# ANALISA RISIKO OPERASIONAL DI DIVISI NETWORK OPERATION CENTER (NOC) PADA PT. INDOSAT OOREDOO

**Oleh :**
**Rindu Eka Bakti Tarigan: Pasca Sarjana Uki**
**Dr. Poerwaningsih Soekarno, M.STr: Dosen UKI**
**Dr. Wilson Rajagukguk, M.Si., M.A:Dosen UKI**
**Email:pps-mih@uki.ac.id**

## Abstarksi

Risiko-risiko yang muncul dalam perusahaan dapat memberikan dampak positif terhadap kualitas layanan yang diberikan kepada para pelanggan terutama dalam network system, sehingga dibutuhkan penanganan atau manajemen terhadap risiko, agar dapat memberikan dampak positif bagi kepuasan konsumen perusahaan.

Indosat seperti juga perusahaan lainnya selalu menjaga agar risiko yang terjadi di perusahaan dapat dikendalikan seminimal mungkin. Namun pada kenyataannya saat bekerja ada saja karyawan yang tidak menjalankan Standard of Procedure (SOP) di pekerjaannya dengan baik sehingga dapat merugikan buat perusahaan.

Pada penelitian ini, data yang digunakan adalah data risiko Operasional yang terjadi di PT Indosat Ooredoo Tbk. Mengenai pendekatan penelitian, penetapan informan, sumber data, dan teknik analisis yang digunakan dalam penelitian ini adalah, menggunakan Metode penelitian kualitatif, dengan tujuan mengidentifikasi, mengukur, dan mengelola risiko operasional pada Divisi Network Operation Center PT Indosat Ooredoo Tbk.

Berdasarkan analisis dan evaluasi yang dilakukan maka didapatkan beberapa kesimpulan Risiko Operasional di divisi Network Operation Center PT. Indosat Ooredoo Tbk yang teridentifikasi dari hasil penelitian ini terdiri atas 9 jenis yang meliputi 49 risiko dari departemen yang ada di divisi tersebut.

## I. PENDAHULUAN

### 1.1. Latar Belakang

Setiap perusahaan yang menghasilkan barang dan jasa mempunyai tujuan untuk mensejahterakan stakeholdernya. Begitu juga perusahaan yang bergerak dibidang telekomunikasi seperti PT Indosat Tbk yang mempunyai modal besar untuk menggerakkan roda bisnisnya dibidang telekomunikasi dan digital. Tujuan Indosat selalu berusaha memberikan yang terbaik kepada stakeholder terutama pemegang sahamnya. Namun Indosat seperti juga perusahaan lainnya selalu menjaga agar risiko yang terjadi di perusahaan dapat dikendalikan seminimal mungkin. Kenyataannya saat bekerja ada saja karyawan yang tidak menjalankan Standard of Procedure (SOP) di pekerjaannya dengan baik sehingga dapat merugikan buat perusahaan. Pada tahun 2014 Indosat pernah mengalami kerugian diatas 5 Miliar karena

network Indosat down dan hampir seharian problem sehingga pelanggan merasakan dampaknya dan complain terhadap Indosat Ooredoo. Setelah di evaluas, diteliti dan diidentifikasi maka didapatkan root causenya bahwa ada karyawan yang teridentifikasi melakukan pelanggaran terhadap SOP. Sehingga karyawan tersebut ada yang di beri sanksi Surat Peringatan (SP) dan ada yang mendapat teguran lisan. Untuk mengantisipasi hal ini maka PT Indosat Ooredoo selalu memperbaiki SOP dan pengawasan yang ada. Dan mitigasi yang dilakukan oleh Indosat selain mendapatkan masukan dari internal juga meminta masukan dari eksternal seperti konsultan.

Dalam dunia bisnis, dinamisnya industri seluler serta meningkatnya persaingan menimbulkan risiko di perusahaan baik dari eksternal maupun dari internal. Perusahaan mengantisipasi risiko yang terjadi melalui pengelolaan risiko oleh manajemen perusahaan. Manajemen perusahaan secara terus menerus mengelola risiko dengan melakukan aktivitas-aktivitas pengelolaan risiko diantaranya mengidentifikasi risiko perusahaan, melakukan pengukuran risiko, penentuan perusahaan melalui respon yang diberikan terhadap risiko, aktivita perusahaan dalam mengendalikan risiko, mengkomunikasikan risiko yang akan dihadapi perusahaan dan pemantauan risiko dari setiap kegiatan yang dilaksanakan oleh perusahaan. Manajemen risiko juga merupakan suatu sistem pengelolaan risiko dan perlindungan terhadap harta benda, hak milik dan keuntungan perusahaan atas kemungkinan timbulnya kerugian karena adanya risiko.

Hasil penelitian risiko operasional yang dilakukan oleh Nurtjahyo dkk (2008) pada perusahaan pembuatan mesin motor diidentifikasi ada lima faktor risiko operasional yang didapatkan melalui proses survey dan observasi di lapangan yakni ketersediaan materail part bagi produksi dengan nilai rata-rata 4,33; risiko yang disebabkan oleh ketersediaan tools atau peralatan kerja dengan nilai rata-rata 3,87; risiko yang disebabkan oleh tenaga kerja didapatkan nilai 3,53; risiko yang disebabkan oleh metode kerja atau prosedur kerja yang tidak jelas dengan nilai rata-rata 3,87 dan terakhir risiko yang disebabkan oleh keadaan lingkungan di sekitar tempat kerja dengan nilai rata-rata 2,87. Penelitian risiko operasional yang dilakukan oleh Dewi (2012) dengan melakukan observasi lapangan pada industri nasional sebagai masukan untuk program PLTN didapatkan sebagai berikut: risiko kapasitas produksi, risiko perubahan tukar mata uang, risiko kualifikasi sumber daya manusia, risiko perubahan harga material, dan risiko perubahan suku bunga bank. Perusahaan PT Krakatau Steel yang bergerak dibidang manufaktur baja memaparkan risiko operasional perusahaan antara lain Risiko pengembangan teknologi, risiko pengembangan produk baru, Risiko ketenagakerjaan (Sumber Daya Manusia), Risiko kekurangan material, Risiko kekurangan energi, Risiko Lingkungan (polusi, gangguan sosial), risiko proses produksi dengan preventif maintenance, risiko sistem pengendalian kualitas produk.

Penelitian risiko operasional pada perusahaan yang dilakukan oleh Tedford (2012) di New Zealand dengan melakukan wawancara pada pengalaman para eksekutif perusahaan manufaktur dengan mengembangkan model assesment risk pada bagian operasional. Hasil penelitian Tedford menyatakan bahwa persepsi manajer pada perusahaan manufaktur masih sebatas pada risiko kesehatan dan keselamatan kerja karyawan, namun pada hasil peneliti mengusulkan agar perusahaan melakukan tahapan untuk mengidentifikasi risiko operasional yakni pertama identifikasi risiko operasional secara kuantitatif dan kualitatif kejadian kecelakaan kerja dengan memperhitungkan waktu yang hilang dan dampaknya pada perusahaan, kedua tahap pengembangan yakni organisasi harus mampu membuat sistem feedback dan assesment loop bagi setiap kejadian dan menginformasikan kepada bagian yang terkait. Ketiga measurement yakni organisasi harus mampu mengukur efek konsekuensi dari kejadian. Tahap keempat Assesment yakni organisasi harus mampu untuk menilai risiko terkait dengan gangguan yang terjadi, dan kelima analysis yakni organisasi harus mampu memprioritaskan tindakan untuk mengurangi kejadian, mengendalikan dan mengelola risiko. Tahap ketujuh dan terakhir adaptasi dan perbaikan yakni organisasi mampu belajar dari peristiwa masa lalu dalam membangun mekanisme kontrol dan mengevaluasi risiko lebih lanjut. Ini akan dapat menghilangkan, mengendalikan dan mengelola risiko diantisipasi sebagai bagian dari proses belajar yang berkesinambungan.

Banyaknya implementasi manajemen risiko pada perusahaan-perusahaan yang dikelola untuk dapat meningkatkan nilai bagi perusahaan sehingga akan berdampak pada profit perusahaan. Indosat sendiri sangat memperhatikan risiko manajemen di perusahaan dengan dibentuknya be-

berapa Divisi yang menangani risiko manajemen. Manajemen risiko (Risk Management) yang dilakukan di PT. Indosat, Tbk mengacu pada ISO 31000:2009 (Risk Management). Risiko-risiko yang muncul dalam perusahaan dapat memberikan dampak positif terhadap kualitas layanan yang diberikan kepada para pelanggan terutama dalam network system, sehingga dibutuhkan penanganan atau manajemen terhadap risiko, sehingga memberikan dampak positif bagi kepuasan konsumen perusahaan. Penelitian ini memfokuskan pada identifikasi faktor-faktor risiko operasional dan menganalisa faktor dan mengendalikan faktor risiko secara berkesinambungan pada perusahaan PT. Indosat untuk meningkatkan kualitas layanan kepada pelanggan dari sisi sistem networking.

## II. LANDASAN TEORI

### 2.1 Definisi Risiko dan Risiko Operasional

Setiap perusahaan yang bisnisnya dibidang telekomunikasi dengan modal yang besar dan usaha yang besar mempunyai banyak permasalahan dalam menjalankan proses organisasi tersebut. Masalah masalah di perusahaan tersebut dapat menimbulkan risiko dan mendapat kerugian yang besar atau kecil tergantung dari apa penyebab risiko dan bagaimana cara penanganannya untuk meminimalisir risiko tersebut. Sebenarnya apakah yang dimaksud dengan risiko itu? T. Sunaryo (Jakarta, 2007, p.12) risiko adalah kerugian karena kejadian yang tidak di harapkan muncul. Sedangkan risiko Operasional menurut:

1. Muhammad Muslich (Jakarta, 2007, p.5) risiko operasional merupakan kerugian finansial yang di sebabkan oleh kegagalan proses internal, kesalahan sumber daya manusia, kegagalan sistem, kerugian yang di sebabkan kejadian dari luar perusahaan, dan kerugian karena pelanggaran peraturan dan hukum yang berlaku
2. James Lam (Jakarta, 2007, p.210) risiko operasional adalah kerugian langsung atau tidak langsung dari ketidak memadai atau kegagalan proses internal, manusia, dan sistem, atau dari peristiwa eksternal.
3. H. Masyhud Ali (Jakarta, 2006, p.272) operational risk di definisikan sebagai risiko kerugian yang terjadi sebagai akibat dari inadequate atau failed internal processes, people dan system atau sebagai akibat dari external events
4. Sulad Sri Hardanto (Jakarta, 2006, p.130) risiko operasional sebagai risiko kerugian yang di sebabkan oleh kegagalan atau ketidak cukupan (tidak memadainya) proses internal, manusia dan sistem atau dari kejadian eksternal
5. Mamduh M. Hanafi (Jakarta, 2006, p.371) risiko operasional di definisikan sebagai risiko kerugian karena proses internal yang tidak memadai atau gagal, sistem dan orang, dan dari kejadian eksternal

#### 2.1.1 Sumber Risiko Operasional

Mamduh M. Hanafi (Jakarta 2009, p.194) sumber-sumber dari risiko operasional :

1. Kegagalan proses internal merupakan risiko yang berkaitan dengan kegagalan proses atau prosedur internal organisasi. Contoh:

a. Risiko yang di akibatkan kurang lengkapnya dokumentasi, atau dokumentasi yang salah
b. Kesalahan transaksi
c. Pengawasan yang kurang memadai
d. Pelaporan yang kurang memadai sehingga kepatuhan terhadap peraturan internal dan eksternal tidak terpenuhi

2. Risiko kegagalan mengelola manusia (karyawan) : karyawan merupakan aset penting bagi perusahaan, tetapi juga merupakan sumber risiko operasional bagi perusahaan. Risiko dari karyawan tersebut akan terjadi baik secara sengaja maupun secara tidak sengaja. Contoh risiko operasional yang bersumber dari manusia

a. Kecelakaan kerja, khususnya kecelakaan kerja karena kecerobohan atau kurang pengalaman dari karyawan
b. Terlalu bergantung pada karyawan yang memegang kunci tertentu, sehingga jika karyawan tersebut meninggal atau berpindah kerja, perusahaan menghadapi masalah
c. Integritas karyawan yang kurang, sehingga karyawan tersebut bisa menggelapkan uang perusahaan, atau melakukan aktifitas yang berada di luar wilayah otoritasnya

3. Risiko Sistem: Sistem teknologi bisa memberikan kontribusi yang signifikan bagi organisasi, di lain pihak, sistem tersebut akan memunculkan risiko baru bagi organisasi. Beberapa risiko yang muncul berkaitan dengan sistem :

a. Kerusakan data
b. Kesalahanan pemrograman

c. Sistem keamanan yang kurang baik (misal, bisa dimasuki oleh hecker)
d. Penggunaan teknologi yang belum teruji
e. Terlalu mengandalkan model tertentu untuk keputusan bisnis

4. Risiko Eksternal berkaitan dengan kejadian yang bersumber dari luar organisasi, dan di luar pengendalian organisasi. Kejadian semacam itu biasanya jarang terjadi, tetapi mempunyai dampak yang cukup besar (frekuensi rendah/severity tinggi).

Untuk menegaskan makna proses tersebut, lihat Inu Kencana Syafiie (2014, p.1) proses adalah suatu kumpulan aktifitas pekerjaan-pekerjaan yang seharusnya terstruktur, tersistem, harmonis, dan teratur sesuai dengan ruang dan waktu yang saling mengkait untuk mengolah dan menyelesaikan masalah tertentu yang selanjutnya menghasilkan suatu keluaran ataupun pelayanan tertentu sesuai dengan keahliah dan sumber daya yang tersedia.

### 2.1.2 Klasifikasi Risiko

1. Klasifikasi risiko korporat adalah sebagai berikut ini: (Bramantyo Djohanputro, 2008, p.35), lihat gambar di bawah ini:

2. Peraturan menteri keuangan No 191/PMK.09/2008 tentang penerapan manajemen risiko di lingkungan departemen keuangan. Pasal 1 :

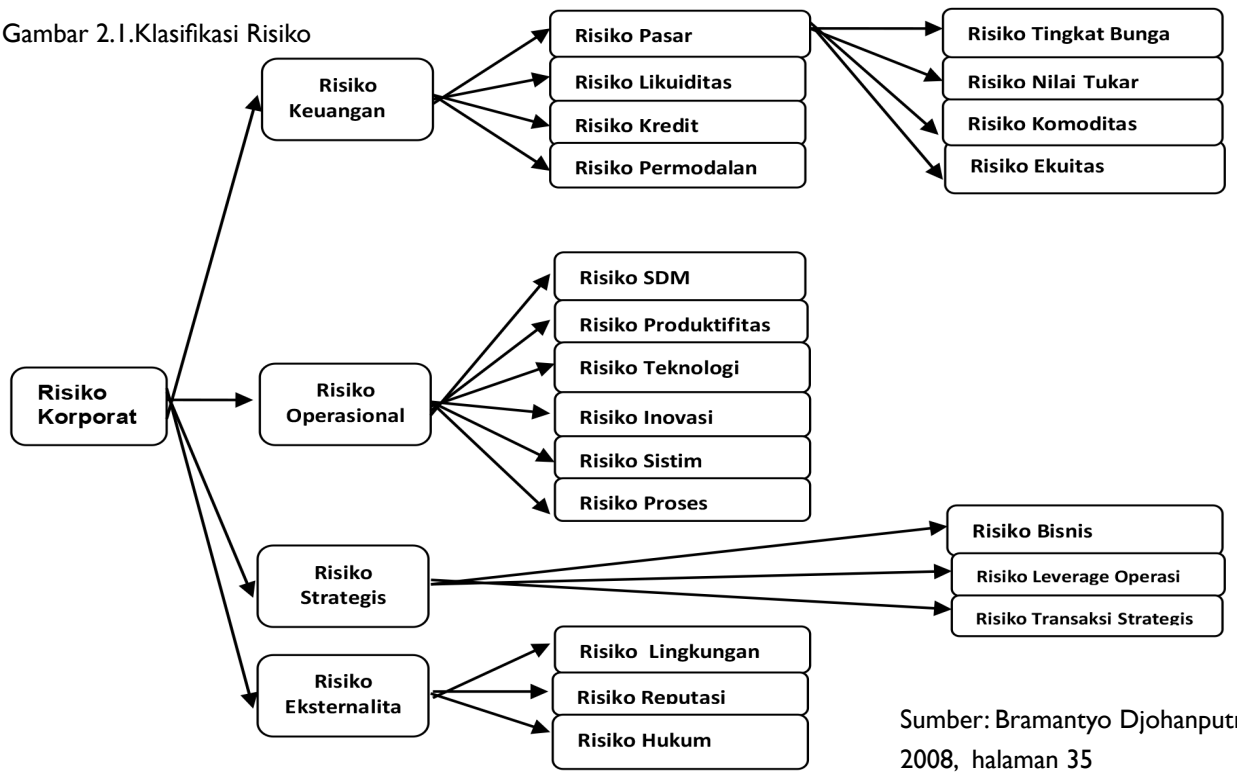
a. Manajemen risiko adalah pendekatan sistematis untuk menentukan tindakan terbaik dalam kondisi ketidak pastian
b. Risiko adalah segala sesuatu yang berdampak negatif terhadap pencapaian tujuan yang di ukur berdasarkan kemungkinan dan dampaknya
c. Compliance officer for risk management adalah inspektorat jenderal yang bertugas melaksanakan audit terhadap penerapan manajemen risiko pada unit eselon I di lingkungan departemen keuangan.

Dan pasal 6 ayat 1 proses manajemen risiko terdiri dari :

a. Penetapan konteks
b. Identifikasi risiko
c. Analisis risiko
d. Evaluasi risiko
e. Penanganan risiko
f. Monitoring risiko
g. Komunikasi dan konsultasi

3. Peraturan Pemerintah Republik Indonesia No 60 tahun 2008 tentang sistem pengendalian intern pe-

Gambar 2.1.Klasifikasi Risiko




Sumber: Bramantyo Djohanputro, 2008, halaman 35

merintah. Pasal 3 huruf b di jelaskan tentang unsur penilaian risiko. Sedangkan pasal 13 penilaian risiko tersebut antara lain :

a. Pimpinan instansi pemerintah wajib melakukan penilaian risiko
b. Penilaian risiko sebagaimana dimaksud pada ayat (1) terdiri atas :
    1. Identifikasi risiko
    2. Analisis risiko
c. Dalam rangka penilaian risiko sebagaimana dimaksud pada ayat (1) pimpinan instansi pemerintah menetapkan :
    1. Tujuan instansi pemerintah dan
    2. Tujuan pada tingkatan kerugian, dengan berpedoman pada peraturan perundang-undangan

### 2.1.3 Jenis Risiko Operasional dan Pemicu Terjadi Fraud

Sulad Sri Hardanto (2006, p.131) mengemukakan beberapa jenis risiko operasional, seperti fraud dan kesalahan pemrosesan, sering terjadi.

Menurut Dewi Hanggraeni (2010, p.152) Fraud dapat di picu oleh :

1. Adanya motif. Seorang fraudster (orang yang melakukan fraud) tentunya memiliki motif tertentu untuk melakukan motif fraud. Bisa saja terdesak oleh kebutuhan ekonomi atau karena merasa dendam terhadap perusahaan tempatnya bekerja.
2. Adanya peluang. Peluang dalam hal ini mencakup peluang untuk mencuri maupun peluang untuk menjual barang curian kembali.
3. Kurangnya kontrol. Kurangnya kontrol dari manajemen akan memperbesar peluang dari terjadinya fraud.

Lebih lanjut menurut Husein Umar (2001, p.96) kecurangan dapat di lakukan oleh kelompok-kelompok orang dalam perusahaan :

1. Blue color worker. Mereka dapat mencuri barang-barang, terutama yang sulit di deteksi saat mereka keluar kantor.
2. Clerical worker. Mereka yang menangani langsung kertas-kertas kerja dan sering di percaya, sehingga mereka dapat melakukan pemalsuan-pemalsuan angka atau menghilangkan dokumen atau menjual informasi pada pesaing.
3. Manager (white color worker) mereka dapat menyetujui faktur-faktur palsu milik perusahaan sendiri.

Sedangkan Amin Widjaya Tunggal (2014, p.13) kecurangan paling sering terjadi bila:

1. Pengendalian internal tidak ada, lemah atau di lakukan dengan longgar
2. Pegawai di pekerjakan tanpa memikirkan kejujuran dan integritas mereka
3. Pegawai di atur, di eksploitasi dengan tidak baik, di salah gunakan atau di tempatkan dengan tekanan yang besar untuk mencapai sasaran dan tujuan keuangan
4. Model manajemen sendiri korupsi, tidak efisien atau tidak cakap
5. Pegawai yang di percaya memiliki masalah pribadi yang tidak dapat di pecahkan, biasanya masalah keuangan, kebutuhan kesehatan keluarga, atau kecanduan alkohol, obat terlarang, judi yang berlebihan, atau selera yang mahal
6. Industri di mana perusahaan menjadi bagiannya, memiliki sejarah atau tradisi korupsi
7. Perusahaan jatuh pada saat yang tidak tepat, misalnya kehilangan uang atau saham produk atau pelayanannya menjadi kuno.

### 2.1.4 Penyebab Bahaya (Peril dan Hazard)

Herman Darmawai (2004, p.22) peril adalah suatu peristiwa yang dapat menimbulkan kerugian. Sedangkan hazard adalah keadaan dan kondisi yang dapat memperbesar kemungkinan terjadinya suatu peril. Peril dan hazard lebih erat hubunganya kepada kemungkinan dari pada risiko :

1. Peril (bencana, musibah) di definisikan sebagai penyebab langsung kerugian
2. Hazard (bahaya) keadaan yang menimbulkan atau meningkatkan terjadinya chance of loss dari suatu bencana tertentu

Lebih lanjut Hinsa Siahaan (2007, p.106) secara garis besar hazard di kelompokkan :

1. Physycal hazard adalah kondisi fisik yang mendorong atau memperbesar kemungkinan terjadinya peril

2. Moral hazard adalah ketidak jujuran atau karakter jelek seseorang yang mendorong keseringan terjadinya kerugian atau memperparah kerugian yang terjadi
3. Morale hazard adalah kelalaian atau kecerobohan seseorang

**2.1.5 Tahapan Manajemen Risiko**

Menurut T. Sunaryo (2007, p.12) proses manajemen risiko ada 3 tahap :

1. Identifikasi risiko
2. Mengukur risiko
3. Manajemen risiko

**2.1.6 Hal Penting Dalam Identifikasi Risiko Operasional**

Ikatan Bankir Indonesia (2015, p.148) hal utama yang diperlukan dalam melakukan identifikasi risiko operasional:

1. Adanya kejadian (events)
2. Terdapat penyebab timbulnya kejadian (cause)
3. Terdapat dampak (impact) kerugian (loss) baik dalam bentuk keuangan maupun non-keuangan
4. Dapat diprediksi terjadinya di kemudian hari (frequency/probability)

**2.1.7 Teknik Identifikasi Risiko Operasional**

Muhammad Muslich (2007, p.10) mengemukakan beberapa teknik identifikasi risiko operasional:

1. Risk Self Assessment (RSA), adalah perusahaan melakukan penilaian sendiri terhadap aktivitas dan operasi perusahaan berdasarkan kejadian risiko. Proses RSA ini di dasarkan keinginan perusahaan sendiri untuk mengidentifikasi kekuatan dan kelemahandari lingkungan risiko operasional. Proses penilaian RSA di lakukan dengan mempergunakan suatu daftar checklists yang berisi butir-butir pertanyaan tentang evaluasi kekuatan dan kelemahan lingkungan risiko operasinal tersebut
2. Risk Mapping, merupakan suatu proses di mana berbagai unit usaha atau departemen, fungsional organisasi, atau arus proses transaksi yang di- mapping berdasarkan tipe risiko
3. Key Risk Indicator atau data statistik keuangan yang dapat memberikan gambaran tentang posisi risiko operasional perusahaan. Indikator ini harus di kaji ulang sekurang-kurangnya setiap triwulan untuk dapat memberikan peringatan tentang terjadinya perubahan yang mengindikasikan adanya risiko yang sedang menjadi bahan pemantauan.
4. Limit threshold, menunjukkan batas kerugian yang dapat di jadikan ukuran toleransi risiko yang di terima. Dengan limit limit threshold ini manajemen perusahaan dapat menentukan di bidang dan tipe risiko yang manakah yang perlu mendapat perhatian.
5. Scorecard, merupakan suatu alat untuk mengkoversi penilaian pengelolaan dan pengendalian berbagai aspek kerugian risiko operasional yang bersifat kualitatif menjadi perhitungan yang bersifat kuantitatif. Selanjutnya, dalam mengidentifikasi risiko operasional, perusahaan harus memerhatikan hal-hal berikut :

a. Bersifat proaktif, antisipatif dan bukan reaktif
b. Identifikasi risiko operasional harus mencakup seluruh aktivitas fungsional
c. Menggabungkan dan menganalisis seluruh risiko operasional dari seluruh sumber informasi yang tersedia.

