisis Risiko Kegagalan pada *Core Network* Perangkat GPRS menggunakan FMEA dan FTA serta Skenario Alokasi Biaya Penanganannya'.

1.2 Diagram Keterkaitan Permasalahan

Berdasarkan latar belakang masalah yang telah diuraikan sebelumnya, dapat dibuat suatu diagram keterkaitan permasalahan seperti terlihat pada Gambar 1.1.

1.3 Rumusan Permasalahan

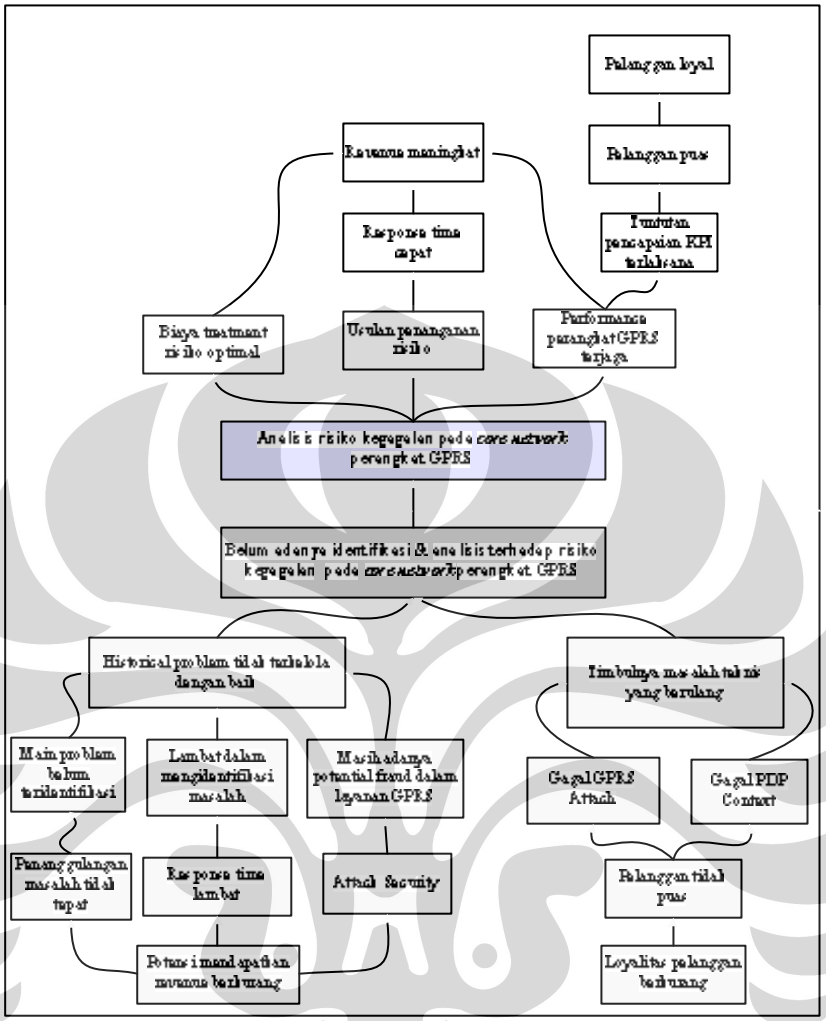
Berdasarkan latar belakang dan diagram keterkaitan permasalahan yang telah diuraikan sebelumnya, pokok permasalahan yang akan dibahas pada penelitian ini adalah mengenai identifikasi risiko kegagalan yang mungkin muncul pada *core network* perangkat GPRS, yang dilanjutkan dengan analisis terhadap risiko tersebut hingga memberikan usulan penanganan risiko.

1.4 Tujuan Penelitian

Tujuan penelitian ini adalah sebagai berikut :

- Memperoleh prioritas risiko kegagalan (risiko kritis) pada *core network* perangkat GPRS untuk dilakukan penanganannya
- Memperoleh usulan penanganan risiko kritis dan skenario alokasi biaya penanganannya

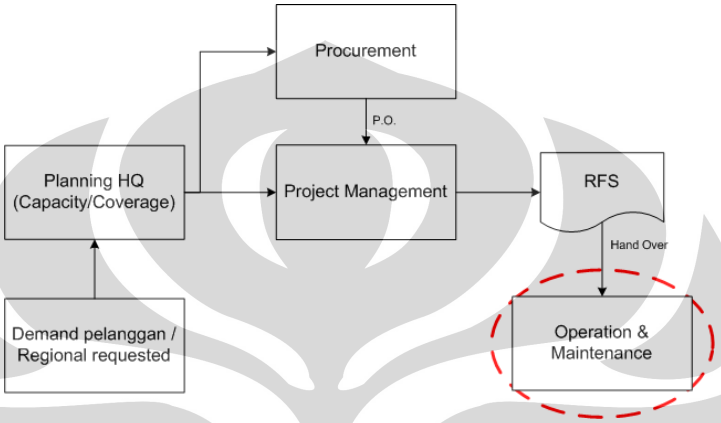
[1] G. Stoneburner, A. Goguen, A. Feringa, (2001). *Risk Management Guide for Information Technology Sistem,* dalam *Recommendations of the National Institute of Standards and Technology*, National Institute of Standards and Technology, U.S. Government Printing Offiice, Washington, hal 4.


Pelanggan loyal
Pelanggan puas
Tuntutan pencapaian KPI terlaksana
Performance perangkat GPRS terjaga
Pendapatan meningkat
Respons time cepat
Biaya treatment risiko optimal
Usulan penanganan risiko
Analisis risiko kegagalan pada core network perangkat GPRS
Belum adanya identifikasi & analisis terhadap risiko kegagalan pada core network perangkat GPRS
Historical problem tidak terkelola dengan baik
Timbulnya masalah-masalah yang berulang
Main problem belum teridentifikasi
Lambat dalam mengidentifikasi masalah
Masih adanya potential fraud dalam layanan GPRS
Gagal GPRS Attach
Gagal PDP Context
Penanggulangan masalah tidak tepat
Respons time lambat
Attach Security
Pelanggan tidak puas
Potensi pendapatan menurun berulang
Loyalitas pelanggan berkurang

1.6 Ruang Lingkup Penelitian

Agar penelitian ini memberikan hasil yang sesuai dengan tujuan penelitian, maka akan dilakukan pembatasan masalah, seperti tercantum di bawah ini :

- Risiko yang ditinjau adalah risiko kegagalan dalam kegiatan operasional dan pemeliharaan perangkat GPRS.



Gambar 1.2 Proses Pengadaan Perangkat GPRS

- Tim *expert* yang dilibatkan pada penelitian ini adalah General Manager, Team Leader, dan Engineer Divisi Network Service O&M Center
- Analisis dan evaluasi risiko yang dilakukan menggunakan *Failure Mode and Effect Analysis* (FMEA) yang dilanjutkan dengan *Fault Tree Analysis* (FTA) dan dilakukan pula skenario alokasi biaya penanganan risiko menggunakan simulasi *OptQuest-Crystal Ball.*

1.7 Metodologi Penelitian

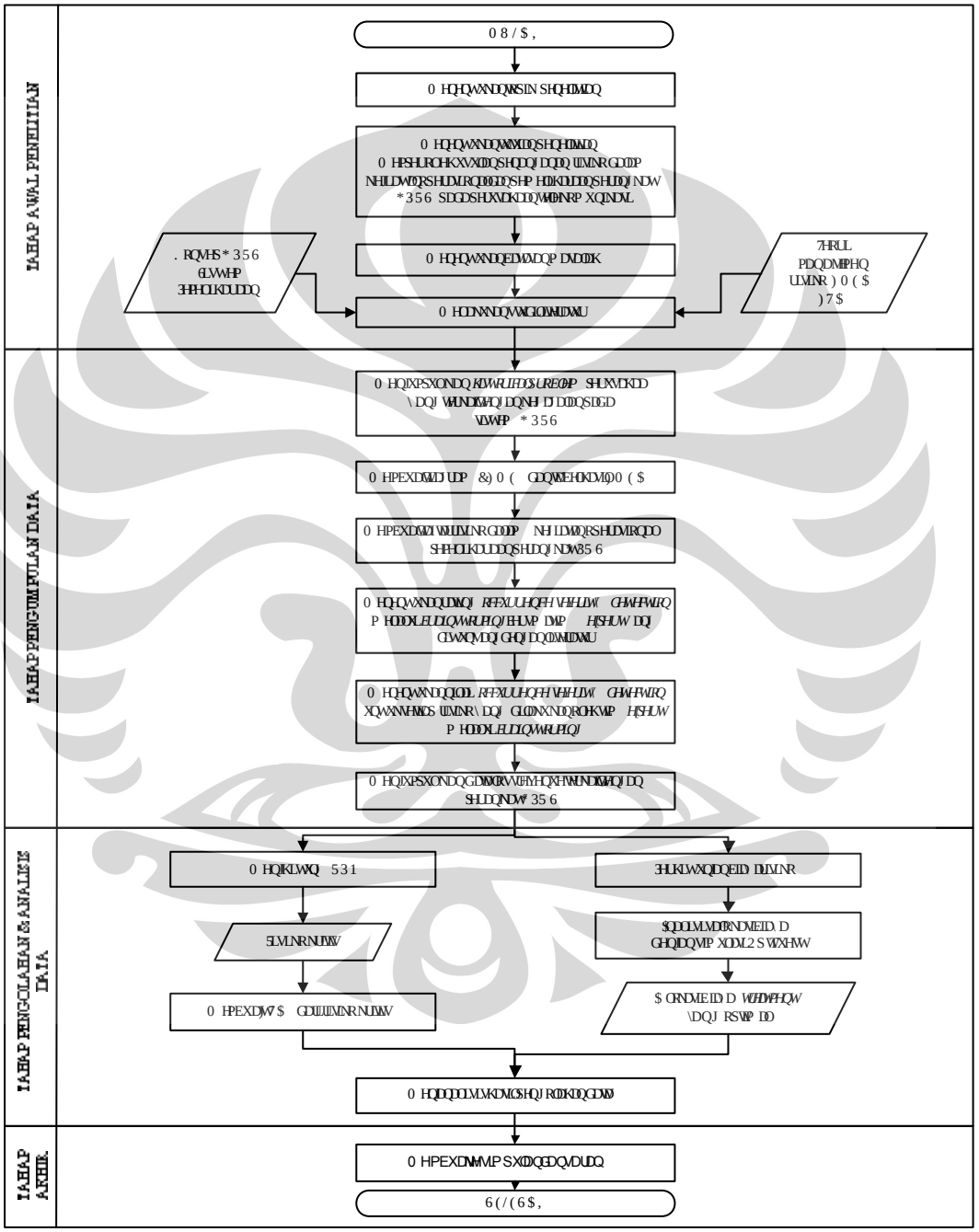
Metodologi penelitian yang digunakan oleh penulis dalam penelitian ini adalah sebagai berikut.

1. Tahap awal penelitian, meliputi :
   a. Menentukan topik penelitian yang akan dilakukan
   b. Menentukan tujuan penelitian
   c. Menentukan batasan masalah

d. Melakukan studi literatur terhadap landasan teori yang akan digunakan sebagai acuan, yaitu konsep GPRS, sistem pemeliharaan, manajemen risiko, *Failure Mode And Effect Analysis* (FMEA), dan *Fault Tree Analysis* (FTA).

2. Tahap pengumpulan data, yang dilakukan dengan cara :
   a. Mengumpulkan *historical data* perusahaan yang terkait dengan kegagalan pada sistem GPRS
   b. Membuat diagram *Cause Failure Mode Effect* (CFME) dan tabel hasil *Failure Mode and Effect Analysis* (FMEA)
   c. Membuat daftar risiko dalam kegiatan operasional dan pemeliharaan perangkat GPRS
   d. Menentukan rating *occurrence*, *severity*, dan *detection* melalui *brainstorming* bersama tim *expert* yang ditunjang dengan literatur
   e. Menentukan nilai *occurrence*, *severity*, dan *detection* untuk setiap risiko yang dilakukan oleh tim *expert* melalui *brainstorming*
   f. Mengumpulkan data *loss revenue* yang terkait dengan permasalahan dalam sistem GPRS
3. Tahap pengolahan data dan analisis, yaitu tahapan dimana data-data yang telah terkumpul diolah dan dianalisis. Tahap ini terdiri dari :
   a. Melakukan rekapitulasi terhadap hasil *brainstorming* tim *expert* sehingga dapat ditentukan *Risk Priority Number* (RPN) dan diperoleh risiko kritis.
   b. Membuat diagram *Fault Tree Analysis* (FTA) dari masing-masing risiko kritis yang diperoleh.
   c. Melakukan perhitungan biaya risiko dengan mengkonversikan beberapa variabel ke dalam nilai uang.
   d. Melakukan analisis alokasi biaya penanganan risiko dengan simulasi *OptQuest* sehingga diperoleh alokasi biaya *treatment* optimal.
   e. Melakukan analisis terhadap risiko yang terjadi sehingga dapat diketahui penyebab terjadinya dan strategi untuk mengatasi risiko tersebut.

4. Tahap akhir, yaitu penarikan kesimpulan dari keseluruhan penelitian yang telah dilakukan kemudian memberi beberapa masukan bagi perusahaan untuk menangani dan mencegah terjadinya risiko.



Gambar 1.3 Diagram Alir Metodologi Penelitian

1.8 Sistematika Penulisan

Sistematika yang digunakan dalam penelitian ini mengacu pada standar buku penulisan skripsi yang terdiri dari lima bab.

Bab 1 adalah pendahuluan yang menjelaskan mengenai latar belakang dilakukan penelitian ini, diagram keterkaitan permasalahan, rumusan permasalahan, tujuan penelitian, manfaat penelitian, batasan masalah, metodologi penelitian dan sistematika penulisan.

Bab 2 menyajikan landasan teori yang mendukung penelitian ini. Landasan teori yang dijelaskan meliputi sistem pemeliharaan, GPRS, risiko, ma najemen risiko, FMEA, FTA, dan simulasi OptQuest.

Bab 3 meliputi pengumpulan data dan pengolahannya. Pada bab ini terdapat berbagai data yang diperlukan dan telah dikumpulkan melalui tinjauan terhadap dokumen terkait, wawancara, *brainstorming*, maupun perolehan data statistik dan finansial dari perusahaan. Pengolahan data dilakukan dengan metode FMEA, FTA, dan simulasi OptQuest.

Bab 4 akan dijelaskan analisis hasil penelitian berdasarkan data yang sudah diolah. Bab ini juga akan menjelaskan usulan tindakan penanganan risiko dan analisis hasil simulasi OptQuest.

Bab 5 menyajikan kesimpulan dari keseluruhan penelitian. Kesimpulan yang diberikan merupakan hasil dari dilakukannya penelitian ini, yaitu berupa usulan penanganan risiko dan alokasi biaya penanganan risiko yang optimal.

BAB II
LANDASAN TEORI

2.1 Pemeliharaan

Saat ini peralatan dan plant yang dioperasikan cenderung semakin kompleks dan membutuhkan modal yang sangat besar baik untuk investasi awal maupun untuk biaya operasional. Untuk itu, strategi dan kebijaksanaan pemeliharaan sangat diperlukan agar semua peralatan yang beroperasi di dalam sistem tidak sering mengalami kegagalan dalam pengoperasiannya. Secara tradisional, pemeliharaan dipandang sebagai sesuatu yang hanya dipertimbangkan jika telah terjadi sesuatu yang salah pada suatu sistem atau sesuatu yang salah akan segera terjadi, bila hal ini terjadi maka biasanya fungsi pemeliharaan yang ada tidak terorganisasi dan tidak sistematis.

Berbagai upaya untuk mengoptimalkan pemeliharaan, baik bentuk maupun biaya pemeliharaan telah banyak dilakukan yang kesemuanya bertujuan untuk menjaga ketersediaan (*availability*) sistem. Oleh karena itu, untuk saat ini teknik pemeliharaan lebih banyak dikonsentrasikan pada pemeliharaan pencegahan/preventif untuk menghindari kerusakan yang lebih serius, dan strategi pemeliharaan pencegahan ini juga difokuskan untuk mempertahankan efisiensi dari sistem sedekat mungkin dengan efisiensi maksimum yang sudah didesain. Umumnya, regulasi dan *policy* baik internal maupun eksternal akan menentukan kebijakan perawatan yang berkaitan dengan keselamatan. Sedangkan pemeliharaan yang berkaitan dengan ketersediaan dan konsumsi energi, optimasi harus dijadikan sebagai basis penentuan kebijaksanaan pemeliharaan, karena penambahan tugas pemeliharaan tidak hanya akan menambah ketersediaan sistem tetapi juga akan menambah biaya pemeliharaannya. Sehingga tujuan dari implementasi pemeliharaan itu hendaknya diharapkan juga mempertimbangkan optimasi berbagai faktor yang saling berkaitan.

Pemeliharaan merupakan hal yang sangat mahal dan merupakan suatu godaan yang kuat untuk menundanya sampai esok hari dan menghemat dana untuk hari ini. Ekspresi *minimal maintenance approach* menunjukkan tindakan pemeliharaan

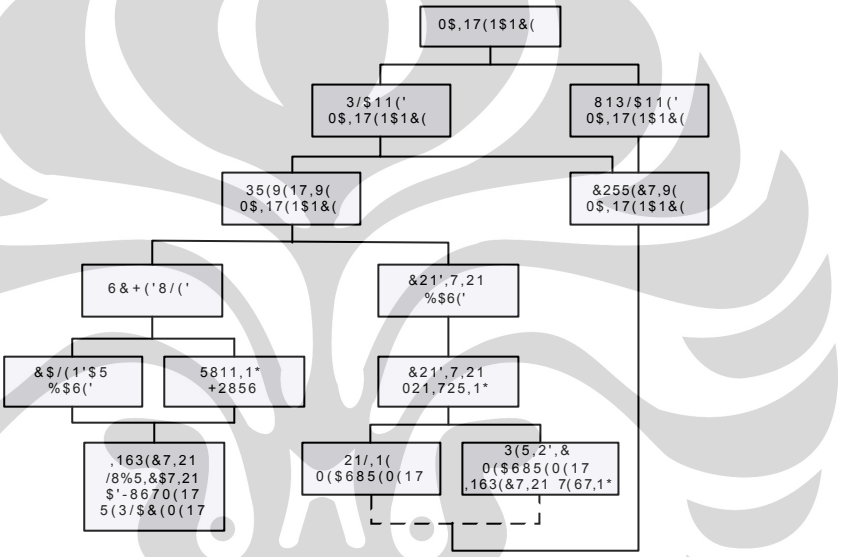
terhadap suatu plant yang dilakukan hanya untuk memenuhi persyaratan dan hukum yang telah ditentukan oleh badan pembuat peraturan. Jika tindakan ini dikombinasikan dengan manajemen pemeliharaan yang terabaikan, maka hal ini akan memperpendek masa berguna (*useful life*) dari plant dan juga mungkin juga akan menambah biaya lainnya seperti biaya kerusakan (*downtime cost*) dan berbagai denda yang timbul akibat dampak yang mungkin ditimbulkan oleh kerusakan sistem.

2.1.1 Jenis Pemeliharaan

Ada berbagai jenis pemeliharaan yang banyak dilakukan secara praktis. Jenis–jenis pemeliharaan ini secara skematis dapat dilihat pada gambar 2.1 di bawah ini, yang secara umum dibagi menjadi *planned maintenance* (pemeliharaan terencana) dan *unplanned maintenance* (pemeliharaan tak terencana). Pemeliharaan terencana adalah pemeliharaan yang diorganisir dan dilakukan dengan perencanaan dan pengontrolan yang sudah ditentukan terlebih dahulu. Sedangkan pemeliharaan tak terencana adalah satu jenis pemeliharaan yang dilakukan tanpa perencanaan terlebih dahulu. Pemeliharaan preventif adalah pemeliharaan yang dilakukan pada interval waktu yang sudah ditentukan – contoh dari strategi ini adalah *scheduled maintenance* - atau berhubungan dengan kriteria yang sudah ditentukan - contoh dari strategi ini adalah *condition maintenance.* Dengan melakukan pemeliharaan preventif, mengandung maksud untuk mengurangi probabilitas kegagalan atau penurunan *performance* dari suatu sistem. Pemeliharaan korektif adalah pemeliharaan yang dilakukan setelah peralatan mengalami kegagalan dan pemeliharaan ini dimaksudkan untuk mengembalikan sistem ke keadaan dimana sistem tersebut dapat melakukan fungsinya kembali. *Emergency maintenance* adalah salah satu jenis dari *corrective maintenance* yang diperlukan untuk memfungsikan kembali peralatan secepatnya agar dampak yang lebih buruk dapat dihindari.

Pemeliharaan preventif dapat dibagi lagi menjadi *scheduled maintenance* (pemeliharaan terjadwal) dan *condition based maintenance* (pemeliharaan yang berbasis pada kondisi sistem). Pemeliharaan terjadwal dilakukan pada interval waktu tertentu, baik itu banyaknya jam kerja, jumlah siklus yang telah dilalui, dan lain–lain.

Pemilihan interval waktu pemeliharaan untuk satu komponen tertentu terbukti sangat sulit. Bentuk dari pemeliharaan preventif biasanya berupa pengecekan (*inspection*) terhadap berbagai komponen secara periodik untuk menentukan apakah pengaturan (*adjustment*) dan penggantian (*replacement*) sudah diperlukan. Jika interval ini terlalu sering, maka pengecekan ini akan mengurangi ketersediaan sistem dan menambah risiko kesalahan *re-assembly.* Sedangkan pengecekan yang jarang mungkin akan menimbulkan kerusakan sistem yang tidak diinginkan.



Gambar 2.1 Jenis – jenis Pemeliharaan

Condition based maintenance (pemeliharaan yang berbasis pada kondisi sistem) adalah pemeliharaan terhadap suatu yang dilakukan sebagai hasil dari suatu kondisi yang sudah diketahui dari hasil pemantauan secara kontinyu atau secara periodik. Kegiatan pemeliharaan dilakukan hanya jika kondisi dari peralatan menunjukkan bahwa peralatan tersebut membutuhkan pemeliharaan. Dengan pendekatan ini pemeliharaan hanya dilakukan bila hal itu diperlukan.

Condition monitoring (pemantauan kondisi) adalah pengukuran secara periodik dan kontinyu dan menginterpretasikan data yang menunjukkan kondisi dari peralatan dan menentukan apakah peralatan tersebut membutuhkan pemeliharaan atau

tidak. Pemantauan kondisi secara normal dilakukan pada saat peralatan sedang beroperasi dan tidak sedang dalam keadaan rusak berat. Aplikasi dari pengukuran secara kontinyu mungkin bisa dibandingkan dengan pemakaian proses sistem alarm. Pada sistem alarm ini parameter operasional yang kritis dimonitor secara terus menerus dan alarm akan berbunyi bila kondisi tertentu dilampaui.

Tujuan dari pemantauan kondisi adalah untuk mengkuantifikasikan kondisi suatu peralatan dan tidak begitu saja memberikan peringatan bila batas operasi yang ditentukan telah dicapai. Pengukuran secara periodik umumnya mempunyai tujuan untuk memberikan proteksi yang cukup dari suatu peralatan terhadap kondisi yang buruk atau kondisi yang perlahan-lahan mengarah ke terjadinya suatu kegagalan. Suatu pengukuran mungkin dapat dilakukan pada interval yang lebih pendek bila *running hours* peralatan semakin bertambah.

2.2 General Packet Radio Service (GPRS)

General Packet Radio Service (GPRS) menyediakan layanan paket data pada sistem global untuk komunikasi bergerak (GSM) dan sistem *Wideband Code Division Multiple Access* (WCDMA). Sebelum ada pengembangan transmisi data lewat GPRS, transmisi data GSM sangat lambat, hal ini dikarenakan kanal radionya yang bersifat tunggal dan berkecepatan rendah, dan diperuntukkan khusus bagi setiap pengguna data selama durasi komunikasi (*dedicated*). Komunikasi yang bersifat *dedicated* ini menyebabkan operator harus menyediakan sambungan yang banyak agar semua pemakai bisa melakukan komunikasi data. Hal ini membuat biaya perawatan dan penambahan sambungan bagi operator semakin mahal.

GPRS menggunakan teknologi *packet switching* memungkinkan semua pengguna dalam sebuah sel dapat berbagi sumber-sumber yang sama, dengan kata lain para pelanggan menggunakan spektrum radio hanya ketika benar-benar mentransmisikan data. Efisiensi penggunaan spektrum pada akhirnya berarti kinerja yang lebih baik dan biaya yang lebih rendah. GPRS dapat menawarkan laju data sampai 115 kbps atau lebih.

GPRS disebut teknologi 2.5 G karena merupakan langkah awal menuju teknologi transfer data kecepatan tinggi lewat jaringan nirkabel (3G). Sehingga sering disebut-sebut sebagai teknologi kunci untuk data bergerak. Secara rinci ada beberapa faktor yang menjadi pertimbangan bahwa GPRS merupakan teknologi kunci untuk data bergerak, yakni :

- mampu memanfaatkan kemampuan cakupan global yang dimiliki GSM (2G)
- memperkaya utiliti investasi untuk perangkat GSM yang sudah ada
- merupakan teknologi jembatan yang bagus menuju generasi ke 3
- berbasis paket data yang lebih efiesian dalam penggunaan sumber daya
- memiliki laju data sampai 115 kbps yang berarti dua kali lipat daripada koneksi 'dial up' 56 kbps yang berlaku

2.2.1 Sistem GPRS

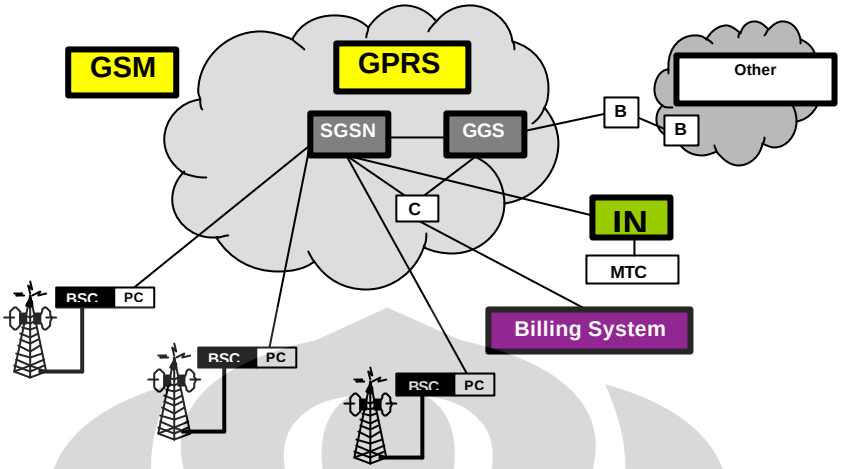
Jaringan GPRS merupakan jaringan terpisah dari jaringan GSM dan saat ini hanya digunakan untuk aplikasi data. Komponen-komponen utama jaringan GPRS adalah :

– **GGSN**; gerbang penghubung jaringan GSM ke jaringan internet
– **SGSN**; gerbang penghubung jaringan BSS/BTS ke jaringan GPRS
– **PCU**; komponen di level BSS yang menghubungkan terminal ke jaringan GPRS

Secara teori kecepatan pengiriman data GPRS dapat mencapai **115 kb/s**. Namun dalam implementasinya sangat tergantung dari berbagai hal seperti :

– Konfigurasi dan alokasi time slot di level Radio/BTS
– Teknologi *software* yang digunakan
– Dukungan ponsel

Ini menjelaskan mengapa pada saat-saat tertentu, di lokasi tertentu, akses GPRS terasa lambat dan bahkan bisa lebih lambat dari akses CSD yang memiliki kecepatan **9,6 kb/s.**



Gambar 2.2 Konfigurasi GPRS

2.2.2 Arsitektur Umum Jaringan GPRS

Gambar 2.3 adalah arsitektur jaringan GPRS secara umum. Dalam gambar di bawah terlihat bahwa jaringan GPRS merupakan bagian dari jaringan GSM. Berikut penjelasan bagian-bagian dalam gambar tersebut:

MS – Mobile Station

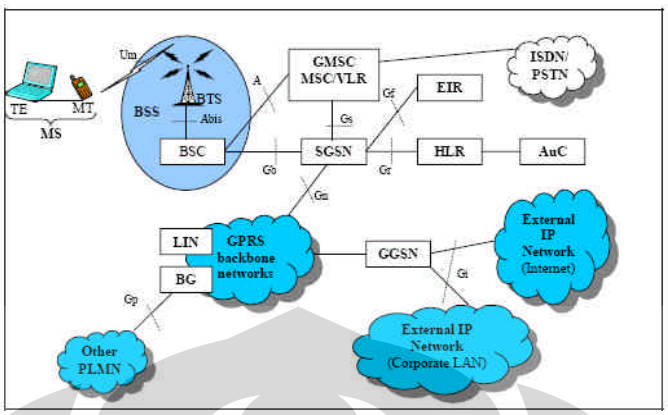
MS dapat dikatakan perangkat selular yang terhubung langsung dengan jaringan GSM, yaitu *SIM (Subscriber Identify Module) Card* dan perangkat keras seperti telepon selular, PDA, perangkat komputer yang terhubung menggunakan jaringan GPRS.

