UNIVERSITAS INDONESIA

AUDIT SISTEM INFORMASI MENGGUNAKAN KERANGKA KERJA *RISK IT* (STUDI KASUS PADA PT. RADIANT UTAMA INTERINSCO Tbk)

TESIS

Diajukan sebagai salah satu syarat
untuk memperoleh gelar Magister Akuntansi

CECEP SETIANA YUSUF

0906653365

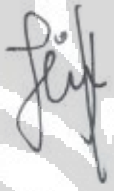
FAKULTAS EKONOMI
PROGRAM STUDI MAGISTER AKUNTANSI
JAKARTA
JANUARI 2012

HALAMAN PERNYATAAN ORISINALITAS

Tesis ini adalah hasil karya saya sendiri. Dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar.

Nama : Cecep Setiana Yusuf

NPM : 0906653365

Tanda Tangan : 

Tanggal : 19 Januari 2012

HALAMAN PENGESAHAN

Tesis ini diajukan oleh

Nama	:	Cecep Setiana Yusuf
NPM	:	0906653365
Program Studi	:	Magister Akuntansi
Judul Tesis	:	Audit Sistem Informasi Menggunakan *Risk IT* (Studi Kasus pada PT. Radiant Utama Interinsco Tbk)

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Magister Akuntansi pada Program Studi Magister Akuntansi, Fakultas Ekonomi, Universitas Indonesia.

DEWAN PENGUJI

Pembimbing	: Dr. Yudho Giri Sucahyo	(	)
Penguji	: Machmudin Eka Prasetya, M.Ak	(	)
Penguji	: Daniel, MTI	(	)

Ditetapkan di : Jakarta
Tanggal : 19 Januari 2012

Mengetahui,
Ketua Program

Prof. Dr. Lindawati Gani
NIP. 196205041987012001

KATA PENGANTAR

Assalamu 'Alaikum Warahmatullahi Wabarakatuh

Alhamdulillahirabbilalamin. Segala puji bagi الله, Tuhan semesta alam atas izin dan limpahan rahmat-Nya sehingga penulis dapat menyelesaikan penulisan tesis ini. Banyak kesulitan yang dihadapi oleh penulis dalam penulisan tesis ini, baik dalam penelitian maupun dalam penyusunannya. Namun berkat kerja keras, bimbingan dan dorongan dari berbagai pihak akhirnya tesis ini dapat diselesaikan.

Untuk itu penulis menghaturkan terima kasih yang sebesar-besarnya kepada :

1. Prof. Dr. Lindawati Gani , SE, Ak., MM, MBA selaku Ketua Program MAKSI PPAK Fakultas Ekonomi Universitas Indonesia
2. Bapak Yudho Giri Sucahyo, Ph.D selaku dosen pembimbing yang telah menyediakan waktu, tenaga dan pikiran untuk mengarahkan saya dalam penulisan tesis ini.
3. Segenap Dosen dan Karyawan Sekretariat Program MAKSI FE UI atas kebijaksanaan, ilmu & pengetahuannya serta bantuan yang diberikan kepada saya selama menuntut ilmu di MAKSI FE UI.
4. Seluruh pihak yang bersedia menjadi Narasumber dalam penelitian ini.
5. Orang tua dan keluarga yang selalu memberikan doa dan dukungan kepada saya dalam menyelesaikan tesis ini.
6. Istri dan putra putri tercinta (Fariz dan Icha) yang menjadi sumber inspirasi penulis
7. Sahabat dan teman-teman yang selalu memberikan dukungan kepada saya dalam penyelesaian tesis ini.

Wassalamu 'Alaikum Warahmatullahi Wabarakatuh

Jakarta, Januari 2012

Penulis

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

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

Nama : Cecep Setiana Yusuf
NPM : 0906653365
Program Studi : Magister Akuntansi
Departemen : Akuntansi
Fakultas : Ekonomi
Jenis Karya : Tesis

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

AUDIT SISTEM INFORMASI MENGGUNAKAN KERANGKA KERJA *RISK IT* STUDI KASUS PADA PT. RADIANT UTAMA INTERINSCO Tbk

beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini Universitas Indonesia berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (*database)*, merawat, dan memublikasikan tugas akhir saya tanpa meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta
Pada Tanggal : 19 Januari 2012
Yang menyatakan

(Cecep Setiana Yusuf)

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Informasi merupakan salah satu sumber daya strategis suatu organisasi, oleh karena itu, untuk mendukung tercapainya visi dan misi suatu organisasi, pengelolaan informasi menjadi salah satu kunci sukses. Sistem informasi merupakan salah satu sub sistem organisasi untuk mengelola informasi.

Saat ini sistem informasi dioperasikan oleh hampir seluruh sumber daya manusia suatu organisasi sehingga tidak dapat dipisahkan dengan operasi dan kehidupan organisasi. Teknologi informasi (TI) merupakan komponen penting dari sistem informasi, selain data/informasi, sumber daya manusia dan organisasi. Teknologi informasi yang dimaksud adalah teknologi telematika, telekomunikasi dan informatika yang mencakup teknologi komputer (perangkat keras, perangkat lunak) dan didukung dengan teknologi telekomunikasi, khususnya komunikasi data digital sebagai infrastruktur dari jaringan komputer. Penggunaan sistem informasi berbasis komputer harus dapat meningkatkan efektivitas dalam pencapaian tujuan organisasi. Hal ini berarti adanya evaluasi sistem informasi dan kebutuhan pemakai terhadap sistem informasi. Penggunaan sistem informasi berbasis komputer harus dapat meningkatkan efisiensi penggunaan sumber daya yang dibutuhkan dalam upaya mendukung efisiensi operasi organisasi. Hal ini berarti adalah sebuah sistem informasi yang efisien yaitu dengan penggunaan sumberdaya seminimal mungkin untuk mencapai tujuan organisasi.