**2.1.8 Teknik Pengukuran Risiko Operasional**

Mamduh M. Hanafi (2006, p.208) salah satu teknik untuk mengukur risiko operasional dengan menggunakan dua klasifikasi :

1. Frekuensi atau probabilitas terjadinya risiko
2. Tingkat keseriusan kerugian atau impact dari risiko tersebut

**2.1.9 Teknik Pengelolaan Risiko Operasional**

Lihat Bramantya Djohanputro (2004, p.210) pada prinsipnya empat teknik pengelolaan risiko:

1. Penghindaran risiko. Perusahaan tidak mengambil tindakan yang dapat memunculkan risiko tertentu. Risiko yang di hindari; tidak sesuai dengan visi perusahaan, dampak sosial terlalu besar, peraturan yang tidak kondusif, total risiko portofolio usaha melebihi batas ambang
2. Pengurangan risiko. Menghindari peril (penyebab) timbulnya risiko, mengambil berbagai tindakan berisiko yang saling menghilangkan secara alamiah (Natural Hedging), Diversifikasi, (mengurangi risiko den-

gan cara menyebar aktivitas usaha)

3. Pemindahan Risiko. Asuransi (untuk aset riil), berbagi bentuk lindung nilai (untuk aset keuangan, Option mirip asuransi),
4. Penanganan risiko. Penanganan risiko terencana (sengaja menangani/menanggung risiko, berdasarkan profil cost-benefit). Penanganan risiko tidak terencana (ketidakmampuan mengidentifikasi risiko, kelalaian mengidentifikasi risiko, risiko yang di abaikan)

Lebih lanjut, James Lam (2007, p.210) bahwa fokus dari program risiko operasional haruslah pada pengelolaan, bukan pada pengukuran. Sejalan dengan pendapat tersebut, T. Sunaryo (2007, p.11) untuk risiko operasional, risiko yang di sebabkan oleh kegagalan atau kesalahan orang, proses sistem dan faktor eksternal, tentu saja lebih cocok dengan solusi perilaku dan pendekatan institusional.

Untuk mempertegas pendapat tersebut, Miriam Budiardjo (2008 : 72) mengemukakan dua pendekatan :

1. Pendekatan legal/ institusional. Pendekatan ini mencakup baik unsur legal maupun unsur institusional.
2. Pendekatan Perilaku. Pendekatan ini mengamati manusia (pelaku atau aktor) seperti bagaimana mereka menjalankan tugas, dan bagaimana mereka memandang perilaku mereka sendiri.

### 2.1.10 Teknik Menentukan Frequency dan Impact Risiko Operasional

Untuk melakukan asesment seberapa sering frequency terjadi operational risk dan seberapa besar impact kerugian yang di derita, Ikatan Bankir Indonesia (2015, p.156) mengklasifikasikan ke dalam matriks :

1. Low frequency/ low impact
2. Low frequency/ high impact
3. High frequency/ low impact
4. High frequency/ high impact

Sedangkan Simon A Burtonshaw-Gunn (2011, p.229) mengemukakan model tiga pertanyaan yang saling berkaitan dan proses yang memfasilitas jawaban atasnya pada inti analisis risiko

Gambar 2.2. Menentukan Frequency dan Impact Risiko


Sumber: Simon A Burtonshaw-Gunn, 2011, halaman 229

### 2.1.11 Manfaat Manajemen Risiko Operasional

James Lam (2007, p.209) menjelaskan manajemen risiko operasional yang efektif memiliki potensi untuk memberikan tiga manfaat secara jelas.

1. Manajemen risiko operasional yang ketat harus meminimalkan kerugian harian sekaligus mengurangi potensi terjadinya peristiwa yang lebih besar akibatnya
2. Manajemen risiko operasional yang efektif meningkatkan kemampuan perusahaan untuk mencapai sasaran bisnisnya
3. Terakhir, akuntansi bagi risiko operasional memperkuat seluruh sistem manajemen risiko perusahaan

### 2.1.12 Kerugian Karena Kejadian Yang Tidak di Kehendaki Muncul

Menurut Kasidi (2010, p.46) kerugian akibat kejadian buruk yang mungkin terjadi dapat di kelompokkan :

1. Kerugian langsung, mempunyai dampak langsung terhadap harta benda.
2. Kerugian tidak langsung, mempunyai dampak tidak langsung terhadap benda
3. Kerugian tidak langsung dapat mempunyai elemen waktu jika di libatkan dalam perhitungan kerugian tersebut

Lebih lanjut, Herman Darmawi (2004, p.161) kerugian yang sifatnya langsung dan tidak langsung

1. Menurunnya pendapatan, meliputi (Kerugian sewa, terganggunya kegiatan perusahaan,terganggunya operasi perusahaan pemasok dan pemakai, berkurangnya laba pada barang jadi, pengumpulan piutang mengecil)

2. Meningkatnya biaya-biaya, meliputi (Kerugian nilai sewa, pengeluaran ekstra agar perusahaan tetap beroperasi, penundaan leasing, kerugian penggunaan oleh penyewa yang terpaksa harus dipindahkan selama masa perbaikan)

Dari beberapa pendapat ahli tersebut, dapat di uraikan risiko operasional adalah potensi kerugian karena kegagalan manusia dalam proses menjalankan operasinya. Risiko operasional tersebut apabila terjadi dapat memicu risiko lain :

1. Risiko kegagalan proses internal merupakan risiko yang berkaitan dengan kegagalan proses atau prosedur internal organisasi (Mahmud M. Hanafi, 2006, p. 206)
2. Reputation risk adalah kemungkinan terjadinya kerusakan potensial yang dapat menimpa perusahaan sebagai akibat beredarnya publik opini yang negatif (H. Masyhud Ali, 2006, p.38)
3. Risiko sosial. Sumber utama risiko ini dari masyarakat. Artinya, tindakan orang–orang menciptakan kejadian yang menyebabkan penyimpangan merugikan. Misalnya; vandalisme, huru-hara, peperangan dan sebagainya. (Kasidi, 2010, p.7)
4. Legal risk adalah risiko yang berakar dari terdapatnya ketidakpastian terkait dengan efektifitasnya langkah hukum (legal actions) atau ketidak pastian dalam penerapan atau penafsiran (intepretation) isi suatu contracts, lows atau regulations. (H. Masyhud Ali, 2006, p.292)
5. Risiko politik adalah sebagai kejadian di negara tujuan investasi (host) yang bisa menggangu aliran kas perusahaan multinasional (Mahmud M. Hanafi, 2006, p.254)
6. Risiko fraud adalah risiko yang di alami oleh suatu perusahaan atau institusi karena faktor terjadinya tindakan fraud atau kecurangan yang di sengaja, baik kerugian yang bersifat materi maupun non mater, di mana kerugian materi di ukur dari segi nilai finansial dengan mengacu pada mata uang yang di pakai (rupiah, dollar, yen, euro, dan sebagainnya) dan dan kerugian non material menyangkut dengan kerugian yang bersifat non keuangan seperti menurunya kepercayaan publik pada perusahaan (Irham Fahmi, 2010, p.135)
7. Risiko gugatan (Liability) eksposur kewajiban legal (liability muncul jika pengadilan memutuskan kita sebagai tertanggung yang harus membayar ganti rugi kepada pihak lainnya (Mahmud M. Hanafi, 2006, p.79)
8. Risiko proses adalah risiko mengenai potensi penyimpangan dari hasil yang diharapkan dari proses karena ada penyimpangan atau kesalahan dalam kombinasi sumber daya manusia (SDM, keahlian, metode, peralatan, teknologi dan material) dan karena perubahan lingkungan. Kesalahan prosedur merupakan salah satu bentuk perwujudan risiko proses (Bramantyo Djohanputro, 2004, p.40)

## 2.2 Tinjauan Umum Tentang Telekomunikasi di Indonesia

Telekomunikasi terdiri dari dua kata yaitu "Tele" yang berarti jarak jauh (at a distance) dan "Komunikasi" yang berarti hubungan pertukaran ataupun penyampaian informasi. Adapun pengertian Telekomunikasi adalah teknik pengiriman atau penyampaian informasi dari suatu tempat ke tempat lain. Bentuk Komunikasi jarak jauh dapat melalui kawat (telegrap, telepon) dan radio. Dan berdasarkan the Annex of the Constitution of the International Telecommunication Union (ITU) Telekomunikasi berarti setiap Transmisi, emisi atau penerimaan tanda, sinyal, tulisan, gambar dan suara atau kecerdasan pikiran apapun melalui kawat, radio, optik atau sistem elektromagnetik lainnya. Di Indonesia Telekomunikasi diatur dalam Undang Undang no 36 tahun 1999 yang menegaskan bahwa Telekomunikasi adalah setiap pemancaran, pengiriman dan atau penerimaan dari setiap jenis informasi dalam bentuk tanda tanda, isyarat, tulisan, gambar, suara, sistem kawat, optik, radio, atau sistem elektromagnetik lainnya.Dari UU diatas dapat disimpulkan bahwa radio, televisi, fiber optik, tv kabel, telepon seluler, Telepon PSTN dan satelit termasuk semuanya bagian dari telekomunikasi. Banyak perusahaan yang bergerak sebagai perusahaan telekomunikasi baik yang berperan murni sebagai operator telekomunikasi, sebagai Vendor, sebagai produsen dan pemasok dan bahkan perusahaan yang membuat divisi telekomunikasi sebagai pendukung perusahaan induknya. Seperti contohnya BRI yang di tahun 2016 ini akan meluncurkan satelit telekomunikasi sebagai penunjang lini bisnisnya dengan nama BRIsat. Bank Indonesia (BI) yang bekerjasama dengan PT. Indosat Ooredoo Tbk dalam

membentuk Perusahaan patungan untuk bisnis data dan ATM bersama yaitu PT. Artajasa.

### 2.2.1 Risiko Pada Perusahaan Telekomunikasi di Indonesia

Perkembangan Telekomunikasi Seluler di dunia ini sangat pesat, dengan jumlah pelanggan mencapai 5 milyar di seluruh dunia. Telekomunikasi seluler sudah menjadi kebutuhan dasar semua orang. Jumlah penduduk Indonesia hampir sekitar 230 juta jiwa yang sudah menggunakan ponsel (Lingga Wardhana, 2014, p.14). Risiko–risiko yang berkaitan dengan bisnis perusahaan telekomunikasi akan sangat berpengaruh ke perusahaan. Regulasi pemerintah yang mengumumkan atau memberlakukan perubahan kebijakan interkoneksi atau tarif dapat memberikan dampak negatif bagi bisnis atau ijin perusahaan telekomunikasi. Peraturan Pemerintah dalam hal ini Menkominfo yang menetapkan biaya interkoneksi yang turun antar operator seluler sebesar 26 % akan disikapi oleh operator telekomunikasi secara berbeda sesuai dengan tujuan perusahaan tersebut. Beberapa operator telekomunikasi seperti Indosat Ooredoo Tbk, Smart Fren dan XL senang dan ingin segera diberlakukan namun PT Telkom dan PT. Telkomsel kurang setuju karena akan menurunkan pendapatan mereka sedangkan biaya operasional BTS dan BSC di daerah terpencil tetap besar. Saat ini pemerintah sedang berdiskusi dengan para pemangku kepentingan industri telekomunikasi dan DPR untuk peraturan–peraturan baru mengenai penyediaan jaringan, penyediaan jasa, interkoneksi, tarif retail, pedoman persaingan, voucher dan distribusi starter pack dan langkah–langkah untuk mengatasi perkembangan terakhir pada industri telekomunikasi dan risikonya tidak membuat salah satu operator telekomunikasi mengalami kerugian yang besar. Adapun beberapa risiko yang dihadapi oleh operator telekomunikasi dalam menjalankan operasional nya yaitu:

**a. Risiko–Risiko yang berkaitan dengan Persaingan Bisnis**

Pemerintah merupakan pemegang saham mayoritas dari PT Telekomunikasi Indonesia Tbk ("Telkom") dan PT Telekomunikasi Selular ("Telkomsel") sehingga memberikan prioritas pada bisnis Telkom dan Telkomsel daripada Perusahaan telekomunikasi lain. Pemerintah memiliki saham sebanyak 14,29% di indosat, termasuk satu saham Seri A, yang memiliki hak suara istimewa dan hak veto atas beberapa hal strategis sebagaimana diatur dalam Anggaran Dasar Perusahaan, termasuk keputusan untuk pembubaran, likuidasi dan mengajukan kepailitan, dan memperbolehkan Pemerintah untuk menominasikan satu Direktur dari Direksi dan satu Komisaris dari Dewan Komisaris sehingga perusahaan telekomunikasi lain jadi kuatir akan keberpihakan pemerintah.

**b. Risiko–Risiko yang berkaitan dengan Peraturan Pemerintah**

Pada tanggal 6 Agustus 2013, Menkominfo mengeluarkan Peraturan Menkominfo No. 21 Tahun 2013 tentang Penyelenggaraan Jasa Penyediaan Konten Pada Jaringan Bergerak Seluler dan Jaringan Tetap Lokal Tanpa Kabel Dengan Mobilitas Terbatas, sebagaimana diubah dengan Peraturan Menkominfo No. 10 Tahun 2014 ("Peraturan Menkominfo 21/2013"), yang antara lain mewajibkan operator jaringan seperti Perusahaan dan penyedia konten untuk memperoleh izin dari Direktorat Jenderal Penyelenggara Pos dan Informatika ("DJPPI") untuk menyelenggarakan layanan konten. Para penyelenggara konten SMS premium diwajibkan untuk memenuhi persyaratan yang lebih ketat yang lebih sulit untuk dipenuhi dan wajib memperoleh izin tersebut paling lambat pada tanggal 6 Agustus 2014.

Apabila penyedia konten belum memperoleh izin dalam jangka waktu tersebut, penyedia konten tidak diperbolehkan untuk melaksanakan usaha mereka sebagai penyedia konten. Gangguan terhadap layanan konten yang diakibatkan tindakan BRTI pada tahun 2011 telah mengakibatkan penurunan yang cukup besar terhadap pendapatan Perusahaan yang berasal dari layanan ini. Operator telekomunikasi mengalami churn rate yang tinggi, terutama di bisnis jasa seluler prabayar. Churn rate yang tinggi disebabkan oleh fakta bahwa banyak pelanggan prabayar yang memiliki lebih dari satu kartu SIM dari berbagai operator seluler, yang memungkinkan mereka untuk memilih paket yang termurah. Tingginya churn rates tersebut dapat berakibat pada menurunnya pendapatan, yang dapat berdampak negatif pada bisnis, keadaan keuangan, hasil usaha dan prospek semua operator telekomunikasi. Dan semuanya tidak dapat menjamin bahwa churn rate yang tinggi tidak akan meningkat di tahun–tahun mendatang sebagai akibat dari program promosi agresif yang diluncurkan oleh operator.

**c. Risiko–Risiko yang berkaitan dengan Perizinan frekuensi dan Infrastruktur**

Operator Telekomunikasi bergantung pada ketersediaan infrastuktur menara telekomunikasi dan yang lainnya, untuk menyediakan jaringan GSM, akses nirkabel tetap serta 3G dan 4G dan jasa telekomunikasi bergerak seluler dengan memasang pemancar dan antena penerima dan fasilitas pendukung BTS lainnya pada menara tersebut. Ketersediaan dan pemasangan menara telekomunikasi tersebut memerlukan izin dari instansi berwenang di daerah. Beberapa instansi berwenang di daerah telah memberlakukan peraturan yang membatasi jumlah dan lokasi menara telekomunikasi dan mensyaratkan kewajiban berbagi penggunaan menara di antara berbagai operator telekomunikasi. Selain itu, pada tanggal 17 Maret 2008, Menkominfo telah mengeluarkan peraturan tentang penggunaan menara bersama telekomunikasi. Suatu peraturan bersama dikeluarkan oleh Menteri Dalam Negeri, Menteri Pekerjaan Umum, Menkominfo, serta Kepala BKPM pada 30 Maret 2009 yang disebut dengan SKB 4 menteri, mewajibkan tiap menara yang dibangun dan digunakan untuk layanan telekomunikasi harus memperoleh ijin mendirikan menara untuk menunjukkan kepatuhan pada beberapa spesifikasi teknis. Apabila pemilik menara tidak memperoleh ijin tersebut, maka pihak berwenang di daerah berhak untuk menentukan denda yang diberikan kepada pemilik menara. Selanjutnya, suatu penyelenggara telekomunikasi yang memiliki menara telekomunikasi atau pemilik menara wajib memperbolehkan operator telekomunikasi lainnya untuk menggunakan menara telekomunikasinya (selain menara yang digunakan sebagai jaringan utamanya), tanpa diskriminasi apapun.

Peraturan ini mewajibkan perusahaan untuk menyesuaikan rencana pembangunan menara telekomunikasi, rencana menyewakan, melakukan relokasi menara telekomunikasi yang sudah ada dan memperbolehkan operator lainnya untuk menggunakan menara operator lain serta melakukan hal–hal lain yang dapat berdampak pada meningkatnya biaya pendirian menara telekomunikasi, keterlambatan dalam konstruksi menara dan gangguan terhadap layanan untuk pelanggan. Ketergantungan operator terhadap menara telekomunikasi digabungkan dengan beban pemasangan menara telekomunikasi bersama dalam kondisi tertentu, dapat menyebabkan dampak negatif terhadap daya saing antar operator tersebut. Hal–hal seperti ini dapat mengakibatkan dampak negatif yang material terhadap kapasitas jaringan, kinerja dan kualitas jaringan dan layanan, reputasi, bisnis, hasil usaha serta prospek Perusahaan. Kemampuan operator untuk memelihara dan memperluas jaringan seluler atau menjalankan usaha dapat dipengaruhi oleh gangguan pemasokan dan layanan dari para pemasok utama untuk menyediakan sebagian besar perangkat yang dibutuhkan untuk memelihara dan memperluas jaringan seluler, termasuk microwave backbone, dan pada beberapa pemasok lainnya berkenaan dengan barang–barang lainnya.

**d. Risiko–Risiko yang berkaitan dengan Frekuensi**

Sejak tanggal 15 Desember 2010, pemerintah telah mengubah biaya berbasis perhitungan frekuensi menjadi suatu perhitungan baru yang didasarkan pada lebar alokasi spektrum yang digunakan oleh para pelaku usaha. Sebelumnya operator besar seperti Telkomsel, Indosat dan XL diwajibkan untuk membayar biaya frekuensi untuk pita frekuensi 800 MHz, 900 MHz dan 1800 Mhz yang didasari pada jumlah stasiun radio. Pada tahun 2012, 2013 dan 2014, indosat misalnya membayar biaya frekuensi masing–masing sejumlah Rp 2,1 triliun, Rp 2,2 triliun dan Rp 2,6 triliun. Sebagai salah satu pemegang spektrum terbesar di Indonesia, indosat diharapkan untuk terus membayar sejumlah dana yang besar untuk biaya frekuensi mulai dari sekarang dan ke depannya. Peningkatan biaya frekuensi di masa mendatang ini didasarkan pada peningkatan indeks harga konsumen dan populasi Indonesia. Akibatnya, perubahan kondisi makro ekonomi di Indonesia dapat mengakibatkan meningkatnya biaya frekuensi yang apabila signifikan dapat berdampak negatif terhadap bisnis, kondisi keuangan dan operasional. Risiko yang berkaitan dengan Bisnis Layanan Data Tetap ("MIDI") meningkat, dan akan ada operator yang mengalami penurunan marjin dari jasa tersebut seiring dengan meningkatnya persaingan Layanan MIDI yang semakin ketat dari para operator baru dan operator yang telah ada, yang mungkin memiliki basis pelanggan yang lebih banyak dan sumber dana yang lebih besar seperti Telkom dan Telkomsel yang memiliki jangkauan internasional dan regional dan infrastruktur dalam negeri yang telah berkembang. Selain itu, para operator seperti Indosat, XL, PT First Media Tbk ("First Media") dan PT Indonesia Comnet Plus

("Icon+") dan PT NAP Info Lintas Nusa ("Matrix Cable System"), beberapa di antaranya yang mempunyai aliansi dengan operator telekomunikasi asing makin bersaing di segmen bisnis ini. Bisnis satelit juga menghadapi persaingan yang semakin ketat seiring dengan diluncurkannya satelit–satelit baru dan berkemampuan lebih besar dan dengan adanya beberapa Perusahaan yang memperoleh ijin eksklusif untuk menyelenggarakan jasa penyiaran di Indonesia. Indosat misalnya perjanjian kapasitas transponder satelit Palapa– C2 dan Palapa D-nya mencakup jangka waktu antara satu sampai lima tahun, dan diperkirakan sisa umur produktif satelit tersebut masing–masing adalah berkisar satu dan enam tahun. Mengingat adanya satelit–satelit lain yang beroperasi misalnya satelit dari BRI dan sewa transponder yang semakin ketat, maka pihak penyewa transponder kemungkinan akan mempunyai opsi yang lebih banyak. Satelit indosat sudah berakhir berakhir pada bulan Agustus 2015 dan digantikan oleh satelit BRI dan sisanya akan berakhir di April 2020.

## 2.3 Risiko Manusia

Nadief Kaelani (2010, p.73) menjelaskan penyebab risiko adalah manusia, bukan teknikal. Artinya dalam setiap kecelakaan memang ada kontribusi dari kegagalan peralatan namun yang perlu dipertanyakan adalah bagaimana bisa gagal. Bukankah faktor kegagalanya disebabkan oleh faktor manusianya juga yang lalai memeliharanya. Senada dengan pendapat tersebut, Gunawan & Waluyo (2015, p.109) mendefenisikan kesalahan manusia adalah keputusan atau perilaku manusia yang menyimpang dari yang seharusnya (misalnya mengambil jalan pintas) yang dapat menurunkan/berpotensi menurunkan daya guna, keselamatan atau kinerja sistem, sehingga berpotensi menimbulkan kerugian.

Selanjutnya, lihat Muhammad Muslich (2007, p.13) BIS, inter- american development bank kesalahan manusia dan fraud yang meliputi kerugian operasional :

1. Integritas dan pertimbangan yang baik, yaitu risiko yang terjadi akibat sumber daya manusia perusahaan dengan tidak sengaja maupun sengaja tidak memenuhi kebijakan, prosedur dan pengendalian yang telah ditetapkan.
2. Sumber daya manusia, yaitu risiko yang timbul dari inefisiensi atau kesalahan dalam proses transaksi akibat kurangnya sumber daya manusia yang memadai, program pelatihan dan turn-over pegawai yang tinggi. Situasi yang sering timbul dalam kasus ini disebabkan oleh perbedaan signifikan dalam program pelatihan bagi satuan kerja unit bisnis dengan staf departemen sdminidtrasi dan pengendalian. Hal tersebut merupakan salah satu factor signifikan yang mengakibatkan tingginya risiko operasional perusahaan.
3. Fraud dan konflik kepentingan, yaitu risiko yang timbul karena sumber daya manusia perusahaan lebih condong kepada kepentingan pribadi dibandingkan kepentingan perusahaan.
4. Kegagalan sistem teknologi informasi, yaitu kerugian operasional yang disebabkan oleh gangguan dalam melaksanakan proses transaksi atau aktivitas kerja, kebocoran dalam sistim informasi dan gangguan lainnya yang ditimbulkan dari tidak berfungsinya sistim teknologi informasi akibat kegagalan hardware, software dan sebagainya.