BSS – Base Station System

BSS terdiri dari BTS (*Base Transceiver Station*) dan BSC (*Base Station Controller*). Di BSS sinyal radio dari BSS akan diterima oleh BTS dan selanjutnya diteruskan ke BSC. BSC menangani sinyal yang dikirimkan oleh beberapa BTS.

HLR – Home Location Register

HLR adalah database yang menyimpan data pengguna jaringan GPRS. Informasi yang disimpan dalam HLR misalnya APN (Access Point Name).



Gambar 2.3 Arsitektur Jaringan GPRS

VLR – Visitor Location Register

VLR adalah database yang berisi informasi semua MS yang sedang terhubung dengan GPRS.

SGSN – Serving GPRS Support Node

SGSN adalah komponen utama jaringan GPRS. SGSN akan meneruskan paket data dari/ke MS. Fungsi SGSN :

1. mengantarkan packet data ke MS
2. Update pelanggan ke HLR
3. Registrasi pelanggan baru

GGSN – Gateway GPRS Support Node

GGSN juga merupakan komponen utama jaringan GPRS. GGSN mengubah paket data GSM dari SGSN menjadi paket TCP/IP. GGSN dan SGSN digunakan sebagai penghitung pembayaran pemakaian internet.

Fungsi GGSN :

1. Interface ke PDN
2. Information Routing
   - ? Transfer data dari PDU ke SGSN
     1. Network Screening
     2. User Screening
     3. Address Mapping

EIR – Equiptment Identity Register

EIR adalah database yang berisi data tentang perangkat bergerak. Dalam EIR bisa berisi data-data IMEI dari telepon selular yang diperbolehkan/tidak diperbolehkan memakai GPRS.

AuC – Authentication Center

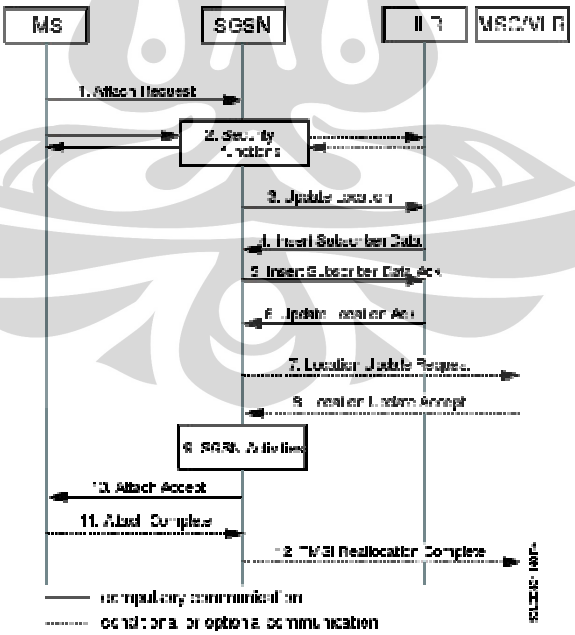
AuC adalah database yang berisi informasi pengguna yang diperbolehkan memakai jaringan GPRS. AuC merupakan bagian dari HLR.

GPRS backbone networks

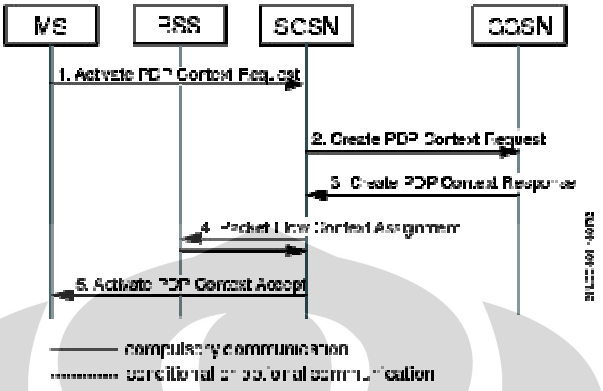
GPRS backbone network adalah intranet dari jaringan GPRS. GPRS backbone networks adalah *IP based.*

2.2.3 GPRS Attach dan PDP Context

Untuk menerima atau mengirimkan data pengguna terakhir harus melakukan dua langkah prosedur,GPRS attach dan PDP context activation. Pada GPRS attach, logical link dibangun antara MS dan SGSN. Dan pada PDP Context, logical link dibangun antara MS sampai GGSN.



Gambar 2.4 GPRS Attach



Gambar 2.5 PDP Context Activation

2.3 Risiko

Risiko dapat diartikan dalam berbagai bentuk. Secara sederhana, risiko merupakan ukuran penyimpangan dari hasil yang diharapkan[2]. Risiko dapat diartikan sebagai ukuran dari kemungkinan dan dampak dari tidak tercapainya tujuan dari suatu proyek[3]. Kebanyakan orang setuju bahwa risiko berhubungan dengan dugaan ketidakpastian. Tujuan A dengan kemungkinan yang terukur sebesar 0.05 dapat diartikan lebih berisiko dibandingkan tujuan B dengan kemungkinan sebesar 0.2, jika dampak dari tidak tercapainya tujuan A empat kali lebih sering terjadi daripada penyimpangan dari tujuan B. Risiko tidak selalu mudah diperkirakan, karena kemungkinan terjadinya dan dampak dari terjadinya biasanya tidak secara langsung berupa parameter yang dapat dihitung dan harus dihitung menggunakan ilmu statistik atau metode yang lain.

Risiko adalah kemungkinan akan terjadinya sesuatu yang dapat merintangi tercapainya suatu sasaran bisnis yang spesifik[4]. Risiko sendiri tidak dapat dikendalikan secara langsung, namun faktor penyebab terjadinya risiko dapat

[2] Claire Lee Reiss. (2001). *Risk Identification and Analysis : A Guide for Small Public Entities*, hal 1.
[3] Harold Kerzner. (2006). *Project Management, A System Approach to Planning, Scheduling, and Controlling 9th ed.* John Wiley & Sons, Inc., hal 709.
[4] Ronald L. Meier. (2000). Integrating Enterprise-Wide Risk Management Concepts into Industrial Technology Curricula. *Journal of Industrial Technology.* Vol 16, hal 2.

dikendalikan (*manageable*). Ada suatu sinyal, peringatan, tanda, atau indikator jika terjadi suatu risiko.

The Standards Australia/New Zealand (2004) memaparkan bahwa Risiko adalah suatu kemungkinan dari suatu kejadian yang tidak diinginkan yang mempunyai dampak pada sasaran atau tujuan. Pernyataan lain mengenai definisi risiko, yakni kesempatan terjadinya sesuatu yang memiliki pengaruh (baik positif maupun negatif) terhadap suatu tujuan[5]. Risiko biasanya dijelaskan dalam istilah sebuah kejadian atau kondisi dan akibat yang mungkin timbul dari kejadian tersebut. Risiko diukur dalam bentuk kombinasi dari akibat sebuah kejadian dan kemungkinannya. Oleh karena itu, dapat dikatakan bahwa pada dasarnya risiko muncul karena adanya ketidakpastian.

Berdasarkan berbagai definisi di atas, maka dapat diketahui bahwa pada dasarnya risiko merupakan kemungkinan terjadinya kerugian, kerusakan, atau kejadian lain yang tidak diharapkan. Pada umumnya, orang menginginkan risiko yang rendah untuk dapat memperoleh hasil yang lebih tinggi.

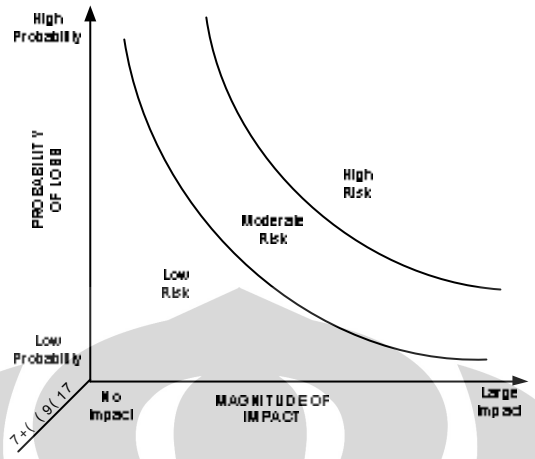
Risiko memiliki tiga elemen utama[6], yaitu :

1. Kejadian (*event*), yaitu peristiwa atau situasi yang terjadi pada tempat tertentu selama selang waktu tertentu.
2. Probabilitas/kemungkinan (*likelihood*), merupakan deskripsi kualitatif dari probabilitas atau frekuensi.
3. Dampak (*consequences*), yaitu hasil dari sebuah kejadian, baik kuantitatif maupun kualitatif, yang berupa kehilangan, luka, atau kerugian.

Dengan demikian, maka risiko dapat dikatakan sebagai sebuah fungsi dari kejadian, probabilitas, dan dampak, sebagaimana dinyatakan pada Persamaan (2.1) :

Risiko = *f* (kejadian, probabilitas, dampak) .....(2.1)

[5] Canterprise Board. (2006). *Risk Management and Compliance Framework*, University of Canterbury. New Zealand, hal 3.
[6] Harold Kerzner, *Opcit*, hal 710.



Gambar 2.6 Risiko sebagai Fungsi dari *Event, Likelihood,* dan *Consequences*

Gambar di atas menunjukkan hubungan tiap elemen yang membentuk risiko. Pada gambar tersebut dapat dilihat bahwa semakin besar probabilitas atau dampak, maka risiko juga semakin besar. Probabilitas (*likelihood*) dan dampak (*Impact*) ini harus diperhitungkan dalam manajemen risiko.

- Probabilitas (*likelihood*)

  Probabilitas adalah kemungkinan terjadinya *hazard event*. *Hazard* itu sendiri dapat didefinisikan sebagai sumber potensial terjadinya *accident*. Jika dalam pendefinisian risiko menggunakan sudut pandang *likelihood*, maka risiko dengan nilai probabilitas mendekati 1 (mengingat nilai probabilitas antara 0 dan 1) dapat dikatakan sebagai risiko dengan kategori tinggi.

- Dampak (*Impact*)

  Dampak atau konsekuensi adalah hasil dari terjadinya *hazard event*, yang mencakup kerusakan, kehilangan, kerugian atau luka pada seseorang. Jika dalam pendefinisian risiko menggunakan sudut pandang *impact*, maka risiko yang menghasilkan *impact* terbesar dapat dikatakan sebagai risiko dengan kategori tinggi.

2.3.1 Jenis Risiko

Berdasarkan ruang lingkupnya, risiko dapat dibedakan menjadi tiga macam[7], yaitu :

1. Risiko strategis (*strategic risk*)

   Risiko strategis merupakan faktor internal dan eksternal yang mungkin memiliki pengaruh yang signifikan dalam pencapaian tujuan organisasi. Penyebab terjadinya risiko ini biasanya kondisi ekonomi nasional dan global serta kebijakan pemerintah. Umumnya, risiko ini tidak dapat diprediksi atau diawasi melalui prosedur operasional. Kewaspadaan dan respon yang cepat dibutuhkan untuk menangani risiko ini. Terkadang, *strategic risk* disebut sebagai risiko bisnis (*business risk*).

2. Risiko operasional (*operational risk*)

   Pada dasarnya, risiko operasional berhubungan dengan kegiatan-kegiatan untuk menjalankan suatu bisnis. Untuk lebih memudahkan pemahamannya maka risiko operasional dibagi menjadi dua komponen, yaitu risiko kegagalan operasional dan risiko strategi operasional.

   Risiko kegagalan operasional berasal dari potensi terjadinya kegagalan dalam menjalankan bisnis. Manusia, proses, dan teknologi adalah beberapa alat perusahaan untuk mencapai tujuannya. Salah satu atau bahkan beberapa faktor tersebut dapat mengalami kegagalan yang beraneka ragam. Oleh karena itu, risiko kegagalan operasional dapat didefinisikan sebagai risiko yang muncul karena terdapat kegagalan manusia, kegagalan proses, atau kegagalan teknologi dalam suatu unit bisnis. Risiko kegagalan operasional sulit untuk diantisipasi karena ketidakpastiannya.

   Risiko strategi operasional muncul dari faktor lingkungan, seperti masuknya pesaing baru yang mengubah paradigma bisnis, perubahan kebijakan organisasi, bencana alam, dan faktor lain yang sejenis yang berada di luar kontrol perusahaan. Segalam macam bisnis mengandalkan orang, proses, dan teknologi di luar unit bisnis tersebut sehingga potensi kegagalan juga terdapat dalam faktor-

[7] Canterprise Board, *Op.Cit*., hal 3.

faktor tersebut. Jenis risiko yang berada di luar kontrol perusahaan juga disebut dengan risiko ketergantungan operasional.

Lebih lanjut, risiko operasional juga dapat dibagi menjadi lima jenis[8], yaitu :

a. Risiko orang, yakni kerugian yang diakibatkan dengan sengaja atau tidak sengaja oleh seseorang atau melibatkan beberapa karyawan, seperti kesalahan tindakan karyawan, ketidakpatuhan karyawan, dan lain-lain.
b. Risiko hubungan, yaitu kerugian hak cipta atau produksi perusahaan dan ditimbulkan melalui hubungan atau kontrak dengan klien, pemegang saham, pihak ketiga, atau pengambil kebijakan pemerintah. Contohnya, penggantian kerugian kepada klien atau pembayaran penalti.
c. Risiko teknologi dan proses, merupakan kegagalan, kerusakan, atau gangguan lainnya pada teknologi dan/atau proses. Kerugian akibat pembajakan atau pencurian data atau informasi, dan kerugian akibat kegagalan teknologi dalam memenuhi kebutuhan bisnis yang diinginkan adalah contoh risiko ini.
d. Risiko fisik adalah risiko kerugian yang dialami melalui kerusakan properti perusahaan atau kerugian pada properti fisik atau aset yang menjadi tanggung jawab perusahaan.
e. Risiko eksternal lainnya, yaitu risiko kerugian yang diakibatkan oleh tindakan pihak eksternal, seperti tanggung jawab atas tindakan kecurangan di perusahaan atau perubahan kebijakan pemerintah yang mempengaruhi kemampuan perusahaan untuk beroperasi di pasar-pasar tertentu.

3. Risiko proyek (*project risk*)

Project risk adalah risiko yang berhubungan dengan proyek, biasanya bersifat lebih spesifik, kadang jangka pendek, dan seringkali berhubungan dengan proses pembelajaran, penelitian, atau pembelian sesuatu yang baru, *change management*, integrasi, atau proyek pengembangan teknologi informasi. Perhatian dan tindakan terhadap risiko ini biasanya didelegasikan kepada manajer proyek. Penanganan

[8] Alvarez, Gene. *Operational Risk Event Classification*. October 2, 2008. www.ic2.zurich.com

risiko proyek dengan baik merupakan suatu usaha untuk menghindari keterlambatan atau biaya yang berlebihan.

2.4 Manajemen Risiko

Secara sederhana, manajemen risiko adalah suatu cara untuk mengelola risiko. Dengan kata lain, ditekankan pada segala aktivitas yang dilakukan untuk mengurangi ketidakpastian dari suatu kejadian. Dalam konteks proyek, manajemen risiko mengurangi dampak dari kejadian yang tidak diharapkan pada suatu proyek[9].

Manajemen risiko bukanlah hanya dilakukan dengan berasuransi bagi perusahaan. Tetapi juga berkenaan dengan risiko yang *insurable* dan *uninsurable,* dan penentuan suatu teknik untuk mengatasi risiko tersebut. Penekanan dari manajemen risiko bukanlah mendapatkan asuransi tinggi tetapi mengurangi biaya penanganan risiko dengan cara yang paling tepat[10].

Proses menilai/mengukur kemudian merancang strategi dan prosedur untuk mengurangi risiko yang teridentifikasi juga merupakan salah satu definisi manajemen risiko[11]. Manajemen risiko pada dasarnya adalah proses menyeluruh yang dilengkapi dengan alat, teknik, dan ilmu yang diperlukan untuk mengenali, mengukur, dan mengelola risiko secara lebih transparan[12]. Untuk meningkatkan pencapaian hasil, sangatlah penting bagi sebuah organisasi untuk memiliki pemahaman yang baik mengenai risiko-risiko potensial sehingga risiko dapat dikuantifikasi secara sistematis, diantisipasi sebab akibatnya, dan akhirnya diharapkan dapat dilakukan tindakan yang sesuai untuk mengatasinya.

Arti dari manajemen risiko jika dikutip dari *The Standards Australia/New Zealand* (2004), adalah suatu proses untuk mengetahui, menganalisis serta mengendalikan risiko dalam setiap kegiatan atau aktivitas perusahaan yang ditujukan/diaplikasikan untuk menuju efektivitas manajemen yang lebih tinggi dalam

---

[9] Misra C.S. (2006). *Differrent Techniques for Risk Management in Software Engineering : A Review*. ASAC. Banff, Alberta. hal 197

[10] Ronald L. Meier, *Opcit,* hal 2.

[11] Jay Tarakkumar Shah. (2004). *Probabilistic Risk Assessment Method for Prioritization Of Risk Faktors,* MSc Thesis, Gujarat University, hal 1.

[12] Dilan, S. Batuparan. (2001). Kerangka Kerja *Risk Management,* EI News, Edisi 5, hal 1.

menangani kesempatan yang potensial dan kerugian yang dapat mempengaruhi perusahaan.

Manajemen risiko adalah suatu proses yang sistematik dan berpikir secara logika, yang akan digunakan untuk menentukan keputusan dalam memperbaiki efektivitas dan efisiensi dari performansi. Hal ini seharusnya diintegrasikan dalam budaya kerja sehari-hari.

Mengidentifikasi dan bersiap-siap untuk sesuatu yang akan terjadi juga merupakan manajemen risiko. Hal ini mencakup melakukan aksi untuk menghindari atau mengurangi kerjadian yang tidak diinginkan dalam organisasi, terhadap biaya atau efek yang lain dari suatu kejadian, atau untuk organisasi dalam memaksimalkan kesempatan potensial yang teridentifikasi. Manajemen risiko mendorong suatu organisasi untuk melakukan tindakan proaktif dibandingkan melakukan tindakan reaktif.

Berdasarkan penjelasan di atas, maka manajemen risiko tidaklah rumit, melainkan bagian dari sebuah manajemen yang baik yang melibatkan pernyataan dan perencanaan untuk kemungkinan dari beberapa hasil yang mungkin. Sebuah bisnis mengelola risiko dengan menjadikannya sebagai salah satu faktor dalam proses pengambilan keputusan. Gagal mengelola risiko dengan efektif dapat menimbulkan beberapa dampak yang merugikan, yaitu :

- kerugian finansial bagi organisasi;
- cedera/luka (*personal injury*);
- kehilangan komunitas;
- kehilangan profesionalisme;
- tuntutan kriminal;
- kerusakan lingkungan;
- krisis kesehatan lingkungan;
- tuntutan atas kerusakan.

Manajemen risiko bukanlah tentang menghindari risiko sepenuhnya, tetapi lebih kepada mengetahui akibat relatif yang muncul untuk tiap tingkat dalam manajemen kemudian mengambil keputusan dengan mempertimbangkan hal tersebut. Beberapa prinsip dasar yang menjadi kerangka kerja manajemen risiko adalah mengintegrasikan manajemen risiko dengan perencanaan, persiapan, dan pelaksanaan misi, membuat keputusan mengenai risiko pada level yang sesuai, dan menerima risiko yang tidak penting.

Cara atau strategi yang tepat dapat dengan cepat diterapkan dan dilaksanakan oleh suatu perusahaan untuk menghindari atau mengurangi besarnya kerugian yang dapat diderita perusahaan akibat dari risiko atau ketidakpastian dari munculnya peristiwa yang merugikan. Penerapan manajemen risiko di suatu perusahaan dapat meningkatkan kontrol terhadap risiko perusahaan mengalami kejadian yang tidak diharapkan di masa mendatang. Secara logika dapat dikatakan bahwa risiko mengalami kerugian akan semakin menurun seiring dengan meningkatnya kontrol, sehingga hasil akhir yang didapat oleh perusahaan adalah laba yang tidak berkurang akibat terjadinya suatu peristiwa yang merugikan.

Setiap perusahaan membutuhkan metoda tertentu untuk mengontrol berbagai risiko yang mungkin timbul. Manajemen risiko dapat diartikan sebagai suatu sistem pengawasan risiko dan perlindungan harta benda, hak milik badan usaha atau perorangan atas kemungkinan timbulnya kerugian karena adanya suatu risiko. Di dalam usaha, ketidakpastian ini dapat dihubungkan dengan penghasilan perusahaan, arus keluar masuk uang dan harta benda yang telah ada.

Sistem manajemen risiko memberikan ukuran bahwa perusahaan mengatur ancaman-ancamannya di dalam suatu cara yang proaktif, terkoordinasi, bernilai, efektif dan memahami pemrioritasan. Dengan memberikan pengertian yang baik pada karyawan maupun manajer mengenai pentingnya manajemen risiko sudah tentu diharapkan mereka dapat turut serta dalam menjalankan perusahaan dengan lebih efektif sehingga perusahaan dapat terus berkembang.

Suatu keseimbangan antara biaya dalam mengelola risiko dengan keuntungan yang akan didapatkan sangat dibutuhkan dalam pelaksanaan program manajemen

risiko. Hal ini dapat membantu untuk menentukan level manajemen risiko yang akan diaplikasikan. Untuk beberapa kasus, biaya perhitungan untuk menghindari risiko atau mengurangi risiko, dapat menjadi lebih tinggi dibandingkan dengan konsekuensi yang diakibatkan oleh risiko tersebut. Sedangkan di kasus lain, pencegahan dari suatu risiko biayanya akan lebih tinggi, dikarenakan risiko tersebut tingkatannya sangat rendah dan dapat diterima.

2.4.1 Aktivitas Manajemen Risiko

Manajemen risiko memiliki beberapa kegiatan yang berhubungan dengan risiko yaitu perencanaan (*planning*), penilaian (identifikasi dan analisis), mengembangkan metode penanganan (*handling*), dan memonitor (*monitoring*). Tujuan utama dari rangkaian proses ini adalah meningkatkan probabilitas dan dampak yang positif serta menurunkan probabilitas dan dampak yang negatif.

Gambar 2.7 di bawah ini menunjukkan aktivitas manajemen risiko, dimana setiap aktivitas saling berinteraksi. Keenam aktivitas tersebut adalah[13]:

1. Perencanaan manajemen risiko, yaitu menentukan pendekatan apa yang akan dilakukan, rencana, dan melaksanakan aktivitas manajemen risiko.
2. Identifikasi risiko, yaitu menentukan risiko yang dapat mempengaruhi proyek dan mendokumentasikan karakteristiknya.
3. Analisis kualitatif terhadap risiko, yaitu memprioritaskan risiko untuk dianalisis lebih jauh atau menilai dan mengkombinasikan probabilitas dan dampaknya.
4. Analisis kuantitatif terhadap risiko, yaitu menganalisis secara numerik efek dari risiko yang teridentifikasi terhadap keseluruhan proyek.
5. Perencanaan respon terhadap risiko, yaitu membuat pilihan dan tindakan untuk meningkatkan peluang dan mengurangi ancaman bagi tujuan proyek.
6. Kontrol dan pengawasan terhadap risiko, yaitu memantau risiko yang teridentifikasi, mengawasi risiko yang tersisa, mengidentifikasi risiko baru,

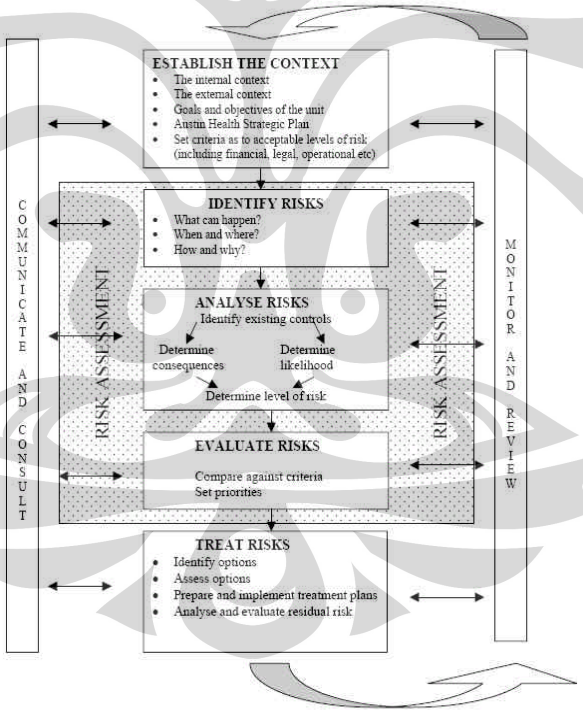
[13] Project Management Institute. (2000) .*A Guide to The Project Management Body of Knowledge : PMBOK Guide.* Pennsylvania : Project Management Institute, Inc., hal 127.

melaksanakan rencana respon terhadap risiko, dan mengevaluasi efektivitasnya sepanjang daur hidup proyek.

Gambar 2.7 Aktivitas Manajemen Risiko menurut *Project Management Institute*

Di samping keenam aktivitas di atas, penjelasan yang lebih lengkap mengenai proses manajemen risiko juga terdapat dalam beberapa standar, salah satunya adalah *Australian/New Zealand Standard for Risk Management (AS/NZ 4360 : 2004).* Menurut standar ini, terdapat beberapa tahapan dalam manajemen risiko sebagaimana terlihat pada Gambar 2.8 di bawah ini, yaitu :

1. Menentukan konteks, meliputi penjelasan mengenai ruang lingkup organisasi, batasan, bagian dari organisasi, penentuan kriteria risiko yang dapat diterima, juga struktur aktivitas secara matematis.
2. Mengidentifikasi risiko, yaitu menentukan kategori sumber risiko, kejaian yang berpotensi menimbulkan risiko, waktu, serta proses terjadinya.
3. Menganalisis risiko, mencakup mengidentifikasi dan menilai kontrol yang sudah ada, serta menilai probabilitas dan dampak dari risiko.
4. Mengevaluasi risiko, yaitu menentukan dan mengevaluasi tingkat risiko berdasarkan kriteria risiko yang telah ditentukan, serta memprioritaskan risiko.
5. Menentukan strategi dan kontrol untuk penanganan risiko, meliputi menilai berbagai alternatif strategi kemudian menentukan kontrol yang sesuai.