Untuk memaksimalkan penerapan TI di perusahaan, dibutuhkan pemahaman yang tepat mengenai konsep dasar dari sistem yang berlaku, teknologi yang dimanfaatkan, aplikasi yang digunakan dan pengelolaan serta pengembangan sistem TI. Di era globalisasi sekarang ini, perusahaan harus dapat mengatasi masalah dan perubahan yang terjadi secara cepat dan sesuai sasaran. Oleh karena itu, faktor yang harus diperhatikan tidak hanya berfokus pada pengelolaan informasi semata, melainkan juga harus fokus untuk menjaga dan meningkatkan mutu informasi perusahaan. Dalam konteks ini, informasi dapat dikatakan

menjadi kunci untuk mendukung dan meningkatkan manajemen perusahaan agar dapat meningkatkan kinerja perusahaan.

Peranan sistem informasi yang signifikan inilah yang tentu saja harus diimbangi dengan pengaturan dan pengelolaan yang tepat sehingga kerugian–kerugian yang mungkin terjadi dapat dihindari. Kerugian yang dimaksud bisa dalam bentuk informasi yang tidak akurat yang disebabkan oleh pemrosesan data yang salah sehingga dapat mempengaruhi pengambilan keputusan yang salah pula. Sehubungan dengan alasan tersebut diperlukan adanya sebuah mekanisme kontrol terhadap pengelolaan teknologi informasi yaitu dengan melakukan audit Sistem Informasi atau audit Teknologi Informasi. Audit SI/TI dalam kerangka kerja COBIT lebih sering disebut dengan istilah *IT Assurance* ini bukan hanya dapat memberikan evaluasi terhadap keadaan tata kelola Teknologi Informasi di PT. Radiant Utama Interinsco Tbk (RUIS) tetapi dapat juga memberikan masukan yang dapat digunakan untuk perbaikan pengelolaannya di masa yang akan datang.

Audit Sistem Informasi adalah sebuah proses yang sistematis dalam mengumpulkan dan mengevaluasi bukti-bukti untuk menentukan bahwa sebuah sistem informasi berbasis komputer yang digunakan oleh organisasi untuk mencapai tujuannya.

Suatu perencanaan Audit Sistem Informasi berbasis teknologi (audit TI) oleh Internal Auditor dapat dimulai dengan menentukan area-area yang relevan dan berisiko paling tinggi, dalam penilaian risiko ini digunakan kerangka kerja *Risk IT*. Beberapa kategori penilaian risiko yang diambil didasarkan pada risiko umum yang sering dijumpai dalam pelaksanaan kontrol perusahaan. Kategori yang dipilih meliputi Operasi *Data Centre*, Sistem Aplikasi (Produksi), Sistem Aplikasi (Pengembangan), Sistem Informasi *Procurement* (Material dan Tenaga Kerja), Akuisisi Paket *Software*, dan Fungsi Sistem Informasi lainnya. Sementara untuk kebutuhan penugasan tertentu, misalnya audit atas proyek TI, dapat dimulai dengan memilih proses yang relevan dari proses-proses tersebut dan melakukan analisis sesuai *risk IT guidelines.*

Risk IT adalah suatu kerangka kerja yang didasarkan pada seperangkat prinsip-prinsip penuntun untuk pengelolaan yang efektif dari risiko TI. *Risk IT* merupakan kerangka kerja pelengkap COBIT, yaitu suatu kerangka kerja yang komprehensif untuk tata kelola dan pengendalian berbasis TI dan layanan. Sedangkan COBIT menyediakan satu set kontrol untuk mengurangi risiko TI. *Risk IT* menyediakan suatu kerangka kerja bagi perusahaan untuk mengidentifikasi, mengatur dan mengelola risiko TI. Risiko memainkan peranan sangat penting dalam pengambilan keputusan dalam perusahaan, hampir setiap keputusan bisnis yang membutuhkan eksekutif dan manajer untuk menyeimbangkan risiko dan keuntungannya. Risiko TI sering terlupakan dalam pengambilan keputusan dimana risiko usaha lainnya seperti risiko pasar, risiko kredit dan risiko operasional telah dimasukan dalam pengambilan keputusan perusahaan. Dalam lingkungan bisnis yang kompetitif, setiap organisasi beroperasi dalam iklim risiko. Tidak pernah mungkin untuk menghapus semua risiko dari bisnis, tetapi penting untuk menilai dan mengurangi risiko ke tingkat yang dapat diterima seminimal mungkin. Oleh karena itu, penting bahwa perusahaan memahami, memantau dan mengendalikan risiko, terutama karena perubahan lingkungan TI dengan cepat dan baru yang mengakibatkan risiko terkait TI muncul secara teratur.