Untuk menegaskan fraud tersebut, Bona P. Purba (2015, p.3) fraud adalah setiap perbuatan tidak jujur (penyalah gunaan kedudukan/jabatan atau penyimpangan) yang bertujuan mengambil uang (atau harta atau sumber daya orang lain/organisasi) melalui akal bulus, tipu muslihat, penipuan, kelicikan, penghilangan, kecurangan, saran yang salah, penyembunyian atau cara-cara yang di lakukan dengan sengaja oleh seseorang, yang mengakibatkan kerugian organisasi atau orang lain dan/atau menguntungkan pelaku.

### 2.3.1 Risiko Operasional disebabkan Oleh Faktor Manusia

Ikatan Bankir indonesia (2015, p.151) risiko operasional yang disebabkan oleh faktor manusia juga bisa disebabkan oleh pelatihan dan manajemen yang tidak memadai, kesalahan manusia, pemisahan tugas dan wewenang yang tidak jelas, ketergantungan terhadap orang-orang tertentu, integritas dan kejujuran yang rendah. Risiko-risiko operasional dapat di atas bisa lebih diperburuk oleh kualitas pelatihan yang tidak memadai, kontrol yang tidak memadai dan kualitas sumber staf yang buruk atau faktor-faktor lainnya

Sedangkan menurut James Lam (2007, p.278) risiko organisasional meliputi kekurangan bakat manajemen dan pekerja yang terampil, hubungan publik yang negatif atau

perilaku karyawan yang tidak tepat akibat praktik rekrutmen yang buruk atau budaya dan isentif perusahaan yang merugikan.

### 2.3.2 Hal-Hal Yang Sering Menimbulkan Risiko Kesalahan Manusia

Sulad Sri Hardanto (2006, p.137) mengatakan hal-hal yang sering menimbulkan risiko kesalahan manusia :

1. Masalah kesehatan dan keselamatan kerja
2. Perputaran karyawan yang tinggi
3. Internal fraud
4. Perselisihan karyawan atau buruh
5. Pelaksanaan manajemen yang buruk
6. Pelatihan karyawan yang buruk
7. Terlalu tergantung pada karyawan kunci
8. Rogue trader (trader nakal)

### 2.3.3 Faktor-Faktor Yang Mempengaruhi Kesalahan Manusia

Penjelasan Gunawan & Waluyo (2015, p.69) terdapat tiga bentuk perilaku manusia :

1. Kesalahan manusia (Human Error), yaitu kesalahan yang tidak di sadari atau di mengerti (slip, lapse, mistake). Untuk kesalahan seperti ini, perlu pembinaann bukan hukuman.
2. Perilaku berbahaya (At-Risk Behavior) yaitu kesalahan karena kurang memahami risiko yang di hadapi ((Unintentiional Risk Taking). Untuk kesalahan seperti ini, perlu di lakukan pembimbingan (coaching) agar lebih tajam memahami risiko kepada pekerja.
3. Perilaku sengaja (Reckless Behavior) yaitu kesalahan yang di lakukan dengan sengaja (Intentional Risk Taking). Untuk kesalahan seperti ini, perlu di beri peringatan, dan jika bersifat sabotase, perlu di lakukan pemecatan.

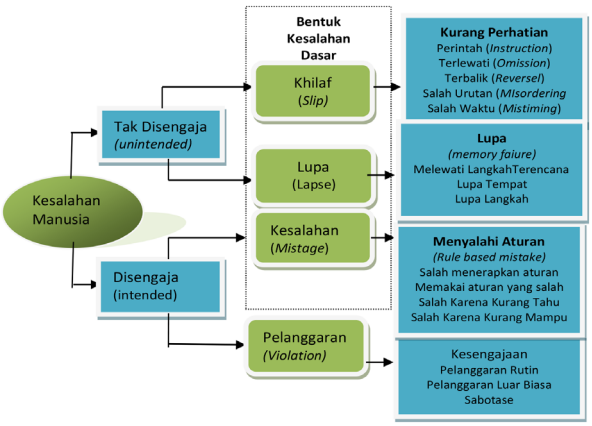
Lebih lanjut, Gunawan & Waluyo (2015, p.110) mengemukakan kesalahan manusia di tempat kerja dapat terjadi karena faktor internal dalam diri pelaku maupun faktor eksternal dari luar diri pelaku

1. Kesalahan manusia karena faktor luar (eksternal) :

a. Rancangan pekerjaan, rancangan peralatan dan rancangan lingkungan fisik di tempat kerja dapat menimbulkan keadaan yang merangsang orang untuk melakukan kesalahan (error provocative situation)
b. Faktor eksternal lain yang dapat mendorong karyawan melakukan kesalahan adalah kelemahan yang ada dalam lingkungan organisasi. Faktor ini meliputi antara lain : kepemimpinan dan kebijakan manajemen, maupun sistem manajemen di perusahaan

2. Kesalahan manusia karena faktor dalam diri (internal).

Gambar 2.3.Kesalahan manusia karena factor dalam diri



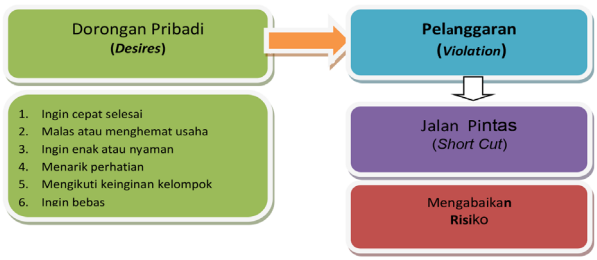

Sumber: Gunawan & Waluyo, 2015, halaman 110

Bentuk kesalahan manusia karena faktor yang ada dalam diri manusia :

1. Khilaf dan lupa. Kesalahan karena ketidaksadaran, hilangnya perhatian, atau lupa sesaat ini dikenal dengan sebutan khilaf atau slip dalam bahasa inggris
2. Kesalahan (mistakes). Kesalahan dalam kelompok ini adalah kesalahan penerapan peraturan (rule-based), kesalahan karena ketidaktahuan (knowledge-based), atau kesalahan karena ketidakmampuan secara fisik, kejiwaan, maupun emosi (skill-based). Kesalahan ini memang dilakukan dengan sengaja dan sadar oleh pelaku, karena keterbatasan pengetahuan pelaku terkait pekerjaan, aturan yang berlaku, dan ketidakmampuan secara fisik dan kejiwaan:
   a. Menyalahi aturan (rule-based mistakes)
   b. Salah karena tidak tahu (knowledge-based mistakes)
   c. Salah karena kurang mampu (skill-based mistakes)
3. Pelanggaran (Violation). Kesalahan karena ketidakmauan/kesengajaan ini di kenal dengan istilah pelanggaran atau jalan pintas (shortcut), yaitu tindakan yang

di sengaja melanggar aturan atau prosedur yang berlaku (intended action, violation)

Gambar 2.4. Pelanggaran Violation




Sumber: Gunawan & Waluyo, 2015, halaman 110

### 2.3.4 Risiko Sumber Daya Manusia

Terkait dengan risiko manusia tersebut, risiko juga dapat disebabkan oleh tidak kompetenya sumber daya manusia (SDM). Dewi Hanggraeni (2010, p.212) mengemukakan, beberapa hal yang dapat meningkatkan risiko sumber daya manusia untuk perusahaan :

1. Rekrutmen. Merekrut karyawan baru yang memiliki kinerja yang buruk sama halnya dengan membawa perusahaan pada risiko yang besar. Dan memang, proses rekrutimen di setiap perusahaan belum dikelola dengan baik. Hal ini dikarenakan dalam menentukan apakah karyawan baru tersebut memiliki kepribadian yang baik atau tidak dan apakah ia dapat bekerja secara efektif atau tidak sangatlah sulit. Secara sederhana, dengan melakukan pengukuran IQ tidak dapat mengindikasikan kinerja yang baik dari karyawan baru. Perusahaan dapat meminimalisir risiko tersebut dengan menerapkan metode ini :

a. Mempersiapkan job specification
b. Membuat spesifikasi calon karyawan yang di butuhkan, seperti membuat standar pengalaman, kemampuan, dan kualifikasinya
c. Melakukan metode rekruitmen dengan benar, apakah akan menggunakan media periklanan atau menggunakan jasa head hunting
d. Melatih manajer agar menjadi interviewer yang efektif
e. Memeriksa CV calon karyawan dan bertanya kepada reference.

2. Struktur perusahaan. Banyak perusahaan menurunkan risiko bisnis dengan memastikan bahwa semakin banyak staf maka akan semakin memenuhi apa yang di inginkan pelanggan
3. Klaim dari pekerja
4. Bullying. Banyak perusahaan yang harus menghadapi klaim/tuntutan dari karyawannya yang merasa di jadikan sebagai subjek dari tindakan bullying atau orang yang di jadikan sebagai objek derita. Jenis-jenis bullying berupa pelecehan seksual, under estimate tentang ras/gender, serangan secara lisan, ataupun bahasa kasar lainnya. Hal ini dapat merendahkan korban baik itu dari segi pendapatnya, kritik, kinerja, isolasi, bahkan gurauan tentang korban. Hal ini dapat di cegah :

a. Implementasi dan mensosialisasikan kebijakan anti-bullying, spesifik bahwa bullying tidak diterima
b. Mendorong staf untuk mengikuti pelatihan tentang perilaku apa saja yang di perkenankan
c. Menetapkan sistem untuk investigasi dan dapat menyelesaikan konflik, ini harus di mulai dengan konseling dan mentoring, memulai konsiliasi dan arbitrasi jika tidak terpecahkan, dan terakhir tindakan pendisplian
d. Menginformasikan kepada staf mengenai tindakan apa yang dapat mereka lakukan, dan memastikan tidak adanya penipuan ketika bullying di laporkan
e. Menginvestigasi keluhan dengan cepat, mengatur kebijakan dan percaya diri, dan melindungin hak individu yang terlibat untuk membuat kasus menjadi efektif perlu adanya catatan tertulis setiap waktu

5. Stres dan kesehatan, stres membuat karyawan mengambil waktu untuk beristrahat dari pekerjaan dan ini merupakan salah satu faktor utama yang menyebabkan pekerja mengalami serangan jantung. Tanda-tanda stress : sakit kepala, kelelahan, eczema, sakit urat syaraf/otot, sakit perut (diare, konstipasi), sering marah-marah (frustasi, kekerasan, agresif, resah, meningkatnya konsumsi minuman beralkohol, rokok, obat-obatan, atau obat tidur, depresi, merasa tidak bertenaga, lekas marah dengan rekan kerja, masalah dalam pekerjaan, sering absen. Pekerja yang sakit tidak hanya membahayakan diri sendiri namun juga membahayakan perusahaan itu sendiri. Solusi untuk mengurangi stress dan absensi yang berlebih :

a. Melakukan audit terhadap perilaku pekerjaan dan

tingkat stres

b. Memberikan deskripsi pekerjaan yang jelas dan alur pelaporan
c. Memastikan komunikasi regular upward dan downward, dan memastikan bahwa pendapat pekerja di dengarkan
d. Membuat pekerja lebih utuh (memastikan pekerja menyelesaikan pekerjaan secara utuh)
e. Meningkatkan level pengendalian terhadap pekerja yang lembur, overtime work
f. Memastikan bahwa kuota pekerjaan teratur dan seimbang
g. Meningkatkan kemampuan teknikal dari pekerja
h. Memberikan kepada pekerja strategi coping seperti diet/olah raga atau strategi untuk berhadapan dengan pelanggan kasar
i. Meningkatkan support dan supervision
j. Memperbaiki lingkungan kerja dengan menurunkan tingkat kebisingan, polusi
k. Mengimplementasikan sistem reward yang adil
l. Meningkatkan keamanan kerja dan membangun karir
m. Meningkatkan fleksibilitas dalam aturan kerja
o. Memperkenalkan pelatihan management training
p. Meningkatkan ergonomics, seperti untuk pekerja yang bekerja di depan layar computer

6. Kasus persengketan. Beberapa sengketa dapat di ramal, seperti hubungan antara manajemen dengan serikat pekerja berangsur-angsur memburuk. Keluhan dapat tumbuh dalam kurun waktu tertentu, dan para pekerja meyakini bahwa kondisi ini hampir pasti tidak di perlakukan secara adil dalam industri. Solusi terbaik adalah dengan memastikan bahwa perusahaan terlihat berlaku secara adil dan jujur.

Lebih lanjut Mamduh M. Hanafi (2006, p.207) menjelaskan beberapa contoh risiko operasional yang berkaitan dengan sumber daya manusia :

1. Kecelakaan kerja, khususnya kecelakaan kerja karena kecerobohan atau kurang pengalaman dari karyawan
2. Terlalu tergantung pada karyawan kunci tertentu, sehingga jika karyawan tersebut meninggal atau berpindah kerja, perusahaan menghadapi masalah
3. Integritas karyawan yang kurang, sehingga karyawan bisa menggelapkan uang perusahaan atau melakukan aktifitas yang berada diluar wilayah otoritasnya.

Sedangkan Irham Fahmi (2010, p.157) menyatakan adapun bentuk tindakan fraud pada bagian sumber daya manusia adalah :

1. Menerima sogok dengan menerima karyawan yang seharusnya tidak lulus namun kemudian meluluskannya
2. Menerima karyawan yang berasal dari hubungan keluarga namun kualitasnya adalah rendah atau di anggap tidak layak
3. Membayar gaji karyawan tidak sesuai dengan isi perjanjian kontrak
4. Menggunakan fasiitas kantor untuk kepentingan pribadi
5. Mengenakan biaya-biaya administrasi yang di luar dari ketentuan yang di buat oleh perusahaan,
6. Menempatkan karyawan yang tidak sesuai dengan keahliannya, dengan tujuan agar mudah di atur dan di bujuk jika melakukan sesuatu. Lebih khusus tidak menerapkan the right man and the right place
7. Tidak memberikan fasilitas pendukung yang maksimal dalam pekerjaan karyawan, sehingga karyawan yang bersangkutan menggunakan fasilitas pribadi untuk pekerjaan kantor. Sementara fasilitas pendukung di ambil oleh pimpinan untuk kepentingan pribadinya
8. Tidak mempromosikan karyawan atas dasar sesuai dengan profesionalisme, namun karena kedekatan dan bisa di ajak kerjasama oleh pimpinan perusahaan

Dari beberapa pendapat di tersebut, dapat di uraikan kerugian karena kejadian yang tidak dikendaki muncul cenderung di sebabkan oleh orang dalam pada sebuah organisasi. Ada dua variabel yang besar menstimulus terjadinya risiko operasional terkait manusia meliputi karakter/ mental manusia yang di dorong oleh kepentingan uang dan barang, serta keinginan untuk mengejar kekuasaan (cinta uang dan cinta kekuasaan kedua-duanya memiliki pengaruh yang sangat berbahaya).

## III . METODOLOGI PENELITIAN

Pada karya akhir ini, data yang digunakan adalah data risiko Operasional yang terjadi di PT Indosat Ooredoo Tbk. Dalam bab ini membahas mengenai pendekatan pene-

litian, penetapan informan, sumber data, dan teknik analisis yang digunakan dalam penelitian.

## 3.1 Tujuan Metodologi Penelitian

Metode penelitian kualitatif, dengan tujuan mengidentifikasi, mengukur, dan mengelola risiko operasional pada Divisi Network Operation Center PT Indosat Ooredoo Tbk.

## 3.2 Unit/Obyek Penelitian

Risiko operasional pada Divisi Network Operation Center PT Indosat Ooredoo Tbk.

### 3.2.1. Metode Pengumpulan Data

Data untuk penelitian ini diperoleh dengan cara :

**a. Kuesioner.**

Teknik pengumpulan data dengan menggunakan pertanyaan yang diajukan kepada karyawan-karyawan yang memiliki kompetensi dalam operasional pusat jaringan PT. Indosat Ooredoo Tbk. Untuk memperoleh data tersebut digunakan kuesioner yang bersifat terbuka yaitu pertanyaan yang dibuat sedemikian rupa hingga responden diberikan kebebasan dalam menjawab pertanyaan sesuai dengan pengalaman dan pengetahuan yang mereka miliki dibagian operasional jaringan.

**b. Wawancara.**

Mendapatkan informasi dengan cara bertanya langsung kepada karyawan-karyawan operasional pusat jaringan PT. Indosat Ooredoo Tbk. Wawancara adalah salah satu bagian yang terpenting dari setiap survey. dengan wawancara, penelitian memiliki kesempatan untuk mendapatkan informasi secara jelas dan tepat dengan jalan bertanya langsung kepada responden.

**c. FGD (Focus Group Discussion).**

Teknik mendapatkan informasi dengan cara membentuk group di setiap departemen untuk menentukan besarnya dampak dan probabilitas risiko yang terjadi. Peneliti mengambil responden yang bersedia dan yang memahami risiko-risiko yang terjadi pada departemennya.

### 3.2.2 Teknik Penetapan Informan

Teknik sampling yang digunakan adalah quota sampling yang dilanjutkan dengan convinience sampling, dimana pengambilan informan sebagai sumber data dari karyawan sebagai responden dengan pertimbangan telah memiliki pengalaman bekerja 5 tahun pada divisinya di PT. Indosat dan kemudian peneliti meminta kepada responden untuk mengisikan daftar-daftar risiko yang pernah terjadi di departemennya masing-masing. Jumlah karyawan yang bekerja pada Divisi Network Operation Center PT Indosat Ooredoo Tbk berjumlah 170 orang. Divisi ini memiliki 9 departemen maka ditetapkan atau di quotakan bahwa satu departemen diambil lima informan mewakili tiap departemen dan khusus tiap region diambil lima informan yang mewakili tiap region yang mampu memberikan atau menguraikan risiko apa yang terjadi pada departemennya. Waktu penelitian diadakan selama 3 bulan yaitu dari bulan 6 sampai bulan 9.

### 3.2.3 Teknik Keabsahan Data

Dalam uji keabsahan data pada penelitian ini, peneliti akan melakukan uji triangulasi. Menurut Sugiyono (2012, p.120), triangulasi diartikan sebagai teknik pengumpulan data yang bersifat menggabungkan berbagai sumber data yang telah ada. Pada penelitian ini, peneliti memilih teknik uji keabsahan data dengan triangulasi sumber. Dalam penelitian ini, keasahan data akan di uji dengan membandingkan hasil wawancara dari para narasumber di Divisi Network Operation Center PT Indosat Ooredoo Tbk.

## 3.3 Menampilkan Proses Bisnis di Divisi NOC PT Indosat Ooredoo Tbk

Proses bisnis yang terjadi di Divisi Network Operation Center PT Indosat Ooredoo Tbk yaitu dari menjelaskan bagaimana proses keseluruhan operasional di tiap departemen yang ada di divisi network operation center. Dan bagaimana hubungan kerja operasional antar setiap departemen di divisi network operation center indosat dan bagaimana pemantauan dan troubleshootimg semua problem di divisi network operation center indosat.

## 3.4 Identifikasi Risiko

Identifikasi risiko dengan menggunakan proses sistematis yang terstruktur, secara dalam, luas dan harus mencakup semua risiko yang berada dalam kendali pada Divisi Network Operation Center PT Indosat Ooredoo Tbk.

Guna memudahkan identifikasi risiko dilakukan berdasarkan kategori risiko yakni risiko-risiko yang terjadi pada fungsi departemen yang terkait yakni pada departemen Transmission Backbone Operation, IP/MPLS Operation, Regional Operation (Jabotabek Operation, Central and West Java Operation, East Java and Bali Nusa Operation, Kalisula Operation, dan Sumatera Operation), Access Operation, CME Operation, Core Operation, Partner Management, Consumer Front Office, dan Configuration Management. Alat identifikasi yang dapat digunakan antara lain Brainstorming yakni meminta kepada setiap karyawan pada departemen yang terkait menuliskan kembali risiko-risiko yang telah terjadi dan akan mungkin terjadi pada setiap departemennya dan Risk Breakdown Structure (RBS) serta kepada karyawan tersebut diminta mengurutkan dari faktor yang paling sering terjadi dan dampaknya terbesar ke yang terkecil. Dokumen utama yang dihasilkan dalam proses ini adalah nama atau daftar Risiko (Risk Register).