Gambar 2.8 Proses Manajemen Risiko berdasarkan *Australian/New Zealand Standard for Risk Management* (AS/NZ 4360 : 2004)

Standar lain yang dapat dijadikan acuan adalah yang dinyatakan oleh COSO *(The Committee of Sponsoring Organization of the Treadway Commission).* COCO mengeluarkan *Enterprise Risk Management – Integrated Framework* (COSO ERM Framework). COSO menyatakan bahwa *Enterprise Risk Management – Integrated Framework* terdiri dari 5 komponen, yang menunjukkan aktivitas manajemen risiko yang saling berinteraksi. Komponen tersebut adalah[14] :

- *Control Environment.* Budaya perusahaan/organisasi yang mempengaruhi kontrol terhadap perilaku orang-orang dalam organisasi tersebut. Termasuk di dalamnya adalah integritas, nilai-nilai etika, dan kompetensi karyawan; penetapan kewenangan dan tanggung jawab; serta masukan yang diberikan oleh BOD (*Board of Directors*).
- *Risk Assessment*. Identifikasi dan analisis risiko yang terkait dengan pencapaian tujuan perusahaan, penentuan risiko apa saja yang harus dikelola, dan implementasi proses untuk risiko-risiko yang berpengaruh terhadap adanya perubahan.
- *Control activities*. Kebijakan-kebijakan, aturan, prosedur, dan proses yang membantu perusahaan dalam hal manajemen.
- *Information and Communication.* Komunikasi internal dalam perusahaan dan komunikasi eksternal dengan customer, regulator, dan shareholder.

  Setiap tahapan kegiatan identifikasi, analisis, evaluasi, dan penanganan risiko dikomunikasikan/dilaporkan kepada pihak yang berkepentingan terhadap aktivitas bisnis yang dilakukan perusahaan untuk memastikan bahwa tujuan manajemen risiko dapat tercapai sesuai dengan keinginan pihak yang berkepentingan. Pihak yang berkepentingan berasal dari internal perusahaan (manajemen, karyawan) dan eksternal perusahaan (pemasok, pemerintah daerah/pusat, masyarakat sekitar).
- *Monitoring*. Penilaian terhadap kualitas dari sistem kontrol internal perusahaan. Perubahan kondisi internal dan eksternal perusahaan menimbulkan risiko baru bagi perusahaan, mengubah tingkat kemungkinan/dampak terjadinya risiko, dan

[14] *The COSO Framework : An Overview, Journal of Accountancy*, 2002, hal 1.

cara penanganan risikonya. Sehingga setiap risiko yang teridentifikasi masuk dalam Register Risiko dan Peta Risiko perlu dipantau perubahannya.

Gambar 2.9 The COSO Framework

Proses manajemen risiko terdiri dari 6 tahap yang dapat digunakan dalam memetakan keputusan bisnis suatu organisasi dan tujuan perusahaan (MDQCG LLC, 1999). Keenam tahap dalam proses manajemen risiko yang dimaksud adalah:

- *Determination of objectives.* Memutuskan secara tepat program manajemen risiko agar dapat sesuai dengan harapan organisasi.
- *Identification of the risks.* Dalam tahap ini mengikutsertakan semua individu yang peduli terhadap risiko. *Tools* atau teknik yang dapat digunakan antara lain kuesioner analisis risiko, *exposure checklist*, *insurance policy checklist*, flowchart, *analysis of finansial statements*, laporan internal, inspeksi, wawancara.
- *Evaluation of the risks.* Makna evaluasi risiko adalah mengukur *potential loss* dan probabilitas kemungkinan terjadinya.
- *Consideration of alternatives and selection of risk treatment.* Menguji beragam pendekatan untuk menangani risiko dan memilih teknik yang dapat digunakan.
- *Implementation of the decision.* Menentukan aturan dan prosedur untuk mengurangi probabilitas maupun frekuensi dari kejadian risiko dan menurunkan tingkat dampak dari risiko tersebut.

- *Evaluation and review*. Merupakan tahap penting karena seiring dengan perubahan yang ada maka akan muncul risiko baru meskipun risiko lama telah hilang, dan teknik yang semula sesuai untuk menangani risiko lama belum tentu akan sesuai pula untuk risiko baru yang muncul. Dengan dilakukannya tahap ini diharapkan akan dapat mengetahui gejala suatu risiko sebelum risiko tersebut terjadi dan menyebabkan kerugian finansial.

Gambar 2.10 Enam Tahap dalam Proses Manajemen Risiko (MDQG LLC, 1999)

2.4.1.1 Perencanaan Risiko (*Risk Planning*)

Perencanaan risiko aktivitas/program yang detail mengenai manajemen risiko, merupakan proses untuk [15] :

- Mengembangkan dan mengarsipkan strategi manajemen risiko yang terorganisir, luas, dan interaktif
- Menentukan metode yang digunakan untuk menjalankan strategi manajemen risiko
- Merencanakan sumber daya yang tepat

[15] Harold Kerzner, *Opcit*, hal 720

Pada perencanaan risiko,di dalamnya termasuk keseluruhan proses untuk manajemen risiko, dengan aktivitas untuk memprediksi (identifikasi dan analisis), penanganan, dan monitor risiko yang berkaitan dengan program. Hasil yang penting dari proses perencanaan ini dalah *risk management plan* (RMP).

Perencanaan risiko ini akan membentuk suatu strategi manajemen risiko yang terdiri dari pendekatan proses dan implementasi. Tahap pertama meliputi penentuan tujuan, menentukan tugas untuk bidang yang spesifik, mengidentifikasikan keahlian yang diperlukan, mendeskripsikan proses peramalan dan bidang yang harus diwaspadai, menjelaskan rating risiko, membuat prosedur untuk menjadi perhatian dalam strategi penanganan, membuat pengukuran performa, dan menentukan kebutuhan untuk pelaporan dan pengarsipan.

Kunci dalam membuat suatu *risk management plan* (RMP) adalah dengan mendapatkan suatu informasi penting sehingga tim mengetahui mengenai tujuan dan teknik dalam proses manajemen risiko, yaitu pelaporan, pengarsipan, dan komunikasi, peraturan dan tanggung jawab organisasi, serta tindakan yang dilakukan guna membuat suatu manajemen risiko yang efektif. RMP dapat berupa rencana yang detail/spesifik seperti tanggung jawab tugas untuk tiap anggota tim, dan bersifat umum di beberapa bidang untuk memberikan pilihan bagi tim dalam menjalankan tugasnya agar menghasilkan manajemen risiko yang efisien misalnya gambaran teknis/metode yang disarankan untuk menganalisis secara tepat tergantung keuntungan dan kerugian dari tiap metode tersebut dan situasi yang dihadapi.

Salah satu aspek penting lainnya dalam perencanaan risiko adalah menyediakan/mengadakan trainin manajemen risiko untuk personel tim. Penting untuk menyelenggarakan training manajemen risiko yang dilakukan oleh seorang individu dengan kemampuan/keahlian dalam manajemen risiko pada dunia nyata, jika tidak maka training manajemen risiko akan lebih bersifat seperti latihan tanpa menghasilkan suatu keahlian.

2.4.1.2 Penilaian Risiko (*Risk Assessment*)

Risk Assessment adalah tahap penting pendefinisian masalah pada manajemen risiko, tahap dimana proses identifikasi dan analisis masalah dalam bentuk probabilitas dan dampak[16]. Hasil dari proses ini menjadi input untuk banyak aktivitas lain dalam manajemen risiko setelah proses ini. Biasanya tahap ini merupakan tahap terlama/terpanjang dalam suatu aktivitas manajemen risiko. *Risk Assessment* merupakan salah satu proses terpenting dalam aktivitas manajemen risiko karena mutu dan kualitas dari penilaian ini dapat berdampak besar pada hasil program. Komponen dari tahap ini adalah identifikasi risiko dan analisis risiko, dimana keduanya merupakan proses yang berurutan.

Identifikasi Risiko

Identifikasi risiko adalah rangkaian proses pengenalan yang seksama atas risiko dan komponen risiko yang melekat pada suatu aktivitas atau transaksi yang diarahkan kepada proses pengukuran serta pengelolaan risiko yang tepat[17]. Identifikasi risiko adalah pondasi, dimana tahapan lainnya dalam proses manajemen risiko dibangun. Proses ini memungkinkan organisasi untuk menentukan lebih awal potensi pengaruh dari realisasi ancaman internal maupun eksternal dalam lingkungan organisasi. Dengan demikian, langkah pertama dalam identifikasi risiko ialah mendefinisikan lingkungan organisasi.

Tahap identifikasi risiko dilakukan berdasarkan kuesioner yang terstruktur. Kuesioner semacam ini harus dirancang dengan mengintegrasikan pengalaman dengan standar yang seharusnya. Kategori harus didefinisikan dengan baik dan harus mencerminkan sumber risiko yang umum. Beberapa contoh kategorisasi dalam kuesioner antara lain, pertanyaan yang berhubungan dengan industri, ruang lingkup proyek, manajemen proyek, pendekatan, pelatihan, dan lain-lain.

Segala kemungkinan risiko yang ada harus dapat diidentifikasi sehingga dapat dianalisis dan dikelola untuk mendapatkan strategi penanganan yang sesuai. Oleh

[16] Ibid, hal 721
[17] Dilan S. Batuparan, *Op.Cit.*, hal 9.

sebab itu, aktvitas utama untuk mengidentifikasi risiko ialah mengumpulkan berbagai informasi yang dibutuhkan, baik informasi internal maupun eksternal, seperti data finansial, standar perusahaan, maupun pendapat para ahli.

Identifikasi terhadap risiko ini dapat dilakukan melalui beberapa teknik, seperti:

1. Pengumpulan informasi, melalui *brainstorming*, wawancara, ataupun analisis SWOT (*Strength, Weaknesses, Opportunities, and Threats*)
2. *Checklist analysis*
3. Teknik pembuatan diagram (*diagramming techniques*), seperti diagram sebab-akibat dan diagram alir

Pada prinsipnya, perlu diperhatikan bahwa pengidentifikasian risiko merupakan tanggung jawab setiap tingkatan dalam perusahaan. Dengan kata lain, tahap ini membutuhkan pendekatan baik secara *bottom-up* maupun *top-down*.

Analisis Risiko

Analisis risiko dimulai dengan studi mendetail mengenai risiko yang telah diidentifikasi dan disetujui oleh para pengambil keputusan. Tujuannya adalah untuk mengumpulkan informasi mengenai persoalan risiko untuk menetapkan kemungkinan dari terjadinya, biaya, jadwal, dan akibat teknis jika risiko tersebut terjadi. Analisis risiko biasanya berdasarkan pada informasi yang mendetail yang dapat berasal dari :

- Perbandingan dengan sistem lain;
- Studi pembelajaran;
- Pengalaman;
- Hasil dari uji coba dan pengembangan prototip;
- Data dari keteknikan atau model;
- Penilaian ahli;
- Analisis rencana dan dokumen terkait;
- Simulasi dan model;
- Analisis sensitivitas dari alternatif.

Setiap kategori dari risiko, di dalamnya termasuk suatu set evaluasi dan terkait kepada hal yang lain. Hubungan ini membutuhkan analisis pada bidang tersebut untuk meyakinkan integritas dari proses.

Setelah melakukan analisis risiko, biasanya hasil dari tahap ini ditransfer menjadi tingkat risiko/level risiko. Rating risiko adalah dampak yang mungkin dari risiko pada sebuah program/proyek. Biasanya merupakan ukuran dari kemungkinan masalah timbul dan dampak dari persoalan tersebut, dan biasanya diwujudkan dalam kategori rendah (*low*), sedang (*medium*), dan tinggi (*high*). Definisi mengenai rating risiko ini adalah sebagai berikut[18]:

- Risiko tinggi (*high risk*) : berpengaruh secara substansial mendasar pada biaya, jadwal, atau teknis. Usaha yang substansial perlu dilakukan untuk mengurangi risiko ini. Prioritas manajemen yang tinggi diperlukan di sini.
- Risiko sedang (*moderate risk*) : beberapa berakibat pada biaya, jadwal atau teknis, usaha yang khusus perlu dilaksanakan untuk mengurangi hal tersebut. Perhatian dari pihak manajemen diperlukan di sini.
- Risiko rendah (*low risk*) : akibat yang rendah/kecil pada biaya, jadwal, atau teknis. Cara pandang pihak manajemen yang biasa diperlukan di sini.

2.4.1.3 Penanganan Risiko (*Risk Handling*)

Penganganan risiko meliputi metode khusus dan teknik untuk mengatasi risiko, mengidentifikasi siapa yang bertanggung jawab untuk risiko tersebut dan menghitung besarnya biaya dan jadwal untuk meminimalkan/mengurangi risiko tersebut. Di dalamnya juga menyangkut perencanaan dan eksekusi dengan tujuan untuk mengurangi risiko sampai tahap yang dapat diterima. Evaluator yang menilai risiko harus memulai proses dengan mengidentifikasikan risiko dan mengembangkan pilihan strategi penanganan. Penanganan risiko harus sejalan dengan RMP (*Risk Management Plan*) dan tambahan kebijakan dari pemimpin program. Bagian kritis dari tahap ini melibatkan filterisasi dan memilih pilihan strategi penanganan yang

[18] Harold Kerzner, *Opcit*, hal 729.

tepat dan pendekatan khusus implementasi untuk risiko. Prosedur dalam membuat suatu penanganan risiko (*risk handling*) dimulai dengan memilih penanganan risiko yang sangat diinginkan, kemudian implementasi terbaik dipilih sebagai pendekatannya. Dalam kasus dimana terdapat alternative rencana cadangan maka langkah ini diulangi terus.

Pilihan penanganan risiko terdiri dari menghindari risiko (*risk avoidance*), mentransfer risiko (*risk transfer*), mengurangi risiko (*risk mitigation*), dan menerima risiko (*risk acceptance*)[19].

1. *Risk Avoidance,* yaitu memutuskan untuk tidak melakukan aktivitas yang menghasilkan risiko. Meskipun tidak keseluruhan kejadian risiko dapat dieliminasi namun beberapa risiko spesifik dapat dihindari. Sebagai contoh pada jaringan perusahaan, menghapuskan jalur masuk jaringan secara keseluruhan untuk menghindari risiko serangan jaringan eksternal atau memutuskan untuk meninggalkan atau tidak memasuki sebuah jalur bisnis.
2. *Risk Transfer,* yaitu memindahkan risiko kepada pihak ketiga. Dengan demikian, pihak ketiga tersebut yang bertanggung jawab terhadap risiko yang terjadi, namun bukan berarti mengeliminasi risiko. Hal ini dapat dilakukan dengan menggunakan asuransi, garansi atau jaminan, atau melakukan kontrak.
3. *Risk Mitigation,* yaitu mengurangi probabilitas atau konsekwensi terjadinya risiko hingga batas yang dapat diterima. Melakukan pencegahan awal untuk mengurangi probabilitas atau dampak terjadinya risiko lebih efisien dibandingkan harus melakukan tindakan perbaikan akibat telah terjadinya risiko.
4. *Risk Acceptance.* Pada tahap ini, organisasi memutuskan untuk tidak mengubah perencanaan awal. Menerima secara aktif melalui pengembangan *contingency plan* (mengidentifikasi risiko yang muncul). Menerima secara pasif artinya adalah tidak melakukan tindakan apapun, membiarkan risiko terjadi.

[19] Project Management Institute, *Opcit*, hal 142.

2.4.1.4 Monitoring Risiko (*Risk Monitoring*)

Memonitor/mengawasi proses secara sistematis dan mengevaluasi keefektifan dari penanganan risiko dalam suatu parameter keberhasilan. Hasil dari proses ini dapat dijadikan untuk proses pengembangan strategi penanganan risiko (*risk handling*) atau men*update* strategi penanganan risiko saat ini dan menganalisis kembali risiko yang bersangkutan. Memonitor risiko bukanlah suatu teknik pemecahan masalah tetapi lebih teknik proaktif untuk mendapatkan informasi yang objektif dalam rangka mengurangi risiko sampai tahan/tingkatan yang diinginkan. Beberapa teknik yang biasa digunakan untuk memonitor risiko adalah:

- *Earned Value* (EV) : menggunakan biaya atau jadwal standar untuk mengevaluasi performa dari biaya program (dan menyediakan indikator dari jadwal performa) dalam suatu kesatuan. Seperti menyediakan dasar untuk menentukan jika penanganan risiko (*risk handling*) mencapai tahap/haisl yang telah diramalkan.
- *Program metrics* (pengukuran program) : ini merupakan penilaian secara formal dan periodik untuk proses pengembangan yang dipilih, mengevaluasi sampai sejauh mana proses pengembangan mencapai tujuannya. Teknik ini dapat digunakan untuk memonitor tindakan koreksi yang timbul dari penilaian dari proses yang kritis.
- Jadwal monitoring performa : untuk mengevaluasi sejauh mana kemajuan program/proyek dari pencapaiannya.
- *Technical Performance Measurement* (Teknis Pengukuran Performa) : merupakan hasil dari perancangan penilaian yang mengukur, melalui analisis keteknikaan dan uji coba, nilai dari parameter performa yang penting dari desain pada saat ini dipengaruhi oleh usaha penanganan risiko.

Sistem indikator dan penilaian kembali secara periodik dari risiko harus dapat menyatukan proses manajemen risiko ke dalam keseluruhan struktur manajemen. Pada akhirnya uji coba yang didefinisikan secara benar dan evaluasi program sering menjadi elemen kunci dalam memonitor performa dari penanganan risiko (*risk handling*) dan mengembangkan penilaian risiko yang baru.

2.4.2 Teknik Analisis Risiko

2.4.2.1 Teknik Analisis Risiko secara Kualitatif

Analisis risiko kualitatif adalah proses untuk menilai dampak dan kemungkinan dari risiko yang teridentifikasi. Proses ini memprioritaskan risiko berdasarkan dampak potensial risiko terhadap pencapaian tujuan organisasi.

1. Probabilitas dan Dampak Risiko. Probabilitas dan dampak risiko dapat digambarkan secara kualitatif seperti sangat tinggi, tinggi, moderat, rendah, dan sangat rendah. Analisis risiko yang mengacu pada probabilitas dan dampak risiko dapat membantu untuk mengidentifikasi risiko mana yang terlebih dahulu harus ditangani secara agresif.
2. Matriks Rating Risiko. Matriks dapat dibangun dengan mengkombinasikan nilai probabilitas dan dampak. Risiko dengan probabilitas tinggi dan dampak besar adalah yang diprioritaskan untuk dilakukan analisis lebih lanjut.
3. *Project Assumptions Testing.* Mengidentifikasi asumsi harus berdasarkan dua kriteria : stabilitas asumsi dan dampak terhadap suatu performansi jika asumsi salah. Asumsi alternatif harus diidentifikasi dan dampaknya terhadap tujuan organisasi harus diuji melalui proses analisis risiko secara kualitatif.
4. *Data Precision Ranking.* Analisis risiko kualitatif yang baik adalah yang memiliki data akurat dan tidak bias. *Data precision ranking* adalah teknik untuk mengevaluasi tingkat manfaat dari data risiko. Termasuk menguji tingkat ketersediaan data risiko, kualitas data, keandalan dan integritas data.

2.4.2.2 Teknik Analisis Risiko secara Kuantitatif

Analisis risiko secara kuantitatif bertujuan untuk menganalisis probabilitas setiap risiko secara numerik dan dampaknya terhadap pencapaian tujuan organisasi. Analisis kuantitatif secara umum mengikuti analisis kualitatif risiko, yang memerlukan adanya identifikasi risiko. Masukan bagi tahap analisis risiko kuantitatif dapat berasal dari *risk management plan*, risiko yang telah teridentifikasi, daftar prioritas risiko, *historical informationi,* dan *expert* judgment. Analisis risiko kualitatif dan kuantitatif dapat digunakan secara terpisah atau digabungkan.

1. Wawancara. Teknik wawancara terhadap para *expert* merupakan langkah pertama dalam mengkuantifikasi risiko.
2. Analisis Sensitivitas. Analisis ini membantu dalam menentukan risiko dengan potensial dampak paling tinggi.
3. *Decision Tree Analysis.* Adalah suatu diagram sederhana yang menunjukkan suatu proses untuk merinci masalah yang dihadapi dalam komponen-komponen, kemudian dibuatkan alternatif pemecahan beserta konsekuensi masing-masing alternatif.
4. Simulasi. Menggunakan suatu model yang menerjemahkan kondisi ketidakpastian menjadi potensial dampak terhadap tujuan organisasi. Contohnya adalah simulasi Monte Carlo yang digunakan untuk menentukan probabilitas pencapaian tujuan organisasi, mengkuantifikasi dampak risiko terhadap proyek, menentukan kebutuhan akan waktu dan biaya, memprioritaskan risiko dengan mengkuantifikasikan kontribusi relatif risiko terhadap proyek, dan mengidentifikasi target yang dapat dicapai dan realistis.

Tabel 2.1 Teknik Manajemen Risiko

Technique	Comments
Risk matrix	A good technique for relative risk ranking and for identifying change in risk as controls are applied. Useful tool for workshops as it allows broad participation.
Consequence modelling	Generally used to identify the possible consequences for significant hazards. Changes in conditions such as weather are considered.
Hazard and Operability Study (HAZOP)	A HAZOP study is used to examine chemical process designs. It is a structured hazard identification tool using a multi-disciplined team to identify process hazards in the design and operation of a facility. It involves the systematic application of combinations of parameters (flow, pressure and temperature) and guide words (no, more, less) to produce deviations (no flow, less pressure) from the design intent or intended operational mode of the plant.
Failure Modes and Effects Analysis (FMEA)	FMEA is commonly used to examine equipment failures. It is used to identify failure modes (i.e. ways in which equipment failures may occur) and evaluate the effects of possible system and component failures in a system. FMEA is quite a detailed and time consuming process and is often used to determine appropriate maintenance requirements.
Fault Tree or Event Tree Analysis	Fault Tree and Event Tree Analyses indicate the time sequence of potential accident scenarios. They are often used by risk experts to quantify the likelihood of an accident and its possible outcomes. Fault trees indicate the connection between undesirable events and the failure in the system's components and/or operator errors. Event Tree Analysis is used to map out the potential outcomes that an undesirable event can have for personnel, the environment, equipment or operation. It can show the potential escalation of accident scenarios.

Tabel di atas menunjukkan teknik umum manajemen risiko yang terdapat dalam *Australian Standard AS/NZS 3931.*

2.5 *Failure Mode And Effect Analysis* (FMEA)

*Failure Mode And Effect Analysis (*FMEA) merupakan salah satu teknik yang sistematis untuk menganalisis kegagalan. Teknik ini dikembangkan pertama kali sekitar tahun 1950-an oleh para *reliability engineers* yang sedang mempelajari masalah yang ditimbulkan oleh peralatan militer yang mengalami malfungsi. Teknik analisis ini lebih menekankan pada *hardware-oriented approach* atau *bottom-up approach*. Dikatakan demikian karena analisis yang dilakukan dimulai dari peralatan dan meneruskannya ke sistem yang merupakan tingkat yang lebih tinggi.

Failure Mode and Effect Analysis (FMEA) adalah pendekatan analitis yang ditujukan untuk pencegahan masalah melalui penentuan prioritas potensial masalah dan penanganannya. Dapat dikatakan juga bahwa FMEA adalah suatu sistem garis petunjuk, sebuah proses dan bentuk identifikasi dan prioritas terhadap potensial kegagalan dan masalah yang mungkin terjadi pada sebuah proses tersebut, yang perlu diperbaiki. Keuntungan dari penggunaan FMEA, antara lain :

- Mencegah kegagalan yang mungkin terjadi dan jaminan pengurangan biaya
- Memperbaiki fungsi produk dan kelemahannya
- Mengurangi masalah-masalah yang terjadi di proses manufaktur dari hari ke hari.
- Mengurangi masalah-masalah proses bisnis

Dengan FMEA memungkinkan tim berbagi pengetahuan. FMEA disebut juga sebagai dokumen hidup (*life document*), karena akan selalu ada selama proses atau produk masih ada. Dokumen FMEA dikenal sebagai catatan perubahan/permasalahan (cacat), meliputi :

- Pengaruhnya terhadap pelanggan (*effect on cutomer*)
- Penyebab potensial (*potensial causes*)
- Kejadian (*occurrence*)
- Bisa tidaknya dideteksi (*ability to detect*)

Failure Mode (kegagalan yang paling sering terjadi), yaitu kegagalan atau proses yang tidak bisa memenuhi spesifikasi dan biasanya dikaitkan dengan CACAT atau KETIDAK SESUAIAN.

Failure Mode Effect Analysis (FMEA), potensi kegagalan atau cacat diranking berdasarkan angka prioritas risiko atau *Risk Priority Number* (RPN) dan RPN dapat dirumuskan sebagai berikut :

RPN = *Severity* * *Occurrence* * *Detection* …….. (2.2)

Keterangan :

1. *Severity* : adalah dampak terjadinya kegagalan
2. *Occurrence* : adalah estimasi kemungkinan kegagalan akan muncul
3. *Detection* : adalah tingkat deteksi penyebab kegagalan

2.5.1 Prosedur Penyusunan FMEA

FMEA sangat sederhana untuk dilakukan. Hal yang diperlukan dalam menganalisis adalah untuk mengetahui dan memahami fungsi dari sistem dan beberapa *constraint* dimana sistem itu harus dapat beroperasi. Berikut ini beberapa pertanyaan dasar yang yang harus dijawab oleh seorang analis dalam melakukan analisis FMEA.

1. Bagaimana masing–masing komponen mengalami kegagalan ?
2. Mekanisme apa yang mungkin menghasilkan suatu mode kegagalan tertentu ?
3. Apa dampak dari kegagalan yang terjadi ?
4. Apakah kegagalan yang terjadi ada kaitannya dengan keselamatan atau tidak ?
5. Bagaimana kegagalan itu dapat dideteksi ?
6. Apa yang harus disediakan desain untuk mengkompensasi kegagalan ?

Tabel 2.2 Tipikal FMEA Worksheet

Process/Product : Date :	**FMEA Template**					
Potential failure mode	Potential failure effects	Severity	Potential causes	Occurrence	Current Controls	Detection RPN

2.5.2 RFMEA

Identifikasi dan meminimalkan risiko adalah langkah yang sangat penting dalam mengatur proyek yang sukses. Teknik analisis risiko termasuk interview dengan ahli, EMV (*Expected Monetary Value*) dan matriks response beserta dengan teknik risiko yang lain seperti metode simulasi Monte Carlo. Salah satu teknik dalam manajemen risiko adalah dengan mengkalikan probabilitas terjadinya risiko dengan tingkat dampak yang diharapkan dari risiko tersebut. Dalam hal ini, metode yang menggunakan perkalian antara probabilitas risiko dengan dampak diperluas dengan menambahkan unsur deteksi terhadap setiap risiko. Mengkalikan 3 nilai yaitu kemungkinan terjadi, dampak dan deteksi merupakan format dari *Failure Modes and Effect Analysis* (FMEA) yang digunakan untuk proses, desain, dan perencanaan servis. Teknik ini merupakan bagian dari ISO-9000 dan QS-9000 sertifikasi kualitas. Di dalam metode untuk mengaplikasikan FMEA dalam risiko, maka FMEA diartikan sebagai RFMEA (*Risk Failure Modes and Effect Analysis*). RFMEA bukan hanya sekedar metode dalam menganalisis proyek, tetapi membantu dalam memfokuskan strategi untuk menghadapi risiko tersebut. Metode yang menggunakan FMEA dengan analisis grafik sederhana digunakan untuk memprioritaskan risiko (*Risk Priority Planning*).

Metode RFMEA

RFMEA dikembangkan seperti halnya FMEA, memodifikasi kolom yang ada dapat dilakukan sesuai dengan spesifikasi pekerjaan. Contoh dari bentuk kolom dalam RFMEA dapat dilihat pada gambar 2.11.