Proses keandalan pengumpulan bukti dalam sebuah sistem yang terkomputerisasi seringkali akan lebih kompleks daripada sebuah sistem manual. Hal ini terjadi karena auditor akan berhadapan dengan keberadaan sebuah pengendalian internal pada sebuah sistem informasi berbasis komputer yang kompleks karena teknologi yang melekat dan sangat berbeda dengan pengendalian sistem manual. Sehingga sebuah sistem informasi berbasis komputer secara alamiah mempunyai *inherent risk* yang lebih tinggi dibandingkan dengan pemrosesan manual. Sehubungan dengan hal ini maka internal audit RUIS, dapat menggunakan *Risk IT guide* sebagai acuan untuk merancang prosedur audit TI. *Risk IT guide* dapat dimodifikasi dengan mudah, sesuai dengan industri dan kondisi TI di Perusahaan, atau objek khusus di lingkungan TI.

1.2 Perumusan Masalah

Atas latar belakang yang telah disebutkan diatas, maka penulis akan membahas dan melaporkan mengenai hasil audit yang telah dilakukan dengan menggunakan kerangka kerja *Risk IT* pada PT. Radiant Utama Interinsco, Tbk dengan tahapan menentukan *management awareness*, kemudian *plotting* terhadap kerangka kerja *Risk IT* dan memberikan rekomendasi berdasarkan hasil audit yang telah dilakukan dengan cara analisis sistem informasi secara langsung pada PT. Radiant Utama Interinsco, Tbk menggunakan kerangka kerja *Risk IT*. Berdasarkan rumusan diatas, maka pembahasan akan dititikberatkan pada masalah pokok yang diidentifikasi sebagai berikut:

1. Sejauh mana implementasi kerangka kerja *Risk IT* dalam audit sistem informasi PT. Radiant Utama Interinsco Tbk dalam menyediakan informasi bagi perusahaan?
2. Bagaimanakah implementasi kerangka kerja *Risk IT* pada internal audit PT. Radiant Utama Interinsco Tbk dengan menggunakan pengujian manajemen dan pengendalian teknologi informasi?

1.3 Tujuan Penelitian

Dari rumusan masalah diatas, maka tujuan penelitian ini adalah sebagai berikut:

1. Untuk mengenalkan penerapan audit sistem informasi menggunakan kerangka kerja *Risk IT*.
2. Untuk menyesuaikan kebutuhan perusahaan serta mencegah atau meminimalisir adanya risiko terhadap penggunaan TI.
3. Memberikan wawasan yang lebih jauh terhadap kemajuan ilmu pengetahuan dalam bidang Audit Sistem Informasi dan Teknologi Informasi menggunakan kerangka kerja *Risk IT*.

1.4 Manfaat Penelitian

Penelitian ini secara umum diharapkan mampu memberi tambahan informasi kepada masyarakat mengenai langkah-langkah audit tata kelola TI dengan menggunakan kerangka kerja *Risk IT* diantaranya adalah:

1. Membantu melakukan pengukuran penerapan audit sistem informasi menggunakan kerangka kerja *Risk IT* dan *IT Governance* pada PT. Radiant Utama Interinsco Tbk sehingga dapat mendukung tercapainya tujuan organisasi.
2. Menjadi salah satu referensi dalam penelitian penerapan audit sistem informasi menggunakan kerangka kerja *Risk IT* dan *IT Governance* pada PT. Radiant Utama Interinsco Tbk dan memberikan kontribusi bagi penelitian selanjutnya.

1.5. Metode Penelitian

Dalam melakukan penelitian ini, metode yang digunakan adalah metode desktiptif (*descriptive study*). Sumber data yang digunakan penulis adalah:

1. Data primer

   Sumber data primer diperoleh dengan mengumpulkan informasi yang berasal dari responden untuk memperoleh jawaban atas pertanyaan penelitian.
2. Data sekunder

   Merupakan data yang diperoleh dari data yang dikumpulkan dan direkam sebelumnya oleh orang lain.

Metode pengumpulan data yang digunakan oleh penulis ada 2 yaitu:

1. *Interview*

   Metode yang digunakan adalah melalui wawancara kepada narasumber yang kompeten, yaitu dari kalangan PT. Radiant Utama Interinsco, Tbk.
2. *Observational study*

   Metode yang digunakan adalah dengan studi literatur dan dokumentasi dari literatur, jurnal ilmiah, artikel, ketentuan audit internal, dan pedoman audit sistem informasi yang ada di negara Indonesia dan peraturan audit sistem informasi yang berlaku umum.

Langkah-langkah audit TI yang dilaksanakan oleh penulis dengan kerangka kerja *Risk IT* antara lain adalah:

1. Menyiapkan kerangka kerja *Risk IT*
2. Menetapkan alat bantu pengukuran RACI *chart* dan tingkat kematangan dengan menggunakan kerangka kerja *Risk IT*.

3. Melakukan kajian lapangan, dengan cara mengumpulkan data primer berupa wawancara dengan pihak-pihak terkait dan penentuan serta data sekunder berupa dokumen-dokumen yang terkait *Risk IT*.

4. Melakukan verifikasi atas data yang diperoleh untuk mendapatkan keyakinan yang cukup mengenai pengelolaan risiko terkait teknologi informasi yang ada di PT. Radiant Utama Interinsco,Tbk.

5. Melakukan analisis terhadap data primer dan sekunder dengan menggunakan kerangka kerja *Risk IT*.

6. Menerapkan praktik RACI *chart* yang ada di perusahaan

7. Mengukur tingkat kematangan dengan menggunakan alat ukur yang telah ditentukan sebelumnya untuk masing-masing elemen *Risk IT*.