## 3.5 Mengukur Risiko

Setiap risiko pada fungsi departemen akan di ukur untuk mengetahui tingkat kemungkinan terjadinya (likelihood) dan impact adalah seberapa besar dampak yang ditimbulkan. Pengukuran risiko terlebih dahulu disepakati konversi ukuran likelihood dan dampak risiko yang akan digunakan dalam pengukuran risiko. Likelihood risiko dinyatakan dengan persentase probabilitas kejadian risiko. Ukuran likelihood dikonversikan menjadi skala ukuran semi kuantitatif dari 1 sampai dengan 5. Ukuran likelihood sebagai berikut:

**Tabel 3.1. Ukuran likelihood (Kemungkinan)**

| Skor | Kejadian | Probabilitas Kejadian (%) | Keterangan dalam 1 tahun |
|---|---|---|---|
| 1 | Jarang | Mungkin terjadi hanya pada kondisi tidak normal, probabilitas ≤ 20 | Terjadi 1- 2 kali |
| 2 | Kemungkinan terjadi | Mungkin terjadi pada beberapa waktu, probabilitas 20 ≤ X ≤ 40 | Terjadi 3-4 kali |
| 3 | Kemungkinan sedang | Dapat terjadi pada beberapa waktu, probabilitas 40 ≤ X ≤ 60 | Terjadi 5-6 kali |
| 4 | Kemungkinan besar | Akan mungkin terjadi pada banyak keadaan, probabilitas 60 ≤ X ≤ 80 | Terjadi 7-8 kali |
| 5 | Hampir pasti | Dapat terjadi pada banyak keadaan, probabilitas 80 ≤ X ≤ 100 | Terjadi > 8 kali |

Sumber: diolah dari www.industrisemen-prosespembuatansemen.blogspot.co.id/

Sedangkan tingkat keseriusan kerugian atau impact dari risiko terkait tentang tujuan perusahaan yakni seberapa besar dampak yang ditimbulkan oleh peristiwa (jika terjadi) pada sasaran. Karena dampak terkait dengan sasaran, maka besaran dampak harus dinyatakan dengan satuan ukuran yang sama. Instrumen di ukur dengan menggunakan skala likert dengan diberi skoring 5 (lima) kategori :

**Tabel 3.2. Ukuran Dampak**

| Skor Dampak | Dampak Finansial | Dampak Keselamatan Kerja | Dampak Citra Perusahaan |
|---|---|---|---|
| Skor 1 = Tidak Signifikan | Kerugian financial sangat kecil | Kecelakaan kerja tanpa bantuan dokter | Citra jelek dilingkungan internal karyawan |
| Skor 2 = Kecil | Kerugian financial kecil | Kecelakaan kerja dengan bantuan dokter umum | Citra jelek dilingkungan pemilik |
| Skor 3 = Sedang | Kerugian financial Sedang | Kecelakaan kerja dengan bantuan dokter spesialis | Citra jelek media lokal setempat |
| Skor 4 = Besar | Kerugian financial besar | Kecelakaan kerja dengan dokter spesialis dan opname | Citra jelek media Nasional |
| Skor 5 = Sangat Besar | Kerugian financial sangat besar | Kecelakaan kerja luka sangat parah dan mengakibatkan kematian | Citra jelek di media internasional |

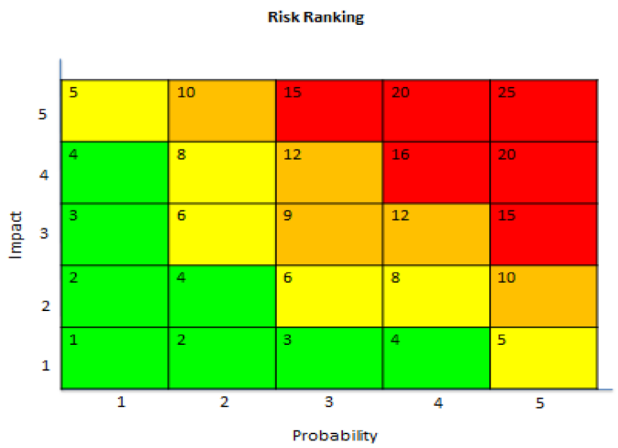
Sumber: diolah dari www.smkiplpse.wordpress.com/2012/07/18

Maka untuk mengukur dan mengelola risiko yang tak diinginkan adalah hasil dari perkalian peluang dan dampak dari potensi kejadian, dengan menggunakan rumus :

$$L = p \times D$$

dengan:
P = Peluang
D = Dampak

**Gambar 3.1. Pengelompokan hasil (ukuran) Risiko**




Sumber: www.smpemeliharaankapal.blogspot.co.id/2016

## 3.6 Analisis Risiko

Tujuan analisis risiko adalah melakukan analisis dampak dan kemungkinan semua risiko yang dapat menghambat tercapainya sasaran pada Divisi Network Opera-

tion Center PT Indosat Ooredoo Tbk dan menyediakan data untuk membantu langkah evaluasi dan memperlakukan risiko. Analisis risiko mencakup pertimbangan dan mengkombinasikan estimasi terhadap consequence dan likelihood didalam konteks untuk mengambil tindakan pengendalian. Analisis risiko dapat berupa analisis kualitatif, semi kuantitatif, kuantitatif atau kombinasi diantaranya, tergantung pada informasi risiko dan data yang tersedia. Analisis kualitatif dapat digunakan pertama kali untuk mendapatkan indikasi umum mengenai level risiko. Selanjutnya dilakukan analisis kuantitatif yang lebih spesifik.
Jenis-jenis analisis risiko tersebut adalah sebagai berikut:

### 3.6.1 Analisis Kualitatif

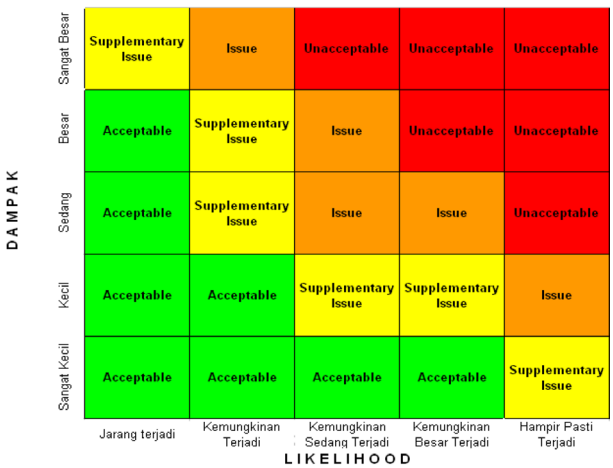
Analisis kualitatif menggunakan istilah atau skala deskriptif untuk menggambarkan besaran konsekuensi yang potensial dan likelihood bahwa konsekuensi akan terjadi. Analisis kualitatif digunakan sebagai suatu aktivitas penyaringan awal untuk mengidentifikasi risiko-risiko yang memerlukan analisis yang lebih rinci hal ini dengan memberikan kuisioner tahap pertama yakni meminta setiap karyawan operasional jaringan menuliskan risiko-risiko apa saja yang ada pada pekerjaannya.

### 3.6.2 Analisis Kuantitatif

Analisis kuantitatif menggunakan nilai angka (daripada menggunakan skala deskriptif seperti digunakan dalam analisis kualitatif dan semi kuantitatif) baik untuk consequence maupun untuk likelihood, dengan menggunakan data dari berbagai sumber. Kualitas analisis tergantung pada akurasi dan kelengkapan nilai numerik yang digunakan. Consequence dapat diestimasi dengan pembuatan model outcome dari suatu atau beberapa peristiwa, atau dengan ekstrapolasi hasil kajian eksperimen atau data masa lalu. Consequence dinyatakan dalam satuan biaya, kriteria teknik (satuan pengukuran) atau manusia (kematian/cedera) atau kriteria lainnya. Dalam beberapa kasus, diperlukan lebih dari satu nilai numerik untuk menentukan konsekuensi pada waktu, tempat, kelompok atau situasi yang berbeda. Likelihood biasanya dinyatakan sebagai probabilitas, frekuensi atau kombinasi antara paparan dan probabilitas.

Prioritas yang digunakan didapatkan dari mengukur risiko yang tak diinginkan adalah hasil dari perkalian peluang dan dampak dari kejadian. Hasil perkalian tersebut merupakan kriteria risiko. Gambar 3.2. dibawah ini digunakan sebagai kriteria risiko untuk menentukan batas antara risiko yang tidak dapat diterima dan dapat diterima.

**Gambar 3.2. Pengelompokan Kriteria Risiko**




Sumber: www.idrismadjidi.wordpress.com/2013

### 3.6.3 Evaluasi Risiko

Evaluasi risiko merupakan pembandingan antara level risiko yang ditemukan selama proses analisis dengan kriteria risiko yang ditetapkan sebelumnya. Dalam evaluasi risiko, level risiko dan kriteria risiko harus diperbandingkan dengan menggunakan basis yang sama. Hasil dari evaluasi risiko adalah daftar prioritas risiko untuk tindakan lebih lanjut. Jika risiko-risiko masuk dalam kategori rendah atau risiko yang dapat diterima, maka risiko-risiko tersebut diterima dengan sedikit perlakuan lanjutan. Risiko-risiko yang rendah atau dapat diterima harus dipantau dan ditelaah secara periodik untuk menjamin bahwa risiko-risiko tersebut tetap dapat diterima. Langkah evaluasi memastikan bahwa tidak semua risiko yang teridentifikasi memerlukan rencana pengendalian lebih lanjut. Hasil dari analisis risiko akan disampaikan kepada penanggung jawab tertinggi pengelola risiko di unit kerja untuk dilakukan validasi. Hasil validasi akan digunakan untuk menetapkan rencana langkah–langkah sistem pengendalian untuk menurunkan kemungkinan terjadinya risiko maupun untuk menurunkan dampak terjadinya risiko. Adapun kriteria risiko adalah sebagai berikut:

**Tabel 3.3. Pembagian Kategori Risiko**

| Kategori Level | Skor | Penjelasan |
|---|---|---|
| Rendah | X.Y ≤ 4 | Tidak diperlukan tindakan (Acceptable) |
| Sedang | 4 < X.Y. ≤ 8 | Disarankan diambil tindakan jika tersedia sumber daya perusahaan *(Supplementary Issue)* |
| Tinggi | 8 < X.Y. ≤ 12 | Diperlukan tindakan untuk mengelola risiko *(Issue)* |
| Ekstrim | 12 < X.Y. ≤ 25 | Diperlukan tindakan segera untuk mengelola risiko *(Unacceptable)* |

Sumber: www.idrismadjidi.wordpress.com/2013

### 3.6.4 Perlakukan Risiko

Risiko-risiko yang telah tersaring pada langkah evaluasi, selanjutnya dibuat rencana pengendalian lebih lanjut, langkah ini disebut perlakukan risiko. Langkah perlakukan risiko meliputi pengidentifikasian opsi untuk menangani risiko, menaksir opsi tersebut, menyiapkan rencana perlakuan risiko dan mengimplementasikan rencana perlakuan risiko.

Mitigasi risiko dibedakan menjadi dua jenis yaitu pengendalian dan penanganan.

**1. Pengendalian**

Pengendalian adalah upaya-upaya untuk merubah risiko. Pengendalian biasanya merupakan upaya-upaya yang telah dimiliki dan bersifat rutin untuk mengantisipasi terjadinya risiko. Contoh pengendalian dapat dalam bentuk prosedur dan work instruction.

**2. Penanganan**

Penanganan adalah upaya-upaya yang akan dilakukan sebagai langkah baru untuk memperlakukan risiko karena upaya-upaya yang sudah ada belum memadai.

## IV. ANALISIS DAN PEMBAHASAN

### 4.1. Bisnis Proses Operasional di Divisi Network Operation Center PT Indosat Ooredoo Tbk

Divisi Network Operation Center PT Indosat Ooredoo Tbk membawahi 9 departemen dengan komposisi 8 departemen yang ada di Headquarter (kantor pusat) dan 1 departemen yang ada di Regional. Adapun 8 departemen tersebut yakni Front Office, Transmission Operation, IP/MPLS Operation, Access Operation, CME Operation, Core Operation, Configuration Management, Partner Management dan 1 departemen yang di regional yang fungsi kerja dan sistemnya sama, hanya dibedakan oleh wilayah yakni Regional Operation (Jabodetabek Operation, CJWJ Operation, EJBN Operation, Kalisula and Papua Operation, dan Sumatera Operation). Bisnis proses operasional di divisi ini dimulai dari:

**a. Front Office.**

Merupakan departemen kedua terbanyak karyawannya di divisi NOC dengan fungsi utama surveilance dan monitoring. Departemen ini sebagian besar karyawannya bekerja dengan sistem shift yaitu: 3 shift yang dibagi dalam 4 team. Setiap hari team shift operasional bekerja dengan durasi kerja setiap shift 8 jam sehingga monitoring dilakukan 24 jam sehari dan 7 hari dalam seminggu setiap tahun. Adapun level kerja di team ini disebut dengan istilah level 0 karena tidak ada melakukan troubleshooting ataupun perbaikan di jaringan. Departemen ini berfungsi menginfokan hasil dari surveillance dan monitoring ke departemen lain di divisi network operation center (NOC) yang level kerjanya level 1 dan level 2, setiap ada problem baik di jaringan maupun impact terhadap pelanggan. Departemen ini mempunyai beberapa group yaitu I-NOC (indosat network operation center) system operation fungsinya sebagai surveilance dan monitoring trouble ticket dan alarm consolidator. Fault handling transport BB dan PDH fungsinya yaitu surveilance dan monitoring untuk alarm di transmisi dan backbone. Back Office Access fungsinya yaitu surveilance dan monitoring untuk alarm access di RAN (Radio Access Network) seperti BSC dan BTS. Fault handling core fungsinya yaitu surveilance dan dan monitoring untuk alarm di core seperti PS dan CS core dan IN-VAS (Intelegent Network Value Added Services). Fault tracking and reporting yaitu tracking alarm dan mengumpulkan serta memberikan report semua alarm dan masalah terhadap team regional. Fault handling IP yaitu monitoring alarm dan masalah IP serta wifi. Customer complain handling yaitu menangani semua complain pelanggan dari sisi teknikal yang diinfokan oleh team CCS (Customer Contact Services).

**b. Regional Operation (Jabodetabek Operation, CJWJ Operation, EJBN Operation, Kalisula and Papua Operation, dan Sumatera Operation).**

Departemen ini merupakan yang terbesar di NOC yang membawahi paling banyak karyawan dan team atau

group yang tersebar di seluruh wilayah Indonesia dan merupakan perpanjangan tangan dari semua departemen yang berhubungan dengan operation di network operation center (NOC) di head quarter, sehingga fungsi team ini adalah sebagai ujung tombak untuk troubleshooting setiap problem operasional dan maintenance di level pertama untuk semua pekerjaan: transmission backbone operation (yang berhubungan dengan kabel, fiber optik dan link transmisi), IP/MPLS operation (masalah yang berhubungan dengan router dan switch dan packet system), access operation (masalah yang berhubungan dengan radio dan akses seperti BTS, BSC, RAN dan PDH), CME operation (problem yang berhubungan dengan genset, gedung, batere, panel, dan tower) dan core operation (problem yang berhubungan dengan PS dan CS Core, IN-VAS, MSC dan HLR)

**c. Transmission Operation**

Departemen ini fungsinya untuk melakukan pengawasan dan pengendalian dan troubleshoot untuk setiap problem operasional yang berhubungan dengan backbone. Adapun level operasional untuk team ini adalah level 2 yang membawahi beberapa team atau group yakni: Satelit (problem yang berhubungan dengan pengoperasian satelit dan arah orbit satelit beserta maintenance-nya), Terrestrial (yang fungsinya untuk operasional dan pengendalian terhadap kabel coaxial dan fiber optic yang berada di dalam tanah), Backbone Core Transmisi (yaitu fungsinya untuk pengawasan dan pengendalian terhadap operasional dan masalah transmisi yang dibangun antar daerah di Indonesia), SKKL atau sistem komunikasi kabel laut (fungsinya melakukan pengawasan dan pengendalian terhadap operasional dan masalah di kabel laut antar pulau di Indonesia dan antar negara seperti Indonesia dengan Singapura, Malaysia, Australia dan lain-lain).

**d. IP/MPLS (Internet Protocol/Multi Packet Label System) Operation**

Departemen ini fungsinya untuk melakukan pengawasan dan pengendalian dan troubleshoot untuk setiap problem operasional yang berhubungan dengan Internet dan router. Adapun level proses operasional di team ini berada di level 2 yang membawahi beberapa team atau group yaitu network access point (NAP) yang fungsinya melakukan pengawasan, pengaturan dan pengendalian terhadap operasional dan masalah di jaringan ISP yang digunakan oleh provider penyewa internet services protocol (ISP) yang terafiliasi dengan PT. Indosat Ooredoo. MPLS operation yang fungsinya untuk operasional dan pengendalian terhadap penyampaian paket pada jaringan backbone berkecepatan tinggi. MPLS infrastructure yaitu fungsinya untuk pengawasan dan pengendalian terhadap infrastructure network dan penambahan kapasitas backbone bandwidth untuk internet dan network security yaitu fungsinya melakukan pengawasan, monitor dan pengendalian terhadap user akses yang mengakses semua operasional di network perangkat yang terhubung dengan perangkat MPLS.

**e. Access Operation**

Departemen ini fungsinya untuk melakukan pengawasan dan pengendalian dan troubleshoot untuk setiap problem operasional yang berhubungan dengan Akses. Adapun level proses operasional di team ini berada di level 2 yang membawahi beberapa team atau group yaitu: Access Operation PM yaitu pengawasan dan preventive maintenance terhadap perangkat RAN dan radio transmisi. Access RAN (Radio Access Network) yang mencakup 2G, 3G dan 4G (Fourth Generation) and BSC (Base Station Controller) dan BTS (Base Transceiver System). Access transport fungsinya untuk pengawasan dan pengendalian terhadap operasional dan masalah di radio transport.

**f. CME Operation**

Departemen ini fungsinya untuk melakukan pengawasan dan pengendalian dan troubleshoot untuk setiap problem operasional yang berhubungan dengan bangunan perangkat, Maintenance dan Electrical atau listrik atau power, penyewaan tanah untuk pembangunan site dan tower. Adapun level proses operasional di team ini berada di level 2 yang membawahi beberapa team atau group Yang fungsinya untuk operasional dan pengendalian terhadap supply batere, listrik sitac, AC, tower, shelter dan PAC. Setiap problem yang diinfokan oleh team Customer Front Office yang berhubungan dengan batere atau listrik akan langsung ditangani dan ditindaklanjuti oleh group ini.

**g. Core Operation**

Departemen ini fungsinya untuk melakukan penga-

wasan dan pengendalian dan troubleshoot untuk setiap problem operasional yang berhubungan dengan perangkat Core. Adapun level proses operasional di team ini berada di level 2 yang membawahi beberapa team atau group yang fungsinya untuk operasional dan pengendalian terhadap core services (CS). perangkat core seperti MSC (mobile station center) dan HLR (home register location). Packet services (PS) core yaitu pengawasan dan pengendalian terhadap operasional dan problem di GPRS (General Packet Radio Services), SGSN (Services GPRS Support Node) dan GGSN (Gateway GPRS support node). Value added services (VAS) yaitu fungsinya melakukan pengawasan dan pengendalian terhadap operasional dan problem di layanan/ features untuk kartu prepaid, SMS, video call, dan RBT (ring back tone). Integrated network (IN) yaitu pengawasan dan pengendalian terhadap operasional dan problem VAS bila ada VAS nya yang bermasalah. Roaming and inter carrier fungsinya untuk pengawasan dan pengendalian terhadap operasional dan poblem roaming saat di luar negeri dan kerjasam antar operator.

**h. Configuration Management**

Departemen ini fungsinya untuk melakukan pengawasan dan pengendalian dan troubleshoot untuk setiap problem operasional yang berhubungan dengan configurasi dan server. Semua departemen di bawah NOC berafiliasi dengan departemen ini baik dalam hal configurasi maupun dalam hal user akses. Adapun level proses operasional di team ini berada di level 2 yaitu menangani semua problem yang diinfokan oleh departemen yang berada di level 1 dan juga berada di level 3 yaitu menangani semua problem yang diinfokan oleh departemen yang berada di level 2. Problem problem yang tidak bisa ditangani oleh team ini akan diinfokan ke vendor sebagai mitra kerja dari perusahaan khususnya divisi NOC. Configuration management merupakan suatu departemen yang membawahi beberapa team atau group yaitu sistem inftrastructure and application support fungsinya melakukan pengawasan dan pengendalian serta prventive maintenance terhadap operasional dan problem di perangkat server OSS (operational support system) dan juga sebagai network security terhadap semua user yang akses di perangkat NOC (network operation center). Integration IP/MPLS transport yaitu integrasi dan configurasi di perangkat IP/MPLS, integration backbone transmisi yaitu integrasi dan configurasi perangkat backbone transmisi, integration BB & PDH transport yaitu integrasi dan configurasi di perangkat BB (Backbone) & PDH (Plesynchronous Digital Hierarki) transport, integration access and CME yaitu integrasi dan configurasi di perangkat access dan CME.

**i. Partner Management**

Departemen ini fungsinya untuk melakukan pengawasan terhadap vendor sebagai mitra kerja divisi NOC dalam menangani semua kegiatan kegiatan dalam menambah jaringan dan perbaikan jaringan, juga sebagai mitra kerja dengan semua departemen dibawah NOC yang berhubungan dengan vendor dalam pekerjaannya. Departmen ini membawahi team contract maintenance management yang fungsinya melakukan kerjasama kontrak maintenance dengan semua vendor yang melayani perangkat yang ada di divisi NOC (network operation center). Team ini melakukan pengawasan dan terhadap kinerja vendor, report vendor, estimasi biaya untuk contract maintenance dan penalty terhadap vendor yang tidak tepat waktu melaksanakan pekerjaannya dan membantu kinerja departemen di NOC untuk setiap kasus yang berhubungan dengan vendor.

## 4.2. Profil Responden

Pengambilan informan pada setiap departemen dilakukan dengan mengambil responden sebanyak 6 orang perwakilan dari departemen dalam mengisi kuisioner tentang identifikasi risiko yang ada pada setiap departemen yakni.. Teknik sampling yang digunakan adalah convenience sampling yakni karyawan yang bersedia secara sukarela mau mengisi kuisioner yang telah diberikan. Berdasarkan hasil penyebaran kusioner adapun karakteristik responden dibagi berdasarkan Jabatan, pendidikan, lama bekerja dan jumlah pelatihan yang pernah diikuti.

### 4.2.1. Karakteristik Responden Berdasarkan Jabatan

Karakteristik responden ditinjau berdasarkan jabatan yang terdapat pada Tabel 4.1.

**Tabel 4.1. Karakteristik Responden Berdasarkan Jabatan Struktural**

| Jabatan dalam struktur | Jumlah | % |
|---|---|---|
| *Manager* | 6 orang | 8 % |
| *Senior Engineer* | 29 orang | 37 % |
| *Engineer* | 21 orang | 27 % |
| *Senior Technician* | 17 orang | 22 % |
| *Technician* | 4 orang | 5% |
| *Junior Technician* | 1 orang | 1 % |
| Total | 78 orang | 100 % |

Sumber: Data Aktual yang diolah dengan excel

Berdasarkan data pada Tabel 4.1 menjelaskan bahwa responden berada pada jabatan terbesar yakni pada senior engineer sebesar 29 responden (37 %) dan kedua terbesar pada engineer sebesar 21 responden (27 %) dan diikuti oleh senior technican sebanyak 17 responden (22 %). Hal ini menggambarkan bahwa tanggung jawab secara operational networking terdapat pada ketiga fungsi tersebut. Sedangkan posisi manager bertanggungjawab atas berjalannya sistem networking pada perusahaan.

### 4.2.2. Karakteristik Responden Berdasarkan Pendidikan

Karakteristik responden berdasarkan tingkat pendidikan yang terdapat pada tabel 4.2.

**Tabel 4.2. Karakteristik Responden Berdasarkan Tingkat Pendidikan**

| Tingkat Pendidikan | Jumlah | % |
|---|---|---|
| D3 | 1 orang | 1 % |
| S1 | 69 orang | 89 % |
| S2 | 8 orang | 10 % |
| Total | 78 orang | 100% |

Sumber: Data Aktual kuesioner yang diolah dengan excel

Berdasarkan Tabel 4.2. diatas, karakteristik responden dari tingkat pendidikan menunjukkan bahwa responden berpendidikan Diploma (D3) sebanyak 1 orang (1 %), responden berpendidikan Sarjana (S1) sebanyak 69 orang (89 %), responden berpendidikan Magister (S2) sebanyak 8 orang (10 %). Hal ini menunjukkan bahwa penanggung jawab dan pengguna analisa data pada divisi networking PT. Indosat telah menempuh pendidikan lanjutan di perguruan tinggi, sehingga dapat diartikan bahwa karyawan pada perusahaan dapat digolongkan yang berpendidikan dan memiliki pengetahuan yang mumpuni pada bidangnya masing-masing.

### 4.2.3. Karakteristik Responden Berdasarkan Lama bekerja

Karakteristik responden ditinjau berdasarkan lama bekerja di perusahaan pada Tabel 4.3, menunjukkan bahwa tidak ada responden yang bekerja dibawah tiga tahun, responden perusahaan dengan implementasi antara 1 tahun < 2 tahun sebanyak 4 buah perusahaan (5 %), responden perusahaan dengan implementasi antara 2 tahun < 3 tahun sebanyak 14 buah perusahaan (18 %), responden perusahaan dengan implementasi antara 3 tahun < 5 tahun sebanyak 30 buah perusahaan (39 %), responden perusahaan dengan implementasi ERP lebih atau sama dengan 5 tahun sebanyak 29 buah perusahaan (38 %). Hal ini menunjukkan bahwa perusahaan sudah lama (77 % lebih dari 3 tahun) mengimplementasikan ISO dan telah mendapatkan benefit yang sesuai dengan harapan perusahaan.

**Tabel 4.3. Karakteristik Responden Berdasarkan Lama Bekerja**

| Lama Bekerja (tahun) | Jumlah | % |
|---|---|---|
| ≤ 3 tahun | 0 orang | 0 |
| 3 < lama bekerja ≤ 6 tahun | 3 orang | 4 % |
| 6 < lama bekerja ≤ 9 tahun | 7 orang | 9 % |
| 9 < lama bekerja ≤ 12 tahun | 10 orang | 13 % |
| 12 < lama bekerja ≤ 15 tahun | 30 orang | 38 % |
| 15 < lama bekerja ≤ 18 tahun | 7 orang | 9 % |
| 18 < lama bekerja ≤ 21 tahun | 15 orang | 19 % |
| 21 < lama bekerja ≤ 24 tahun | 6 orang | 8 % |
| Total | 78 orang | 100% |

Sumber: Data Aktual kuesioner yang diolah dengan excel

### 4.2.4. Karakteristik Responden Berdasarkan Jumlah Pelatihan

Karakteristik responden ditinjau berdasarkan jumlah pelatihan di perusahaan pada Tabel 4.4.