Typical FMEA Columns	Failure ID	Failure Mode	Occurrence	Severity		Detection	RPN
Typical RFMEA Columns	Risk ID	Risk Event	Likelihood	Impact	Risk Score	Detection	RPN

Gambar 2.11 Perbedaan FMEA dan RFMEA

RFMEA ini dibuat selama pertemuan dalam rangka perencanaan tim, dengan menggunakan *template* dengan modifikasi sesuai kebutuhan. Modifikasi dapat berupa detail, persen, waktu spesifik, ataupun akibat yang berbentuk uang. Langkah-langkah dalam penyusunan RFMEA adalah sebagai berikut[20] :

1. Mengidentifikasi *risk event*. Pada tahap pertama ini *risk event* diidentifikasikan dengan cara *brainstorming* oleh tim. Setiap risiko yang diidentifikasikan dibuat dalam bentuk, "jika x terjadi, maka y akan terukur", dimana x adalah risiko dan y adalah akibat jika risiko tersebut terjadi. Akibat mungkin saja keterlambatan yang serius, atau peningkatan dalam biaya, atau keduanya. Risiko tersebut mungkin saja memiliki beberapa dampak, dan dalam kasus seperti itu, ID risiko diberikan untuk setiap dampak yang dapat diidentifikasikan. Sementara dampak dan *contingency plan* untuk beberapa risiko biasanya berbeda, kemungkinan dan nilai deteksi untuk tiap kejadian akan sama.
2. Penilaian kemungkinan (*likelihood*), akibat, dan nilai deteksi. Nilai untuk kemungkinan, akibat dan deteksi dilakukan oleh tim. Tim mendiskusikan nilai (*score*) dan menyetujui nilai dimana data tambahan dari ahli diperlukan atau review dar RFMEA terdahulu. Kualitas dari analisis akan meningkat. Contoh dari penilaian RFMEA dapat dilihat pada tabel 2.3, 2.4, dan 2.5.

Tabel 2.3 Bobot Probabilitas RFMEA

Probabilitas	**Penjelasan**
9 – 10	Sangat mungkin/pasti terjadi
7 – 8	Akan kemungkinan terjadi
5 – 6	Kemungkinan terjadi 50%
3 – 4	Kemungkinan tidak terjadi
1 - 2	Tidak mungkin terjadi

[20] Carbone, T & Tippett, D. (2004). Project Risk Management Using the Project Risk FMEA. *Engineering Management Journal*. Vol 16, No.4. hal 31.

Tabel 2.4 Bobot Dampak RFMEA

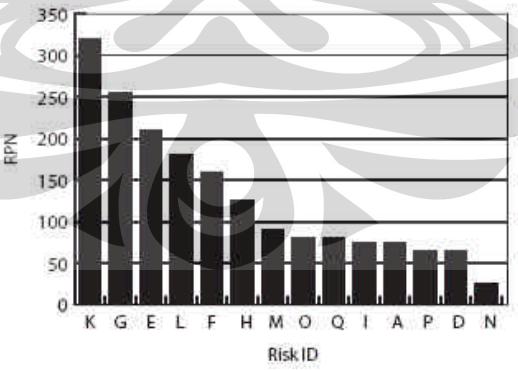
Over Cost	Penjelasan
9 – 10	>20% Over Cost
7 – 8	10% - 20% Over Cost
5 – 6	5% - 10% Over Cost
3 – 4	<5% Over Cost
1 - 2	Tidak terjadi Over Cost

Tabel 2.5 Bobot Deteksi RFMEA

Deteksi	Penjelasan
9 – 10	Tidak ada metode dalam pendeteksian risiko
7 – 8	Metode belum terpercaya/keefektivan belum diketahui
5 – 6	Metode memiliki efektivitas yang sedang
3 – 4	Metode deteksi efektif
1 - 2	Metode deteksi sangat efektif sehingga risiko pasti terdeteksi/terselesaikan

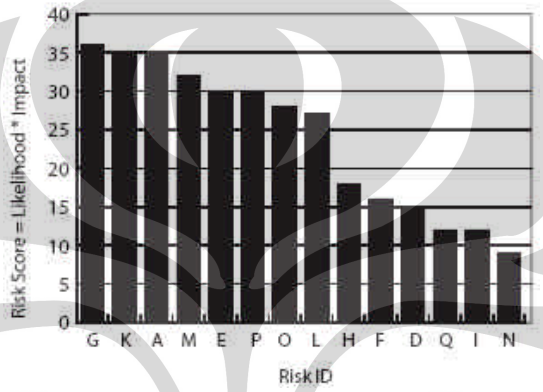
Ketika nilai ketiga parameter tersebut telah ada maka akan didapatkan *risk score* dan RPN (*Risk Priority Number*).

3. Review RPN pareto dan menentukan nilai kritis RPN. Langkah ketiga ini adalah mereview tentang RPN dan menentukan nilai kritisnya, dimana nilai untuk setiap proses berbeda. Analisis pareto merupakan salah satu langkah kritis dalam metode ini.



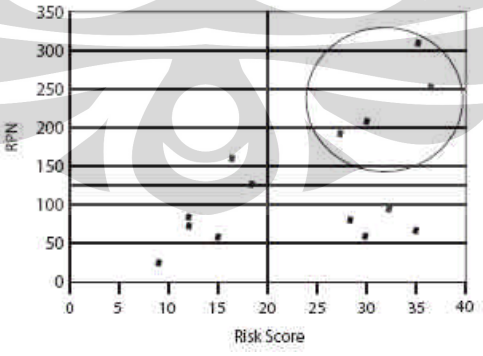
Gambar 2.12 Pareto RPN

4. Membuat pareto untuk *risk score* dan menentukan nilai kritis untuk risiko-risiko tersebut. Tidak ada metode ilmiah yang digunakan untuk memilih nilai kritis, dalam beberapa kasus nilai ini nyata namun dalam kasus lain memiliki distribusi dan kontinu yang membuat pilihan makin sulit. Catatan penting dalam langkah ini, bahwa hal ini merupakan langkah awal yang mudah. Nilai kritis menyediakan suatu aturan sederhana untuk memprioritaskan rencana respon risiko.



Gambar 2.13 Pareto *Risk Score*

5. Membuat diagram pencar (*scatter diagram*) untuk RPN dan *risk score*. Setelah nilai kritis diketahui untuk RPN dan *risk score* maka langkah selanjutnya adalah membuat diagram pencar (*scatter diagram*) untuk RPN dan *risk score*. Tidak ada ketentuan bahwa data akan memiliki pola khusus dalam persebarannya.



Gambar 2.14 Diagram Pencar RPN dan *Risk Score*

6. Menentukan perpotongan antara *risk score* dan nilai kritis dari RPN. Tujuan dari langkah keenam ini adalah untuk menentukan perpotongan dari 2 nilai kritis untuk menentukan keadaan inisial dari risiko yang membutuhkan rencana respon yang akan dihasilkan. Risiko yang memiliki *risk score* dan RPN di atas nilai kritis memiliki prioritas untuk rencana response. Ada risiko yang memiliki *risk score* yang tinggi tetapi karena dapat diantisipasi terlebih dahulu maka memiliki nilai deteksi yang kecil sehingga nilai RPN menjadi rendah. *Risk score* dan RPN harus selalu dievaluasi kembali karena kedua hal tersebut memiliki tujuan yang berbeda.
7. Mengembangkan rencana respon risiko untuk risiko kritis. Setelah mengidentifikasikan risiko kritis, dalam langkah ketujuh ini tim harus memikirkan mengenai strategi respon risiko seperti pencegahan, transfer, mengurangi dan menerima serta dokumentasi rencana respon.
8. Mengevaluasi kembali *risk score* dan RPN berdasarkan rencana respon. Langkah terakhir adalah menghitung kembali *risk score* dan nilai RPN berdasarkan kegiatan dalam rencana respon.

Keuntungan Metode RFMEA

Penggunaan RFMEA memiliki keuntungan secara nyata (*tangible*) dan tidak nyata (*intangible*). Keuntungan *tangible* dari RFMEA ini adalah mengurangi waktu perencanaan risiko. West (2002) menjelaskan bahwa pendekatan dengan menggunakan matrix untuk menangkap kejadian, probabilitas, akibat dan *risk score* membutuhkan waktu yang relatif lama dalam proses ini, namun dengan RFMEA maka tidak seluruh risiko perlu dikenali pada tahap awal. Hal ini disebabkan adanya metode deteksi dalam perhitungan RPN. Metode deteksi memberikan pengukuran untuk mempersiapkan waktu yang tepat dalam merespon risiko. RFMEA memberikan metode yang lebih baik dalam menentukan rencana risiko yang dapat ditunda dengan memberikan waktu untuk fokus pada risiko kritis. Nilai deteksi memberikan manfaat lain, dengan *risk score*, yaitu dengan memberikan proses belajar. Dengan proses belajar ini maka tim dapat menemukan ide inovatif yang lebih

banyak lagi untuk mengidentifikasi gejala dari risiko, dalam kasus lain dapat memberikan metode deteksi yang baru.

Selain keuntungan *tangible,* RFMEA juga memberikan keuntunga n *intangible* yaitu menurunkan tingkat stres dari tim. Dengan memberikan waktu yang lebih banyak dalam mendeteksi terhadap gejala risiko maka risiko akan dapat diidentifikasikan lebih awal sehingga tekanan terhadap tim dapat dikurangi. Selain hal tersebut manfaat lainnya adalah meningkatkan pembelajaran organisasi.

2.6 *Fault Tree Analysis* (FTA)

Teknik untuk mengidentifikasikan kegagalan *(failure)* dari suatu sistem dengan memakai FT *(fault tree)* diperkenalkan pertama kali pada tahun 1962 oleh *Bell Telephone Laboratories* dalam kaitannya dengan studi tentang evaluasi keselamatan sistem peluncuran *minuteman misile* antar benua. Boeing company memperbaiki teknik yang dipakai oleh Bell Telephone Laboratories dan memperkenalkan progam komputer untuk melakukan analisis dengan memanfaatkan FT baik secara kualitatif maupun secara kuantitatif.

FTA *(Fault Tree Analysis)* berorientasi pada fungsi (*function oriented*) atau yang lebih dikenal dengan pendekatan " *top down* "karena analisis ini berawal dari system level *(top)* dan meneruskannya ke bawah. Titik awal dari analisis ini adalah pengidentifikasikan mode kegagalan fungsional pada top level dari suatu sistem atau subsistem.

FTA adalah teknik yang banyak dipakai untuk studi yang berkaitan dengan risiko dan keandalan dari suatu system engineering. *Event* potensial yang menyebabkan kegagalan dari suatu sistem engineering dan probabilitas terjadinya event tersebut dapat ditentukan dengan FTA. Sebuah *TOP event* yang merupakan definisi dari kegagalan suatu sistem *(system failure),* harus ditentukan terlebih dahulu dalam mengkonstrusikan FTA. Sistem kemudian dianalisis untuk menemukan semua kemungkinan yang didefinisikan pada TOP event. FT adalah sebuah model grafis yang terdiri dari beberapa kombinasi kesalahan *(fault)* secara pararel dan secara berurutan yang mungkin menyebabkan awal dari *failure event* yang sudah ditetapkan.

Setelah mengidentifikasi TOP event, event-event yang memberi kontribusi secara langsung terjadinya top event diidentifikasi dan dihubungkan ke TOP event dengan memakai hubungan logika *(logical link).* Gerbang AND (AND gate) dan sampai dicapai event dasar yang independent dan seragam *(mutually independent basic event).* Analisis deduktif ini menunjukan analisis kualitatif dan kuantitatif dari sistem engineering yang dianalisis.

Sebuah *fault tree* mengilustrasikan keadaan dari komponen sistem *(basic event)* dan hubungan antara basic event dan TOP event. Simbol grafis yang dipakai untuk menyatakan hubungan disebut gerbang logika (logika gate). Output dari sebuah gerbang logika ditentukan oleh event yang masuk ke gerbang tersebut. Sebuah FTA secara umum dilakukan dalam 5 tahapan, yaitu :

? Mendefinisikan problem dan kondisi batas (*boundary condition*) dari sistem
? Pengkontruksian fault tree
? Mengidentifikasi minimal cut set atau minimal path set
? Analisis kualitatif dari fault tree
? Analisis kuantitatif fault tree

2.6.1 Definisi Masalah dan Kondisi Batas

Aktivitas pertama dari *fault tree analysis* terdiri dari dua step, yaitu :

? Mendefinisikan *critical event* yang akan dianalisis
? Mendefinisikan *boundary condition* untuk analisis

Critical event yang akan dianalisis secara normal disebut dengan *TOP event*. TOP event harus didefinisikan secara jelas dan tidak kabur (*unambiguous*). Diskripsi dari TOP event seharusnya selalu memberikan jawaban terhadap pertanyaan apa (*what*), dimana (*where*), dan kapan (*when*).

Agar analisis dapat dilakukan secara konsisten, adalah hal yang penting bahwa kondisi batas bagi analisis didefinisikan secara hati–hati. Dari kondisi batas, kita akan memilliki beberapa pemahaman sebagai berikut :

? *Batas fisik sistem.*

Bagian mana dari sistem yang akan dimasukkan dalam analisis dan bagian mana yang tidak ?

? *Kondisi awal.*

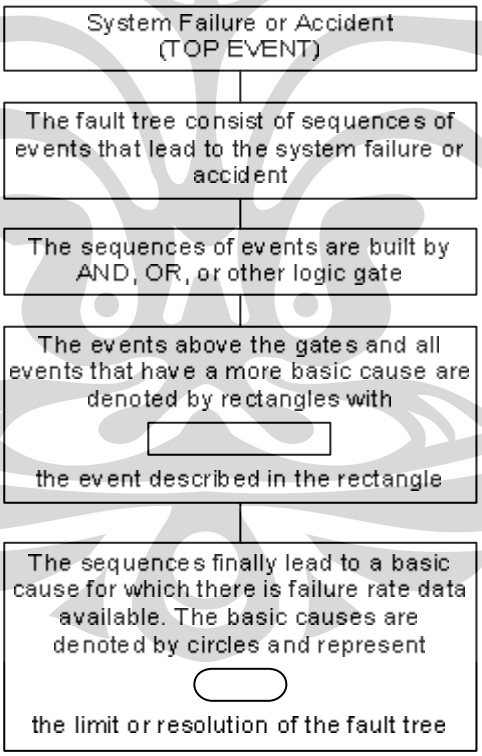
Kondisi pengoperasian sistem yang bagaimana pada saat TOP event terjadi ? Apakah sistem bekerja pada kapasitas yang penuh / sebagian ?

? *Kondisi batas yang berhubungan dengan stress eksternal.*

Apa tipe stress eksternal yang seharusnya disertakan dalam analisis?

? *Level dari resolusi.*

Seberapa detail kita akan mengidentifikasi berbagai alasan potential yang menyebabkan kegagalan ?



Gambar 2.15 Struktur Fundamental *Fault Tree*

2.6.2 Pengkonstruksian *Fault Tree*

Pengkonstruksian fault tree selalu bermula dari TOP event. Oleh karena itu, berbagai *fault event* yang secara langsung, penting, dan berbagai penyebab terjadinya TOP event harus secara teliti diidentifikasi. Berbagai penyebab ini dikoneksikan ke TOP event oleh sebuah gerbang logika. Penting kiranya bahwa penyebab level pertama di bawah TOP event harus disusun secara terstruktur. Level pertama ini sering disebut dengan *TOP structure* dari sebuah *fault tree*. *TOP structure* ini sering diambil dari kegagalan modul – modul utama sistem, atau fungsi utama dari sistem. Analisis dilanjutkan level demi level sampai semua *fault event* telah dikembangkan sampai pada resolusi yang ditentukan. Analisis ini merupakan analisis deduktif dan dilakukan dengan mengulang pertanyaan "Apa alasan terjadinya event ini ?". Gambar 2.15 menunjukkan struktur fundamental dari sebuah *fault tree*, sedangkan tabel 2.6 menunjukkan berbagai simbol yang dipakai untuk mengkostruksi sebuah *fault tree*.

Ada beberapa aturan yang harus dipenuhi dalam mengkonstruksi sebuah fault tree. Berikut ini beberapa aturan yang dipakai untuk mengkonstruksi sebuah fault tree.

1. Deskripsikan *fault event*

   Masing – masing basic event harus didefiniskan secara teliti (apa, dimana, kapan) dalam sebuah kotak.

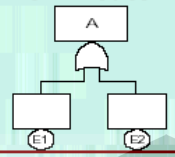
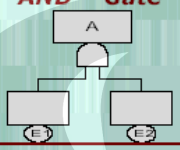
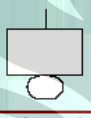
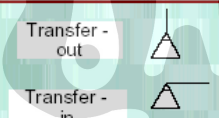
2 Evaluasi *fault event*

   Kegagalan komponen dikelompokkan dalam tiga kelompok yaitu, *primary failures*, *secondary failures,* dan *command faults.*

3. Lengkapi semua gerbang logika

   Semua input ke gate tertentu harus didefinisikan dengan lengkap dan dideskripsikan sebelum memproses *gate* lainnya. Fault tree harus diselesaikan pada masing – masing level sebelum memulai level berikutnya.

Tabel 2.6 Simbol *Fault Tree*

NAMA	SIMBOL	DISKRIPSI
Logic gates	**OR – Gate** 	*OR-Gate* menunjukkan output dari event A terjadi jika sembarang input *event* Ei terjadi.
	AND – Gate 	*AND – Gate* menunjukkan output dari *event* A akan terjadi jika semua input event Ei terjadi secara serentak.
Input events	**Basic event** 	Basic event menyatakan kegagalan sebuah basic equipment yang tidak memerlukan penelitian lebih lanjut dari penyebab kegagalan
	Undeveloped event 	*Undeveloped event* menyatakan sebuah event yang tidak diteliti lebih lanjut karena tidak tersedianya/cukupnya informasi atau karena konsekuensi dari event ini tidak terlalu penting
Description of state	**Comment rectangle** 	*Comment rectangle* dimanfaatkan untuk informasi tambahan
Transfer symbols		Simbol transfer-out menunjukkan bahwa fault tree dikembangkan lebih jauh dan berkaitan dengan simbol transfer-in

Sebuah normal basic event di dalam sebuah fault tree merupakan sebuah *primary failures* yang menunjukkan bahwa komponen merupakan penyebab dari kegagalan. *Secondary failures* dan *command faults* merupakan *intermediate event* yang membutuhkan investigasi lebih mendalam untuk mengidentifikasi alasan utama. Pada saat mengevaluasi sebuah fault event, seorang analis akan bertanya, "Dapatkah *fault* ini dikategorikan dalam *primary failure*?" Jika jawabannya adalah YA, maka analis tersebut dapat mengkalsifikasikan fault event sebagai *normal basic event*. Jika jawabannya adalah TIDAK, maka analis tersebut dapat mengklasifikasikan *fault event* sebagai *intermediate event*, yang harus didevelop lebih jauh, atau sebagai *secondary basic event. Secondary basic event* sering

disebut dengan *undeveloped event* dan menunjukkan sebuah fault event yang tidak dikaji lebih jauh karena informasinya tidak tersedia atau karena dampak yang ditimbulkan tidak signifikan.

2.6.3 Pengidentifikasian Minimal Cut Set

Sebuah fault tree memberikan informasi yang berharga tentang berbagai kombinasi dari fault event yang mengarah pada *critical failure system*. Kombinasi dari berbagai fault event disebut dengan *cut set*. Pada terminologi fault tree, sebuah cut set didefiniskan sebagai basic event yang bila terjadi (secara simultan) akan mengakibatkan terjadinya *TOP event.* Sebuah *cut set* dikatakan sebagai *minimal cut set* jika cut set tersebut tidak dapat direduksi tanpa menghilangkan statusnya sebagai cut set.

Jumlah *basic event* yang berbeda di dalam sebuah *minimal cut set* disebut dengan orde cut set. Untuk fault tree yang sederhana adalah mungkin untuk mendapatkan minimal cut set dengan tanpa menggunakan prosedur formal / algoritma. Untuk fault tree yang lebih besar, maka diperlukan sebuah algoritma untuk mendapatkan minimal cut set pada fault tree. MOCUS (*method for obtaining cut sets*) merupakan sebuah algoritma yang dapat dipakai untuk mendapatkan minimal cut set dalam sebuah fault tree. Algoritma ini akan dijelaskan dengan menggunakan contoh.

2.6.4 Evaluasi Kualitatif *Fault Tree*

Evaluasi kualitatif dari sebuah fault tree dapat dilakukan berdasarkan minimal cut set. Kekritisan dari sebuah cut set jelas tergantung pad jumlah *basic event* di dalam cut set (orde dari cutset). Sebuah cut set dengan orde satu umumnya lebih kritis daripada sebuah cut set dengan orde dua atau lebih. Jika sebuah fault tree memiliki cut set dengan orde satu, maka TOP event akan terjadi sesaat setelah basic event yang bersangkutan terjadi. Jika sebuah cut set memiliki dua basic event, kedua event ini harus terjadi secara serentak agar TOP event dapat terjadi.

Faktor lain yang penting adalah jenis basic event dari sebuah minimal cut set. Kekritisan dari berbagai cut set dapat dirangking berdasarkan dari basic event berikut ini :

? *Human error*

? Kegagalan komponen / peralatan yang aktif (*active equipment failure*)

? Kegagalan komponen / peralatan yang pasif (*passive equipment failure*)

Peringkat ini disusun berdasarkan asumsi bahwa human error lebih sering terjadi dari pada komponen / peralatan yang aktif dan komponen / peralatan yang aktif lebih rentan terhadapa kegagalan bila dibandingkan komponen / peralatan yang pasif.

2.7 Model Optimasi menggunakan Simulasi *Optquest - Crystal Ball*

Simulasi adalah sebuah metode analitis yang bertujuan untuk mendapatkan suatu bentuk representasi sebuah sistem. Tujuan utama dari pembuatan model simulasi adalah untuk memudahkan pelaksanaan eksperimen, terutama jika manipulasi-manipulasi sistem pada kondisi nyata memerlukan biaya yang besar atau ada kendala-kendala lain yang sulit untuk direalisasikan.

Simulasi Monte Carlo dinamai dari nama suatu tempat kasino yaitu Monte Carlo - Monaco yang merujuk *games of chance* seperti *roulette*, *dice*, dan *slot machines*[21]. Monte Carlo digunakan oleh sistem yang menunjukkan kemungkinan pada perilakunya, misalnya antrian. Simulasi ini berdasarkan atas penggunaan bilangan acak (random number), dan digunakan untuk mengestimasi distribusi hasil yang bergantung pada input probabilistik (misalnya keuntungan bisnis, durasi proyek, rencana pensiun, dll.). Simulasi Monte Carlo saat ini digunakan secara luas untuk memecahkan masalah-masalah tertentu pada statistik yang tidak dapat ditelusuri secara analitik. Sebagai contoh, metode ini telah diterapkan untuk estimasi nilai kritis derajat tes hipotesis.

Salah satu software yang memiliki fitur simulasi Monte Carlo adalah *Crystal Ball. Crystal Ball* adalah *analytical tool* yang membantu para eksekutif,

[21] *Crystal Ball® 7.2.2 User Manual*

menganalisis, dan membuat keputusan lainnya melalui simulasi pada model spreadsheet. *Forecast* yang dihasilkan dari simulasi ini membantu mengkuantifikasi risiko yang dapat membantu pembuat keputusan untuk mendapatkan informasi sebanyak mungkin. Software ini mampu menggambarkan daerah dari nilai yang mungkin untuk setiap sel yang berisi ketidakpastian dalam *spreadsheet* juga dapat memperlihatkan hasil berupa diagram yang menggambarkan semua kejadian yang mungkin beserta frekuensinya masing-masing. Proses dasar penggunaan *Crystal Ball* adalah :

1. Membangun model *spreadsheet* yang menggambarkan kondisi tidak pasti
2. Menjalankan simulasi
3. Menganalisis hasil simulasi

Salah satu fungsi penting yang terdapat dalam *Crystal Ball* adalah fungsi optimasi, yaitu *OptQuest*. Dalam hal ini, sebuah model optimasi dapat dianalisis sehingga dapat memberikan solusi dan keputusan yang terbaik. Masalah optimasi dalam *OptQuest* dapat diselesaikan dengan mengevaluasi model, menganalisis, dan mengintegrasikannya dengan simulasi sebelumnya yang telah dihitung dalam *Crystal Ball*.

Sebagai *add-in* dalam *Crystal Ball*, *OptQuest* meningkatkan model simulasi dengan mencari dan menemukan solusi optimal secara otomatis. *OptQuest* juga dapat digunakan untuk analisis portafolio untuk menentukan strategi investasi yang mengoptimalkan keuntungan dengan mempertimbangkan ketidakpastian tingkat pengembalian tahunan setiap aset.

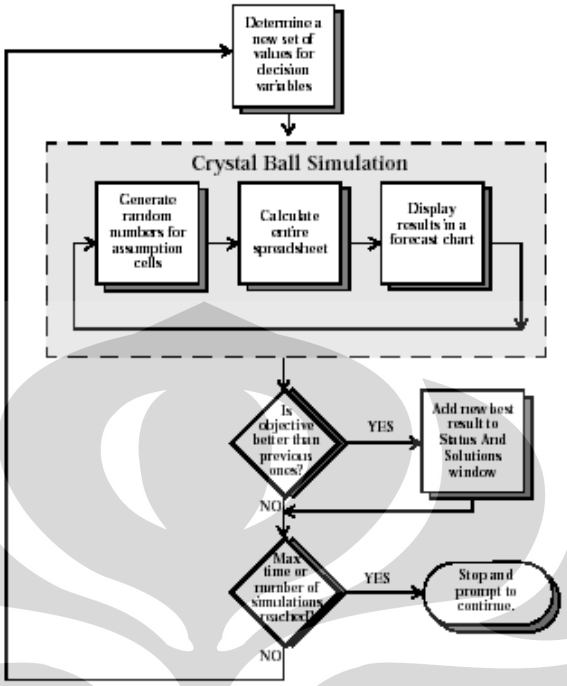
Model optimasi *OptQuest* memiliki tiga eleven utama, yaitu variabel keputusan, batasan, dan tujuan. Variabel keputusan adalah variabel yang dapat dikontrol, seperti jumlah produk yang akan diproduksi, besarnya investasi yang akan dilakukan, dan lain-lain. Batasan adalah nilai yang menjadi batasan atas hubungan beberapa variabel keputusan, seperti jumlah total investasi yang akan diberikan ke beberapa proyek. Tujuan adalah gambaran tujuan dari model secara matematis, misalnya memaksimalkan laba atau meminimalkan biaya.

Selain ketiga elemen di atas, model optimasi yang bersifat probabilitas umumnya mempunyai beberapa elemen lain, yaitu :

1. asumsi, menggambarkan ketidakpastian dari model data yang digunakan, dengan menggunakan distribusi probabilitas
2. peramalan, yaitu sejumlah distribusi frekuensi atas hasil yang mungkin dari sebuah model
3. statistik peramalan, yakni kumpulan dari nilai distribusi peramalan, seperti nilai rata-rata dan standar deviasi
4. kebutuhan, yaitu batasan tambahan untuk statistik peramalan

Proses optimasi dalam *OptQuest* dapat dilihat pada Gambar 2.17. Pada tingkat dasar, *OptQuest* memilih sebuah nilai untuk setiap variabel keputusan, memasukkan nilai tersebut ke dalam *spreadsheet*, menjalankan simulasi Monte Carlo, merekam hasil, kemudian mengulangi proses tersebut. Sebenarnya *user* dapat melakukan proses optimasi ini secara manual, namun seiring dengan bertambahnya jumlah variabel keputusan, jumlah kemungkinan kombinasi probabilitas menjadi semakin tidak terkendali.

Pada tingkat lanjut, *OptQuest* melakukan tugas yang lebih baik dalam menemukan solusi optimal dibandingkan dengan perhitungan secara manual. *OptQuest* melebihi keterbatasan optimasi pada algoritma genetik karena menggunakan metodologi pencarian yang lebih banyak dan lebih lengkap, termasuk *tabu search* dan *scatter search*, untuk membantu menemukan solusi global yang terbaik.