8. Menarik kesimpulan serta memberi rekomendasi berdasarkan hasil analisis yang diperoleh.

1.6. Sistematika Pembahasan

Pembahasan dalam penelitian ini dibagi dalam lima bab dan tiap bab dibagi menjadi beberapa sub bab dengan urutan pembahasan sebagai berikut:

BAB 1 Pendahuluan

Bagian ini berisi latar belakang, perumusan masalah, ruang lingkup penelitian, tujuan penelitian, tujuan penelitian,manfaat penelitian, metode penelitian, dan sistematika pembahasan.

BAB 2 Tinjauan Pustaka

Bagian ini berisi kajian pustaka terhadap teoti dan literatur yang digunakan dalam pengerjaan karya akhir. Pembahasan terdiri dari pemahaman mengenai *Risk Based Audit, IT Governance,* Audit Sistem Informasi dan kerangka kerja *Risk IT*.

BAB 3 Gambaran Perusahaan

Bagian ini berisi tentang gambaran profil PT Radiant Utama Interinsco Tbk sebagai objek penelitian karya akhir ini. Gambaran mengenai latar

belakang organisasi antara lain visi, misi, struktur organisasi, dan kebijakan *IT Governance* yang diterapkan saat ini.

BAB 4 Analisis dan Pembahasan Hasil Penelitian

Bagian ini berisi tentang analisis yang dilakukan oeh penulis terhadap hasil audit sistem informasi dengan menggunakan kerangka kerja *Risk IT*

BAB 5 Kesimpulan dan Rekomendasi

Bagian ini berisi bagian penutup berupa kesimpulan dari hasil penelitian dan rekomendasi yang dapat diberikan kepada PT Radiant Utama Interinsco Tbk dalam penerapan audit sistem informasi dengan menggunakan kerangka kerja *Risk IT*

BAB II

TINJAUAN PUSTAKA

Bab 2 ini membahas mengenai teori-teori yang dipakai dalam karya akhir ini, yaitu teori-teori yang membahas mengenai risiko, risiko audit, audit sistem informasi dan kerangka kerja Risk IT sebagai pedoman dan panduan dalam penulisan karya akhir ini.

2.1 Pengertian Risiko

Definisi Risiko Menurut Kloman (2000), kata *"risk"* dalam bahasa Inggris berasal dari bahasa Italia kuno yaitu *"riscare"*. Risiko mempunyai definisi yang begitu beragam dengan begitu banyak pengertian dan interpretasi, tergantung dari cara orang memandangnya. Risiko dapat dipandang sebagai:

a. Sesuatu yang merugikan terjadi *(risk of loss)*

b. Suatu ketidakpastian *(risk of volatility)*

c. Sesuatu yang menguntungkan tidak terjadi *(risk of lost opportunity)*.

Sedangkan menurut The Institute of Internal Auditors (1991) dalam buku pegangan bagi anggota *The Institute of Internal Auditors* (IIA), yang berjudul *Standard For Professional Practice Of Internal Auditing* memberikan definisi *risk* sebagai berikut: "*Risk is probability that an event may adversely affect the organization or activity under audit*", yaitu risiko adalah kemungkinan suatu peristiwa yang mungkin memberikan dampak yang merugikan organisasi atau aktivitas yang sedang diperiksa.

Menurut Bank Indonesia (2003) risiko adalah potensi timbulnya suatu kerugian akibat terealisasinya suatu kejadian tertentu yang diperkirakan.

Risiko merupakan konsep yang digunakan oleh auditor dan manajemen untuk menyatakan perhatian mereka tentang dampak yang mungkin terjadi atas lingkungan yang penuh dengan ketidakpastian. Setiap peristiwa yang terjadi dapat mempunyai dampak yang material atau konsekuensi yang signifikan bagi organisasi dan tujuan organisasi. Akibat yang bersifat negatif disebut dengan risiko *(risk)* dan akibat yang bersifat positif disebut dengan kesempatan *(opportunities)*.

Organisasi menggunakan sumber daya yang tersedia untuk mencapai tujuan dan dalam proses penggunaan sumber daya tersebut terdapat kondisi ketidakpastian sehingga memunculkan risiko ataupun kesempatan. Risiko dan kesempatan mempunyai kecenderungan yang berbeda dalam perspektif waktu, dimana risiko cenderung akan semakin mengecil seiring dengan berjalannya waktu, namun tidak demikian dengan kesempatan.

Dari perspektif auditor, manajemen cenderung akan semakin memahami aspek operasionalisasi organisasi sehingga mampu merancang pengendalian intern untuk meminimalisasi risiko dan berupaya meningkatkan kesempatan.

2.2 Audit Risk

Laporan audit standar menjelaskan bahwa audit dirancang untuk memperoleh keyakinan yang memadai -bukan absolute- bahwa laporan keuangan telah bebas dari salah saji yang material. Karena audit tidak menjamin bahwa laporan keuangan telah bebas dari salah saji material, maka terdapat beberapa derajat risiko bahwa laporan keuangan mengandung salah saji yang tidak terdeteksi oleh auditor.

Dengan demikian dalam perencanaan pekerjaannya, auditor harus mempertimbangkan risiko audit tersebut. Menurut SA seksi 312 (PSA No. 25) yang dikutip oleh Soekrisno Agoes (2004), risiko audit adalah risiko yang timbul karena auditor, tanpa disadari tidak memodifikasikan pendapatnya sebagaimana mestinya, atas suatu laporan keuangan yang mengandung salah saji material.