**Tabel 4.4. Karakteristik Responden Berdasarkan Jumlah Pelatihan**

| Jumlah Pelatihan (kali) | Jumlah | % |
|---|---|---|
| Jumlah Pelatihan < 10 kali | 1 orang | 1 % |
| 10 ≤ Jumlah Pelatihan < 20 kali | 12 orang | 14 % |
| 20 ≤ Jumlah Pelatihan < 30 kali | 34 orang | 39 % |
| 30 ≤ Jumlah Pelatihan < 40 kali | 25 orang | 29 % |
| 40 ≤ Jumlah Pelatihan < 50 kali | 15 orang | 17 % |
| Total | 78 orang | 100% |

Sumber: Data Aktual kuesioner yang diolah dengan excel

Berdasarkan Tabel 4.4. diatas, karakteristik responden dari tingkat jumlah pelatihan kurang dari sepuluh kali didapatkan seorang responden sebesar 1 %. Sedangkan jumlah responden terbesar sebanyak 34 responden (39 %) mengikuti pelatihan antara dua puluh sampai dengan tiga puluh kali. Diikuti dengan jumlah responden kedua terbesar sebanyak 25 responden (29 %) mengikuti pelatihan tigapuluh kali sampai dengan empat puluh kali. Sedangkan jumlah pelatihan yang lebih dari sepuluh kali sebesar 99 %, hal ini memberikan gambaran bahwa responden yang telah terpilih memiliki kemampuan dalam mengikuti perkembangan teknologi yang ada. Hasil pelatihan ini juga didapatkan oleh responden untuk mengatasi permasalahan-permasalahan yang ada pada departemen, dan juga menambah kemampuan untuk mengidentifikasi risiko-risiko yang terjadi pada perusahaan.

## 4.3 Identifikasi Risiko

Identifikasi risiko adalah suatu proses untuk mengidentifikasi peristiwa yang memiliki unsur ketidakpastian yang secara negatif mempengaruhi pencapaian sasaran. Peristiwa didefenisikan sebagai suatu kejadian dari sumber internal maupun eksternal perusahaan, yang dapat mempengaruhi pencapaian sasaran. Hasil penyebaran kuisioner terhadap setiap departemen pada perusahaan PT. Indosat Ooredoo Tbk.

**a. Front Office.**

Berdasarkan penyebaran kuisioner dan wawancara dengan manager, senior engineer dan engineer pada bagian consumer front office didapatkan beberapa risiko yang telah terjadi dan potensi terjadi pada bagian tersebut yakni: memberikan informasi profile customer ke pihak yang tidak berkepentingan, adanya risiko perjalanan untuk team karyawan shift yang pulang malam, teknisi ketiduran sehingga alarm problem diinfokan terlambat, karyawan sering mensharing user dan passwordnya ke karyawan yang tidak berkepentingan dan kesalahan menjelaskan informasi roote cause dari teknikal ke CCS.

**b. Regional Operation (Jabodetabek Operation, CJWJ Operation, EJBN Operation, Kalisula and Papua Operation, dan Sumatera Operation).**

Berdasarkan penyebaran kuisioner dan wawancara dengan manajer, senior engineer, senior technican, technican dan engineer pada bagian regional operation yang terdiri atas lima departemen tersebut didapatkan beberapa risiko yang telah terjadi dan potensi terjadi pada bagian tersebut yakni: Kurangnya SDM Teknisi, sehingga BTS tidak termonitor dan tertangani dengan baik; complain pelanggan sinyal jelek; Tidak Adanya Kendaraan Operasional, Penanganan complain pada pelanggan menjadi lambat; Pencurian Batere, Genset dan antena sehingga services ke pelanggan terganggu dan sinyal jelek; Premanisme (Setiap ke site di ganggu oleh preman dan minta uang keamanan) dan Stock Modul/Perangkat Tidak ada sehingga Perangkat BTS dan MSC (Mobile Switching Center) tidak bisa diperbaiki akibatnya complain pelanggan sinyal jelek dan Bencana alam (Gempa bumi dan Gunung Api meletus)

**c. Transmission Operation.**

Berdasarkan penyebaran kuisioner dan wawancara dengan manajer dan senior technican serta senior engineer pada departemen tersebut didapatkan beberapa risiko yang telah terjadi dan potensi terjadi pada bagian tersebut yakni: Kabel Fiber Optic putus karena tercangkul, Saluran Kabel laut Putus, Banjir yang menyebabkan kabel coaxial putus, Satelit yang hilang dari Orbitnya dan link VSAT yang terkena petir dan cuaca buruk sehingga akses ATM di Bank lambat.

**d. IP/MPLS (Internet Protocol/Multi Packet Label System) Operation.**

Berdasarkan penyebaran kuisioner dan wawancara dengan manajer, senior engineer dan engineer pada departemen tersebut didapatkan beberapa risiko yang telah terjadi dan potensi terjadi pada bagian tersebut yakni: vendor Indosat melakukan pekerjaan di sistem MPLS Jaringan Indosat dengan salah IP destination sehingga akses data

indosat down, Karyawan melakukan salah setting routing dan layer di Network sehingga jaringan data putus, Jaringan MPLS tiba tiba down karena salah ubah network layer sehingga internet, video streaming dan akses sosial media problem, topologi/Network Backbone internasional Indosat Down mengakibatkan pelanggan sulit akses, Network Indosat Putus karena kesalahan karyawan

**e. Access Operation.**

Berdasarkan penyebaran kuisioner dan wawancara dengan senior engineer, engineer dan senior technican pada bagian accsess operation didapatkan beberapa risiko yang telah terjadi dan potensi terjadi pada bagian tersebut yakni: Kurangnya SDM sementara perangkat dan teknologi semakin bertambah, keamanan lingkungan kerja juga harus menjadi perhatian karena sering terjadi kehilangan laptop/ hp, Risiko Human Error dan Employee Accident perlu diperhatikan, Kurangnya kendaraan operasional, fasilitas computer/laptop untuk pegawai Outsourching masih minim sehingga kinerja lambat.

**f. CME (Civil, Maintenance and Electrical) Operation**

Berdasarkan penyebaran kuisioner dan wawancara dengan manajer, senior engineer dan engineer pada departemen CME operation didapatkan beberapa risiko yang telah terjadi dan potensi terjadi pada bagian tersebut yakni: PLN sering off di daerah sehingga perangkat BTS dan BSC down, pengecekan genset yang dilakukan terlambat, genset tidak otomatis menyala, sehingga dilakukan pergantian secara manual, AC untuk inner di site (MSC, BSC dan BTS) rusak dan part lama pergantian, dan Kemampuan karyawan tentang AC, batere dan genset masih kurang dan tanah yang disewa untuk penempatan tower tidak diperpanjang kontraknya oleh pemiliknya.

**g. Core Operation**

Berdasarkan penyebaran kuisioner dan wawancara dengan senior engineer dan engineer pada bagian core operation didapatkan beberapa risiko yang telah terjadi dan potensi terjadi pada bagian tersebut yakni: kesalahan konfigurasi pada sistem core seperti PS, CS dan IN-VAS, kesalahan action hardware pada saat pekerjaan onsite ke MSC, kurangnya pengawasan terhadap vendor, karyawan memberikan sms dan voice pelanggan tanpa seijin perusahaan dan polisi, karyawan outsourching diberikan user yang tidak sesuai level yang telah ditetapkan.

**h. Configuration Management.**

Berdasarkan penyebaran kuisioner dan wawancara dengan senior engineer, engineer dan technican pada bagian configuration management didapatkan beberapa risiko yang telah terjadi dan potensi terjadi pada bagian tersebut yakni: perangkat server mati, server rusak, server kena virus, password admin server di sharing ke team yang tidak bertanggung jawab, modul dan sparepart server adalah import sehingga membutuhkan waktu yang lama.

**i. Partner Management.**

Berdasarkan penyebaran kuisioner dan wawancara dengan manager, senior engineer, engineer, dan junior technican pada bagian partner management didapatkan beberapa risiko yang telah terjadi dan potensi terjadi pada bagian tersebut yakni: vendor Indosat melakukan pendekatan ke karyawan lewat hadiah agar mempermudah kerjasama kontrak maintenance, karyawan bekerjasama dengan vendor untuk mempermudah report maintenance, karyawan mendapatkan hadiah vendor agar memenangkan tender kontrak, karyawan mengurangi pinalty buat vendor yang tidak tepat waktu dalam menjalankan pekerjaan, dan karyawan tidak objektif dalam menentukan vendor yang menang.

## 4.4. Pengukuran Risiko

Pengukuran risiko adalah suatu proses untuk mengukur tingkat likelihood dan dampak terjadinya risiko. Pengukuran risiko yang dilakukan atas risiko inhern merupakan risiko sebelum adanya tindakan apapun untuk mengubah likelihood maupun dampak risiko yakni risiko dengan kondisi departemen pada perusahaan saat dilakukan wawancara atau pemetaan oleh personal-personal yang ada pada departemen tersebut. Pengukuran untuk setiap risiko pada setiap departemen berbeda dengan departemen lain karena berbedan jenis pekerjaan dan tanggung jawabnya. Dari data di Tabel 3.1 di bab 3.5 tentang pengukuran risiko dijelaskan tentang kejadian, probabilitas kejadian dan berapa kali kejadian dalam 1 tahun. Dari data tersebut didapatkan skor peluangnya. Maka dari hasil data yang diolah didapatkan sebagai berikut:

**a. Front Office.**

Berdasarkan hasil penyebaran kuesioner dengan didapatkan hasil identifikasi risiko maka dapat diberikan penilaian besarnya risiko yang terjadi pada bagian front

office berdasarkan hasil fokus group discussion terhadap enam karyawan dan didapatkan nilai dampak dan peluang terjadi sebagai berikut:

**Tabel 4.5. Pengukuran Risiko pada Front Office**

| Identifikasi Risiko | Dampak | | Peluang terjadi | |
|---|---|---|---|---|
| | Ukuran | Skor | Potensi Kejadian | skor |
| Memberikan informasi profile customer ke pihak yang tidak berkepentingan | Besar | 4 | Jarang | 1 |
| Adanya risiko perjalanan untuk team karyawan shift yang pulang malam | sedang | 3 | Kemungkinan sedang | 3 |
| Teknisi ketiduran sehingga alarm problem diinfokan terlambat | Kecil | 2 | Kemungkinan Besar | 4 |
| Karyawan sering mensharing user dan passwordnya ke karyawan yang tidak berkepentingan | Kecil | 2 | Kemungkinan Besar | 4 |
| Kesalahan menjelaskan informasi route cause dari teknikal ke CCS | Kecil | 2 | Kemungkinan sedang | 3 |

Sumber: Data Aktual kuesioner yang diolah dengan excel

b. Regional Operation (Jabodetabek Operation, CJWJ Operation, EJBN Operation, Kalisula and Papua Operation, dan Sumatera Operation).

Berdasarkan hasil identifikasi risiko maka dapat diberikan penilaian besarnya risiko yang terjadi pada departemen regional operation berdasarkan hasil fokus group discussion terhadap enam karyawan di Jabotabek operation, enam karyawan di Central and West Java operation, enam karyawan pada East java and Bali Nusa operation, Kalisula operation dan Sumatera operation didapatkan nilai dampak dan peluang terjadi sebagai berikut:

**Tabel 4.6. Pengukuran Risiko pada Regional Operation**

| Identifikasi Risiko | Dampak | | Peluang terjadi | |
|---|---|---|---|---|
| | Ukuran | Skor | Potensi Kejadian | skor |
| Kurangnya SDM Teknisi | Sedang | 3 | Kemungkinan sedang | 3 |
| Complain pelanggan sinyal jelek | Besar | 4 | Kemungkinan sedang | 3 |
| Tidak Adanya Kendaraan Operasional | Kecil | 2 | Kemungkinan sedang | 3 |
| Penanganan complain pelanggan lambat | Besar | 4 | Kemungkinan sedang | 3 |
| Pencurian Batere, Genset dan antena | Besar | 4 | Jarang | 1 |
| Premanisme (Setiap ke site di ganggu oleh preman dan minta uang keamanan) | Sedang | 3 | Hampir pasti | 4 |
| Stock Modul/Perangkat Tidak ada sehingga Perangkat BTS dan MSC tidak bisa diperbaiki. | Besar | 4 | Kemungkinan terjadi | 2 |
| Bencana alam (Gempa bumi dan Gunung Api meletus) | Sangat Besar | 5 | Jarang | 1 |

Sumber: Data Aktual kuesioner yang diolah dengan excel

**c. Transmission Operation.**

Berdasarkan hasil identifikasi risiko maka dapat diberikan penilaian besarnya risiko yang terjadi pada departemen Transmission Backbone Operation berdasarkan hasil fokus group discussion terhadap enam karyawan didapatkan nilai dampak dan peluang terjadi adalah sebagai berikut:

**Tabel 4.7. Pengukuran Risiko pada Transmission Operation**

| Identifikasi Risiko | Dampak | | Peluang terjadi | |
|---|---|---|---|---|
| | Ukuran | Skor | Potensi Kejadian | skor |
| Kabel Fiber Optic putus karena tercangkul | Besar | 4 | Kemungkinan terjadi | 2 |
| Saluran Kabel laut Putus | Besar | 4 | Kemungkinan terjadi | 2 |
| Banjir yang menyebabkan kabel coaxial putus | Besar | 4 | Kemungkinan terjadi | 2 |
| Satelit yang hilang dari Orbitnya | Sangat besar | 5 | Jarang | 1 |
| link VSAT yang terkena petir dan cuaca buruk sehingga akses ATM di Bank lambat | sedang | 3 | Kemungkinan terjadi | 2 |

*Sumber: Data Aktual kuesioner yang diolah dengan excel*

Sumber: Data Aktual kuesioner yang diolah dengan excel

d. IP/MPLS Operation.

Berdasarkan hasil identifikasi risiko maka dapat diberikan penilaian besarnya risiko yang terjadi pada departemen IP/MPLS berdasarkan hasil fokus group discussion terhadap enam karyawan didapatkan nilai dampak dan peluang terjadi sebagai berikut:

**Tabel 4.8. Pengukuran Risiko pada IP/MPLS Operation**

| Identifikasi Risiko | Dampak | | Peluang terjadi | |
|---|---|---|---|---|
| | Ukuran | Skor | Potensi Kejadian | skor |
| Vendor Indosat melakukan pekerjaan di system MPLS Jaringan Indosat dengan salah IP destination sehingga akses data indosat down | Besar | 4 | Kemungkinan terjadi | 2 |
| Karyawan melakukan salah setting routing dan layer di Network sehingga jaringan data putus | Besar | 4 | Kemungkinan terjadi | 2 |
| Jaringan MPLS tiba tiba down karena salah ubah network layer sehingga internet, video streaming dan akses sosial media problem | Besar | 4 | Kemungkinan terjadi | 2 |
| Topologi/Network Backbone internasional Indosat Down mengakibatkan pelanggan sulit akses | Besar | 4 | Jarang | 1 |
| Network Indosat Putus karena kesalahan karyawan | Sangat besar | 5 | Jarang | 1 |

Sumber: Data Aktual kuesioner yang diolah dengan excel

e. Access Operation.

Berdasarkan hasil identifikasi risiko maka dapat diberikan penilaian besarnya risiko yang terjadi pada departemen access operation berdasarkan hasil fokus group

discussion terhadap enam karyawan didapatkan nilai dampak dan peluang terjadi sebagai berikut:

**Tabel 4.9. Pengukuran Risiko pada Access Operation**

| Identifikasi Risiko | Dampak | | Peluang terjadi | |
|---|---|---|---|---|
| | Ukuran | Skor | Potensi Kejadian | skor |
| Kurangnya SDM sementara perangkat dan teknologi semakin bertambah | Sedang | 3 | Kemungkinan besar | 4 |
| Keamanan lingkungan kerja juga harus menjadi perhatian karena sering terjadi kehilangan laptop/hp | Kecil | 2 | Kemungkinan besar | 4 |
| Risiko Human Error dan Employee Accident perlu diperhatikan | Kecil | 2 | Kemungkinan besar | 4 |
| Kurangnya kendaraan operasional | Kecil | 2 | Kemungkinan sedang | 3 |
| Fasilitas computer/laptop untuk pegawai Outsourching masih minim sehingga kinerja lambat | Kecil | 2 | Kemungkinan besar | 4 |

Sumber: Data Aktual kuesioner yang diolah dengan excel

f. CME Operation

Berdasarkan hasil identifikasi risiko maka dapat diberikan penilaian besarnya risiko yang terjadi pada bagian CME operation berdasarkan hasil fokus group discussion terhadap enam karyawan didapatkan nilai dampak dan peluang terjadi sebagai berikut:

**Tabel 4.10. Pengukuran Risiko pada CME Operation**

| Identifikasi Risiko | Dampak | | Peluang terjadi | |
|---|---|---|---|---|
| | Ukuran | Skor | Potensi Kejadian | skor |
| PLN sering off di daerah sehingga perangkat BTS dan BSC down | Sedang | 3 | Kemungkinan besar | 4 |
| Pengecekan genset yang dilakukan terlambat | Kecil | 2 | Kemungkinan sedang | 3 |
| Genset tidak otomatis menyala, sehingga dilakukan pergantian secara manual | Sedang | 3 | Kemungkinan terjadi | 2 |
| AC untuk inner di site (MSC, BSC dan BTS) rusak dan part lama pergantian | Sedang | 3 | Kemungkinan terjadi | 2 |
| Kemampuan karyawan tentang AC, batree dan genset masih kurang | Sedang | 3 | Kemungkinan terjadi | 3 |
| Tanah yang disewa untuk penempatan tower tidak diperpanjang kontraknya oleh pemiliknya | Sedang | 3 | Kemungkinan terjadi | 3 |

Sumber: Data Aktual kuesioner yang diolah dengan excel

g. Core Operation

Berdasarkan hasil identifikasi risiko maka dapat diberikan penilaian besarnya risiko yang terjadi pada bagian core operation berdasarkan hasil fokus group discussion terhadap enam karyawan didapatkan nilai dampak dan peluang terjadi sebagai berikut:

**Tabel 4.11. Pengukuran Risiko pada Core Operation**

| Identifikasi Risiko | Dampak | | Peluang terjadi | |
|---|---|---|---|---|
| | Ukuran | Skor | Potensi Kejadian | skor |
| Kesalahan konfigurasi pada system core seperti PS, CS dan IN-VAS | Kecil | 2 | Kemungkinan sedang | 3 |
| Kesalahan action hardware pada saat pekerjaan on site ke MSC | Sedang | 3 | Kemungkinan terjadi | 2 |
| Kurangnya pengawasan terhadap vendor | Kecil | 2 | Kemungkinan sedang | 3 |
| Karyawan memberikan isi sms dan voice pelanggan tanpa seijin perusahaan dan polisi | Besar | 4 | Jarang | 1 |
| Karyawan outsourching diberikan user yang tidak sesuai level yang telah ditetapkan | Besar | 4 | Kemungkinan terjadi | 2 |

Sumber: Data Aktual kuesioner yang diolah dengan excel

h. Configuration Management.

Berdasarkan hasil identifikasi risiko maka dapat diberikan penilaian besarnya risiko yang terjadi pada configuration management berdasarkan hasil fokus group discussion maka didapatkan nilai dampak dan peluang terjadi yakni:

**Tabel 4.12. Pengukuran Risiko pada Configuration Management**

| Identifikasi Risiko | Dampak | | Peluang terjadi | |
|---|---|---|---|---|
| | Ukuran | Skor | Potensi Kejadian | skor |
| Perangkat server mati | Kecil | 2 | Kemungkinan sedang | 3 |
| Server rusak | Sedang | 2 | Kemungkinan terjadi | 2 |
| Server kena virus | Kecil | 2 | Kemungkinan sedang | 3 |
| Password admin server di sharing ke team yang tidak bertanggung jawab | Besar | 3 | Jarang | 1 |
| Modul dan sparepart server adalah import sehingga membutuhkan waktu yang lama | Besar | 4 | Kemungkinan terjadi | 2 |

Sumber: Data Aktual kuesioner yang diolah dengan excel

i. Partner Management.

Berdasarkan hasil identifikasi risiko maka dapat diberikan penilaian besarnya risiko yang terjadi pada partner management berdasarkan hasil fokus group discussion terhadap enam karyawan didapatkan nilai dampak dan peluang terjadi sebagai berikut:

**Tabel 4.13. Pengukuran Risiko pada Partner Management**

| Identifikasi Risiko | Dampak | | Peluang terjadi | |
|---|---|---|---|---|
| | Ukuran | Skor | Potensi Kejadian | skor |
| Vendor (supplier) Indosat melakukan pendekatan ke karyawan lewat hadiah agar mempermudah kerjasama kontrak maintenance | Besar | 4 | Jarang | 1 |
| Karyawan bekerjasama dengan vendor untuk mempermudah report maintenance | Sedang | 3 | Kemungkinan terjadi | 2 |
| Karyawan mendapatkan hadiah dari vendor (supplier) agar memenangkan tender kontrak | Besar | 4 | Jarang | 1 |
| Karyawan mengurangi pinalty buat vendor yang tidak tepat waktu dalam menjalankan pekerjaan | Besar | 4 | Jarang | 1 |
| Karyawan tidak objektif dalam menentukan vendor yang menang | Besar | 4 | Jarang | 1 |

Sumber: Data Aktual kuesioner yang diolah dengan excel

## 4.5. Analisis Risiko

Analisis risiko digunakan untuk penentuan kriteria risiko yang terjadi pada departemen masing-masing. Analisis risiko adalah analisa dampak dan kemungkinan semua risiko yang dapat menghambat tercapainya sasaran organisasi. Analisis risiko mencakup pertimbangan dan mengkombinasikan estimasi terhadap consequence (dampak) dan likelihood di dalam konteks untuk mengambil tindakan pengendalian.

a. Front Office.

Berdasarkan hasil pengukuran risiko consumer front office didapatkan analisis risiko sebagai berikut:

**Tabel 4.14. Penentuan Risiko pada Front Office**

| Identifikasi Risiko | Dampak X Peluang terjadi | | | Kriteria Risiko |
|---|---|---|---|---|
| | Skor dampak | Skor peluang | Hasil risiko | |
| Memberikan informasi profile customer ke pihak yang tidak berkepentingan | 4 | 1 | 4 | Acceptable |
| Adanya risiko perjalanan untuk team karyawan shift yang pulang malam | 3 | 3 | 9 | Issue |
| Teknisi ketiduran sehingga alarm problem diinfokan terlambat | 2 | 4 | 8 | Supplementary Issue |
| Karyawan sering mensharing user dan passwordnya ke karyawan yang tidak berkepentingan | 2 | 4 | 8 | Supplementary Issue |
| Kesalahan menjelaskan informasi root cause dari teknikal ke CCS | 2 | 3 | 6 | Supplementary Issue |
| Nilai rata rata risiko departemen | (4 + 9 + 8 + 8 + 6) : 5 = 7 | | | |

Sumber: Data Aktual kuesioner yang diolah dengan excel

b. Regional Operation (Jabodetabek Operation, CJWJ Operation, EJBN Operation, Kalisula and Papua Operation, dan Sumatera Operation). Berdasarkan hasil pengukuran risiko regional operation didapatkan analisa risiko sebagai berikut:

**Tabel 4.15. Penentuan Risiko pada Regional Operation**

| Identifikasi Risiko | Dampak X Peluang terjadi | | | Kriteria Risiko |
|---|---|---|---|---|
| | Skor dampak | Skor dampak | Skor dampak | |
| Kurangnya SDM Teknisi | 3 | 3 | 9 | Supplementary Issue |
| Complain pelanggan sinyal jelek | 4 | 3 | 12 | Issue |
| Tidak Adanya Kendaraan Operasional | 2 | 3 | 6 | Supplementary Issue |
| Penanganan complain pelanggan lambat | 4 | 3 | 12 | Issue |
| Pencurian Batere, Genset dan antena | 4 | 1 | 4 | Acceptable |
| Premanisme (Setiap ke site di ganggu oleh preman dan minta uang keamanan) | 3 | 4 | 12 | Issue |
| Stock Modul/Perangkat Tidak ada sehingga Perangkat BTS dan MSC tidak bisa diperbaiki. | 4 | 2 | 8 | Supplementary Issue |
| Bencana alam (Gempa bumi dan Gunung Api meletus) | 5 | 1 | 5 | Supplementary Issue |
| Nilai rata rata risiko departemen | (9 + 12 + 6 + 12 + 4 + 12 + 8 + 5) : 8 = 8,5 | | | |

Sumber: Data Aktual kuesioner yang diolah dengan excel

c. Transmission Operation.