Gambar 2.16 Proses Optimasi dalam *OptQuest*

(Sumber : *OptQuest User Manual*)

OptQuest juga memeriksa kesesuaian hasil denga n kendala dan kebutuhan yang ada sambil mencari solusi yang optimal. Sebagai tambahan, *OptQuest* menerapkan teknologi jaringan kerja yang adaptif untuk membantu mempelajari hasil optimasi sebelumnya sehingga dapat mencapai hasil yang lebih baik dalam waktu yang lebih singkat.

Pada dasarnya, tidak setiap masalah memerlukan optimasi. Untuk beberapa pertanyaan, simulasi sendiri dapat memberikan pengetahuan dan solusi yang berguna. Namun, ketika bertujuan untuk memperoleh keputusan yang lebih baik dan peramalan yang optimal, kombinasi *Crystal Ball* dan *OptQuest* dapat membantu tujuan tersebut melalui kecepatan dan keakuratan.

BAB III
PENGUMPULAN DAN PENGOLAHAN DATA

3.1 Pengumpulan Data

3.1.1 Data Kegagalan pada *Core Network* Perangkat GPRS

Pada penelitian ini dilakukan pengumpulan data kegagalan pada *Core Network* perangkat GPRS yang diambil dari data histroris perusahaan. Pengumpulan data ini merupakan langkah awal dalam tahap identifikasi risiko. Berikut adalah data kegagalan yang pernah terjadi di perusahaan.

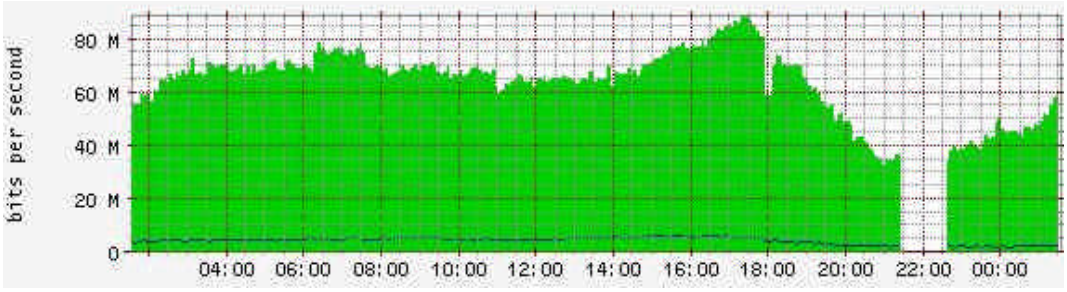
- SGSN hardware problem : adanya masalah/kerusakan pada hardware SGSN
- HLR hardware problem : adanya masalah/kerusakan pada hardware HLR
- SGSN software problem : adanya masalah pada software SGSN yang umumnya karena adanya sistem bugs
- SS7 signaling link down : koneksi link antara SGSN ke HLR down
- BSS link failure : koneksi link antara SGSN ke BSC terputus
- SS7 routing error : SS7 signaling link misconfiguration atau hang
- GGSN hardware problem : adanya masalah/kerusakan pada hardware GGSN
- Radius hardware problem : adanya masalah/kerusakan pada hardware Radius
- GGSN software problem : terjadi kesalahan konfigurasi pada sistem konfigurasi dalam GGSN, atau adanya sistem Bugs dalam software GGSN sehingga software release perlu di-update
- Radius software problem : service software radius tidak berjalan dengan semestinya, hal ini bisa dikarenakan adanya bugs, over capacity atau misconfiguration
- GGSN – Radius link failure : koneksi link antara GGSN dan radius terputus
- High ISRAU failure : adanya kegagalan sinyal sewaktu user berpindah dari satu area SGSN ke area SGSN yang lain
- Not enough address allocation on GGSN : kehabisan IP address untuk diberikan kepada user

- EMM problem : terjadi paling sering akibat EMM software hang dikarenakan over capacity sehingga akan menimbulkan masalah pada sistem *real time charging* untuk pelanggan *prepaid*
- SACC problem : adanya kesalahan konfigurasi pada SACC
- DNS hardware problem : adanya masalah/kerusakan pada hardware DNS
- DNS software problem : adanya kesalahan konfigurasi ataupun sistem bugs dalam software problem
- GN link failure : koneksi link antara antara SGSN dan GGSN terputus
- GI link problem : koneksi link antara GGSN dan internet terputus
- Free charging Mentari GPRS : pemakaian GPRS oleh pelanggan kartu Mentari yang bebas tagihan karena adanya *fraud* dalam system charging
- Fraud free internet access via handset : pelanggan dapat melakukan akses internet secara bebas dari handset-nya tanpa ada penagihan karena adanya sistem fraud
- SNMP problem : sistem monitoring tidak dapat memantau perangkat GGSN karena protocol SNMP terputus

3.1.2 Data Kehilangan Pendapatan (*Loss Revenue*)

Pada penelitian ini akan dibuat pula skenario alokasi biaya penanganan risiko untuk risiko kritis yang diperoleh dari hasil pengolahan data menggunakan metode FMEA. Untuk menunjang hal tersebut maka diperlukan adanya data kehilangan pendapatan (*loss* revenue). Data *loss revenue* diperoleh dari data historis perusahaan dan *expert judgment.*

Data *loss revenue* akibat munculnya masalah di perangkat GGSN dapat diambil dari grafik utilisasi jaringan di perangkat tersebut. Grafik dapat dilihat dari server SNMP seperti terlihat pada gambar 3.1.



Gambar 3.1 Utilisasi Traffic Jaringan di Perangkat GGSN

Tabel 3.1 Rekapitulasi *Loss Revenue* di Perangkat GGSN

Bulan	Tahun 2008		Tahun 2007		Tahun 2006	
	GGSN (*duration based*)	GGSN (*volume based*)	GGSN (*duration based*)	GGSN (*volume based*)	GGSN (*duration based*)	GGSN (*volume based*)
Januari	Rp306,600,000	Rp246,000,000	Rp243,720,000	Rp195,060,000	Rp200,100,000	Rp205,500,000
Februari	Rp212,160,000	Rp198,000,000	Rp312,300,000	Rp231,360,000	Rp242,160,000	Rp154,440,000
Maret	Rp252,300,000	Rp211,200,000	Rp253,200,000	Rp198,660,000	Rp476,820,000	Rp254,700,000
April	Rp263,520,000	Rp331,800,000	Rp411,060,000	Rp165,600,000	Rp444,600,000	Rp213,600,000
Mei	Rp345,720,000	Rp181,500,000	Rp224,880,000	Rp182,760,000	Rp265,500,000	Rp202,500,000
Juni	Rp486,720,000	Rp172,200,000	Rp378,900,000	Rp212,100,000	Rp453,900,000	Rp244,800,000
Juli	Rp292,800,000	Rp224,400,000	Rp321,360,000	Rp155,460,000	Rp246,960,000	Rp129,600,000
Agustus	Rp306,000,000	Rp156,900,000	Rp254,400,000	Rp264,000,000	Rp395,040,000	Rp242,700,000
September	Rp397,680,000	Rp243,900,000	Rp439,800,000	Rp234,000,000	Rp392,700,000	Rp273,300,000
Oktober	Rp340,860,000	Rp246,300,000	Rp343,680,000	Rp192,600,000	Rp397,620,000	Rp231,360,000
November	Rp473,820,000	Rp160,800,000	Rp405,600,000	Rp209,100,000	Rp450,600,000	Rp204,000,000
Desember			Rp381,600,000	Rp239,100,000	Rp464,100,000	Rp311,160,000

Dari hasil rekapitulasi pada tabel 3.1 di atas ditentukan nilai mean dan standar deviasi sebagai berikut :

- GGSN (volume based)
  - Mean : Rp 345.108.000
  - Standar deviasi : 87460770
- GGSN (duration based)
  - Mean : Rp 214.870.286
  - Standar deviasi : 43856839

Untuk *loss revenue* saat perangkat SGSN down, tidak terdapat sistem monitoring otomatis untuk melihat utilisasi jaringan, sehingga data *loss revenue* per bulan diperoleh dari *expert judgment* yaitu maksimum Rp 360.000.000 dan minimum Rp 12.000.000.

3.2 Pengolahan Data

3.2.1 Pengolahan Data Menggunakan *Failure Mode and Effect Analysis* (FMEA)

Pengolahan data menggunakan metode FMEA bertujuan untuk mendapatkan risiko kritis yang merupakan risiko-risiko yang akan dianalisis lebih lanjut. Risiko kritis tersebut diperoleh setelah dilakukan perhitungan *Risk Priority Number* (RPN) untuk setiap risiko yang telah teridentifikasi. Berikut adalah langkah penentuan risiko kritis menggunakan metode FMEA.

3.2.1.1 Identifikasi Risiko

Identifikasi risiko merupakan tahap terpenting dan sangat menentukan dalam manajemen risiko sebelum dilanjutkan ke tahap berikutnya. Identifikasi risiko melibatkan penentuan risiko yang mungkin mempengaruhi kinerja perangkat GPRS. Tujuan tahapan ini adalah untuk mengenali risiko yang mungkin terjadi lebih awal sehingga dapat mengurangi atau mengeliminir keterkejutan akibat risiko tersebut. Selain itu, identifikasi risiko dilakukan untuk mengidentifikasi risiko-risiko apa saja yang perlu diatur.

Dalam proses identifikasi ini digunakan metode *Brainstorming* dan ditunjang pula oleh sumber objektif yaitu data kegagalan (*historical problem*) periode Januari – Oktober 2008 yang berkaitan dengan perangkat GPRS dan literatur (Information Risk Management. GPRS/3G Services : Security. An O2 White Paper). *Brainstorming* pada proses identifikasi risiko ini dilakukan dengan para *expert* yaitu General Manager Network Service O&M Center, VAS Celullar Team Leader, dan VAS Cellular Engineer yang memiliki pengalaman kerja lebih dari 5 tahun.

Semua item kegagalan dan potensi kegagalan yang diperoleh dari hasil *brainstorming* para *expert*, *historical problem,* dan *literatur,* disusun dalam suatu diagram *Cause Failure Mode Effect* (CFME) yang dapat dilihat pada gambar 3.2. Metode ini digunakan sebelum pembuatan *Failure Mode and Effect Analysis* (FMEA). Hasil CFME akan mempermudah pembuatan FMEA dalam hal pengidentifikasian efek, modus kegagalan, dan akar penyebab permasalahan. Tabel hasil FMEA dapat dilihat pada tabel 3.2

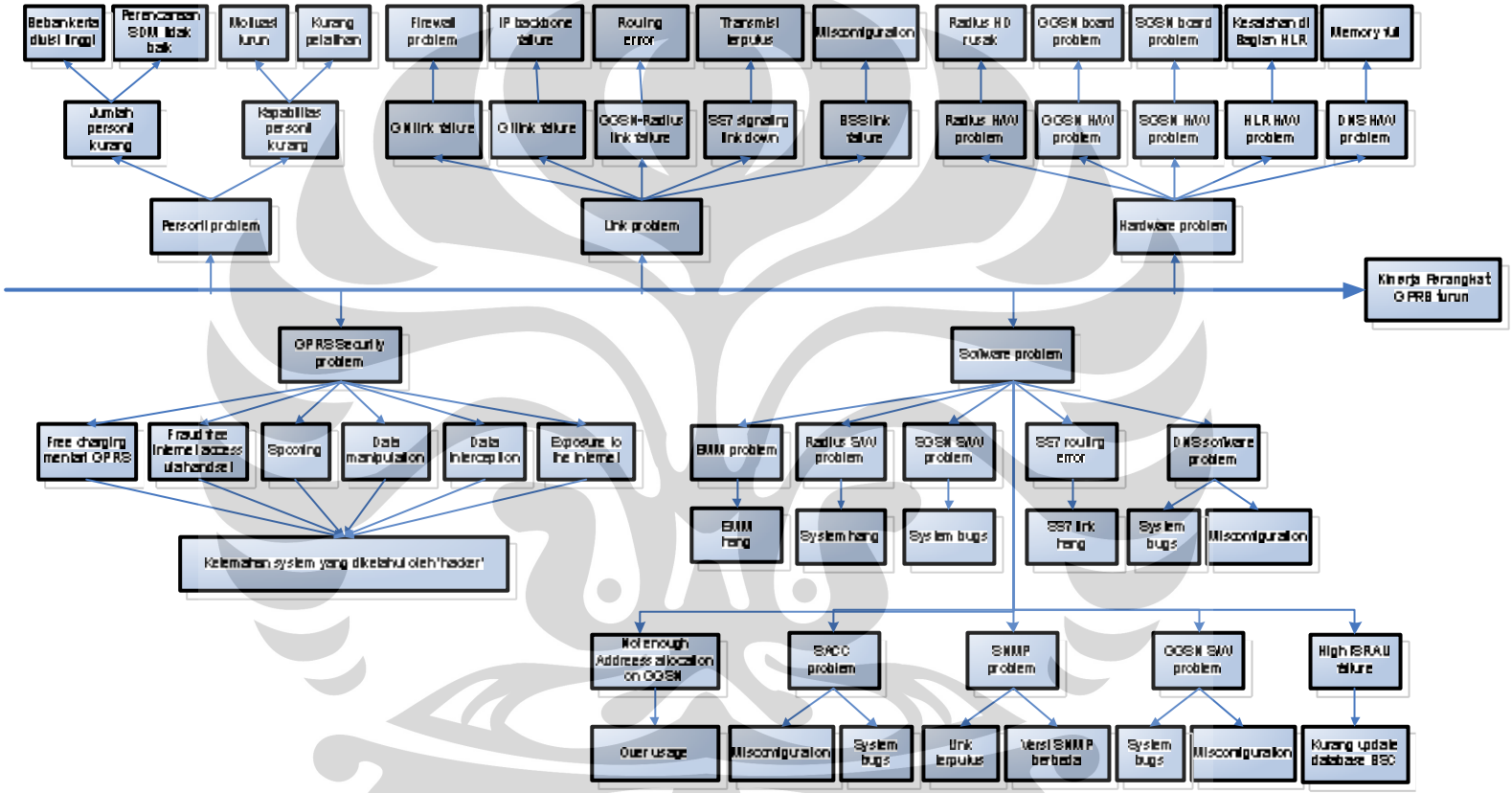
Berdasarkan hasil *brainstorming,* maka secara garis besar penulis membagi risiko yang ada menjadi 3 kategori yaitu :

- GPRS Attach Success Rate

  Merupakan risiko yang dapat menyebabkan penurunan GPRS attach success rate yang akan menurunkan kinerja perangkat GPRS. Efek dari masalah yang timbul adalah customer tidak mendapatkan sinyal GPRS.
- PDP Context Success Rate

  Merupakan risiko yang dapat menyebabkan penurunan PDP context success rate yang akan menurunkan kinerja perangkat GPRS. Efek dari masalah yang timbul adalah customer tidak dapat *connect* internet.
- System Fraud

  Merupakan masalah-masalah yang dapat menyebabkan kekacauan dalam sistem (*system fraud*) yang umumnya berhubungan dengan *GPRS security* sehingga perusahaan akan mengalami kerugian finansial karena bermasalah dalam hal *charging*.



Gambar 3.2 Diagram *Cause Failure Mode Effect* (CFME)

Tabel 3.2 Daftar Risiko, Kemungkinan Penyebab, dan Kemungkinan Efeknya

Kelompok Risiko	Risiko	Kemungkinan Penyebab Risiko	Kemungkinan Efek yang Terjadi
GPRS Attach Success Rate	SGSN Hardware Problem	System bugs	Hardware problem
	HLR Hardware Problem	Kesalahan di bagian HLR	Hardware problem
	SGSN Software Problem	System bugs	Software problem
	SS7 signaling link down	Transmisi terputus	Link problem
	BSS link failure	Misconfiguration	Link problem
	SS7 routing error	SS7 link hang	Software problem
PDP Context Success Rate	GGSN Hardware Problem	GGSN board rusak	Hardware problem
	Radius hardware problem	Radius hard disk rusak	Hardware problem
	GGSN Software problem	Misconfiguration	Software problem
		System bugs	
	Radius sofware problem	System hang	Software problem
	GGSN-radius link failure	Routing error	Link problem
	High ISRAU failure	Kurang update database BSC antar SGSN	Software problem
	Not enough address allocation on GGSN	Over usage	Software problem
	EMM problem	EMM hang	Software problem
	SACC problem	Misconfiguration	Software problem
		System bugs	
	DNS hardware problem	Memory full	Hardware problem
	DNS software problem	System bugs	Software problem
		Misconfiguration	
	GN link failure	IP backbone problem	Link problem
	GI link problem	Firewall problem	Link problem
System Fraud	Free charging mentari GPRS	Kelemahan system yang diketahui oleh *hacker*	GPRS Security problem
	Fraud free internet access via handset	Kelemahan system yang diketahui oleh *hacker*	GPRS Security problem
	Spoofing	Kelemahan system yang diketahui oleh *hacker*	GPRS Security problem
	Data manipulation	Kelemahan system yang diketahui oleh *hacker*	GPRS Security problem
	Data interception/unauthorized access to confidential data	Kelemahan system yang diketahui oleh *hacker*	GPRS Security problem
	Exposure to the internet	Kelemahan system yang diketahui oleh *hacker*	GPRS Security problem
Else	SNMP problem	Link terputus	Software problem
		Versi SNMP berbeda	
	Jumlah personil kurang	Perencanaan SDM tidak baik	Personil problem (operator overload)
		Beban kerja divisi tinggi	
	Kapabilitas personil kurang	Kurang pelatihan	Personil Problem (kinerja turun)
		Motivasi turun	

3.2.1.2 Penentuan Rating *Occurrence, Severity,* dan *Detection*

Dalam langkah pengerjaan FMEA, setelah diperoleh item risiko maka langkah berikutnya adalah penentuan rating probabilitas terjadinya risiko (*occurrence*), dampak akibat risiko (*severity*), dan deteksi risiko (*detection*). Penentuan ketiga rating tersebut akan sangat menentukan proses memprioritaskan daftar risiko / penentuan risiko kritis.

Penentuan rating ditentukan melalui proses *brainstorming* dengan para *expert* yang disesuaikan dengan kondisi perusahaan. Rating dari *occurrence* merupakan kuantifikasi dari kemungkinan terjadinya risiko. Skala yang digunakan mulai dari rentang 1 – 5, yang mana skala 1 menyatakan probabilitas sangat rendah dan skala 5 menyatakan probabilitas terjadinya sangat tinggi, tabel dapat dilihat pada tabel 3.3.

Rating dari *severity* adalah kuantifikasi dari tingkat dampak akibat terjadinya risiko. Skala yang digunakan mulai dari rentang 1 - 5, yang mana skala 1 menyatakan bahwa risiko tidak memberikan efek terhadap sistem maupun servis dan skala 5 menyatakan bahwa terjadinya risiko akan memberikan dampak berupa gangguan terhadap sistem secara keseluruhan, tabel dapat dilihat pada tabel 3.4.

Adapun rating dari *detection* adalah kuantifikasi dari kontrol atau prosedur atau strategi yang ada yang mengatur fungsi atau yang membuat suatu kegagalan dapat dideteksi. Fungsi deteksi disini adalah untuk melihat apakah risiko yang ada dapat diketahui sebelum terjadinya kegagalan dan juga apakah kontrol yang dimiliki dapat mengurangi risiko kegagalan yang dapat terjadi. Skala yang digunakan mulai dari rentang 1 - 5, yang mana semakin tinggi skala maka semakin rendah tingkat kontrol yang dimiliki untuk mendeteksi terjadinya kegagalan. Tabel dapat dilihat pada tabel 3.5.

Tabel 3.3 Rating Probabilitas Terjadinya Risiko (*Occurrence*)

Skala	Probabilitas Risiko	Keterangan
5	Sangat tinggi : tidak dapat dielakkan	Probabilitas terjadinya risiko per thn : 81 - 100
4	Tinggi : kejadian yang berulang	Probabilitas terjadinya risiko per thn : 61 - 80
3	Moderate	Probabilitas terjadinya risiko per thn : 41 - 60
2	Rendah : jarang terjadi	Probabilitas terjadinya risiko per thn : 21 - 40
1	Sangat rendah : sangat jarang terjadi	Probabilitas terjadinya risiko per thn : 0 - 20

Tabel 3.4 Rating Dampak Akibat Terjadinya Risiko (*Severity*)

Skala	Dampak Risiko	Keterangan
5	Emergency	Gangguan sistem secara keseluruhan, menyebabkan kehilangan data charging
4	Critical	Seringkali menyebabkan sistem error, gangguan tersebut berpengaruh terhadap sistem manajemen revenue
3	Major	Gangguan berpengaruh terhadap area kerja tertentu namun tidak terhadap sistem secara keseluruhan
2	Minor	Memiliki efek minor terhadap fungsi produk, namun tidak berpengaruh terhadap traffic jaringan dan servis
1	Warning	Tidak memberikan efek terhadap sistem maupun servis

Tabel 3.5 Rating Deteksi Risiko

Skala	Keterangan	Keterangan
5	Sangat rendah	Tidak ada metode dalam pendeteksian risiko atau tidak ada *alert*
4	Rendah	Metode belum andal/keefektifan metode belum diketahui untuk dapat mendeteksi tepat pada waktunya
3	Cukup	Metode memiliki efektivitas yang sedang sehingga masih memerlukan cukup waktu untuk dapat mendeteksi
2	Tinggi	Metode deteksi cukup efektif sehingga dapat mendeteksi dalam waktu tertentu yang relatif cukup singkat
1	Sangat tinggi	Metode deteksi sangat efektif sehingga risiko pasti terdeteksi dalam waktu singkat

3.2.1.3 Penentuan Nilai *Occurence, Severity, Detection* dan Perhitungan *Risk Priority Number* (RPN)

Risiko yang telah teridentifikasi selanjutnya ditentukan nilai *occurrence*, *severity*, dan *detection*. Penentuan nilai tersebut menggunakan kuesioner yang pengisiannya dilakukan melalui *brainstorming* para *expert* dan melibatkan penulis sebagai pemandu pengisian kuesioner. Nilai *occurrence, severity*, dan *detection* untuk tiap risiko dapat dilihat pada tabel 3.6.

Perhitungan RPN merupakan bagian penting dalam FMEA karena dari nilai RPN akan diketahui prioritas risiko yang termasuk risiko kritis. RPN dihitung menggunakan persamaan berikut :

RPN = *Occurrence* * *Severity* * *Detection*

Tabel 3.6 Nilai *Occurrence, Severity, Detection,* dan RPN untuk tiap Risiko

Risk ID	Daftar risiko pada c*ore network* perangkat GPRS	*Occurrence*	*Severity*	*Detection*	RPN
1	SGSN Hardware Problem	1	4	3	12
2	HLR Hardware Problem	1	4	3	12
3	SGSN Software Problem	1	3	3	9
4	SS7 signaling link down	3	4	3	36
5	BSS link failure	3	3	3	27
6	SS7 routing error	3	3	4	36
7	GGSN Hardware Problem	1	4	4	16
8	Radius hardware problem	1	4	5	20
9	GGSN Software problem	3	4	4	48
10	Radius sofware problem	2	4	5	40
11	GGSN-radius link failure	4	5	5	100
12	High ISRAU failure	2	3	4	24
13	Not enough address allocation on GGSN	2	3	3	18
14	EMM problem	5	5	5	125
15	SACC problem	1	4	5	20
16	DNS hardware problem	2	4	3	24
17	DNS software problem	4	4	5	80
18	GN link failure	1	4	4	16
19	GI link problem	4	4	4	64
20	Free charging mentari GPRS	1	5	5	25

Risk ID	Daftar risiko pada c*ore network* perangkat GPRS	*Occurrence*	*Severity*	*Detection*	RPN
21	Fraud free internet access via handset	1	5	5	25
22	Spoofing	1	5	5	25
23	Data manipulation	1	5	5	25
24	Data interception/unauthorized access to confidential data	1	5	5	25
25	Exposure to the internet	1	5	5	25
26	SNMP problem	2	1	2	4
27	Jumlah personil kurang	2	3	5	30
28	Kapabilitas personil kurang	2	3	5	30

Dari risiko yang telah terdaftar dan diketahui nilai RPN masing-masing, selanjutnya ditentukan risiko kritis. Risiko kritis tersebut yang akan dianalisis lebih lanjut sebagai langkah awal dari tindakan penanganan risiko untuk mempertahankan kinerja perangkat GPRS. Suatu risiko dikategorikan sebagai risiko kritis jika memiliki nilai RPN di atas nilai kritis. Nilai kritis RPN ditentukan dari rata-rata nilai RPN dari seluruh risiko.

$$Nilai\ Kritis\ RPN = \frac{Total\ RPN}{Jumlah\ Risiko} = \frac{986}{31} = 31{,}81$$

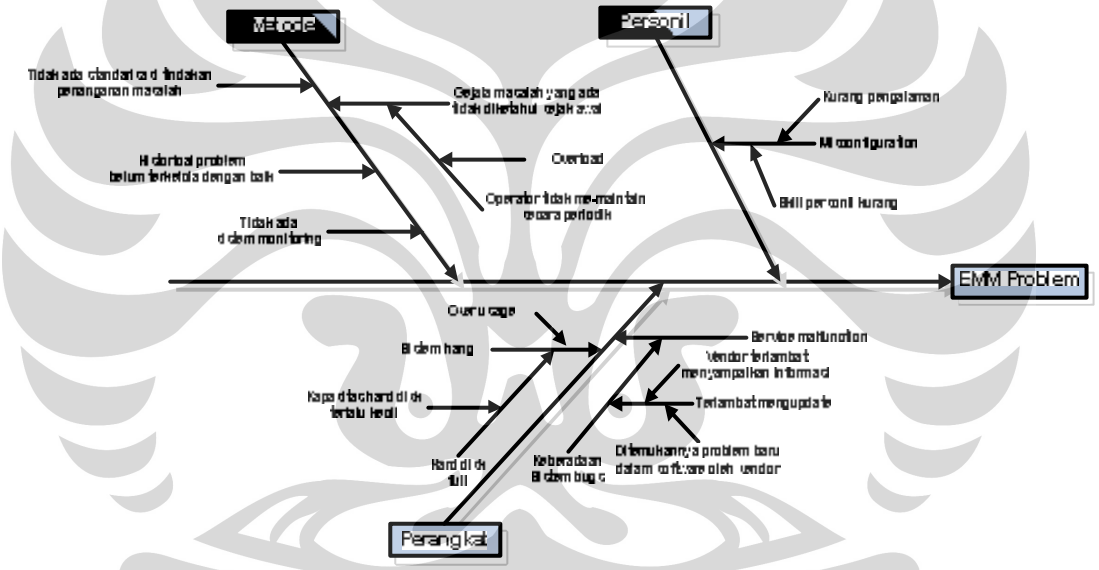
Berdasarkan nilai kritis RPN dan atas persetujuan tim *expert* (kebutuhan perusahaan) maka diperoleh 8 risiko kritis. Nilai RPN dari kedelapan risiko tersebut berada di atas 31,81 yang merupakan nilai kritis RPN.