Konsep keseluruhan mengenai risiko audit merupakan kebalikan dari konsep keyakinan yang memadai. Semakin tinggi kepastian yang ingin diperoleh auditor dalam menyatakan pendapat yang benar, semakin rendah risiko audit yang akan ia terima. Jika 99% kepastian diinginkan, maka risiko audit adalah 1%, sementara jika kepastian sebesar 95 % dianggap memuaskan, maka risiko audit adalah 5%. Biasanya pertimbangan professional berkenaan dengan keyakinan yang memadai dan keseluruhan tingkat risiko audit dirancang sebagai satu kebijakan kantor akuntan public, dan risiko audit akan dapat dibandingkan antara satu audit dengan audit lainnya. (Boynton, Jhonson, Kell, 2003). Tantangan akhir dari suatu audit

adalah bahwa auditor tidak dapat memeriksa semua bukti yang berkaitan dengan setiap asersi untuk setiap saldo akun dan golongan transaksi. Model risiko audit menjadi pedoman para auditor dalam pengumpulan bukti audit, sehingga auditor dapat mencapai tingkat keyakinan yang memadai yang diinginkan.

2.2.1 Komponen Risiko Audit

Dalam praktik, seorang auditor tidak hanya harus mempertimbangkan risiko audit untuk setiap saldo akun dan golongan transaksi saja, tetapi juga setiap asersi yang relevan dengan saldoakun dan golongan transaksi yang material. Faktor risiko yang relevan dengan suatu asersi biasanya berbeda dengan faktor risiko yang relevan dengan asersi lainnya untuk saldo akun atau golongan transaksi yang sama.

SAS NO. 47 (AU 312.20) menyatakan bahwa risiko audit terdiri dari 3 komponen:

1. Risiko bawaan (*Inherent risk)* merupakan kerentanan asersi terhadap salah saji (*misstatement)* yang material, dengan mengasumsikan bahwa tidak ada pengendalian yang berhubungan. Risiko salah saji (*misstatement)* seperti itu lebih besar dalam beberapa asersi laporan keuangan dan saldo-saldo atau pengelompokan yang berhubungan dari pada yang lainnya. Risiko ini dipertimbangkan pada tahap perencanaan audit. Sebagai contoh, perhitungan yang rumit lebih mungkin disajikan salah jika dibandingkan dengan perhitungan yang sederhana. Akun yang terdiri dari jumlah yang berasal estimasi akuntansi cenderung mengandung risiko lebih besar dibandingkan dengan akun yang sifatnya relatif rutin dan berisi data berupa fakta.

2. Risiko Pengendalian (*Control Risk)* merupakan risiko bahwa suatu salah saji yang material yang akan terjadi dalam asersi tidak dapat dicegah atau dideteksi secara tepat waktu oleh pengendalian perusahaan. Risiko ini merupakan fungsi keefektifan perancangan dan operasi pengendalian internal dalam mencapai tujuan entitas yang relevan untuk menyusun laporan keuangan entitas. Beberapa risiko pengendalian akan selalu ada karena keterbatasan yang melekat pada pengendalian internal.

3. Risiko Deteksi (*Detection Risk)* merupakan risiko bahwa auditor tidak dapat mendeteksi salah saji yang material dalam suatu perusahaan. Risiko ini merupakan fungsi keefektifan prosedur audit dan aplikasinya oleh auditor. Hal ini sebagian muncul dari ketidakpastian yang ada ketika auditor tidak memeriksa semua saldo akun atau kelompok transaksi untuk mengumpulkan bukti tentang asersi lainnya.

2.2.2 Konsep *Risk Based Auditing*

Perkembangan kegiatan bisnis ternyata mampu mempengaruhi dan membawa perubahan paradigma pelaksanaan audit dari pendekatan dengan pengendalian ke pendekatan audit berdasarkan Risiko (*Risk Based Auditing)*. Pergeseran fokus audit dari pengendalian ke risiko telah membuat suatu revolusi yang besar dalam pendekatan audit masa kini.

Risk assessment merupakan bagian dari tahapan pertama metodologi *Risk Management Based Auditing* yang harus dilakukan dalam melaksanakan audit keuangan dengan berbasis pada manajemen risiko. Tahapan tersebut adalah memahami operasi auditee yang bertujuan untuk mengidentifikasi dan memprioritaskan risiko kegagalan, risiko kekeliruan, dan risiko kecurangan yang dapat mempengaruhi audit laporan keuangan.

Salah satu model *Risk Based Auditing* yang dapat digunakan adalah model yang diperkenalkan oleh The Committee of Sponsoring Organizations of the Treadway Commissions **(**COSO)**.** Model COSO menunjukkan bahwa penentuan pengendalian yang dibutuhkan oleh organisasi harus melalui tahapan penilaian risiko (risk assessment). Pengendalian yang telah berorientasi kepada risiko akan lebih efektif karena jelas risiko terkait yang akan di minimalisasi (mitigate). Pengendalian intern yang telah berorientasi kepada risiko akan memberikan tingkat keyakinan yang lebih tinggi kepada auditor atas efektivitas pengendalian tersebut. Semakin efektif pengendalian maka audit juga akan menjadi semakin efisien dan efektif.