Berdasarkan hasil pengukuran risiko transmission backbone operation didapatkan analisa risiko sebagai berikut:

**Tabel 4.16. Penentuan Risiko pada Transmission Operation**

| Identifikasi Risiko | Dampak X Peluang terjadi | | | Kriteria Risiko |
|---|---|---|---|---|
| | Skor dampak | Skor dampak | Skor dampak | |
| Kabel Fiber Optic putus karena tercangkul | 4 | 2 | 8 | Supplementary Issue |
| Saluran Kabel laut Putus | 4 | 2 | 8 | Supplementary Issue |
| Banjir yang menyebabkan kabel coaxial putus | 4 | 2 | 8 | Supplementary Issue |
| Satelit yang hilang dari Orbitnya | 5 | 1 | 5 | Supplementary Issue |
| link VSAT yang terkena petir dan cuaca buruk shg akses ATM di Bank lambat | 3 | 2 | 6 | Supplementary Issue |
| Nilai rata rata risiko departemen | (8 + 8 + 8 + 5 + 6 ) : 5 = 7 | | | |

*Sumber: Data Aktual kuesioner yang diolah dengan excel*

Sumber: Data Aktual kuesioner yang diolah dengan excel

d. IP/MPLS Operation.

Berdasarkan hasil pengukuran risiko IP/MPLS operation didapatkan analisa risiko sebagai berikut:

**Tabel 4.17. Penentuan Risiko pada IP/MPLS Operation**

| Identifikasi Risiko | Dampak X Peluang terjadi | | | Kriteria Risiko |
|---|---|---|---|---|
| | Skor dampak | Skor dampak | Skor dampak | |
| vendor Indosat melakukan pekerjaan di system MPLS Jaringan Indosat dengan salah IP destination sehingga akses data indosat down | 4 | 2 | 8 | Supplementary Issue |
| Karyawan melakukan salah setting routing dan layer di Network sehingga jaringan data putus | 4 | 2 | 8 | Supplementary Issue |
| Jaringan MPLS tiba tiba down karena salah ubah network layer sehingga internet, video streaming dan akses sosial media problem | 4 | 2 | 8 | Supplementary Issue |
| Topologi/Network Backbone internasional Indosat Down mengakibatkan pelanggan sulit akses | 4 | 1 | 4 | Acceptable |
| Network Indosat Putus karena kesalahan karyawan | 5 | 1 | 5 | Supplementary Issue |
| Nilai rata rata risiko departemen | (8 + 8 + 8 + 4 + 5 ) : 5 = 6,6 | | | |

Sumber: Data Aktual kuesioner yang diolah dengan excel

e. Access Operation.

Berdasarkan hasil pengukuran risiko accsess operation didapatkan analisa risiko sebagai berikut:

**Tabel 4.18. Penentuan Risiko pada Access Operation**

| Identifikasi Risiko | Dampak X Peluang terjadi | | | Kriteria Risiko |
|---|---|---|---|---|
| | Skor dampak | Skor dampak | Skor dampak | |
| Kurangnya SDM sementara perangkat dan teknologi semakin bertambah | 3 | 4 | 12 | Issue |
| Keamanan lingkungan kerja juga harus menjadi perhatian karena sering terjadi kehilangan laptop/hp | 2 | 4 | 8 | Supplementary Issue |
| Risiko Human Error dan Employee Accident perlu diperhatikan | 2 | 4 | 8 | Supplementary Issue |
| Kurangnya kendaraan operasional | 2 | 3 | 6 | Supplementary Issue |
| Fasilitas computer/laptop untuk pegawai Outsourching masih minim sehingga kinerja lambat | 2 | 4 | 8 | Supplementary Issue |
| Nilai rata rata risiko departemen | (12 + 8 + 8 + 6 + 8 ) : 5 = 8,4 | | | |

Sumber: Data Aktual kuesioner yang diolah dengan excel

f. CME Operation

Berdasarkan hasil pengukuran risiko CME operation didapatkan analisa risiko sebagai berikut:

**Tabel 4.19. Penentuan Risiko pada CME Operation**

| Identifikasi Risiko | Dampak X Peluang terjadi | | | Kriteria Risiko |
|---|---|---|---|---|
| | Skor dampak | Skor dampak | Skor dampak | |
| PLN sering off di daerah sehingga perangkat BTS dan BSC down | 3 | 4 | 12 | Issue |
| Pengecekan genset yang dilakukan terlambat | 2 | 3 | 6 | Supplementary Issue |
| Genset tidak otomatis menyala, sehingga dilakukan pergantian secara manual | 3 | 2 | 6 | Supplementary Issue |
| AC untuk inner di site (MSC, BSC dan BTS) rusak dan part lama pergantian | 3 | 2 | 6 | Supplementary Issue |
| Kemampuan karyawan tentang AC, batree dan genset masih kurang | 3 | 3 | 9 | Supplementary Issue |
| Tanah yang disewa untuk penempatan tower tidak diperpanjang oleh pemiliknya | 3 | 3 | 9 | Supplementary Issue |
| Nilai rata rata risiko departemen | (12 + 6 + 6 + 6 + 9 + 9 ) : 6 = 8 | | | |

Sumber: Data Aktual kuesioner yang diolah dengan excel

g. Core Operation

Berdasarkan hasil pengukuran risiko core operation didapatkan analisa risiko sebagai berikut:

**Tabel 4.20. Penentuan Risiko pada Core Operation**

| Identifikasi Risiko | Dampak X Peluang terjadi | | | Kriteria Risiko |
|---|---|---|---|---|
| | Skor dampak | Skor dampak | Skor dampak | |
| Kesalahan konfigurasi pada system core seperti PS, CS dan IN-VAS | 2 | 3 | 6 | Supplementary Issue |
| Kesalahan action hardware pada saat pekerjaan on site ke MSC | 3 | 2 | 6 | Supplementary Issue |
| Kurangnya pengawasan terhadap vendor | 2 | 3 | 6 | Supplementary Issue |
| Karyawan memberikan sms dan voice pelanggan tanpa seijin perusahaan dan polisi | 4 | 1 | 4 | Acceptable |
| Karyawan outsourching diberikan user yang tidak sesuai level yang telah ditetapkan | 4 | 2 | 8 | Supplementary Issue |
| Nilai rata rata risiko departemen | (6 + 6 + 6 + 4 + 8 ) : 5 = 6 | | | |

Sumber: Data Aktual kuesioner yang diolah dengan excel

h. Configuration Management.

Berdasarkan hasil pengukuran risiko configuration management didapatkan analisa risiko sebagai berikut:

**Tabel 4.21. Penentuan Risiko pada Configuration Management**

| Identifikasi Risiko | Dampak X Peluang terjadi | | | Kriteria Risiko |
|---|---|---|---|---|
| | Skor dampak | Skor dampak | Skor dampak | |
| Perangkat server mati | 2 | 3 | 6 | Supplementary Issue |
| Server rusak | 2 | 2 | 4 | Acceptable |
| Server kena virus | 2 | 3 | 6 | Supplementary Issue |
| Password admin server di sharing ke team yang tidak bertanggung jawab | 3 | 1 | 3 | Acceptable |
| Modul dan sparepart server adalah import sehingga membutuhkan waktu yang lama | 4 | 2 | 8 | Supplementary Issue |
| Nilai rata rata risiko departemen | (6 + 4 + 6 + 3 + 8 ) : 5 = 5,4 | | | |

Sumber: Data Aktual kuesioner yang diolah dengan excel

i. Partner Management.

Berdasarkan hasil pengukuran risiko partner management didapatkan analisa risiko sebagai berikut:

**Tabel 4.22. Penentuan Risiko pada Partner Management**

| Identifikasi Risiko | Dampak X Peluang terjadi | | | Kriteria Risiko |
|---|---|---|---|---|
| | Skor dampak | Skor dampak | Skor dampak | |
| Vendor Indosat melakukan pendekatan ke karyawan lewat hadiah agar mempermudah kerjasama kontrak maintenance | 4 | 1 | 4 | Acceptable |
| Karyawan bekerjasama dengan vendor untuk mempermudah report maintenance | 3 | 2 | 6 | Supplementary Issue |
| Karyawan mendapatkan hadiah vendor agar memenangkan tender kontrak | 4 | 1 | 4 | Acceptable |
| Karyawan mengurangi pinalty buat vendor yang tidak tepat waktu dalam menjalankan pekerjaan | 4 | 1 | 4 | Acceptable |
| Karyawan tidak objektif dalam menentukan vendor yang menang | 4 | 1 | 4 | Acceptable |
| Nilai rata rata risiko departemen | (4 + 6 + 4 + 4 + 4 ) : 5 = 4,5 | | | |

Sumber: Data Aktual kuesioner yang diolah dengan excel

6. Evaluasi Risiko

Langkah evaluasi memastikan bahwa tidak semua risiko yang teridentifikasi memerlukan rencana pengendalian lebih lanjut. Dari daftar jenis risiko pada semua departemen di divisi network operation center tersebut didapatkan bahwa total jenis risiko sebanyak 49 dengan kategori Issue sebanyak 6, kategori Supplementary Issue sebanyak 33 dan kategori acceptable sebanyak 10. Hasil dari analisis risiko akan disampaikan kepada penanggung jawab tertinggi pengelola risiko di unit kerja untuk dilakukan validasi.

Hasil validasi akan digunakan untuk menetapkan rencana langkah–langkah sistem pengendalian untuk menurunkan kemungkinan terjadinya risiko maupun untuk menurunkan dampak terjadinya risiko pada setiap departemen.

Evaluasi yang dilakukan untuk setiap departemen di bagian network operation PT Indosat Ooredoo Tbk adalah sebagai berikut:

**a. Front Office.**

Departemen Front Office didapatkan tiga risiko termasuk kategori issue yang dimaksudkan untuk diperlukan suatu tindakan untuk mengelola risiko dan empat risiko termasuk pada kategori risiko supplementary issue yang didefinisikan untuk mengambil tindakan bila terjadi sumber daya yang memadai pada perusahaan dan satu risiko masuk pada kategori acceptable yakni tidak perlu dilakukan tindakan. Dari hasil analisis risiko yang terdapat di bab 4.5 maka didapatkan proses survey dan observasi di lapangan yakni di departemen Front Office dengan nilai rata-rata 7. Berdasarkan hasil wawancara dengan pihak manajer dan supervisor pada departemen ini maka telah dilakukan evaluasi dari daftar risiko yang kategori issue dan supplementary issue sebagai berikut ini:

1. Adanya risiko perjalanan untuk team karyawan shift yang pulang malam, menurut manager dan supervisor masalah ini ditangani dengan cara telah memberikan instruksi dan keputusan kepada karyawan yang masuk shift 2 (jam 14:00 s/d 22:00) dan pulangnya malam hari bila hari hujan atau keadaan tidak memungkinkan agar melanjutkan bekerja sampai shift 3 (22:00 s/d 06:00) menggantikan rekan kerja yg shift 3 dan pulangnya pagi hari. Di hari berikutnya rekan yang digantikan akan mengambil bagian lagi lanjut bekerja dengan 2 shift dari shift 2 sampai shift 3 sehingga risiko dapat dihindari.
2. Teknisi ketiduran sehingga alarm problem diinfokan terlambat, risiko ini ditangani manager dengan membuat IK (instruksi kerja) bahwa tidur di ruang kerja pada saat jam kerja maupun pada saat off akan dikenakan sanksi, bila memang karyawan karena kelelahan atau sakit sehingga tanpa sadar ketiduran di ruang kerja maka shift leadernya wajib mengawasi dan membangunkan. Setiap shift leader harus memperhatikan teamnya 10 sampai 15 menit sekali sehingga risiko alarm kelewatan dapat dihindari.
3. Karyawan sering mensharing user dan passwordnya ke karyawan yang tidak berkepentingan, risiko ini ditangani Manager dan Supervisor dengan membuat aturan tertulis dan SOP di departemennya bahwa karyawan tidak boleh mensharing user dan password ke karyawan lain. Ada konsekuensi buat yg melanggar atau punishment (hukuman) teguran untuk perbuatan sekali dan bila dilakukan berulang kali maka akan terkena sanksi Surat Peringatan (SP) dan bila karyawan telah mensharing user dan passwordnya ke karyawan lain dan mengakibatkan kerugian di perusahaan maka karyawan tersebut ikut bertanggung jawab dan sanksinya langsung dari HRD dan bisa berupa pemecatan. Departemen juga bekerjasama dengan team dari Security Management untuk melakukan pencegahan dengan metode :
   a. Karyawan hanya diberikan akses pada informasi dan system jaringan yang dibutuhkannya
   b. Mengimplementasikan metode identifikasi dan autentifikasi data yang dimiliki oleh security management serta menonaktifkan password dari user karyawan jikat tidak digunakan oleh karyawan dalam jangka waktu tertentu
4. Kesalahan menjelaskan informasi route cause dari teknikal ke CCS, risiko ini ditangani manager dengan cara memfasilitasi two weekly meeting dengan Customer Contact Services (CCS) untuk menyelesaikan issue seputar keluhan pelanggan di bagian network dan informasi root cause secara simple dan sederhana sehingga mudah dipahami oleh team CCS. Team CCS memfasilitasi sharing knowledge yang dilakukan oleh team Teknikal terkait jaringan ke team CCS sehingga karyawan di team CCS lebih mengerti dalam hal teknikal dan bisa lebih detail menjelaskan ke pelanggan. CCS membuat laporan tentang keluhan pelanggan kepada team teknikal secara tertulis dan lisan untuk menjelaskannya agar kedua belah pihak terjadinya sinkronisasi dalam hal mengisi form keluhan pelanggan.

**b. Regional Operation (Jabodetabek Operation, CJWJ Operation, EJBN Operation, Kalisula and Papua Operation, dan Sumatera Operation).**

Departemen regional operation didapatkan tiga

risiko yang termasuk pada kategori issue yang diartikan diperlukan tindakan segera untuk mengelola risiko dan empat pada kategori risiko supplementary issue yang didefinisikan untuk mengambil tindakan bila terjadi sumber daya yang memadai pada perusahaan, satu risiko masuk pada kategori acceptable yakni tidak perlu dilakukan tindakan. Dari hasil analisis risiko yang terdapat di bab 4.5 maka didapatkan proses survey dan observasi di lapangan yakni di departemen Regional Operation dengan nilai rata-rata yaitu: 8,5 Berdasarkan hasil wawancara dengan pihak manajer dan supervisor pada departemen ini maka telah dilakukan evaluasi dari daftar risiko yang kategori issue dan supplementary issue sebagai berikut ini:

1. Komplain pelanggan sinyal jelek, untuk case ini ada beberapa cara yang dilakukan yaitu:
   a. Di daerah urban atau perkotaan besar team Teknikal akan diberangkatkan ke lokasi yang diinfokan oleh pelanggan untuk mengetes kekuatan sinyal melalui alat BER TEST dan performansi data melalui Ookla Speedtest. Bila didapatkan sinyal jelek maka team Teknikal merokemendasikan agar di tambah Repeater yaitu penguat sinyal. Dalam hal ini akan dilakukan secepatnya penambahan repeater.
   b. Di dalam gedung bila didapatkan sinyal jelek maka akan dilakukan penambahan repeater atau BTS Indoor khusus untuk gedung, hotel dan mall
   c. Di daerah perkotaan kecil maka ditinjau terlebih dahulu dari sisi bisnis dengan koordinasi dengan team sales dan marketing, bila dirasa peluang pelanggan berpotensial atau pemasukan dari sisi pelanggan besar maka secepatnya diusulkan ke Divisi untuk penambahan BTS agar team Planning dan Project dapat menambah BTS ditambah BTS Outdoor dan ini bisa dilakukan pada tahun berjalan.
   d. Di daerah pedesaan atau non urban maka akan di chek seberapa besar jumlah pelanggan di daerah tersebut dan dari sisi bisnis dan biaya akan di lakukan koordinasi dengan team sales, dan marketing. Bila dari team sales dan marketing merekomendasikan untuk ditambah BTS maka di usulkan ke Divisi untuk penambahan BTS agar team Planning dan Project dapat menambah BTS yang dimaksud. Namun untuk hal ini bisa dilakukan dalam tahun berikutnya atau 2 tahun lagi tergantung dana OPEX dari perusahaan.
2. Premanisme, masalah ini paling sering di perkotaan besar seperti Jakarta dan Surabaya dimana banyak oknum organisasi pemuda yang berkedok menjaga keamanan tapi minta jatah uang keamanan dan oknum preman di daerah tersebut, untuk case ini ada beberapa cara yang dilakukan yaitu:
   a. Perusahaan bekerjasama dengan polisi untuk sewaktu waktu menemani, mengawasi dan siap bertindak bila ada laporan terkait pemerasan oleh oknum organisasi pemuda ataupun oleh preman setempat
   b. Personal Approach, yaitu melakukan pendekatan ke kelompok pemuda atau orang yang berpengaruh di daerah site tersebut untuk bekerjasama menjaga keamanan site dan kenyamanan karyawan bila dating ke site, dan cara ini juga ada biaya yang dialokasikan untuk pendekatan tersebut
   c. Menjadikan preman setempat atau pemuda di daerah tersebut menjadi satpam atau petugas keamanan site sehingga pemuda atau preman lain enggan untuk mengganggu.
3. Penanganan complain pelanggan lambat, masalah ini biasanya ditangani dengan cepat bila pelanggan dekat dengan kantor atau di daerah perkotaan yang dapat dijangkau oleh kenderaan Operasional. Untuk di daerah di luar jawa atau daerah lain di Indonesia masih disesuaikan dengan keadaan geografis daerah tersebut dan fasilitas yang dimililiki oleh departemen. Untuk mengatasi hal ini hal yg dapat dilakukan oleh departemen yaitu membuat team reaksi cepat bila ada complain pelanggan yang dekat akan secepatnya ditangani oleh team teknikal yang dipersiapkan.
4. Kurangnya SDM Teknisi: Untuk masalah ini langkah yang diambil yaitu melatih dan memberi sharing knowledge kepada team yang sudah ada agar bisa menguasai dan menangani problem teknikal berb-

agai hal misalnya akses (BTS, BSC dan PDH) juga Core (HLR, MSC, MGW) dan didiskusikan juga ke divisi agar menyiapkan budget untuk penambahan karyawan baru semisal karyawan Outsourching (OS) agar biayanya tidak mahal dan sesuai dengan OPEX.

5. Tidak adanya kenderaan operasional: Untuk masalah ini menurut manager bahwa kenderaan Operasional ada, namun tidak sebanyak diharapkan oleh karyawan dibandingkan dengan 5 atau 10 tahun yang lalu karena factor efisiensi dan persaingan perusahaan makin ketat. Sehingga langkah yang diambil manager yaitu memaksimalkan mobil Operasional yang ada dengan membawa team secara bersamaan untuk wilayah yang jauh. Untuk wilayah yang dekat dapat dilakukan dengan dengan motor karyawan dan biaya bisa di klaim ke departemen.
6. Stock Modul/Perangkat Tidak ada sehingga Perangkat BTS dan MSC tidak bisa diperbaiki, untuk masalah ini hal yang bisa dilakukan oleh manager yaitu menginfokan ke divisi dan ke departemen partner management untuk secepatnya mengorder modul ke vendor yang telah ditunjuk agar perangkat dapat diperbaiki.
7. Bencana alam (Gempa bumi dan Gunung api meletus), untuk masalah ini hal yang dapat dilakukan adalah menyiapkan spare part di kantor pusat sehingga bila sewaktu waktu ada bencana alam secepatnya dapat di kirim ke daerah tersebut untuk pergantian part.

**c. Transmission Operation.**

Departemen Transmission operation didapatkan kelima risiko termasuk pada kategori risiko supplementary issue yang didefinisikan untuk mengambil tindakan bila terjadi sumber daya yang memadai pada perusahaan. Dari hasil analisis risiko yang terdapat di bab 4.5 maka didapatkan proses survey dan observasi di lapangan yakni di departemen Transmission Operation dengan nilai rata-rata yaitu: 7. Berdasarkan hasil wawancara dengan pihak manajer dan supervisor pada departemen ini maka telah dilakukan evaluasi dari daftar risiko yang kategori supplementary issue sebagai berikut ini:

1. Kabel Fiber Optic putus karena tercangkul, Untuk masalah ini dilakukan kerjasama antara PT.Indosat diwakili oleh Departemen Transmission dengan Departemen PU (Dinas PU di Propinsi atau kota) dan PDAM agar bila ada pekerjaan menggali tanah atau jalan maka menginformasikan ke team indosat agar dapat dipantau oleh team indosat apakah melewati kabel indosat yang tertanam atau tidak.
2. Saluran Kabel laut Putus, untuk masalah ini dilakukan kerjasama antara PT.Indosat Ooredoo Tbk dengan TNI AL dan Polair agar pasukan TNI AL dan Polair melakukan pengawasan, pemantauan dan pengecekan jalur kabel laut PT Indosat.
3. Banjir yang menyebabkan kabel coaxial putus, untuk masalah ini hal yang dapat dilakukan adalah Departemen yaitu bekerjasama dengan team SAR PT Indosat agar sewaktu waktu ada kabel coaxial yang putus dapat ditangani secepatnya setelah banjir reda
4. Satelit yang hilang dari Orbitnya, untuk masalah ini sudah ditangani oleh PT. Indosat dengan metode risk transfer yaitu pengalihan potensi kerugian yang dialami perusahaan ke perusahaan asuransi.
5. Link VSAT yang terkena petir dan cuaca buruk sehingga akses ATM di Bank lambat, untuk masalah ini ditangani dengan menambah perangkat anti petir di setiap gedung yang ada penempatan VSAT.

**d. IP/MPLS Operation.**

Departemen IP/MPLS operation didapatkan empat risiko termasuk pada kategori risiko supplementary issue yang didefinisikan untuk mengambil tindakan bila terjadi sumber daya yang memadai pada perusahaan, satu risiko masuk pada kategori acceptable yakni tidak perlu dilakukan tindakan. Dari hasil analisis risiko yang terdapat di bab 4.5 maka didapatkan proses survey dan observasi di lapangan yakni di departemen IP/MPLS Operation dengan nilai rata-rata yaitu: 6,6. Berdasarkan hasil wawancara dengan pihak manajer dan supervisor pada departemen ini maka telah dilakukan evaluasi dari daftar risiko yang kategori supplementary issue sebagai berikut ini:

1. Vendor Indosat melakukan pekerjaan di sistem MPLS Jaringan Indosat dengan salah IP destination sehingga akses data indosat down, masalah ini dilakukan dengan cara yaitu sebelum vendor yang akan melakukan pekerjaan harus menunjukkan SOP pekerjaan tersebut dan apa saja impact yg bisa terjadi. Pada

saat vendor melakukan pekerjaan maka waspang dari teknikal harus selalu mengawasi pekerjaan tersebut berdasarkan SOP sampai pekerjaan selesai sehingga kesalahan dapat ditangani. Vendor boleh pulang 30 menit setelah pekerjaan selesai untuk memastikan tidak ada impact terhadap data maupun jaringan.