Tabel 3.7 Risiko Kritis

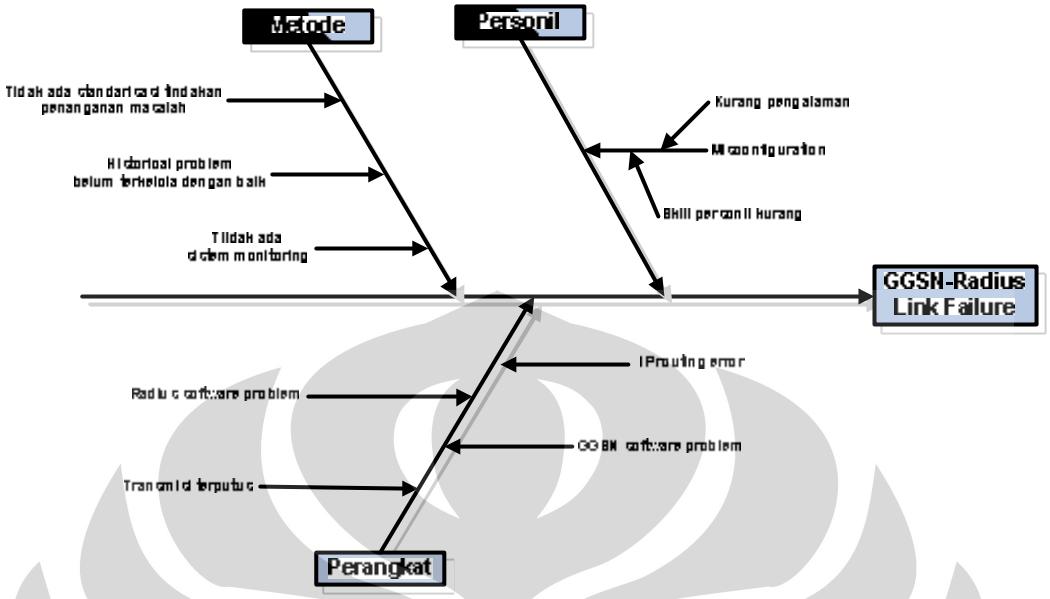
Risk ID	Daftar risiko kegagalan pada *core network* perangkat GPRS	*Occurrence*	*Severity*	*Detection*	RPN
14	EMM problem	5	5	5	125
11	GGSN-radius link failure	4	5	5	100
17	DNS software problem	4	4	5	80
19	GI link problem	4	4	4	64
9	GGSN Software problem	3	4	4	48
10	Radius sofware problem	2	4	5	40
4	SS7 signaling link down	3	4	3	36
6	SS7 routing error	3	3	4	36

3.2.2 *Fishbone Diagram* dari Risiko Kritis

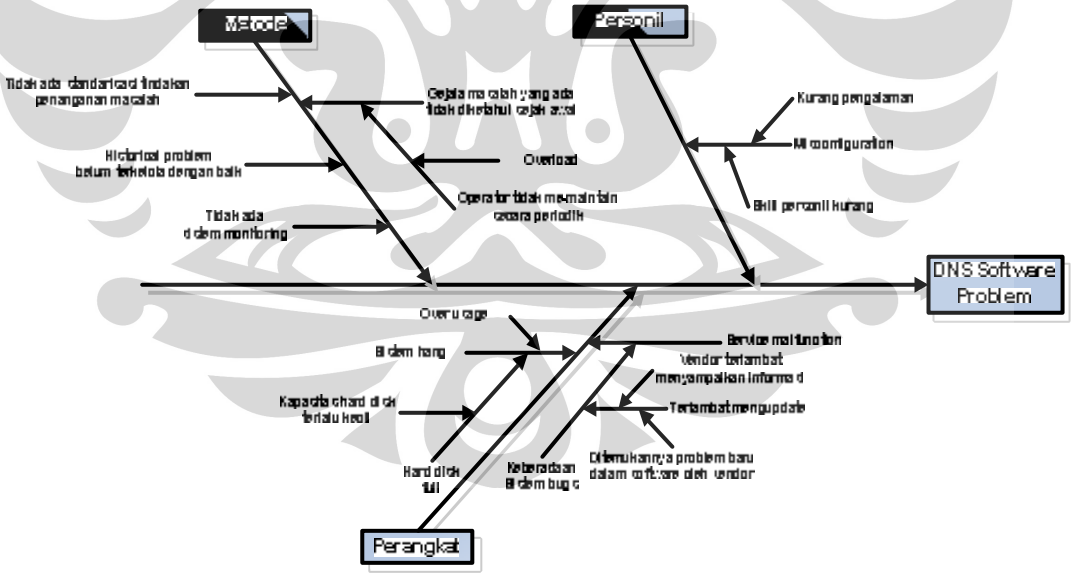
Fishbone diagram atau diagram sebab-akibat merupakan alat (*tool*) yang digunakan untuk lebih menyelidiki penyebab mendasar dari sebuah permasalahan atau akar penyebabnya, yang dikelompokkan berdasarkan 5M & 1E (*Man/Personnel, Method, Machine, Material, Measurement, Environment*). Berdasarkan hasil *brainstorming* dengan tim *expert*, penyebab dari risiko kritis dapat dikelompokkan menjadi 3 kriteria yaitu metode, personil, dan perangkat. Hasil dari *fishbone diagram* ini kemudian akan dikerucutkan lagi menggunakan *Fault Tree Analysis* (FTA) untuk mendapatkan *basic event* penyebab terjadinya *top event* (risiko kritis).



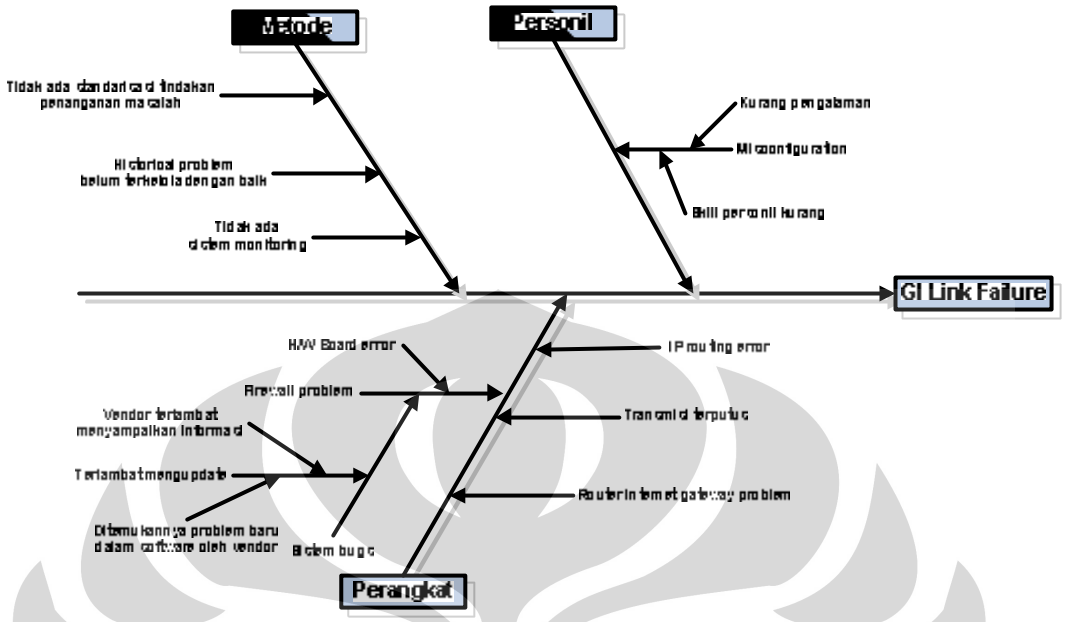
Gambar 3.3 *Fishbone Diagram* dari EMM Problem



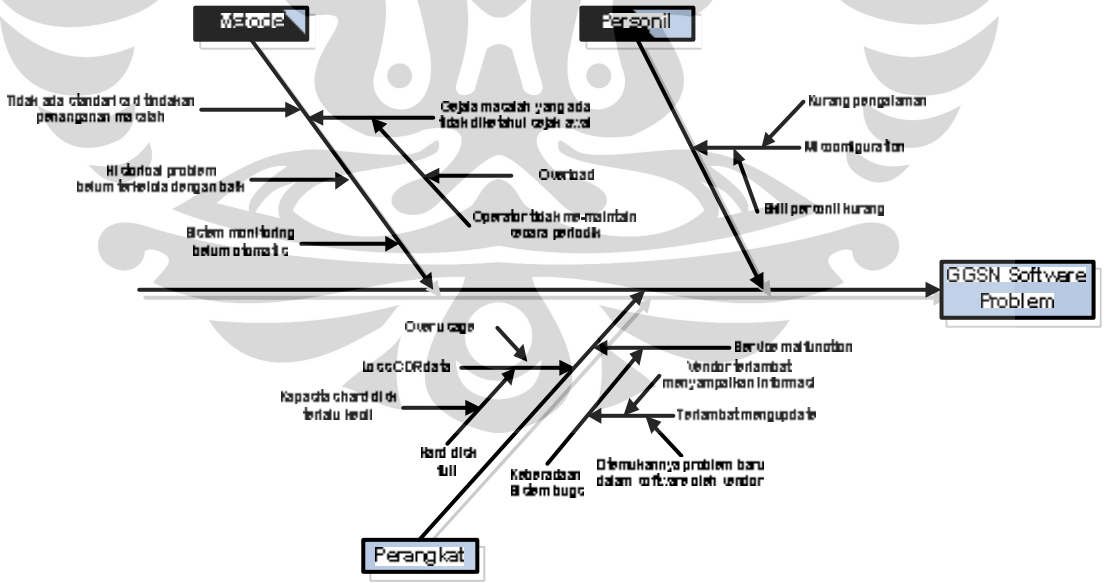
Gambar 3.4 *Fishbone Diagram* dari GGSN-Radius Link Failure



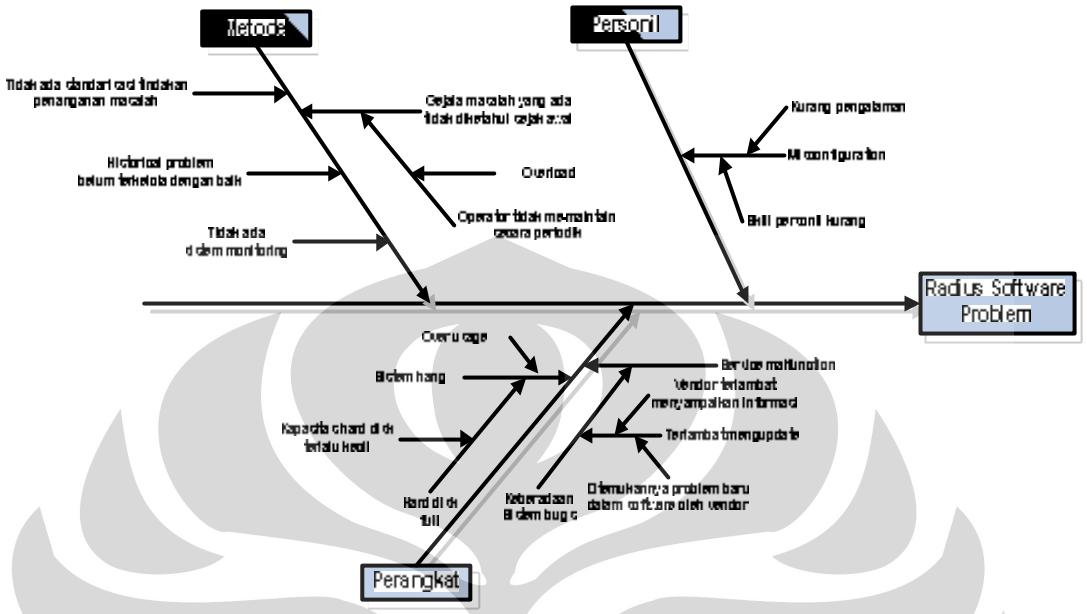
Gambar 3.5 *Fishbone Diagram* dari DNS Software Problem



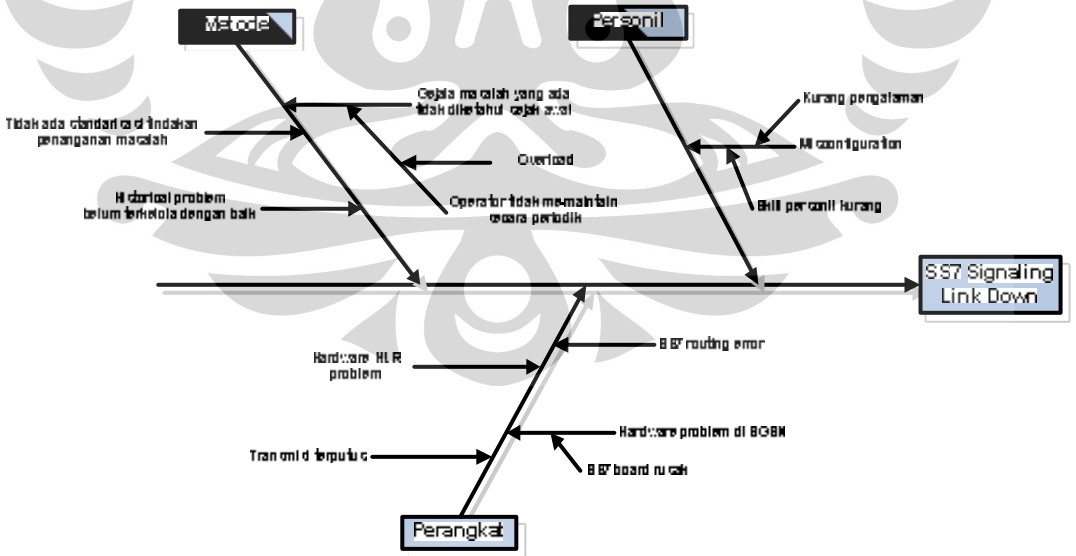
Gambar 3.6 *Fishbone Diagram* dari GI Link Failure



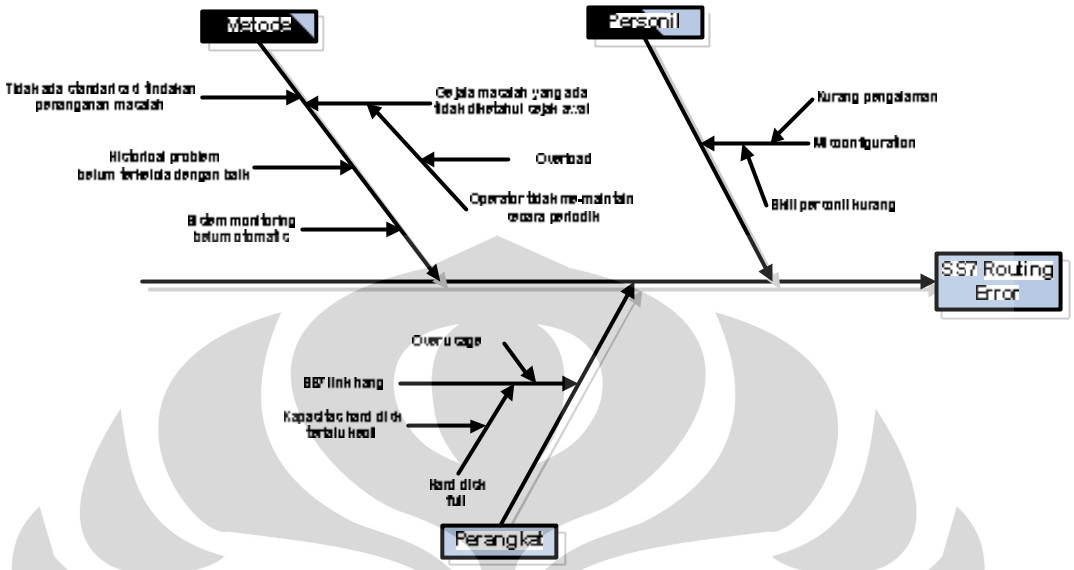
Gambar 3.7 *Fishbone Diagram* dari GGSN Software Problem



Gambar 3.8 *Fishbone Diagram* dari Radius Software Problem



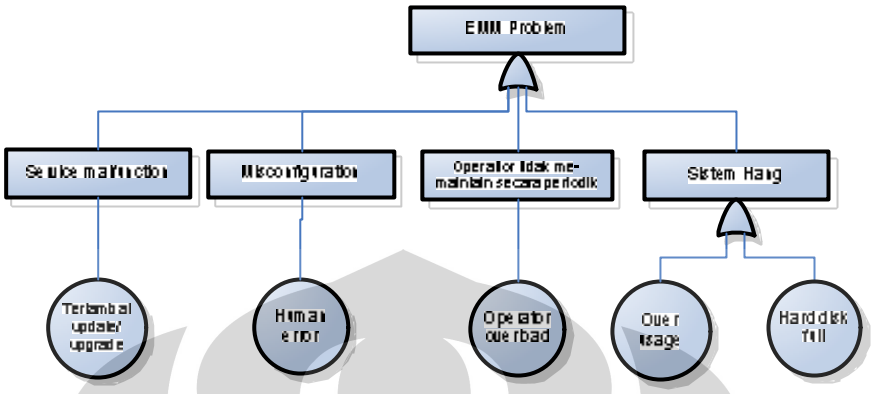
Gambar 3.9 *Fishbone Diagram* dari SS7 Signaling Link Down



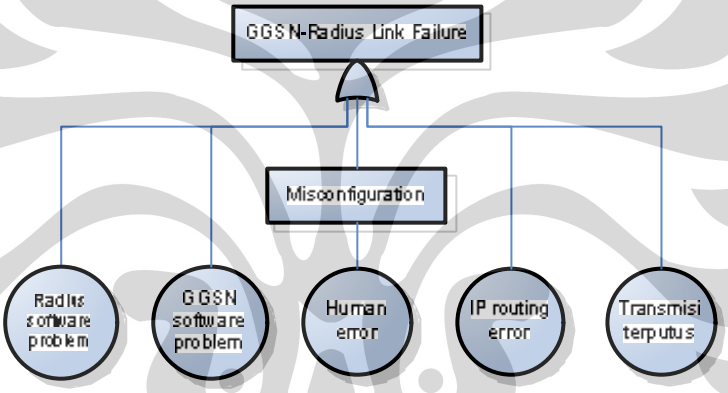
Gambar 3.10 *Fishbone Diagram* dari SS7 Routing Error

3.2.3 *Fault Tree Analysis Diagram* dari Risiko Kritis

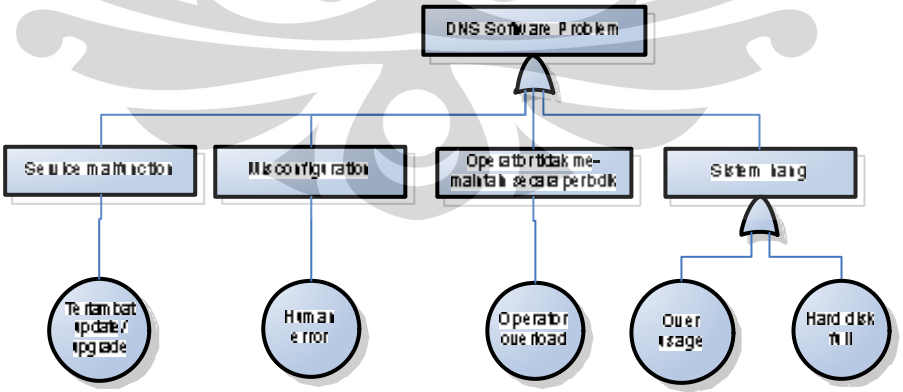
Fault Tree Analysis (FTA) adalah sebuah model grafis yang terdiri dari beberapa kombinasi kesalahan *(fault)* secara pararel dan secara berurutan yang mungkin menyebabkan awal dari *failure event* yang sudah ditetapkan. Pada FTA yang dibuat, ditetapkan masing-masing risiko kritis sebagai top event. Pada akhirnya akan diperoleh basic event yang merupakan penyebab terjadinya top event (risiko kritis), sehingga langkah-langkah yang tepat dapat diambil untuk menyelesaikan permasalahan terjadinya risiko kritis tersebut. Basic event yang diperoleh telah memperhitungkan penyebab permasalahan dari berbagai sisi (personil, metode, dan perangkat) karena merupakan pengerucutan dari hasil *fishbone diagram* sehingga memudahkan dalam pembuatan FTA. Setelah diketahui penyebab terjadinya risiko kritis selanjutnya dapat diketahui biaya yang harus dikeluarkan untuk mengatasi risiko kritis (*treatment cost*). Berikut adalah gambar *fault tree analysis* dari masing-masing risiko kritis.



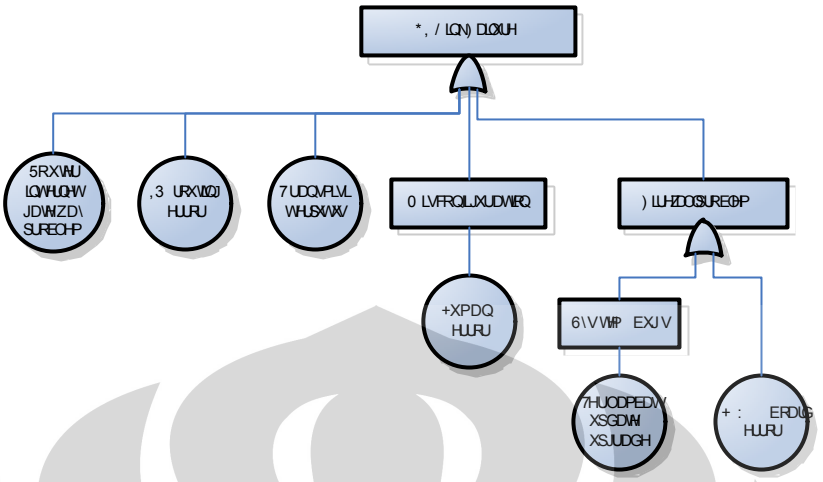
Gambar 3.11 FTA dari EMM Problem



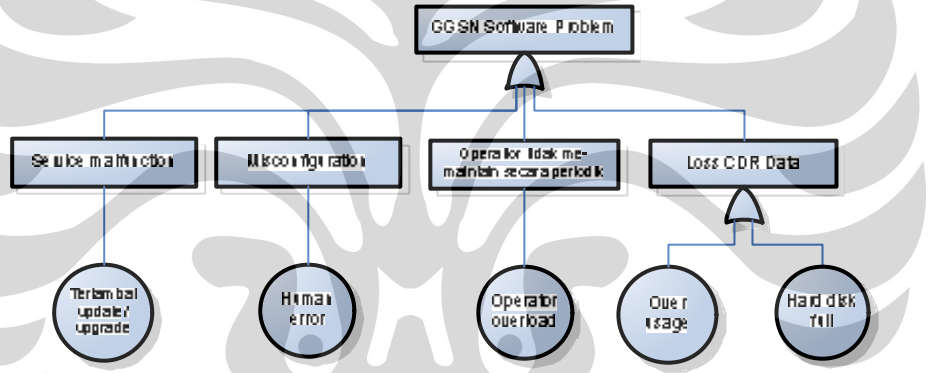
Gambar 3.12 FTA dari GGSN-Radius Link Failure



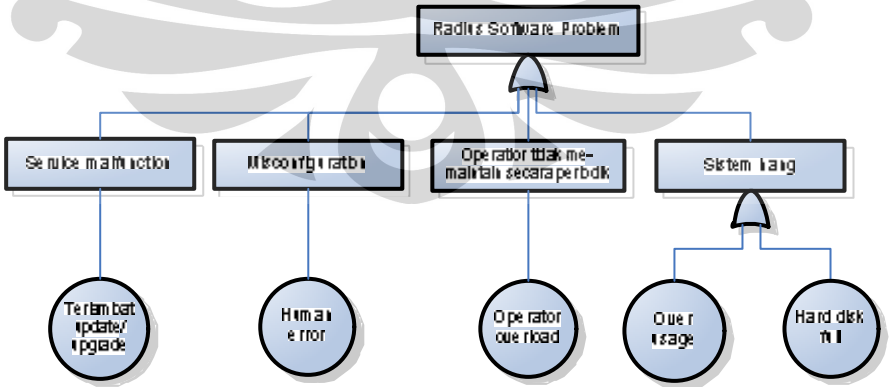
Gambar 3.13 FTA dari DNS Software Problem



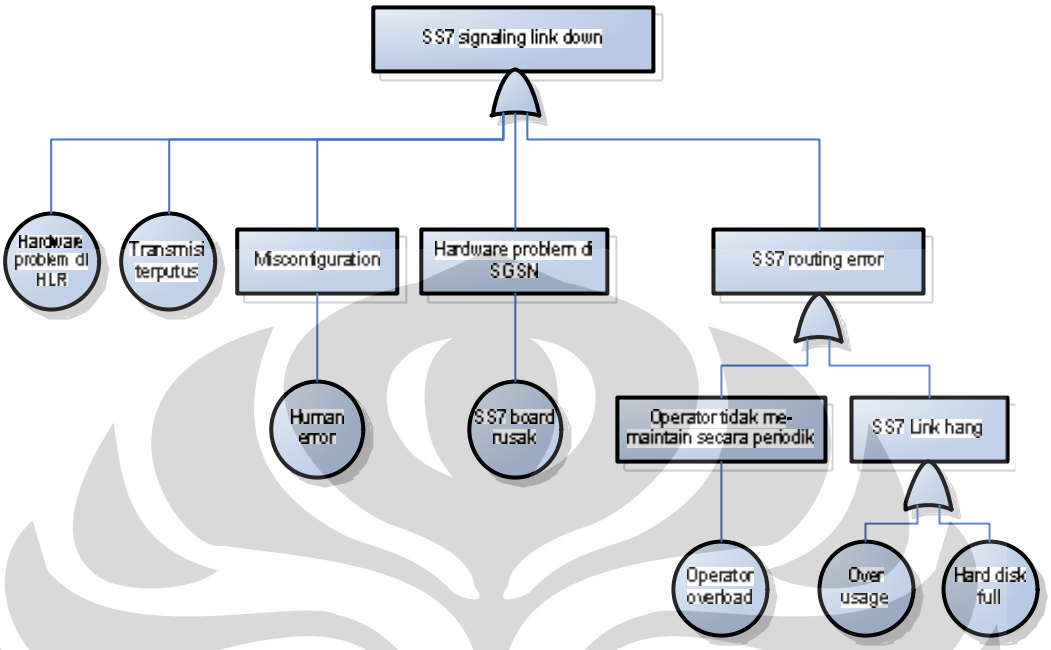
Gambar 3.14 FTA dari GI Link Failure



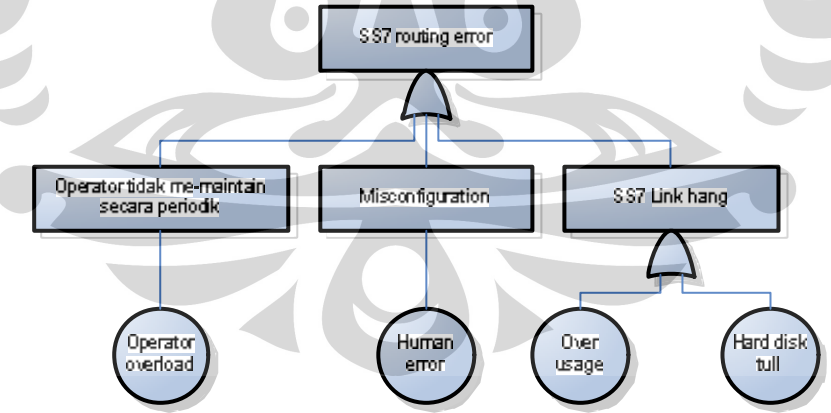
Gambar 3.15 FTA dari GGSN Software Problem



Gambar 3.16 FTA dari Radius Software Problem



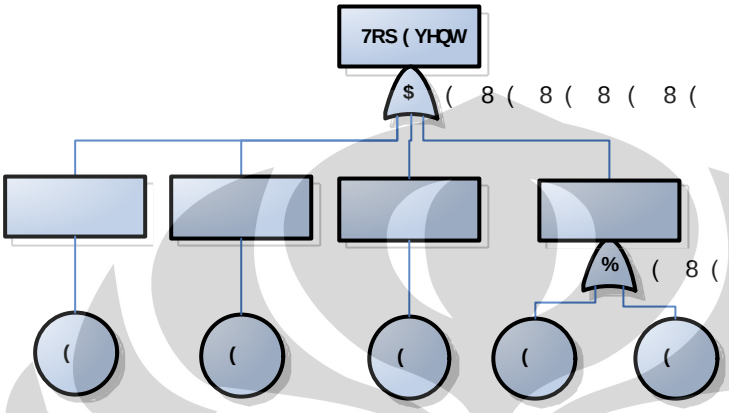
Gambar 3.17 FTA dari SS7 Signaling Link Down



Gambar 3.18 FTA dari SS7 Routing Error

3.2.3.1 Cut Set

a. Cut Set untuk Top Event EMM Problem, DNS Software Problem, GGSN Software Problem, Radius Software Problem

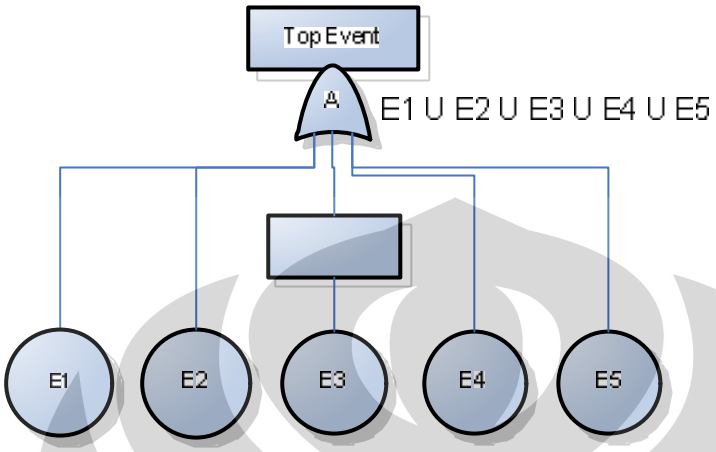


Langkah 1	Langkah 2
E1	E1
E2	E2
E3	E3
B	E4
	E5

Semua event yang diperoleh pada langkah 2 merupakan basic event, sehingga kita mendapatkan cut set dari fault tree ini adalah {1}, {2}, {3}, {4}, dan {5} yang semuanya merupakan minimal cut set. Artinya bila event 1 atau 2 atau 3 atau 4 atau 5 terjadi (secara simultan) akan mengakibatkan terjadinya Top Event.