2.3 Audit Sistem Informasi

Menurut Laura schneider dalam artikelnya definisi Audit Sistem Informasi adalah *An information technology audit is an examination of the checks and balances, or controls, within an information technology (IT) group. An IT audit collects and evaluates "evidence" of an organization's information systems, practices, and operations. The evaluation of this evidence determines if the information systems are safeguarding the infomation assets, maintaining data integrity, and operating effectively and efficiently to achieve the organization's business goals or objectives (*Laura Schneider: 2009) Pengertian ini selaras dengan tujuan audit mutu internal dalam ISO 9001:2000. Audit Sistem Informasi sendiri merupakan gabungan dari berbagai macam ilmu, antara lain: Traditional Audit, Manajemen Sistem Informasi, Sistem Informasi Akuntansi, Ilmu Komputer, dan Behavioral Science.

Pada dasarnya, Audit TI dapat dibedakan menjadi dua kategori, yaitu Pengendalian Aplikasi (*Application Control*) dan Pengendalian Umum (*General Control*). Tujuan pengendalian umum lebih menjamin integritas data yang terdapat di dalam sistem komputer dan sekaligus meyakinkan integritas program atau aplikasi yang digunakan untuk melakukan pemrosesan data. Sementara, tujuan pengendalian aplikasi dimaksudkan untuk memastikan bahwa data di-input secara benar ke dalam aplikasi, diproses secara benar, dan terdapat pengendalian yang memadai atas output yang dihasilkan.

Audit terhadap aplikasi, biasanya pemeriksaan atas pengendalian umum juga dilakukan mengingat pengendalian umum memiliki kontribusi terhadap efektivitas atas pengendalian-pengendalian aplikasi.

Praktiknya, tahapan-tahapan dalam audit sistem informasi tidak berbeda dengan audit pada umumnya. Tahapan perencanaan, sebagai suatu pendahuluan, mutlak perlu dilakukan agar auditor mengenal benar objek yang akan diperiksa. Di samping, tentunya, auditor dapat memastikan bahwa *qualified resources* sudah dimiliki, dalam hal ini aspek SDM yang berpengalaman dan juga referensi praktik-praktik terbaik (*best practices*). Tahapan perencanaan ini akan menghasilkan suatu program audit yang didesain sedemikian rupa, sehingga

pelaksanaannya akan berjalan efektif dan efisien, dan dilakukan oleh orang-orang yang kompeten, serta dapat diselesaikan dalam waktu sesuai yang disepakati.

Dalam pelaksanaannya, auditor sistem informasi mengumpulkan bukti-bukti yang memadai melalui berbagai teknik termasuk survei, interview, observasi dan review dokumentasi (termasuk review *source-code* bila diperlukan). Satu hal yang unik, bukti-bukti audit yang diambil oleh auditor biasanya mencakup pula bukti elektronis (data dalam bentuk file *softcopy*). Biasanya, auditor sistem informasi menerapkan teknik audit berbantuan komputer, disebut juga dengan CAAT (*Computer Aided Auditing Technique*). Teknik ini digunakan untuk menganalisis data, misalnya saja data transaksi penjualan, pembelian, transaksi aktivitas persediaan, aktivitas nasabah, dan lain-lain.

Sesuai dengan standar auditing ISACA (*Information Sistems Audit and Control Association),* selain melakukan pekerjaan lapangan, auditor juga harus menyusun laporan yang mencakup tujuan pemeriksaan, sifat dan kedalaman pemeriksaan yang dilakukan. Laporan ini juga harus menyebutkan organisasi yang diperiksa, pihak pengguna laporan yang dituju dan batasan-batasan distribusi laporan. Laporan juga harus memasukkan temuan, kesimpulan, rekomendasi sebagaimana layaknya laporan audit pada umumnya.

2.4 Risk IT

Risk IT based on COBIT dikembangkan oleh *Information Technology Governance Institute* (ITGI) yang merupakan bagian dari *Information Sistem Audit & Control Association* (ISACA). Sesuai namanya, *Risk IT* merupakan kerangka kerja untuk manajemen risiko TI yang disusun berdasarkan kerangka kerja COBIT yang juga disusun oleh ITGI. *Risk IT* merupakan kerangka kerja yang berisi petunjuk manajemen risiko TI yang efektif dalam sebuah perusahaan sehingga akan memberikan manfaat bagi perusahaan yaitu:

1. Mengintegrasikan manajemen risiko TI ke *enterprise risk management.*
2. Menghasilkan keputusan risiko yang akan dihadapi, selera risiko dan tingkat toleransi terhadap risiko.

3. Melakukan mitigasi terhadap risiko.

Risk IT memberikan panduan bagaimana pengelolaan aktivitas-aktivitas utama dalam sebuah proses manajemen risiko TI, tanggung jawab setiap pihak, alur-alur informasi sehingga bisa mengukur kinerja setiap proses. Panduan dibagi menjadi tiga domain, secara umum yaitu: *risk governance*, *risk evaluation* dan *risk response.*

Gambar 2.1 Risk IT Framework

Sumber: ITGI (2008)

Risk IT memberikan panduan identifikasi melalui *risk scenario* yang berisi 36 *high level* skenario terkait TI. *Risk scenario* merupakan bagian panduan *Risk IT* pada area *collect data* dalam *domain risk evaluation*. Secara umum, proses identifikasi risiko menurut *Risk IT* bisa dilihat dimana, *high level scenario* digunakan dan dibandingkan dengan objektif bisnis pada PT. Radiant Utama Interinsco.