2. Karyawan melakukan salah setting routing dan layer di Network sehingga jaringan data putus, untuk masalah ini manager akan membuat SOP yang harus dipatuhi oleh semua karyawan sehingga pada saat ada kerjaan setting routing dan layer maka berdasarkan SOP tersebut. Untuk karyawan baru atau yang belum berpengalaman harus didampingi oleh karyawab senior urtnuk pekerjaan tersebut.
3. Jaringan MPLS tiba tiba down karena salah ubah network layer sehingga internet, video streaming dan akses sosial media problem, untuk masalah ini penyelesaian sama dengan no 2 yaitu manager akan membuat SOP yang harus dipatuhi oleh semua karyawan sehingga pada saat ada kerjaan ubah network layer maka berdasarkan SOP tersebut. Untuk karyawan baru atau yang belum berpengalaman harus didampingi oleh karyawab senior urtnuk pekerjaan tersebut.
4. Network Indosat Putus karena kesalahan karyawan, untuk masalah ini penyelesaian sama dengan no 2 yaitu manager akan membuat SOP yang harus dipatuhi oleh semua karyawan sehingga pada saat ada kerjaan pada core network maka berdasarkan SOP tersebut. Untuk karyawan baru atau yang belum berpengalaman harus didampingi oleh karyawab senior urtnuk pekerjaan tersebut.

**e. Access Operation.**

Departemen access operation didapatkan satu risiko pada kategori issue yang dimaksudkan untuk diperlukan suatu tindakan untuk mengelola risiko dan empat risiko termasuk pada kategori risiko supplementary issue yang didefinisikan untuk mengambil tindakan bila terjadi sumber daya yang memadai pada perusahaan. Dari hasil analisis risiko yang terdapat di bab 4.5 maka didapatkan proses survey dan observasi di lapangan yakni di departemen Access Operation dengan nilai rata-rata yaitu: 8,4. Berdasarkan hasil wawancara dengan pihak manajer dan supervisor pada departemen ini maka telah dilakukan evaluasi dari daftar risiko yang kategori issue dan supplementary issue sebagai berikut ini:

1. Kurangnya SDM sementara perangkat dan teknologi semakin bertambah, untuk masalah ini langkah yang diambil yaitu melatih dan memberi sharing knowledge kepada team yang sudah ada agar bisa menguasai dan menangani problem teknikal berbagai hal terkait akses (BTS, BSC dan PDH) dan bekerjasama dengan team akses regional agar problem terkait akses di level 2 yang pekerjaannya tidak terlalu sulit dapat ditangani oleh team regional tanpa harus dari team Akses pusat yang datang menanganinya ke daerah. Untuk kedepannya tetap didiskusikan juga ke divisi agar menyiapkan budget untuk penambahan karyawan baru semisal karyawan Outsourching (OS) agar biayanya tidak mahal dan sesuai dengan budget divisi yang telah ditetapkan di OPEX.
2. Keamanan lingkungan kerja juga harus menjadi perhatian karena sering terjadi kehilangan laptop/hp, untuk case ini ada beberapa cara yang telah dilakukan yaitu:
    a. Sudah memasang CCTV yang mengarah ke pintu masuk di belakang meja security yang menjaga sehingga setiap orang yang keluar masuk dapat dipantau aktifitasnya
    b. Bekerjasama dengan team CME Indosat membuat machine access reader di pintu masuk ruangan kerja sehingga setiap karyawan yang masuk ke ruangan harus menggunakan ID Cardnya. Setiap Vendor dan sub-cont yang masuk harus mendaftar melalui security dan menunggu di ruang tunggu sampai dijemput oleh karyawan yang telah melakukan perjanjian.

Dan beberapa hal yang akan dilakukan yaitu:

a. Mengingatkan dan memberi pengarahan ke semua karyawan untuk mematuhi peraturan bahwa ID Card tidak bisa dipinjamkan ke siapapun terutama vendor atau bukan karyawan
b. Setiap karyawan wajib menjaga dan mengawasi laptop dan HP nya, bila ada meeting dalam waktu yg lama atau ada kegiatan yang meninggalkan meja maka hp dibawa dan laptop dimasukkan ke loker atau laci.
c. Setiap karyawan wajib memperhatikan orang yang ti-

dak dikenal datang ke ruangan dan menanyakan mau bertemu dengan siapa dan ada keperluan apa sehingga kejahatan dapat di hindari.

3. Risiko Human Error dan Employee Accident perlu diperhatikan, untuk masalah human error ini ditangani dengan selalu memberi pelatihan dan sharing knowledge kepada karyawan agar dapat diminimalisir dan karyawan setiap tahun disertakan outing divisi untuk refreshing dan kebersamaan dan family gathering dari perusahaan untuk keakraban dan kebersamaan. Untuk employee accident bekerjasama dengan team K3 Indosat agar selalu mematuhi dan melakukan sesuai SOP yang ada untuk setiap ada pekerjaan yang agak berbahaya sehingga dapat menghindari kecelakaan.
4. Kurangnya kendaraan operasional, untuk masalah ini menurut manager bahwa harus mengoptimalkan kenderaan operasional yang sudah ada demi efisiensi. Langkah yang diambil manager yaitu memaksimalkan mobil operasional yang ada dengan membawa team secara bersamaan untuk pekerjaan diluar kantor. Untuk pekerjaan yang sifatnya tidak urgent dan masih bisa di remote dari kantor atau dari rumah diluar jam kantor maka sebaiknya tidak pergi ke site cukup via remote saja.
5. Fasilitas komputer/laptop untuk pegawai outsourching masih minim sehingga kinerja lambat, untuk masalah ini hal yang bisa dilakukan oleh manager yaitu mengusahakan agar semua karyawan OS mendapatkan komputer baik baru maupun bekas pakai. Namun untuk pengadaan laptop maka memasukkan proposal ke divisi agar ada alokasi budget pembelian laptop buat karyawan OS namun bukan menjadi prioritas karena bergantung dari budget divisi.

**f. CME Operation**

Departemen CME operation didapatkan satu risiko pada kategori issue yang dimaksudkan untuk diperlukan suatu tindakan untuk mengelola risiko dan lima risiko termasuk pada kategori risiko supplementary issue yang didefinisikan untuk mengambil tindakan bila terjadi sumber daya yang memadai pada perusahaan. Dari hasil analisis risiko yang terdapat di bab 4.5 maka didapatkan proses survey dan observasi di lapangan yakni di departemen CME Operation dengan nilai rata-rata yaitu: 8. Berdasarkan hasil wawancara dengan pihak manajer dan supervisor pada departemen ini maka telah dilakukan evaluasi dari daftar risiko yang kategori supplementary issue sebagai berikut ini:

1. PLN sering off di daerah sehingga perangkat BTS dan BSC down, untuk masalah ini maka dilakukan kerjasama antara PT.Indosat dengan PLN dengan perjanjian bahwa setiap ada rencana pemadaman listrik maupun ada pekerjaan pembangkit listrik yang berpotensi padamnya listrik maka pihak PLN segera memberitahukan ke pihak Indosat agar Indosat bersiap siap menyediakan genset dan batere sebagai cadangan alternatif untuk tenaga di BTS maupun di BSC.
2. Pengecekan genset yang dilakukan terlambat, untuk masalah ini manager akan membuat SOP yang harus dipatuhi oleh semua teknikal yang bertugas sesuai jadwalnya. Setiap teknikal yang bertugas harus mengisi checklist pengecekan genset dan batere sehingga bila sewaktu waktu mau digunakan genset dan batere sudah siap.
3. Genset tidak otomatis menyala, sehingga dilakukan pergantian secara manual, untuk masalah ini sama dengan no 2, manager akan membuat SOP yang harus dipatuhi oleh semua teknikal yang bertugas sesuai jadwalnya. Setiap teknikal yang bertugas harus mengisi checklist pengecekan genset dan batere sehingga bila sewaktu waktu listrik mati atau PLN off maka genset dapat digunakan secara otomatis.
4. Kemampuan karyawan tentang AC, batere dan genset masih kurang, untuk masalah ini langkah yang diambil yaitu melatih dan memberi sharing knowledge kepada karyawan melalui karyawan senior maupun kerjasama dengan vendor agar bisa menguasai dan menangani problem tersebut dan menguasainya karena akan menjadi job desk dari karyawan tersebut, dengan budget terbatas vendor yang didatangkan cukup lokal tapi memilki kemampuan yang bagus.
5. Tanah yang disewa untuk penempatan tower tidak diperpanjang oleh pemiliknya, untuk masalah ini diinfokan ke divisi agar divisi melakukan kerjasama dengan team planning dan partner management bagaimana negosiasi terbaik dengan pemilik tanah.

Apakah faktor yang membuat pemilik tanah tidak memperpanjang sewanya, apabila karena harga sewa yang naik maka bisa didiskusikan. Bila perlu dan budget ada maka tanah tersebut bisa dibeli oleh Indosat. Namun bila pemilik tetap tidak memperpanjang sewa maka pihak planning dan CME siap siap cari tanah lain untuk disewa.

**g. Core Operation**

Departemen Core operation didapatkan empat risiko termasuk pada kategori risiko supplementary issue yang didefinisikan untuk mengambil tindakan bila terjadi sumber daya yang memadai pada perusahaan, satu risiko masuk pada kategori acceptable yakni tidak perlu dilakukan tindakan. Dari hasil analisis risiko yang terdapat di bab 4.5 maka didapatkan proses survey dan observasi di lapangan yakni di departemen CME Operation dengan nilai rata-rata yaitu 6. Berdasarkan hasil wawancara dengan pihak manajer dan supervisor pada departemen ini maka telah dilakukan evaluasi dari daftar risiko yang kategori supplementary issue sebagai berikut ini:

1. Kesalahan konfigurasi pada sistem core seperti PS, CS dan IN-VAS, untuk masalah ini pernah dilakukan oleh vendor yang belum expert maupun karyawan baru dari indosat. Langkah yang diambil oleh manager yaitu membuat SOP yang harus dipatuhi oleh vendor maupun karyawan. Dan khusus karyawan diberi pelatihan dan sharing knowledge agar bisa menguasai dan menangani problem maupun cara mengkonfigure pada sistem core.
2. Kesalahan action hardware pada saat pekerjaan on site ke MSC, untuk masalah ini sama dengan di no 1 manager akan membuat SOP yang harus dipatuhi oleh semua teknikal yang bertugas ke site MSC dalam pengecekan perangkat Dan khusus karyawan baru diberi pelatihan dan sharing knowledge agar bisa menguasai dan menangani problem maupun cara memperbaiki hardware.
3. Kurangnya pengawasan terhadap vendor, untuk masalah ini manager akan mempertegas lagi SOP yang sudah ada agar dipatuhi oleh semua karyawan sehingga pada saat ada kerjaan yang dilakukan oleh vendor maka karyawan wajib mendampingi dari mulai pekerjaan sampai vendor selesai melakukan pekerjaan dan sampai 30 menit setelahnya vendor dan karyawan wajib memastikan bahwa tidak ada lagi problem di jaringan dan di sistem. Vendor boleh pulang 30 menit setelah pekerjaan selesai untuk memastikan tidak ada impact terhadap system maupun jaringan.
4. Karyawan outsourching diberikan user yang tidak sesuai level yang telah ditetapkan, untuk masalah ini manager dan supervisor akan mengawasi setiap karyawan outsouring dalam menggunakan user dan passwordnya. Ada konsekuensi buat karyawan yg melanggar bila memberikan ke karyawan OS user dan passwordnya, kecuali sdh disetujui oleh manager. Departemen juga bekerjasama dengan team dari Security Management untuk melakukan pencegahan dengan metode:
    a. Karyawan outsourching hanya diberikan akses pada informasi dan system jaringan yang dibutuhkannya
    b. Mengimplementasikan metode identifikasi dan autentifikasi data yang dimiliki oleh security management serta menonaktifkan password dari user karyawan OS jika dalam keadaan off dan kontrak tidak diperpanjang.

**h. Configuration Management.**

Departemen Configuration Management didapatkan tiga risiko termasuk pada kategori risiko supplementary issue yang didefinisikan untuk mengambil tindakan bila terjadi sumber daya yang memadai pada perusahaan dan dua risiko masuk pada kategori acceptable yakni tidak perlu dilakukan tindakan. Dari hasil analisis risiko yang terdapat di bab 4.5 maka didapatkan proses survey dan observasi di lapangan yakni di departemen Configuration Management dengan nilai rata-rata yaitu 5,4. Berdasarkan hasil wawancara dengan pihak manajer dan supervisor pada departemen ini maka telah dilakukan evaluasi dari daftar risiko yang kategori supplementary issue sebagai berikut ini:

1. Perangkat server mati, langkah yang diambil oleh manager yaitu mengingatkan kembali agar karyawan selalu bekerja berdasarkan SOP dan melakukan checklist pada server 2 kali sehari yaitu pada saat datang kerja dan sebelum pulang kerja sehingga serv-

er bisa dideteksi lebih awal bila ada tanda tanda problem atau mati.

2. Server kena virus, untuk masalah ini manager akan bekerjasama dengan divisi IT untuk selalu mengupgrade anti virus terbaru di semua perangkat server dsan karyawan rajin melakukan scan di setiap server. Bila ada vendor atau karyawan yang menggunakan flashdisk maka wajib di scan terlebih dulu untuk mengantisipasi virus.
3. Modul dan sparepart server adalah import sehingga membutuhkan waktu yang lama untuk bisa diinstal karena waktu pengiriman yang lama dan waktu penginstalan yg lama, untuk menyiasati hal ini maka manager bekerjasama dengan departemen partner management dan team dari divisi project agar mengordernya 6 sampai 1 tahun sebelumnya sehingga team vendor bisa menyiapkan waktu dan spesifikasi yang baik.

**i. Partner Management.**

Departemen Partner Management didapatkan sebuah risiko termasuk pada kategori risiko supplementary issue yang didefinisikan untuk mengambil tindakan bila terjadi sumber daya yang memadai pada perusahaan dan empat risiko masuk pada kategori acceptable yakni tidak perlu dilakukan tindakan. Dari hasil analisis risiko yang terdapat di bab 4.5 maka didapatkan proses survey dan observasi di lapangan yakni di departemen partner management dengan nilai rata-rata yaitu 4,5. Berdasarkan hasil wawancara dengan pihak manajer pada departemen ini maka telah dilakukan evaluasi dari daftar risiko yang kategori supplementary issue sebagai berikut:

1. Karyawan bekerjasama dengan vendor untuk mempermudah report maintenance, untuk masalah ini manager mempertegas lagi SOP yang sudah ada agar dipatuhi oleh semua karyawan bahwa ada konsekuensi bila melakukan pembiaran terhadap vendor dalam melakukan maintenance dan membuat report maintenance. Karena ada team dari internal audit yang melakukan pengawasan terhadap setiap kegiatan yang dianggap melakukan pelanggaran.

## 4.7. Penentuan Respon terhadap Risiko

Risiko-risiko yang telah tersaring pada langkah evaluasi, selanjutnya dibuat rencana pengendalian lebih lanjut, langkah ini disebut penentuan respon terhadap risiko. Langkah penentuan respon terhadap risiko atau mitigasi risiko meliputi pengidentifikasian opsi untuk menangani risiko, menaksir opsi tersebut, menyiapkan rencana perlakuan risiko dan mengimplementasikan rencana perlakuan risiko. Mitigasi risiko dibedakan menjadi dua jenis yaitu pengendalian dan penanganan. Yakni:

**1. Pengendalian**

Pengendalian adalah upaya-upaya untuk merubah risiko. Pengendalian biasanya merupakan upaya-upaya yang telah dimiliki dan bersifat rutin untuk mengantisipasi terjadinya risiko. Contoh pengendalian yang dilakukan oleh manager dalam hal ini departemen yaitu dalam bentuk prosedur (SOP), kontrak, dan sebagainya.

**2. Penanganan**

Penanganan adalah upaya-upaya yang akan dilakukan sebagai langkah baru untuk memperlakukan risiko karena upaya-upaya yang sudah ada belum memadai.

Opsi perlakuan risiko dan mitigasi secara umum meliputi

1. Menghindari risiko (risk avoidance), berarti tidak melaksanakan atau meneruskan kegiatan yang menimbulkan risiko tersebut.
2. Mengurangi risiko (risk reduction), yaitu perlakuan risiko untuk mengurangi kemungkinan terjadinya atau mengurangi paparan dampaknya, atau mengurangi keduanya.
3. Transfer risiko (risk sharing), yaitu suatu tindakan untuk mengurangi kemungkinan timbulnya risiko melalui antara lain: asuransi, outsourcing, subcontracting, tindak lindung, transaksi nilai mata uang asing, dll.
4. Menerima risiko (risk acceptance), yaitu tidak melakukan perlakuan apapun terhadap risiko tersebut.
5. Dari pembahasan risiko diatas dibuat dokumen utama yang dihasilkan dari tahapan identifikasi, analisis, evaluasi, dan mitigasi/ perlakuan risiko adalah berupa Daftar Risiko (Risk Register). Daftar risiko yang dimasukkan dalam tabel ini adalah risiko yang masuk kategori Issue dan Supplementary Issue sedangkan kategori Acceptable tidak dimasukkan karena tidak perlu ada tindakan. Ada 35 risiko yang diambil tindakan seperti dibawah ini:

**Tabel 4.23. Penanganan dan pengendalian terhadap risiko pada Divisi Network Operation Center**

| No | Nama SOP/Instruksi kerja/Kontrak | Unit Yang bertanggung Jawab | Kode Dokumen |
|---|---|---|---|
| 1 | Kontrak kerjasama PT.Indosat dengan PU dan PDAM | **Transmission Backbone Operation** | PRR-TBO-01 |
| 2 | Kontrak kerjasama PT.Indosat dengan TNI | **Transmission Backbone Operation** | PRR-TBO-02 |
| 3 | Kontrak kerjasama PT.Indosat dengan POLAIR | **Transmission Backbone Operation** | PRR-TBO-03 |
| 4 | IK- Pergantian antar Shift | **Consumer Front Office** | IK |
| 5 | IK-Shift Malam | **Consumer Front Office** | IK |
| 6 | SOP Security User | **Consumer Front Office** | SOP |
| 7 | Form Keluhan Pelanggan | **Consumer Front Office** | Form |
| 8 | SOP turun kelapangan<br>IK - | **Regional Operation** | SOP<br>IK- |
| 9 | SOP turun ke lapangan<br>IK - | **Regional Operation** | SOP<br>IK |
| 10 | IK-Keselamatan Karyawan | **Regional Operation** | IK - |
| 11 | Kontrak kerjasama dengan POLRES | **Regional Operation** | |
| 12 | Pembentukan Team reaksi cepat | **Regional Operation** | IK- |
| 13 | Penambahan kompetensi karyawan (IK-Profesionalisme) | **Regional Operation** | |
| 14 | Kontrak dengan ASTRA Rent Car | **Regional Operation** | |
| 15 | Kebutuhan module standard kerja | **Regional Operation** | IK-SPMS |
| 16 | SOP-Penanggulangan Gempa | **Regional Operation** | SOP- |
| 17 | SOP-Penanggulangan Kebakaran | **Regional Operation** | SOP- |
| 18 | SOP IP/MPLS System | **IP/MPLS Operation** | SOP- |
| 19 | SOP Configuration Routing | **IP/MPLS Operation** | SOP- |
| 20 | SOP Monitoring Traffic | **IP/MPLS Operation** | SOP- |
| 21 | Penambahan kompetensi karyawan (IK-Profesionalisme)<br>Pengangkatan Karyawan OS | **Access Operation** | IK-Training |
| 22 | SOP Keamanan Lingkungan | **Access Operation** | SOP- |
| 23 | SOP – Pengecekan perangkat | **Access Operation** | SOP- |
| 24 | Division System Budgeting | **Access Operation** | |
| 25 | SOP-persiapan Genset | **CME Operation** | SOP- |
| 26 | IK Checklist Genset | **CME Operation** | IK-Cheklist |
| 27 | Penambahan kompetensi karyawan (IK-Profesionalisme) | **CME Operation** | IK-Training |
| 28 | Ikatan Kontrak dengan pemilik Tanah | **CME Operation** | IK-Project |
| 29 | SOP Configuration System | **Core Operation** | SOP- |
| 30 | SOP hardware and Software Protection | **Core Operation** | SOP- |
| 31 | SOP Monitoring Vendor | **Core Operation** | SOP- |
| 32 | SOP Security User | **Core Operation** | SOP- |
| 33 | SOP pengecekan server | **Configuration Management** | SOP- |
| 34 | SOP pengadaan Barang | **Configuration Management** | SOP- |
| 35 | SOP code ethic with vendor | **Partner Management** | SOP- |