- Top Event : EMM Problem, DNS Software Problem, GGSN Software Problem, Radius Software Problem
- Basic event 1 : Terlambat update/upgrade software
- Basic event 2 : Human error
- Basic event 3 : Operator overload
- Basic event 4 : Over usage
- Basic event 5 : Harddisk full

b. Cut Set untuk Top Event GGSN-Radius Link Failure

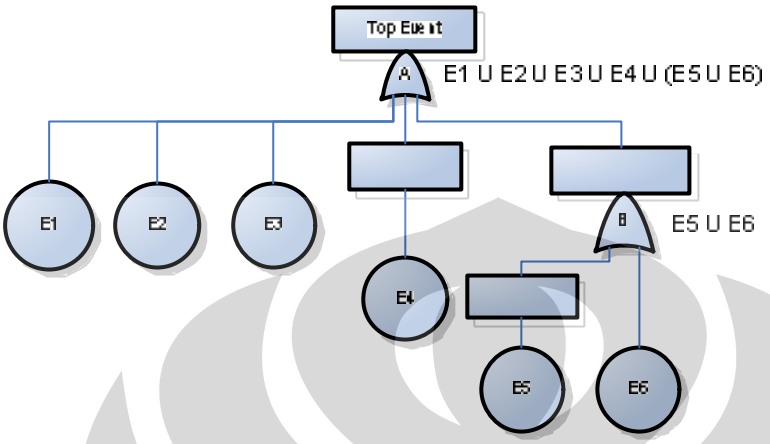


Langkah 1
E1
E2
E3
E4
E5

Semua event yang diperoleh pada langkah 1 merupakan basic event, sehingga kita mendapatkan cut set dari fault tree ini adalah {1}, {2}, {3}, {4}, dan {5} yang semuanya merupakan minimal cut set. Artinya bila event 1 atau 2 atau 3 atau 4 atau 5 terjadi (secara simultan) akan mengakibatkan terjadinya Top Event.

- Top Event : GGSN – Radius Link Failure
- Basic event 1 : Radius software problem
- Basic event 2 : GGSN software problem
- Basic event 3 : Human error
- Basic event 4 : IP routing error
- Basic event 5 : Transmisi terputus

c. Cut Set untuk Top Event GI Link Failure

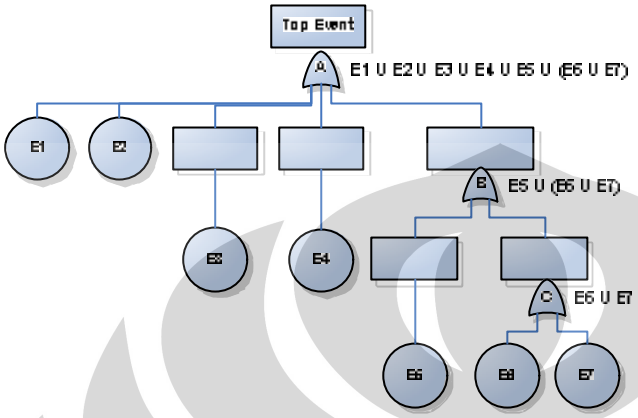


Langkah 1	Langkah 2
E1	E1
E2	E2
E3	E3
E4	E4
B	E5
	E6

Semua event yang diperoleh pada langkah 2 merupakan basic event, sehingga kita mendapatkan cut set dari fault tree ini adalah {1}, {2}, {3}, {4}, {5}, dan {6} yang semuanya merupakan minimal cut set. Artinya bila event 1 atau 2 atau 3 atau 4 atau 5 atau 6 terjadi (secara simultan) akan mengakibatkan terjadinya Top Event.

- Top Event : GI Link Failure
- Basic event 1 : Router internet gateway problem
- Basic event 2 : IP routing error
- Basic event 3 : Transmisi terputus
- Basic event 4 : Human error
- Basic event 5 : Terlambat update/upgrade
- Basic event 6 : Hardware board rusak

d. Cut Set untuk Top Event SS7 Signaling Link Down

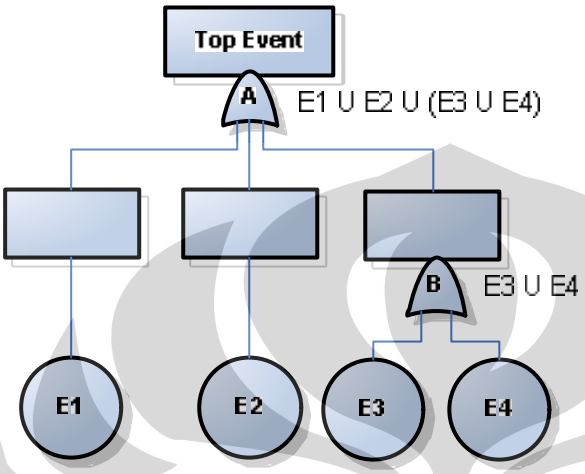


Langkah 1	Langkah 2	Langkah 3
E1	E1	E1
E2	E2	E2
E3	E3	E3
E4	E4	E4
B	E5	E5
	C	E6
		E7

Semua event yang diperoleh pada langkah 3 merupakan basic event, sehingga kita mendapatkan cut set dari fault tree ini adalah {1}, {2}, {3}, {4}, {5}, {6} dan {7} yang semuanya merupakan minimal cut set. Artinya bila event event 1 atau 2 atau 3 atau 4 atau 5 atau 6 atau 7 terjadi (secara simultan) akan mengakibatkan terjadinya Top Event.

- Top Event : SS7 signaling link down
- Basic event 1 : HLR Hardware problem
- Basic event 2 : Transmisi terputus
- Basic event 3 : Human error
- Basic event 4 : SS7 board rusak
- Basic event 5 : Operator overload
- Basic event 6 : Over usage
- Basic event 7 : Harddisk full

e. Cut Set untuk Top Event SS7 Routing Error



Langkah 1	Langkah 2
E1	E1
E2	E2
B	E3
	E4

Semua event yang diperoleh pada langkah 2 merupakan basic event, sehingga kita mendapatkan cut set dari fault tree ini adalah {1}, {2}, {3} dan {4} yang semuanya merupakan minimal cut set. Artinya bila event 1 atau 2 atau 3 atau 4 terjadi (secara simultan) akan mengakibatkan terjadinya Top Event.

- Top Event : SS7 routing error
- Basic event 1 : Operator overload
- Basic event 2 : Human error
- Basic event 3 : Over usage
- Basic event 4 : Harddisk full

3.2.4 Perhitungan Biaya Risiko

Langkah selanjutnya, dilakukan perhitungan biaya risiko untuk risiko kritis. *Treatment cost* diperoleh dari biaya yang diperlukan untuk mengatasi masing-masing risiko kritis dengan merujuk pada hasil dari *fault tree analysis*, adapun *loss revenue* diperoleh dari data historis perusahaan dan *expert judgment*.

3.2.4.1 *Treatment Cost*

Total *treatment cost* untuk seluruh risiko kritis adalah sebesar Rp505.000.000, dengan rincian sebagai berikut.

a. *Treatment Cost* untuk EMM Problem : Rp 130.000.000
b. *Treatment Cost* untuk DNS Software Problem : Rp 20.000.000
c. *Treatment Cost* untuk GI Link Failure : Rp 20.000.000
d. *Treatment Cost* untuk GGSN Software Problem : Rp 130.000.000
e. *Treatment Cost* untuk Radius Software Problem : Rp 55.000.000
f. *Treatment Cost* untuk SS7 Routing Error : Rp 50.000.000
g. *Treatment Cost* untuk SS7 Signaling Link Down : Rp 100.000.000
h. *Treatment Cost* untuk GGSN-Radius Link Failure

Alokasi dana untuk GGSN-link failure tidak masuk dalam simulasi karena berdasarkan hasil *fault tree analysis*, tindakan yang memerlukan biaya untuk menangani masalah GGSN-link failure merupakan gabungan dari GGSN software problem dan radius software problem sehingga telah secara otomatis akan ter*cover* jika kedua permasalahan tadi telah didanai.

3.2.4.2 *Loss Revenue*

Untuk kepentingan penentuan *loss revenue*, kedelapan risiko kritis dikelompokkan menjadi tiga besar berdasarkan fungsi dari item yang bermasalah di perangkat yang berbeda. EMM problem merujuk pada *loss revenue* yang ter-*capture* di perangkat GGSN-*duration based*; DNS software problem, GI link failure, GGSN software problem, dan radius software problem merujuk pada *loss revenue* yang ter-

capture di perangkat GGSN-*volume based*; sedangkan SS7 signaling link down dan SS7 routing error merujuk pada *loss revenue* dari perangkat SGSN yang down.

Berdasarkan hasil pengumpulan data, maka diperoleh data *loss revenue* untuk setiap risiko kritis sebagai berikut.

- EMM problem (distribusi normal) :
  - Mean : Rp 214.870.286
  - Standar deviasi : 43856839
- DNS software problem, GI link failure, GGSN software problem, dan radius software problem (distribusi normal) :
  - Mean : Rp 345.108.000
  - Standar deviasi : 87460770
- SS7 signaling link down dan SS7 routing error (distribusi uniform) :
  - Maksimum : Rp 360.000.000
  - Minimum Rp 12.000.000.

3.2.5 Optimasi Alokasi Biaya Penanganan Risiko menggunakan Simulasi OptQuest

OptQuest merupakan salah satu fungsi yang terdapat dalam Crystal Ball. OptQuest ini dapat digunakan untuk menentukan alokasi biaya yang menghasilkan keuntungan optimal.

Ada beberapa istilah yang digunakan dalam alokasi biaya dengan OptQuest, yaitu :

- *Risk cost/loss revenue*, yaitu biaya yang harus dikeluarkan / kehilangan pendapatan ketika risiko terjadi
- *Risk coverage*, yaitu biaya risiko / kehilangan pendapatan yang ter*cover* dengan alokasi biaya treatment yang diberikan
- *Decision*, merupakan variable penentu seberapa besar dana yang dialokasikan untuk suatu risiko, bernilai 1 jika diberikan alokasi dana untuk suatu risiko
- *Advantage*, yaitu selisih *risk coverage* dengan *treatment cost* yang kemudian dikalikan dengan variable *decision*

Langkah berikutnya adalah menjalankan fungsi *OptQuest* dalam *Crystal Ball*. Simulasi masing-masing dilakukan untuk setiap asumsi anggaran dana yang tersedia, dan masing-masing simulasi dilakukan dengan 1000 kali percobaan. Diasumsikan perusahaan menyediakan anggaran untuk penanganan risiko ini masing-masing maksimal 25%, 50%, 75%, dan juga jika perusahaan dapat menyediakan dana penuh 100% dari total biaya *treatment* yang diperlukan. Hasil akhir dari simulasi ini berbeda untuk setiap kendala dana yang diberikan. Keempat tabel berikut menunjukkan hasil simulasi alokasi biaya *treatment* yang optimal sesuai keterbatasan dana yang tersedia.

3.8 Hasil Optimasi Alokasi Biaya *Treatment* dengan Asumsi Ketersediaan Dana ≤ 25% dari Biaya *Treatment* Total

Risk	Loss Revenue	Treatment Cost	Treatment Cost Allocation	% Allocation	Risk Coverage	Decision	Advantage
EMM problem	Rp214,870,286	Rp130,000,000	Rp0	0.00%	Rp0	0	Rp0
DNS software problem	Rp345,108,000	Rp20,000,000	Rp20,000,000	100.00%	Rp345,108,000	1	Rp325,108,000
GI link problem	Rp345,108,000	Rp20,000,000	Rp20,000,000	100.00%	Rp345,108,000	1	Rp325,108,000
GGSN Software problem	Rp345,108,000	Rp130,000,000	Rp0	0.00%	Rp0	0	Rp0
Radius sofware problem	Rp345,108,000	Rp55,000,000	Rp53,657,000	97.56%	Rp336,681,090	1	Rp283,024,090
SS7 Signaling Link Down	Rp360,000,000	Rp100,000,000	Rp0	0.00%	Rp0	0	Rp0
SS7 routing error	Rp360,000,000	Rp50,000,000	Rp32,593,000	65.19%	Rp234,669,600	1	Rp202,076,600
? (Total)	Rp2,315,302,286	Rp505,000,000	Rp126,250,000			**Total Advantages**	Rp1,135,316,690

Tabel 3.9 Hasil Optimasi Alokasi Biaya *Treatment* dengan Asumsi Ketersediaan Dana ≤ 50% dari Biaya *Treatment* Total

Risk	Loss Revenue	Treatment Cost	Treatment Cost Allocation	% Allocation	Risk Coverage	Decision	Advantage
EMM problem	Rp214,870,286	Rp130,000,000	Rp0	0.00%	Rp0	0	Rp0
DNS software problem	Rp345,108,000	Rp20,000,000	Rp20,000,000	100.00%	Rp345,108,000	1	Rp325,108,000
GI link problem	Rp345,108,000	Rp20,000,000	Rp20,000,000	100.00%	Rp345,108,000	1	Rp325,108,000
GGSN Software problem	Rp345,108,000	Rp130,000,000	Rp107,580,000	82.75%	Rp285,590,143	1	Rp178,010,143
Radius sofware problem	Rp345,108,000	Rp55,000,000	Rp55,000,000	100.00%	Rp345,108,000	1	Rp290,108,000
SS7 Signaling Link Down	Rp360,000,000	Rp100,000,000	Rp0	0.00%	Rp0	0	Rp0
SS7 routing error	Rp360,000,000	Rp50,000,000	Rp49,727,000	99.45%	Rp358,034,400	1	Rp308,307,400
? (Total)	Rp2,315,302,286	Rp505,000,000	Rp252,307,000		Rp1,678,948,543	**Total Advantages**	Rp1,426,641,543

Tabel 3.10 Hasil Optimasi Alokasi Biaya *Treatment* dengan Asumsi Ketersediaan Dana ≤ 75% dari Biaya *Treatment* Total

Risk	Loss Revenue	Treatment Cost	Treatment Cost Allocation	% Allocation	Risk Coverage	Decision	Advantage
EMM problem	Rp214,870,286	Rp130,000,000	Rp4,704,900	3.62%	Rp7,776,486	1	Rp3,071,586
DNS software problem	Rp345,108,000	Rp20,000,000	Rp20,000,000	100.00%	Rp345,108,000	1	Rp325,108,000
GI link problem	Rp345,108,000	Rp20,000,000	Rp20,000,000	100.00%	Rp345,108,000	1	Rp325,108,000
GGSN Software problem	Rp345,108,000	Rp130,000,000	Rp130,000,000	100.00%	Rp345,108,000	1	Rp215,108,000
Radius sofware problem	Rp345,108,000	Rp55,000,000	Rp55,000,000	100.00%	Rp345,108,000	1	Rp290,108,000
SS7 Signaling Link Down	Rp360,000,000	Rp100,000,000	Rp99,045,000	99.05%	Rp356,562,000	1	Rp257,517,000
SS7 routing error	Rp360,000,000	Rp50,000,000	Rp50,000,000	100.00%	Rp360,000,000	1	Rp310,000,000
? (Total)	Rp2,315,302,286	Rp505,000,000	Rp378,749,900		Rp2,104,770,486	**Total Advantages**	Rp1,726,020,586

Tabel 3.11 Hasil Optimasi Alokasi Biaya *Treatment* dengan Asumsi Ketersediaan Dana sebesar 100% dari Biaya *Treatment* Total

Risk	Loss Revenue	Treatment Cost	Treatment Cost Allocation	% Allocation	Risk Coverage	Decision	Advantage
EMM problem	Rp214,870,286	Rp130,000,000	Rp130,000,000	100%	Rp214,870,286	1	Rp84,870,286
DNS software problem	Rp345,108,000	Rp20,000,000	Rp20,000,000	100%	Rp345,108,000	1	Rp325,108,000
GI link problem	Rp345,108,000	Rp20,000,000	Rp20,000,000	100%	Rp345,108,000	1	Rp325,108,000
GGSN Software problem	Rp345,108,000	Rp130,000,000	Rp130,000,000	100%	Rp345,108,000	1	Rp215,108,000
Radius sofware problem	Rp345,108,000	Rp55,000,000	Rp55,000,000	100%	Rp345,108,000	1	Rp290,108,000
SS7 Signaling Link Down	Rp360,000,000	Rp100,000,000	Rp100,000,000	100%	Rp360,000,000	1	Rp260,000,000
SS7 routing error	Rp360,000,000	Rp50,000,000	Rp50,000,000	100%	Rp360,000,000	1	Rp310,000,000
? (Total)	Rp2,315,302,286	Rp505,000,000	Rp505,000,000			**Total Advantages**	Rp1,810,302,286

BAB IV
ANALISIS DATA

4.1 Usulan Tindakan Penanganan Risiko Kritis

Usulan penanganan risiko yang diberikan adalah untuk risiko-risiko yang termasuk risiko kritis. Karena termasuk risiko kritis maka tindakan respon dengan menerima risiko (*Risk Acceptance*) tidak tepat, begitupun dengan tindakan mencegah risiko (*Risk Avoidance*) karena beberapa permasalahan timbul disebabkan adanya kegiatan operasional dan pemeliharaan perangkat GPRS serta dari pemakaian sistem GPRS oleh pelanggan yang tidak bisa untuk tidak dilakukan.

Usulan tindakan penanganan risiko dilakukan dengan mengurangi risiko (*Risk Mitigation*). Dengan pengurangan risiko, perusahaan akan mencoba mengurangi risiko dalam dua cara yaitu mengurangi peluang terjadinya risiko dan mengurangi dampak yang ditimbulkan akibat terjadinya risiko. Pengurangan dampak terjadinya risiko dilakukan dengan melaksanakan *remedy action* yaitu tindakan pertama yang harus dilakukan oleh operator seketika saat diketahui timbul/terjadi risiko kritis tersebut. Agar *remedy action* dapat dilaksanakan dengan efisien dan efektif, maka berdasarkan hasil analisis dan evaluasi data dapat diberikan usulan tindakan yang perlu dilakukan, yaitu :

- Dibuat sistem monitoring yang otomatis untuk semua perangkat yang ada dalam infrastruktur GPRS
- Dibuat standarisasi tindakan penanganan masalah
- Mengelola *historical problem* dengan baik

Jika kemudian ternyata operator masih tidak dapat menyelesaikan permasalahan yang timbul, baru kemudian dieskalasi kepada vendor (*risk transfer*). Sedangkan untuk mengurangi peluang terjadinya risiko maka berdasarkan hasil *fault tree analysis* dapat dilakukan langkah-langkah seperti berikut.

a. EMM problem
   - Menambah operator untuk mengatasi beban operator yang ada yang telah overload
   - Memberi training kepada personil mengenai EMM
   - Meng-upgrade harddisk EMM agar sistem tidak hang karena harddisk full akibat over usage
   - Meminta komitmen vendor untuk tidak pernah terlambat meng-update informasi mengenai perangkat EMM sehingga kejadian sistem bugs dapat dihindari

b. DNS software problem
   - Menambah operator untuk mengatasi beban operator yang ada yang telah overload
   - Memberi training kepada personil mengenai DNS
   - Meng-upgrade harddisk DNS agar sistem tidak hang karena harddisk full akibat over usage
   - Meminta komitmen vendor untuk tidak pernah terlambat meng-update informasi mengenai perangkat DNS sehingga kejadian sistem bugs dapat dihindari

c. GI link failure
   - Memberi training kepada personil mengenai GI link
   - Meminta komitmen vendor untuk tidak pernah terlambat meng-update informasi mengenai firewall sehingga kejadian sistem bugs dapat dihindari
   - Melakukan pemeriksaan rutin terhadap hardware board dan segera melakukan penggantian jika diketahui terdapat kerusakan
   - Berkoordinasi dengan bagian terkait mengenai permasalahan pada IP routing, tranmisi, dan router internet gateway sehingga segala kegagalan yang mungkin terjadi dapat dihindari dan jika telah terjadi dapat segera teratasi

d. GGSN software problem
   - Menambah operator untuk mengatasi beban operator yang ada yang telah overload
   - Memberi training kepada personil mengenai GGSN
   - Meng-upgrade harddisk GGSN agar tidak terjadi loss CDR data
   - Meminta komitmen vendor untuk tidak pernah terlambat meng-update informasi mengenai perangkat GGSN sehingga kejadian sistem bugs dapat dihindari

e. Radius software problem
   - Menambah operator untuk mengatasi beban operator yang ada yang telah overload
   - Memberi training kepada personil mengenai Radius
   - Meng-upgrade / mengganti harddisk Radius agar sistem tidak hang karena harddisk full akibat over usage
   - Meminta komitmen vendor untuk tidak pernah terlambat meng-update informasi mengenai perangkat Radius sehingga kejadian sistem bugs dapat dihindari

f. GGSN-Radius link failure
   - Melakukan tindakan penanganan permasalahan yang timbul pada GGSN software dan Radius software
   - Berkoordinasi dengan bagian terkait mengenai permasalahan pada IP routing dan transmisi

g. SS7 routing error
   - Menambah operator untuk mengatasi beban operator yang ada yang telah overload
   - Memberi training kepada personil mengenai SS7 routing
   - Meng-upgrade harddisk agar SS7 tidak hang karena harddisk full akibat over usage

h. SS7 Signaling Link Down
   - Melakukan tindakan penanganan permasalahan yang timbul pada SS7 routing
   - Berkoordinasi dengan bagian terkait mengenai permasalahan pada hardware HLR dan transmisi
   - Melakukan pemeriksaan rutin terhadap hardware SGSN dan segera melakukan penggantian SS7 board jika diketahui terdapat kerusakan

Beberapa tindakan penanganan risiko untuk mengurangi peluang terjadinya risiko kritis yang diusulkan di atas memerlukan biaya dalam pelaksanaannya. Sehingga langkah selanjutnya dari penelitian ini adalah melakukan analisis alokasi biaya penanganan risiko yang optimal.

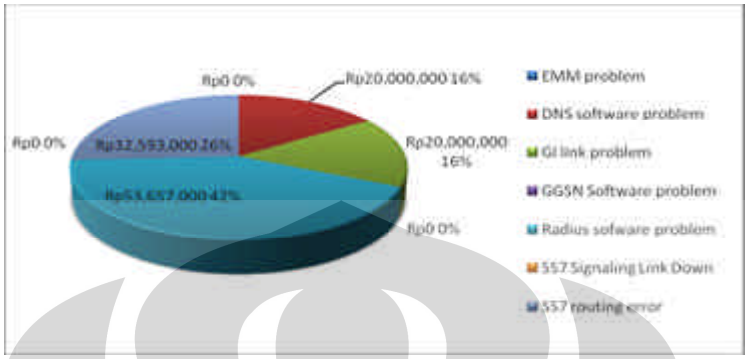
4.2 Analisis Optimasi Alokasi Biaya Penanganan Risiko menggunakan Simulasi OptQuest

Berikut akan dijelaskan analisis hasil simulasi optimasi OptQuest, adapun hasil dari simulasi dapat dijadikan referensi bagi pihak perusahaan, dan keputusan akhir mengenai pemanfaatan hasil simulasi diserahkan pada pihak perusahaan.

4.2.1 Asumsi Ketersediaan Dana Maksimal sebesar 25% dari Total Biaya yang Dibutuhkan

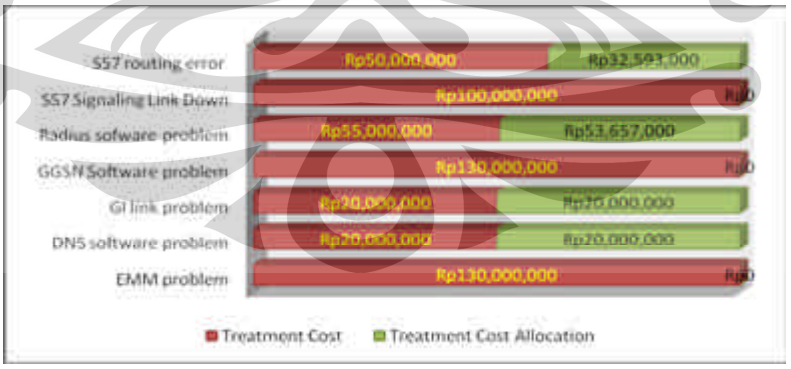
Berdasarkan hasil simulasi optimasi yang memaksimalkan nilai total *advantage*, dengan ketersediaan dana maksimal sebesar 25% dari total biaya yang dibutuhkan, optimasi diperoleh ketika total alokasi biaya *treatment* sebesar Rp126.250.000 dengan komposisi alokasi dana untuk setiap risiko kritis yang dapat dilihat pada gambar 4.1. Pada gambar terlihat bahwa alokasi dana terbesar diberikan untuk tindakan penanganan risiko radius software problem yang didanai sebesar Rp53.657.000 yaitu sekitar 42% dari total alokasi biaya *treatment*. Adapun EMM problem, GGSN software problem, dan SS7 signaling link down tidak mendapat alokasi dana. Dengan kondisi tidak mendapat alokasi dana, perusahaan dapat melakukan tindakan penanganan risiko yang diusulkan yang lainnya yang tidak

memerlukan dana karena seperti telah dijelaskan bahwa tidak semua usulan tindakan penanganan risiko memerlukan dana untuk dapat dilaksanakan.