Seperti telah disebutkan sebelumnya, *risk IT* merupakan kerangka manajemen risiko TI yang disusun berdasarkan kerangka kerja COBIT, sehingga untuk setiap *high level scenario* yang disebutkan dalam *risk scenario Risk IT* dapat dipetakan ke setiap *control objective* yang ada dalam kerangka COBIT.

Oleh karena itu, dalam *Risk IT* juga telah memberikan contoh kontrol yang dapat memitigasi masing-masing *risk scenario* yang ada, dimana contoh kontrol tersebut diambil dari COBIT *control practices* (ISACA, 2009). Setiap perusahaan dapat memilih kontrol mana yang dapat diimplementasikan atau lebih cocok dengan karakteristik perusahaannya.

2.5. RACI *CHART*

RACI *chart* adalah salah satu informasi yang dikumpulkan ketika melakukan audit tata kelola TI dengan menggunakan kerangka kerja Risk IT. RACI chart memperlihatkan bagaimana pembagian peran dan tanggung jawab atas pengelolaan risiko TI di dalam perusahaan, yaitu dengan melihat siapa (*who*) yang bertugas (*role*) atau memiliki tanggung jawab (*responsibility*) atas apa (*what*) yang dilaksanakan dalam setiap prosesnya.

Definisi-definisi yang digunakan dalam RACI *chart* antara lain adalah:

R: *Responsibilty*, yaitu orang yang memiliki tugas dan tanggung jawab untuk menjalankan aktivitas yang sudah diputuskan.

A: *Accountabel*, yaitu orang yang memiliki tugas dan tanggung jawab untuk melakukan persetujuan atas aktivitas yang dilaksanakan.

C: *Consulted*, yaitu orang yang memiliki tugas dan tanggung jawab untuk memberikan masukan atas aktivitas yang dilaksanakan. Kegiatan ini merupakan proses komunikasi dua arah.

I: *Informed*, yaitu orang yang memiliki tugas dan tanggung jawab untuk memberikan informasi setelah aktivitas selesai dilaksanakan, kegiatan ini merupakan proses komunikasi satu arah.

Gambar 2.1 adalah salah satu contoh dari RACI *chart*, yaitu RG1: membangun dan memelihara risiko secara umum. RACI *chart* tersebut menjelaskan siapa saja orang-orang yang terkait dalam proses RG1, serta bagaimana peran dan tanggung jawab dari masing-masing orang tersebut.

RACI Chart

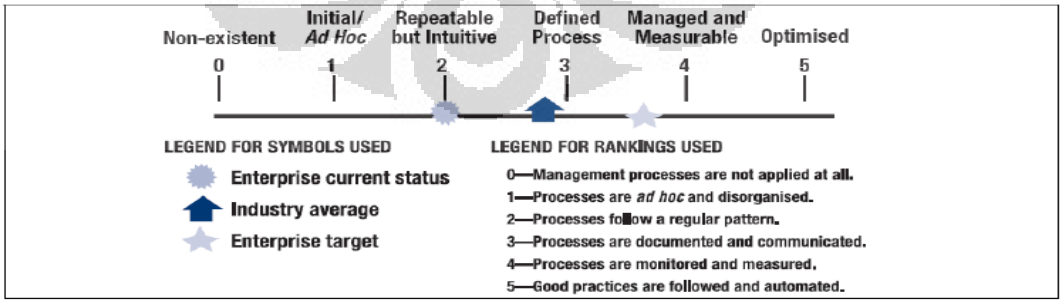
Key Activities / Roles	Board	CEO	CRO	CIO	CFO	Enterprise Risk Committee	Business Management	Business Process Owner	Risk Control Functions	HR	Compliance and Audit
RG1.1 Develop an enterprise-specific IT risk management framework.	A	R	R	R	C	I	R	I	C	I	C
RG1.2 Develop IT risk management methods.	C	C	A	R	C	I	C	C	C	I	C
RG1.3 Perform an enterprise-wide IT risk assessment.	I	A	R	R	C	I	R	C	R	C	C
RG1.4 Propose IT risk tolerance thresholds.	I	I	C	R	C	I	A	C	C		C
RG1.5 Approve IT risk tolerance.	A	C	C	C	C	R	C	C	C	C	C
RG1.6 Align policy and standards statements with IT risk tolerance.		I	A	R	I	C	R	I	C	R	I
RG1.7 Promote an IT risk-aware culture.	A	R	R	R	R	R	R	R	R	R	R
RG1.8 Promote effective communication of IT risk.	A	R	R	I	I	R	I	I	I	I	C

A RACI chart identifies who is Responsible, Accountable, Consulted and/or Informed.

Gambar 2.2 contoh RACI *chart* RG 1
Sumber: ITGI (2008)

2.6 Maturity Model

Dewan dan manajemen eksekutif perlu mempertimbangkan seberapa efektif perusahaan dalam mengelola risiko TI. Untuk mengukur efektivitas pengelolaan risiko TI, perusahaan menggunakan *tools maturity model* yang dapat memungkinkan perusahaan untuk menilai pengelolaan risiko TI nya dari tingkat kematangan paling rendah (0 – *Non existent)* ke tingkat kematangan paling optimal (5 – *Optimised)* yang digambarkan seperti pada gambar 2.3 berikut ini:



Gambar 2.3 *Maturity Model*
Sumber: ITGI (2008)

Secara umum, tujuan dari model kematangan ini adalah untuk mengidentifikasi ada di tingkat manakah perusahaan berada saat ini dan menyarankan mengatur prioritas untuk perbaikan. Tingkat kematangan risiko TI dirancang sebagai profil di mana perusahaan dapat mengidentifikasi gejala saat ini dan mungkin di masa depan.