Sumber: Data hasil yang diolah dengan excel

## 4.8 Resume hasil risiko

**Tabel 4.24 Resume hasil risiko di Divisi Network Operation Center**

| No | Departemen | | Risiko-risiko yang muncul | Peluang terjadi | | | Dampak | | | | | Skor Risiko | | | Kriteria risiko | Skor Rata rata Risiko |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Periode Kejadian/ tahun | Potensi Kejadian | Skor Peluang | Finansial | Keselamatan Kerja | Citra perusahaan | Ukuran Dampak | Skor Dampak | Skor Dampak | Skor Peluang | Skor Hasil | | |
| 1 | Front Office | 1 | Informasi profile customer ke pihak yang tidak berkepentingan | 1 kali | Jarang | 1 | Diabaikan | Diabaikan | Berpengaruh | Besar | 4 | 4 | 1 | 4 | Acceptable | (4 + 9 + 8 + 8 + 6) : 5 = 35 : 5 = 7 |
| | | 2 | Adanya risiko perjalanan untuk team karyawan shift yang pulang malam | 6 kali | Kemungkinan sedang | 3 | Diabaikan | Berpengaruh | Diabaikan | sedang | 3 | 3 | 3 | 9 | Issue | |
| | | 3 | Teknisi ketiduran sehingga alarm problem diinfokan terlambat | 5 kali | Kemungkinan Besar | 4 | Diabaikan | Diabaikan | Berpengaruh | Kecil | 2 | 2 | 4 | 8 | Supplementary Issue | |
| | | 4 | Karyawan sering mensharing user dan passwordnya ke karyawan yang tidak berkepentingan | 8 kali | Kemungkinan Besar | 4 | Diabaikan | Diabaikan | Berpengaruh | Kecil | 2 | 2 | 4 | 8 | Supplementary Issue | |
| | | 5 | Kesalahan menjelaskan informasi route cause dari teknikal ke CCS | 4 kali | Kemungkinan sedang | 3 | Diabaikan | Diabaikan | Berpengaruh | Kecil | 2 | 2 | 3 | 6 | Supplementary Issue | |
| 2 | Regional Operation (JBRO, CWRO, EJBNRO, KSPRO, dan SO) | 1 | Kurangnya SDM Teknisi | 6 kali | Kemungkinan sedang | 3 | Berpengaruh | Diabaikan | Diabaikan | Sedang | 3 | 3 | 3 | 9 | Supplementary Issue | (9 + 12 + 6 + 12 + 4 + 12 + 8 + 5) : 8 = 68 : 8 = 8,5 |
| | | 2 | Complain pelanggan sinyal jelek | 6 kali | Kemungkinan sedang | 3 | Diabaikan | Diabaikan | Berpengaruh | Besar | 4 | 4 | 3 | 12 | Issue | |
| | | 3 | Tidak Adanya Kendaraan Operasional | 6 kali | Kemungkinan sedang | 3 | Berpengaruh | Diabaikan | Diabaikan | Kecil | 2 | 2 | 3 | 6 | Supplementary Issue | |
| | | 4 | Penanganan complain pelanggan lambat | 6 kali | Kemungkinan sedang | 3 | Diabaikan | Diabaikan | Berpengaruh | Besar | 4 | 4 | 3 | 12 | Issue | |
| | | 5 | Pencurian Batere, Genset dan antena | 1 kali | Jarang | 1 | Berpengaruh | Diabaikan | Diabaikan | Besar | 4 | 4 | 1 | 4 | Acceptable | |
| | | 6 | Premanisme (Setiap ke site di ganggu oleh preman dan minta uang keamanan) | 8 kali | Hampir pasti | 4 | Berpengaruh | Diabaikan | Diabaikan | Sedang | 3 | 3 | 4 | 12 | Issue | |
| | | 7 | Stock Modul/Perangkat Tidak ada sehingga Perangkat BTS dan MSC tidak bisa diperbaiki. | 3 kali | Kemungkinan terjadi | 2 | Berpengaruh | Diabaikan | Diabaikan | Besar | 4 | 4 | 2 | 8 | Supplementary Issue | |
| | | 8 | Bencana alam (Gempa bumi dan Gunung Api meletus) | 1 kali | Jarang | 1 | Berpengaruh | Diabaikan | Diabaikan | Sangat Besar | 5 | 5 | 1 | 5 | Supplementary Issue | |
| 3 | Transmission Backbone Operation | 1 | Kabel Fiber Optic putus karena tercangkul | 3 kali | Kemungkinan terjadi | 2 | Berpengaruh | Diabaikan | Diabaikan | Besar | 4 | 4 | 2 | 8 | Supplementary Issue | (8 + 8 + 8 + 5 + 6) : 5 = 35 : 5 = 7 |
| | | 2 | Saluran Kabel laut Putus | 3 kali | Kemungkinan terjadi | 2 | Berpengaruh | Diabaikan | Diabaikan | Besar | 4 | 4 | 2 | 8 | Supplementary Issue | |
| | | 3 | Banjir yang menyebabkan kabel coaxial putus | 3 kali | Kemungkinan terjadi | 2 | Berpengaruh | Diabaikan | Diabaikan | Besar | 4 | 4 | 2 | 8 | Supplementary Issue | |
| | | 4 | Satelit yang hilang dari Orbitnya | 1 kali | Jarang | 1 | Berpengaruh | Diabaikan | Diabaikan | Sangat besar | 5 | 5 | 1 | 5 | Supplementary Issue | |
| | | 5 | Link VSAT yang terkena petir dan cuaca buruk sehingga akses ATM di Bank lambat | 3 kali | Kemungkinan terjadi | 2 | Berpengaruh | Diabaikan | Diabaikan | sedang | 3 | 3 | 2 | 6 | Supplementary Issue | |
| 4 | IP/MPLS Operation | 1 | Vendor Indosat melakukan pekerjaan di system MPLS Jaringan Indosat dengan salah IP destination sehingga akses data indosat down | 3 kali | Kemungkinan terjadi | 2 | Berpengaruh | Diabaikan | Diabaikan | Besar | 4 | 4 | 2 | 8 | Supplementary Issue | (8 + 8 + 8 + 4 + 5) : 5 = 33 : 5 = 6,6 |
| | | 2 | Karyawan melakukan salah setting routing dan layer di Network sehingga jaringan data putus | 3 kali | Kemungkinan terjadi | 2 | Berpengaruh | Diabaikan | Diabaikan | Besar | 4 | 4 | 2 | 8 | Supplementary Issue | |
| | | 3 | Jaringan MPLS tiba tiba down karena salah ubah network layer sehingga internet, video streaming dan akses sosial media problem | 3 kali | Kemungkinan terjadi | 2 | Berpengaruh | Diabaikan | Diabaikan | Besar | 4 | 4 | 2 | 8 | Supplementary Issue | |
| | | 4 | Topologi/Network Backbone internasional Indosat Down mengakibatkan pelanggan sulit akses | 1 kali | Jarang | 1 | Berpengaruh | Diabaikan | Diabaikan | Besar | 4 | 4 | 1 | 4 | Acceptable | |
| | | 5 | Network Indosat Putus karena kesalahan karyawan | 1 kali | Jarang | 1 | Berpengaruh | Diabaikan | Diabaikan | Sangat besar | 5 | 5 | 1 | 5 | Supplementary Issue | |
| 5 | Access Operation | 1 | Kurangnya SDM sementara perangkat dan teknologi semakin bertambah | 7 kali | Kemungkinan besar | 4 | Berpengaruh | Diabaikan | Diabaikan | Sedang | 3 | 3 | 4 | 12 | Issue | (12 + 8 + 8 + 6 + 8) : 5 = 42: 5 = 8,4 |
| | | 2 | Keamanan lingkungan kerja juga harus menjadi perhatian karena sering terjadi kehilangan laptop/hp | 7 kali | Kemungkinan besar | 4 | Diabaikan | Berpengaruh | Diabaikan | Kecil | 2 | 2 | 4 | 8 | Supplementary Issue | |
| | | 3 | Risiko Human Error dan Employee Accident perlu diperhatikan | 7 kali | Kemungkinan besar | 4 | Berpengaruh | Diabaikan | Diabaikan | Kecil | 2 | 2 | 4 | 8 | Supplementary Issue | |
| | | 4 | Kurangnya kendaraan operasional | 6 kali | Kemungkinan sedang | 3 | Berpengaruh | Diabaikan | Diabaikan | Kecil | 2 | 2 | 3 | 6 | Supplementary Issue | |
| | | 5 | Fasilitas computer/laptop untuk pegawai Outsourching masih minim sehingga kinerja lambat | 8 kali | Kemungkinan besar | 4 | Berpengaruh | Diabaikan | Diabaikan | Kecil | 2 | 2 | 4 | 8 | Supplementary Issue | |
| 6 | CME Operation | 1 | PLN sering off di daerah sehingga perangkat BTS dan BSC down | 7 kali | Kemungkinan besar | 4 | Berpengaruh | Diabaikan | Diabaikan | Sedang | 3 | 3 | 4 | 12 | Issue | (12 + 6 + 6 + 6 + 9 + 9) : 6 = 48: 6 = 8 |
| | | 2 | Pengecekan genset yang dilakukan terlambat | 6 kali | Kemungkinan sedang | 3 | Berpengaruh | Diabaikan | Diabaikan | Kecil | 2 | 2 | 3 | 6 | Supplementary Issue | |
| | | 3 | Genset tidak otomatis menyala, sehingga dilakukan pergantian secara manual | 3 kali | Kemungkinan terjadi | 2 | Berpengaruh | Diabaikan | Diabaikan | Sedang | 3 | 3 | 2 | 6 | Supplementary Issue | |
| | | 4 | AC untuk inner di site (MSC, BSC dan BTS) rusak dan part lama pergantian | 3 kali | Kemungkinan terjadi | 2 | Berpengaruh | Diabaikan | Diabaikan | Sedang | 3 | 3 | 2 | 6 | Supplementary Issue | |
| | | 5 | Kemampuan karyawan tentang AC, batree dan genset masih kurang | 3 kali | Kemungkinan terjadi | 3 | Berpengaruh | Diabaikan | Diabaikan | Sedang | 3 | 3 | 3 | 9 | Supplementary Issue | |
| | | 6 | Tanah yang disewa untuk penempatan tower tidak diperpanjang kontraknya oleh pemiliknya | 1 kali | Kemungkinan terjadi | 3 | Berpengaruh | Diabaikan | Diabaikan | Sedang | 3 | 3 | 3 | 9 | Supplementary Issue | |
| 7 | Core Operation | 1 | Kesalahan konfigurasi pada system core seperti PS, CS dan IN-VAS | 6 kali | Kemungkinan sedang | 3 | Berpengaruh | Diabaikan | Diabaikan | Kecil | 2 | 2 | 3 | 6 | Supplementary Issue | (6 + 6 + 6 + 4 + 8) : 5 = 30 : 6 = 6 |
| | | 2 | Kesalahan action hardware pada saat pekerjaan on site ke MSC | 4 kali | Kemungkinan terjadi | 2 | Berpengaruh | Diabaikan | Diabaikan | Sedang | 3 | 3 | 2 | 6 | Supplementary Issue | |
| | | 3 | Kurangnya pengawasan terhadap vendor | 6 kali | Kemungkinan sedang | 3 | Berpengaruh | Diabaikan | Diabaikan | Kecil | 2 | 2 | 3 | 6 | Supplementary Issue | |
| | | 4 | Karyawan memberikan isi sms dan voice pelanggan tanpa seijin perusahaan dan polisi | 1 kali | Jarang | 1 | Diabaikan | Diabaikan | Berpengaruh | Besar | 4 | 4 | 1 | 4 | Acceptable | |
| | | 5 | Karyawan outsourching diberikan user yang tidak sesuai level yang telah ditetapkan | 3 kali | Kemungkinan terjadi | 2 | Diabaikan | Diabaikan | Berpengaruh | Besar | 4 | 4 | 2 | 8 | Supplementary Issue | |
| 8 | Configuration Management | 1 | Perangkat server mati | 6 kali | Kemungkinan sedang | 3 | Berpengaruh | Diabaikan | Diabaikan | Kecil | 2 | 2 | 3 | 6 | Supplementary Issue | (6 + 4 + 6 + 3 + 8) : 5 = 27 : 5 = 5,4 |
| | | 2 | Server rusak | 4 kali | Kemungkinan terjadi | 2 | Berpengaruh | Diabaikan | Diabaikan | Sedang | 2 | 2 | 2 | 4 | Acceptable | |
| | | 3 | Server kena virus | 6 kali | Kemungkinan sedang | 3 | Berpengaruh | Diabaikan | Diabaikan | Kecil | 2 | 2 | 3 | 6 | Supplementary Issue | |
| | | 4 | Password admin server di sharing ke team yang tidak bertanggung jawab | 1 kali | Jarang | 1 | Diabaikan | Diabaikan | Berpengaruh | Besar | 3 | 3 | 1 | 3 | Acceptable | |
| | | 5 | Modul dan sparepart server adalah import sehingga membutuhkan waktu yang lama | 3 kali | Kemungkinan terjadi | 2 | Berpengaruh | Diabaikan | Diabaikan | Besar | 4 | 4 | 2 | 8 | Supplementary Issue | |
| 9 | Partner Management | 1 | Vendor (supplier) Indosat melakukan pendekatan ke karyawan lewat hadiah agar mempermudah kerjasama kontrak maintenance | 1 kali | Jarang | 1 | Diabaikan | Diabaikan | Berpengaruh | Besar | 4 | 4 | 1 | 4 | Acceptable | (4 + 6 + 4 + 4 + 4) : 5 = 22 : 5 = 4,5 |
| | | 2 | Karyawan bekerjasama dengan vendor untuk mempermudah report maintenance | 3 kali | Kemungkinan terjadi | 2 | Diabaikan | Diabaikan | Berpengaruh | Sedang | 3 | 3 | 2 | 6 | Supplementary Issue | |
| | | 3 | Karyawan mendapatkan hadiah dari vendor (supplier) agar memenangkan tender kontrak | 1 kali | Jarang | 1 | Diabaikan | Diabaikan | Berpengaruh | Besar | 4 | 4 | 1 | 4 | Acceptable | |
| | | 4 | Karyawan mengurangi pinalty buat vendor yang tidak tepat waktu dalam menjalankan pekerjaan | 1 kali | Jarang | 1 | Diabaikan | Diabaikan | Berpengaruh | Besar | 4 | 4 | 1 | 4 | Acceptable | |

Sumber: Data hasil yang diolah dengan excel

# V. KESIMPULAN DAN SARAN

## 5.1 Kesimpulan

Berdasarkan analisis dan evaluasi yang dilakukan maka didapatkan beberapa kesimpulan sebagai berikut:

1. Risiko Operasional di divisi Network Operation Center PT. Indosat Ooredoo Tbk yang teridentifikasi dari hasil penelitian ini terdiri atas 9 jenis yang meliputi 49 risiko dari departemen yang ada di divisi tersebut yaitu:

a. Front Office, risikonya:
   1. Memberikan informasi profile customer ke pihak yang tidak berkepentingan
   2. Adanya risiko perjalanan untuk team karyawan shift yang pulang malam
   3. Teknisi ketiduran sehingga alarm problem diinfokan terlambat
   4. Karyawan sering mensharing user dan passwordnya ke karyawan yang tidak berkepentingan
   5. Kesalahan menjelaskan informasi root cause dari teknikal ke CCS.

b. Regional Operation (Jabotabek, Central and West Java, East Java and Bali Nusa, Kalisula, dan Sumatera), risikonya:
   1. Kurangnya SDM Teknisi
   2. komplain pelanggan sinyal jelek
   3. Tidak Adanya Kendaraan Operasional
   4. Penanganan komplain pada pelanggan menjadi lambat
   5. Pencurian Batere, Genset dan antena
   6. Premanisme (Setiap ke site di ganggu oleh preman dan minta uang keamanan)
   7. Stock Modul/Perangkat Tidak ada sehingga Perangkat BTS dan MSC tidak bisa diperbaiki
   8. Bencana alam (Gempa bumi dan Gunung Api meletus)

c. Transmission Operation, risikonya:
   1. Kabel Fiber Optic putus karena tercangkul
   2. Saluran Kabel laut Putus
   3. Banjir yang menyebabkan kabel coaxial putus
   4. Satelit yang hilang dari Orbitnya
   5. Link VSAT yang terkena petir dan cuaca buruk sehingga akses ATM di Bank lambat

d. IP/MPLS (Internet Protocol/Multi Packet Label System) Operation, risikonya:
   1. Vendor Indosat melakukan pekerjaan di system MPLS Jaringan Indosat dengan salah IP destination sehingga akses data indosat down
   2. Karyawan melakukan salah setting routing dan layer di Network sehingga jaringan data putus
   3. Jaringan MPLS tiba tiba down karena salah ubah network layer sehingga internet, video streaming dan akses sosial media problem
   4. Topologi/Network Backbone internasional Indosat down mengakibatkan pelanggan sulit akses
   5. Network Indosat Putus karena kesalahan karyawan

e. Access Operation, risikonya:
   1. Kurangnya SDM sementara perangkat dan teknologi semakin bertambah
   2. Keamanan lingkungan kerja juga harus menjadi perhatian karena sering terjadi kehilangan laptop/hp
   3. Risiko Human Error dan Employee Accident perlu diperhatikan
   4. Kurangnya kendaraan operasional
   5. Fasilitas komputer/laptop untuk pegawai Outsourching masih minim sehingga kinerja lambat.

f. CME (Civil, Maintenance and Electrical) Operation, risikonya:
   1. PLN sering off di daerah sehingga perangkat BTS dan BSC down
   2. Pengecekan genset yang dilakukan terlambat
   3. Genset tidak otomatis menyala, sehingga dilakukan pergantian secara manual
   4. AC untuk inner di site (MSC, BSC dan BTS) rusak dan partnya lama pergantian
   5. Kemampuan karyawan tentang AC, batere dan genset masih kurang
   6. Tanah yang disewa untuk penempatan tower tidak diperpanjang kontraknya oleh pemiliknya.

g. Core Operation, risikonya:
   1. kesalahan konfigurasi pada sistem core seperti PS, CS dan IN-VAS
   2. Kesalahan action hardware pada saat pekerjaan on site ke MSC

3. Kurangnya pengawasan terhadap vendor
4. Karyawan memberikan sms dan voice pelanggan tanpa seijin perusahaan dan polisi
5. Karyawan outsourching diberikan user yang tidak sesuai level yang telah ditetapkan.

h. Configuration Management, risikonya:
1. Perangkat server mati
2. Server rusak
3. Server kena virus
4. Password admin server di sharing ke team yang tidak bertanggung jawab
5. Modul dan sparepart server adalah import sehingga membutuhkan waktu yang lama.

i. Partner Management, risikonya:
1. Vendor Indosat melakukan pendekatan ke karyawan lewat hadiah agar mempermudah kerjasama kontrak maintenance
2. karyawan bekerjasama dengan vendor untuk mempermudah report maintenance
3. Karyawan mendapatkan hadiah vendor agar memenangkan tender kontrak
4. Karyawan mengurangi pinalty buat vendor yang tidak tepat waktu dalam menjalankan pekerjaan
5. Karyawan tidak objektif dalam menentukan vendor yang menang.

2. Nilai rata rata risiko tiap departemen dari hasil perhitungan dan penelitian didapatkan yaitu:

a. Front Office, nilai rata rata risikonya: 7
b. Regional Operation (Jabodetabek Operation, Central and West Java Operation, East Java and Bali Nusa Operation, Kalisula & Papua Operation, dan Sumatera Operation), nilai rata rata risikonya: 8,5
c. Transmission Operation, nilai rata rata risikonya: 7
d. IP/MPLS Operation, nilai rata rata risikonya: 6,6
e. Access Operation, nilai rata rata risikonya: 8,4
f. CME Operation, nilai rata rata risikonya: 8
g. Core Operation, nilai rata rata risikonya: 6
h. Configuration Management, nilai rata rata risikonya: 5,4
i. Partner Management, nilai rata rata risikonya: 4,5

3. Risiko yang paling tinggi didapatkan di departemen Regional Operation, hal ini disebabkan oleh: wilayah operasional paling luas dan sebagai ujung tombak dari divisi noc untuk menjaga kualitas jaringan indosat di seluruh indonesia yaitu akhir tahun 2015 jaringan Indosat Ooredoo terdiri dari 23.596 2G BTS ( Base Transceiver Stations ) dan 23.730 Node-B (3G BTS) dengan total 47.326 BTS, dan 3.361 Enode-B 4G, dana operasional dan sdm yang terbatas, kondisi daerah yang berat (jalan, perijinan, geografis wilayah dll)

4. Risiko kedua terbesar ada di departemen Access Operation, karena lingkup kerjanya juga mencakup BTS dan BSC yang besar, sedangkan risiko paling kecil terdapat pada departemen Partner Management, fungsi dari departemen ini lebih banyak ke administrasi yaitu berhubungan dengan vendor dan di internal indosat berhubungan team procurement untuk biaya maintenance kontrak.

5. Penyebab risiko operasional dan jenis risiko yang terdapat di divisi Network Operation Center PT. Indosat Ooredoo Tbk didapatkan yaitu:
a. Risiko yang disebabkan kesalahan manusia (Human Error), ada sekitar 12 risiko
b. Risiko kepuasan pelanggan (Customer Satisfaction Risk). Ada sekitar 2 risiko
c. Risiko kerjasama (Partnering Risk), ada sekitar 6 risiko
d. Risiko Fraud (Fraud Risk), ada sekitar 3 risiko
e. Risiko pengadaan barang (Procurement Risk), ada sekitar 3 risiko
f. Risiko sumber daya manusia (Human Resources risk), ada sekitar 3 risiko
g. Risiko gangguan bisnis (Business Interuption Risk), ada sekitar 4 risiko
h. Risiko ketersediaan modal (Capital Availibility Risk), ada sekitar 3 risiko
i. Risiko Bencana (Disaster Risk), ada sekitar 3 risiko
j. Risiko Prosedure (Procedure Risk), yaitu prosedur kerja yang belum benar atau kesalahan prosedur kerja ada sekitar 4 risiko
k. Risiko lingkungan dan keamanan (Einvorement Risk), ada sekitar 2 risiko
l. Risiko peralatan/perangkat (Equipment Risk), ada sekitar 4 risiko

6. Dari 49 risiko yang teridentifikasi di divisi Network Operation Center PT. Indosat Ooredoo Tbk dari hasil penelitian ini didapatkan kriteria risiko untuk Acceptable atau risiko yang dapat diterima atau tidak perlu diambil tindakan yaitu sebanyak 10 risiko. Kriteria risiko untuk Supplementary Issue atau risiko yang diambil tindakan bila terjadi ada sumber daya yang memadai pada perusahaan atau dana/modal yang cukup, ada sebanyak 32 risiko dan kriteria risiko untuk Issue yang dimaksudkan untuk diperlukan suatu tindakan segera untuk mengelola risiko atau mengurangi risiko ada sebanyak 7 risiko.

## a. SARAN

1. Di PT Indosat Ooredoo Tbk, Manajemen risiko ditangani oleh sebuah divisi yang menangani juga internal audit. Sebaiknya setiap divisi ada team kecil yang bertugas melakukan identifikasi risiko mulai dari hal kecil sampai hal yang besar untuk diinfokan ke kepala divisi agar ditangani dan dikelola lebih baik
2. Penelitian ini belum sepenuhnya menjelaskan tentang bagaimana mitigasi yang dilakukan secara keseluruhan terutama terhadap peluang potensi risiko, jadi masih sebatas evaluasi dan penanganan yang dilakukan oleh manager dan senior engineer untuk mitigasinya. Sebaiknya dilakukan penelitian lanjutan mengenai mitigasinya di tingkat divisi bahkan di tingkat direktur
3. Dilakukan penelitian lanjutan mengenai besarnya kerugian finansial akibat risiko risiko yang diidentifikasi tersebut.
4. Dalam penelitian ini Citra Perusahaan tidak dibahas mendetail, sebaiknya dilakukan penelitian lanjutan bagaimana ukuran nya dan apa saja jenis pencitraannya yang berpengaruh terhadap perusahaan dan stake holder
5. Dilakukan penelitian lanjutan terhadap keselamatan kerja misalnya penduduk yang terpapar di bawah tower telekomunikasi baik radiasi maupun bangunannya. Juga risiko karyawan di daerah yang rawan konflik maupun rawan kejahatan seberapa besar risiko yang dihadapi.
6. Setiap perusahaan pasti ada risiko yang dihadapi, risiko bersifat kekal, tidak bisa dihilangkan dan hanya bisa berubah bentuk dan ditransfer jadi sebaiknya penanganan setiap risiko harus mulai dibiasakan dari Unit terbesar sampai terkecil sehingga tujuan manajemen risiko perusahaan searah dengan tujuan perusahaan.

## DAFTAR PUSTAKA


Kaderi Wiryono, S. dan Suharto, (2008), Analisis Risiko Operasional di PT. TELKOM dengan pendekatan metode ERM, prosideing seminar nasional teknologi Vol 7, SMB ITB

Boy Nurtjahyo, Erlinda Muslim dan M. Arif Rahman, 2008, Analisis Manajemen Risiko pada Produksi Mesin Motor di PT. X dengan pendekatan sistem dinamis, proceedings seminar nasional Teknologi Simulasi UGM 16 Oktober.

Dewi, D., 2012, Penerapan Sistem Manajemen Risiko pada Industri Nasionalsebagai masukan untuk Program PLTN, Prosiding Seminar Nasional Pengembangan Energi Nuklir V, 7 Maret.

Dewi, Hanggraeni (2010), Pengelolaan Risiko Usaha. Penerbit Fakultas Ekonomi UI.

Rury, Tisyana, (2011), Mitigasi Risiko para pihak dalam pemberian kredit ke perusahaan menara Telekomunikasi (Analisis perjanjian Kredit), FH UI 1 Juli.

Ariful Islam dan Tedford (2012), Risk Determinants of small and medium-sized manufacturing Enterprise (SMEs) –an exploratory study in New Zealand Dec

Bramantyo, Djohanputro., (2004), Jakarta, Manajemen Risiko Korporat Terintegrasi. Penerbit PPM

T. Sunaryo, ( 2007), Manajemen Risiko Finansial. Jakarta, Penerbit Salemba Empat.

Muhammad Muslich. (2007), Manajemen Risiko Operasional, Jakarta, Penerbit PT. Bumi Aksara

Gunawan & Waluyo, (2015), Risk Based Behavioral Safety, Jakarta, Penerbit PT. Gramedia Pustaka Utama

James Lam. (2007), Enterprise Risk Management,. Jakarta. Alih Bahasa Tim BSMR. Penerbit PT. Ray

H. Masyhud Ali, (2006), Manajemen Risiko, Strategi Perbankan dan Dunia Usaha Menghadapi Tantangan Globalisasi Bisnis., Jakarta, Penerbit PT. Raja Grafindo Persada

Sulad, Sri Hardanto (2006), Manajemen Risiko., Jakarta, Penerbit PT. Elex Media Komputindo Kelompok Gramedia.