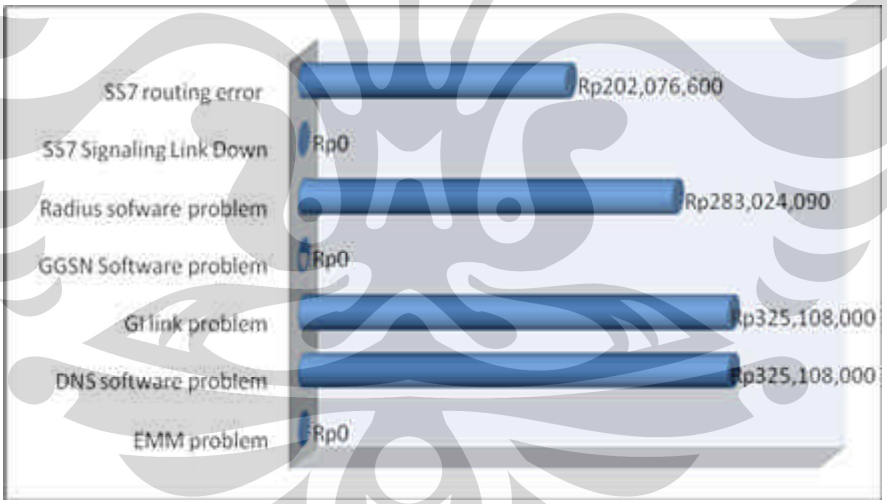
Gambar 4.1 Komposisi Alokasi Biaya *Treatment* untuk setiap Risiko Kritis dengan Asumsi Ketersediaan Dana Maksimal sebesar 25% dari Total Biaya yang Dibutuhkan

Dengan komposisi alokasi biaya *treatment* hasil optimasi, diperoleh bahwa risiko yang mendapatkan alokasi biaya *treatment* dengan utuh adalah DNS software problem dan GI link problem. Sedangkan radius software problem yang mendapat alokasi terbesar dari total alokasi biaya *treatment* tidak dibiayai secara penuh karena alokasi biaya yang diberikan masih lebih kecil daripada biaya *treatment* yang dibutuhkan. Adapun perbandingan antara biaya *treatment* ideal yang diusulkan dengan biaya *treatment* yang dialokasikan dapat dilihat pada gambar 4.2.



Gambar 4.2 Perbandingan Biaya *Treatment* Ideal dan Biaya *Treatment* yang Dialokasikan dengan Asumsi Ketersediaan Dana Maksimal sebesar 25% dari Total Biaya yang Dibutuhkan

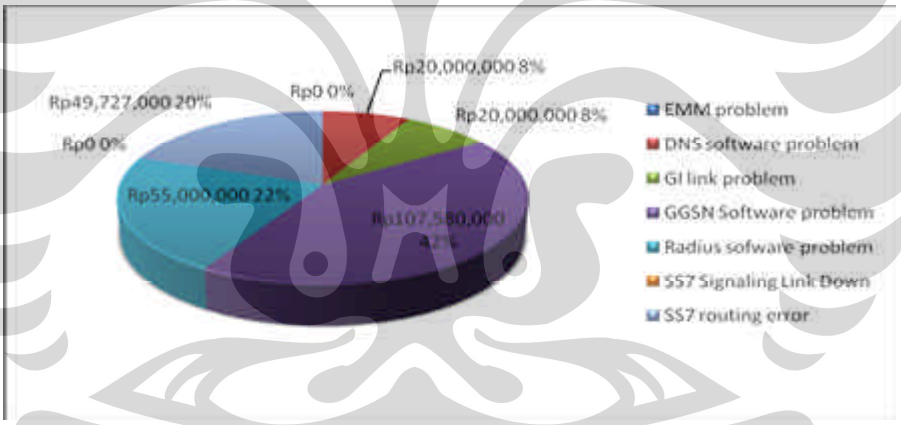
Melalui hasil simulasi juga dapat diketahui besarnya nilai manfaat (*advantage*) yang diperoleh dengan alokasi biaya *treatment* yang diberikan. Secara keseluruhan, dengan mengalokasikan biaya *treatment* sebesar Rp126.250.000, perusahaan akan memperoleh *maximum advantage* sebesar Rp 1.135.316.690. Nilai total *advantage* tersebut berasal dari nilai *advantage* masing-masing risiko yang dapat dibiayai pada kondisi dana yang tersedia maksimal sebesar 25% dari total biaya yang dibutuhkan, sebagaimana terlihat pada gambar 4.3. Pada gambar terlihat bahwa risko DNS software problem dan GI link failure memberikan nilai manfaat terbesar yaitu Rp 325.108.000 karena telah dibiayai secara penuh. Adapun radius software problem yang mendapat alokasi dana terbesar dari dana yang tersedia, tidak memberikan manfaat lebih besar daripada DNS software problem dan GI link problem. Hal ini dapat disebabkan oleh tingkat dampak dan biaya *treatment* yang diperlukan dari masing-masing risiko yang berbeda.



Gambar 4.3 Nilai Manfaat dari setiap Risiko Kritis dengan Asumsi Ketersediaan Dana Maksimal sebesar 25% dari Total Biaya yang Dibutuhkan

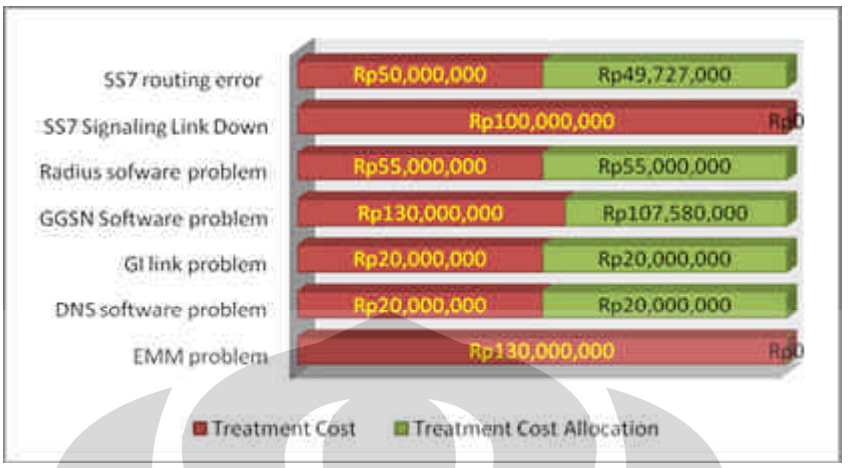
4.2.2 Asumsi Ketersediaan Dana Maksimal sebesar 50% dari Total Biaya yang Dibutuhkan

Berdasarkan hasil simulasi optimasi yang memaksimalkan nilai total *advantage*, dengan ketersediaan dana maksimal sebesar 50% dari total biaya yang dibutuhkan, optimasi diperoleh ketika total alokasi biaya *treatment* sebesar Rp252.307.000 dengan komposisi alokasi dana untuk setiap risiko kritis yang dapat dilihat pada gambar 4.4. Pada gambar terlihat bahwa alokasi dana terbesar diberikan untuk tindakan penanganan risiko GGSN software problem yang didanai sebesar Rp107.580.000 yaitu sekitar 42% dari total alokasi biaya *treatment*. Adapun EMM problem dan SS7 signaling link down masih tidak mendapat alokasi dana meskipun asumsi ketersediaan dana telah bertambah, karena simulasi memperhitungkan total *advantage* yang akan diperoleh dalam mengalokasikan biaya *treatment* yang optimal.



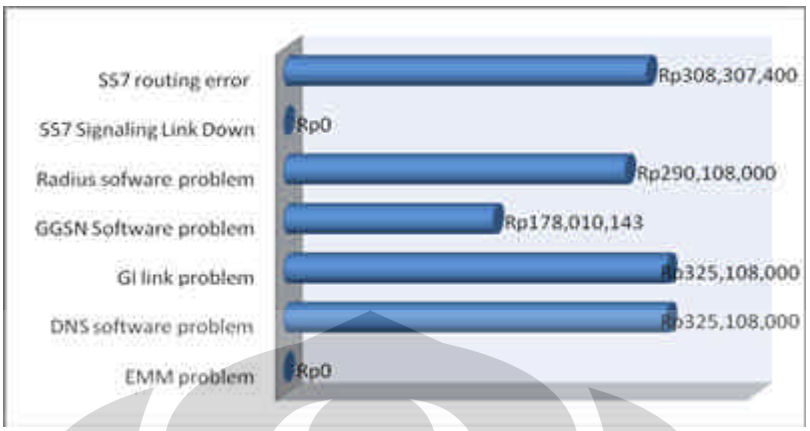
Gambar 4.4 Komposisi Alokasi Biaya *Treatment* untuk setiap Risiko Kritis dengan Asumsi Ketersediaan Dana Maksimal sebesar 50% dari Total Biaya yang Dibutuhkan

Dengan komposisi alokasi biaya *treatment* hasil optimasi, diperoleh bahwa terdapat tiga item risiko kritis yang mendapatkan alokasi biaya *treatment* dengan utuh yaitu DNS software problem, GI link problem, dan radius software problem. Adapun perbandingan antara biaya *treatment* ideal yang diusulkan dengan biaya *treatment* yang dialokasikan dapat dilihat pada gambar 4.5.



Gambar 4.5 Perbandingan Biaya *Treatment* Ideal dan Biaya *Treatment* yang Dialokasikan dengan Asumsi Ketersediaan Dana Maksimal sebesar 50% dari Total Biaya yang Dibutuhkan

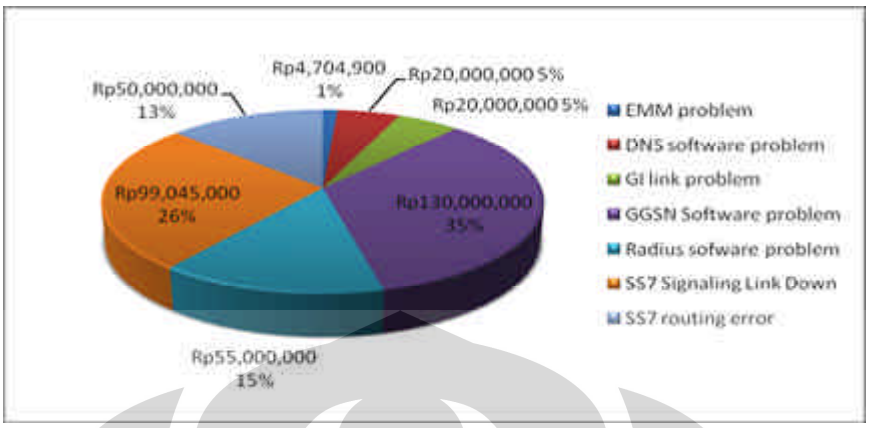
Secara keseluruhan, dengan mengalokasikan biaya *treatment* sebesar Rp252.307.000, perusahaan memperoleh *maximum advantage* sebesar Rp1.426.641.543. Nilai total *advantage* tersebut berasal dari nilai *advantage* masing-masing risiko yang dapat dibiayai pada kondisi dana yang tersedia maksimal sebesar 50% dari total biaya yang dibutuhkan, sebagaimana terlihat pada gambar 4.6. Pada gambar terlihat bahwa risiko DNS software problem dan GI link failure yang masih memberikan nilai manfaat terbesar yaitu Rp 325.108.000 karena telah dibiayai secara penuh. Adapun radius software problem yang juga dibiayai penuh, hanya memberikan nilai manfaat sebesar Rp 290.108.000. Hal ini dapat disebabkan oleh tingkat dampak dan biaya *treatment* yang diperlukan dari masing-masing risiko yang berbeda.



Gambar 4.6 Nilai Manfaat dari setiap Risiko Kritis dengan Asumsi Ketersediaan Dana Maksimal sebesar 50% dari Total Biaya yang Dibutuhkan

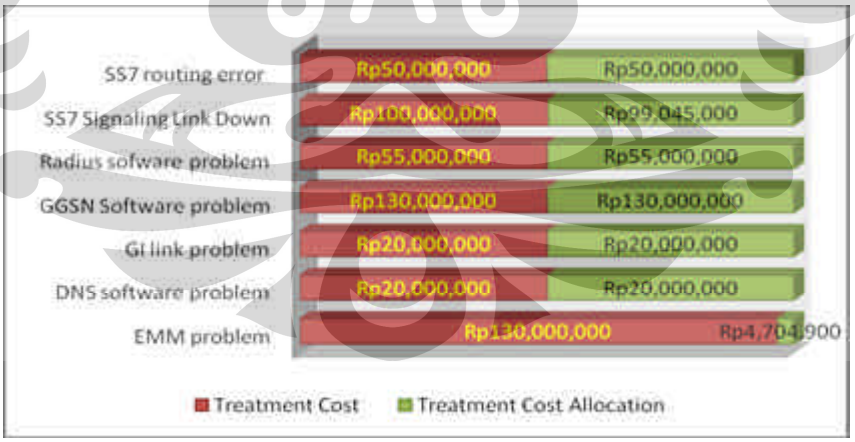
4.2.3 Asumsi Ketersediaan Dana Maksimal sebesar 75% dari Total Biaya yang Dibutuhkan

Berdasarkan hasil simulasi optimasi yang memaksimalkan nilai total *advantage*, dengan ketersediaan dana maksimal sebesar 75% dari total biaya yang dibutuhkan, optimasi diperoleh ketika total alokasi biaya *treatment* sebesar Rp378.749.900 dengan komposisi alokasi dana untuk setiap risiko kritis yang dapat dilihat pada gambar 4.7. Pada gambar terlihat bahwa alokasi dana terbesar diberikan untuk tindakan penanganan risiko GGSN software problem yang didanai penuh sebesar Rp 130.000.000 yaitu sekitar 33% dari total alokasi biaya *treatment.* Semua risiko telah mendapat alokasi dana, namun yang mendapat alokasi dana terendah adalah EMM problem yaitu sebesar Rp4.709.900 atau sekitar 1% dari total alokasi biaya *treatment*.



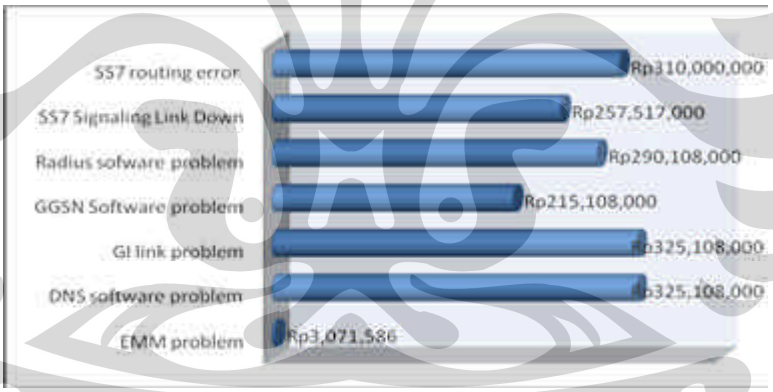
Gambar 4.7 Komposisi Alokasi Biaya *Treatment* untuk setiap Risiko Kritis dengan Asumsi Ketersediaan Dana Maksimal sebesar 75% dari Total Biaya yang Dibutuhkan

Dengan komposisi alokasi biaya *treatment* hasil optimasi, diperoleh bahwa semakin banyak risiko yang dapat didanai penuh yaitu terdapat lima item risiko kritis yang mendapatkan alokasi biaya *treatment* dengan utuh adalah DNS software problem, GI link problem, GGSN software problem, radius software problem, dan SS7 routing error. Adapun perbandingan antara biaya *treatment* ideal yang diusulkan dengan biaya *treatment* yang dialokasikan dapat dilihat pada gambar 4.8.



Gambar 4.8 Perbandingan Biaya *Treatment* Ideal dan Biaya *Treatment* yang Dialokasikan dengan Asumsi Ketersediaan Dana Maksimal sebesar 75% dari Total Biaya yang Dibutuhkan

Secara keseluruhan, dengan mengalokasikan biaya *treatment* sebesar Rp378.749.900, perusahaan memperoleh *maximum advantage* sebesar Rp1.726.020.586. Nilai total *advantage* tersebut berasal dari nilai *advantage* masing-masing risiko yang dapat dibiayai pada kondisi dana yang tersedia maksimal sebesar 75% dari total biaya yang dibutuhkan, sebagaimana terlihat pada gambar 4.9. Pada gambar terlihat bahwa risiko DNS software problem dan GI link failure memberikan nilai manfaat terbesar yaitu Rp 325.108.000 karena telah dibiayai secara penuh. Disusul kemudian secara berurut oleh SS7 routing error, radius software problem, SS7 signaling link down, dan GGSN software problem, yang juga dibiayai penuh, masing-masing tetap berkontribusi memberikan nilai manfaat yang besar namun tidak sebesar yang diberikan oleh DNS software problem dan GI link failure. Hal ini dapat disebabkan oleh tingkat dampak dan biaya *treatment* yang diperlukan dari masing-masing risiko yang berbeda.

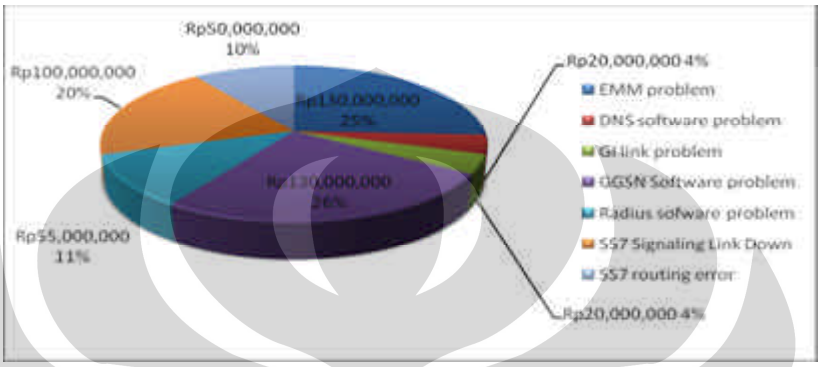


Gambar 4.9 Nilai Manfaat dari setiap Risiko Kritis dengan Asumsi Ketersediaan Dana Maksimal sebesar 75% dari Total Biaya yang Dibutuhkan

4.2.4 Asumsi Ketersediaan Dana sebesar Total Biaya yang Dibutuhkan (100%)

Untuk kondisi saat perusahaan dapat dengan penuh mendanai seluruh dengan biaya *treatment* yang diperlukan yaitu sebesar Rp505.000.000, maka komposisi alokasi dana untuk setiap risiko kritis yang dihasilkan dapat dilihat pada gambar 4.10. Dari 100% dana yang ada, sekitar 26% dialokasikan untuk *treatment* risiko GGSN

software problem, 25% untuk *treatment* risiko EMM problem, 20% untuk *treatment* risiko SS7 signaling link down, 11% untuk *treatment* risiko radius software problem, 10% untuk *treatment* risiko SS7 routing error, dan masing-masing 4% untuk DNS software problem dan GI link problem.

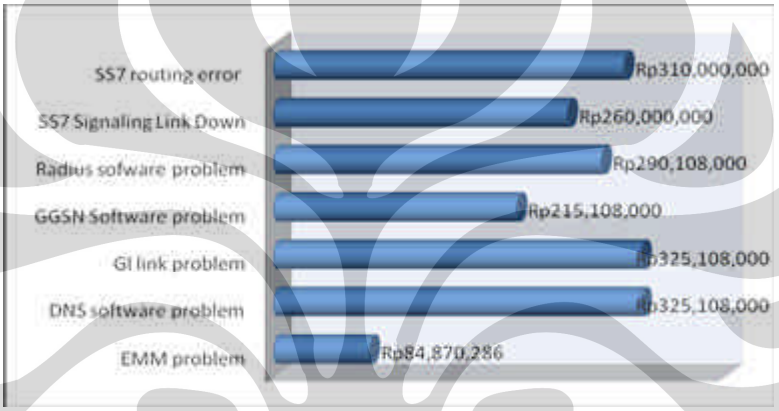


Gambar 4.10 Komposisi Alokasi Biaya *Treatment* untuk setiap Risiko Kritis dengan Asumsi Ketersediaan Dana sebesar 100% dari Total Biaya yang Dibutuhkan

Dengan tersedianya dana penuh untuk membiayai *treatment* risiko, maka semua risiko yang ada dapat dibiayai sepenuhnya sebagaimana terlihat pada gambar 4.11.

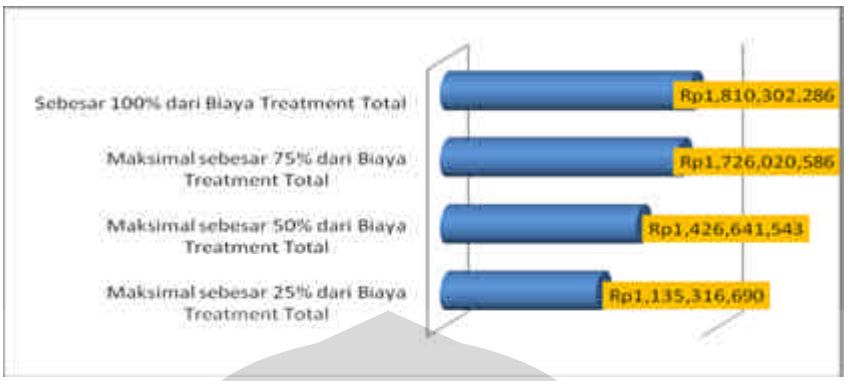
Gambar 4.11 Perbandingan Biaya *Treatment* Ideal dan Biaya *Treatment* yang Dialokasikan dengan Asumsi Ketersediaan Dana sebesar 100% dari Total Biaya yang Dibutuhkan

Nilai *maximum advantage* yang diperoleh dengan kondisi kebutuhan biaya *treatment* yang dapat dibiayai secara penuh merupakan total *advantage* tertinggi yaitu sebesar Rp1.810.302.286. Nilai total *advantage* tersebut berasal dari nilai *advantage* masing-masing risiko pada kondisi semua *treatment* item risiko dapat dibiayai secara penuh, sebagaimana terlihat pada gambar 4.12. Pada gambar terlihat bahwa risiko DNS software problem dan GI link failure memberikan kontribusi terbesar pada nilai total *advantage* yaitu Rp 325.108.000. Dan yang berkontribusi paling rendah terhadap total *advantage* adalah EMM problem.



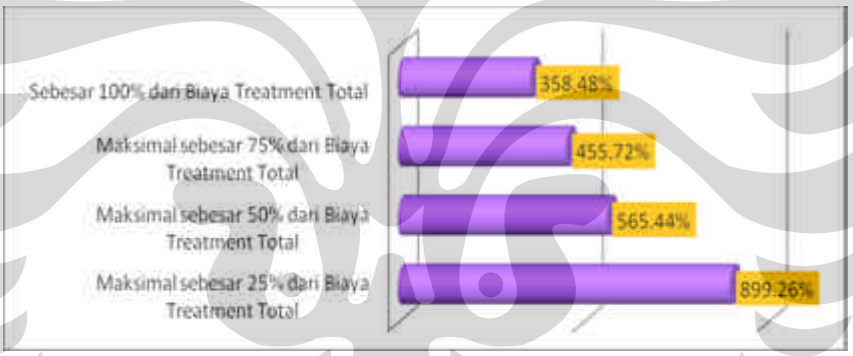
Gambar 4.12 Nilai Manfaat dengan Asumsi Ketersediaan Dana sebesar 100% dari Total Biaya yang Dibutuhkan

Dapat terlihat bahwa DNS software problem dan GI link failure yang hanya memerlukan 4% dari total biaya *treatment* ternyata berkontribusi paling besar terhadap *maximum total advantage,* lain halnya dengan EMM problem yang memerlukan sekitar 25% dari total biaya *treatment* dan memberikan kontribusi terendah terhadap *maximum total advantage*.



Gambar 4.13 Total Advantage pada Tiap Kondisi Ketersediaan Dana

Berdasarkan hasil simulasi, menunjukkan bahwa semakin besar alokasi dana yang diberikan maka *total advantage* yang diperoleh akan semakin besar pula, hal ini dapat dilihat pada gambar 4.13.



Gambar 4.14 Perbandingan Prosentase Total Advantage terhadap Alokasi Dana yang Diberikan untuk Tiap Kondisi Ketersediaan Dana

Meskipun *total advantage* yang diperoleh berbanding lurus dengan alokasi dana yang diberikan, namun prosentase *total advantage* terhadap alokasi dana yang diberikan pada kondisi ketersediaan dana maksimal sebesar 25% dari biaya total *treatment* menunjukkan angka tertinggi yaitu 899,26% yang artinya bahwa pada alokasi dana tersebut memberikan keuntungan hingga hampir 9 (sembilan) kali lipat. Nilai prosentase tersebut semakin menurun dengan semakin bertambahnya alokasi dana yang diberikan, hal ini dapat dilihat pada gambar 4.14.

BAB V
KESIMPULAN

5.1 Kesimpulan

Berdasarkan hasil pengolahan data dan analisis yang telah dilakukan, maka terkait dengan tujuan penelitian ini dapat disimpulkan beberapa hal sebagai berikut :

1. Terdapat 8 item risiko kritis dari 28 risiko yang teridentifikasi yaitu EMM problem, GGSN-Radius link problem, DNS software problem, GI link problem, GGSN software problem, Radius software problem, SS7 signaling link down, dan SS7 routing error.
2. Setiap risiko kritis akan memperoleh usulan tindakan penanganan yang berbeda-beda. Usulan tindakan penanganan risiko kritis dilakukan dengan mengurangi risiko (*Risk Mitigation*) dan memindahtangankan penanggung jawab risiko (*Risk Transfer*).
3. Hasil alokasi biaya dengan menggunakan OptQuest dapat dilihat pada bagian pengolahan dan analisis data. Semakin besar dana yang dialokasikan untuk melakukan *treatment* atas risiko kritis yang ada, maka semakin besar pula total manfaat yang diperoleh.

5.2 Usulan

Pada waktu mendatang, penelitian ini dapat dikembangkan lebih lanjut dengan melakukan studi komprehensif terhadap setiap faktor risiko yang dimungkinkan terjadi seiring dengan kemajuan teknologi yang bersifat dinamis. Selanjutnya dapat pula dikembangkan segala kemungkinan alternatif penyelesaian masalah, sehingga pada akhirnya kerangka berfikir ini dapat dijadikan standar analisis risiko kegagalan pada *core network* perangkat GPRS. Materi penelitian pun dapat difokuskan dengan melakukan analisis risiko pada aplikasi 3G ataupun Blackberry.

DAFTAR REFERENSI

Alvarez, Gene. *Operational Risk Event Classification*. October 2, 2008. www.ic2.zurich.com.

Australia/New Zealand Risk Management Guideline (AS/NZS 4360:2004).

Canterprise Board. (2006). *Risk Management and Compliance Framework*, University of Canterbury. New Zealand.

Carbone, T & Tippett, D. (2004). Project Risk Management Using the Project Risk FMEA. *Engineering Management Journal.* Vol 16, No.4. hal 31.

Claire Lee Reiss. (2001). *Risk Identification and Analysis : A Guide for Small Public Entities.*

Crystal Ball® 7.2.2 User Manual.

Dilan, S. Batuparan. (2001). Kerangka Kerja *Risk Management,* EI News, Edisi 5.

G. Stoneburner, A. Goguen, A. Feringa, (2001). *Risk Management Guide for Information Technology Sistem*, dalam *Recommendations of the National Institute of Standards and Technology,* National Institute of Standards and Technology, U.S. Government Printing Offiice, Washington.

Harold Kerzner,(20060. *Project Management, A System Approach to Planning, Scheduling, and Controlling 9th ed*. John Wiley & Sons, Inc.

Information Risk Management. *GPRS/3G Services : Security.* O2 White Paper.

Jay Tarakkumar Shah. (2004). *Probabilistic Risk Assessment Method for Prioritization Of Risk Faktors,* MSc Thesis, Gujarat University.

Misra C.S. (2006). *Differrent Techniques for Risk Management in Software Engineering : A Review.* ASAC. Banff, Alberta.

Project Management Institute. (2000) .*A Guide to The Project Management Body of Knowledge : PMBOK Guide.* Pennsylvania : Project Management Institute, Inc.

Ronald L. Meier. (2000). Integrating Enterprise-Wide Risk Management Concepts into Industrial Technology Curricula. *Journal of Industrial Technology.* Vol16.

The COSO Framework : An Overview, Journal of Accountancy, 2002.