Setiap perusahaan mengakui banyak proses pada setiap tingkat kematangan yang berbeda-beda, misalnya, beberapa proses pada tingkat 1, beberapa di tingkat 3 dan lain-lain di tingkat 4. Dengan cara ini, model kematangan dirancang untuk memungkinkan manajemen fokus pada bidang utama yang memerlukan perhatian dari pada mencoba mendapatkan semua proses stabil pada satu tingkat sebelum pindah ke proses berikutnya. Dengan menggunakan model kematangan risiko TI, manajemen dapat mengidentifikasi:

a. Kinerja sebenarnya dari perusahaan saat ini
b. Target perusahaan dalam pengembangani (misalnya, selera risiko, gaya manajemen, kemampuan respon risiko, dan/atau pengembangan pada semua sudut pandang risiko)

Untuk memudahkan hasil pengukuran digunakan oleh manajemen, dimana dapat mendukung perencanaan pengembangan dimasa depan atas tat kelola risiko, evaluasi risiko dan respon risiko dapat disajikan secara grafis. Untuk setiap domain Risiko TI, telah disediakan pemodelan tingkat tinggi dan model kematangan lebih rinci yang dibangun di sekitar atribut berikut, yang masing-masing berkembang melalui tingkat:

a. Kesadaran dan komunikasi
b. Tanggung jawab dan akuntabilitas
c. Tujuan pengaturan dan pengukuran
d. Kebijakan, standar dan prosedur
e. Keterampilan dan keahlian
f. Peralatan dan otomatisasi

Skala kematangan model ini dapat membantu manajemen memahami dimana kelemahan yang ada dan menetapkan target yang diperlukan. Tingkat kematangan yang paling sesuai untuk suatu perusahaan akan dipengaruhi oleh tujuan bisnis perusahaan, lingkup operasi dan praktik industri. Secara khusus, tingkat kematangan manajemen risiko TI akan tergantung pada ketergantungan perusahaan pada TI, kecanggihan teknologi dan peran eksekutif dan manajemen terhadap teknologi informasi.

2.7 Tujuan dan Metrik

Risiko TI menyajikan proses dari tujuan dan metrik, tingkat domain dan aktivitas. Tujuan menentukan bisnis apa yang diharapkan, sementara metrik memberikan langkah-langkah hasil aktual atau potensial. Tujuan domain yang dicapai oleh interaksi proses, masing-masing memiliki tujuan proses yang berbeda, pada gilirannya, bergantung pada tujuan aktivitas. Metrik bisa menjadi indikator, yang memberikan ukuran dari apa yang sebenarnya telah dilakukan atau dicapai, atau indikator utama, yang memberikan ukuran apa yang berpotensi dapat dicapai. Metrik merupakan titik awal, terkait dengan tingkat kematangan perusahaan.

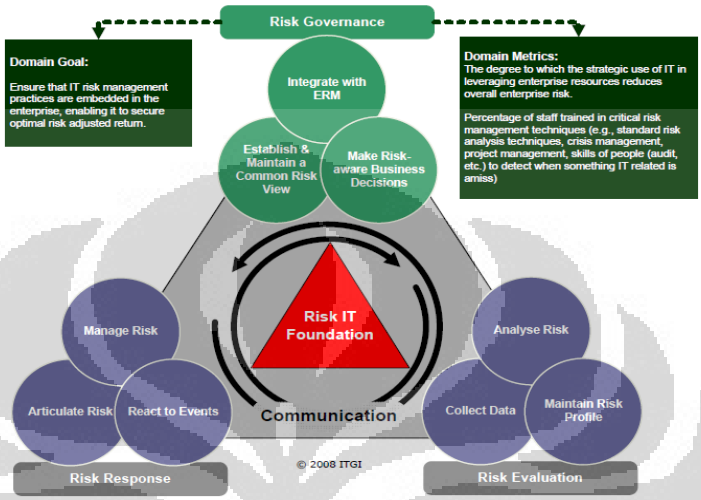
2.8 Komponen Kerangka Risiko TI

Kerangka kerja Risk IT terdiri dari tiga bagian, yaitu *Risk Governance*, *Risk Evaluate* dan *Risk Response* seperti yang digambarkan pada gambar 2.4 dibawah ini. Kemudian, masing-masing bagian tersebut terbagi menjadi sejumlah proses dan manajemen praktis.

Gambar 2.4 Komponen *Risk IT*
Sumber: ITGI (2008)

2.8.1 Domain- Tata Kelola Risiko (*Risk Governance*)

Domain ini untuk memastikan bahwa praktik manajemen risiko TI telah melekat di perusahaan sehingga memberikan keamanan yang optimal atas pengelolaan risiko terkait TI.



Gambar 2.5 Domain- Tata Kelola Risiko (*Risk Governance*)

Sumber: ITGI (2008)

1. **RG1 Membangun dan memelihara risiko secara Umum**

   Bertujuan untuk memastikan bahwa kegiatan manajemen risiko sejalan dengan kapasitas tujuan perusahaan untuk TI terkait kerugian dan toleransi subjektif pemimpin atas toleransi ini.

2. **RG2 Mengintegrasikan dengan ERM**

   Bertujuan untuk mengintegrasikan strategi dan kegiatan risiko TI dengan keputusan risiko bisnis strategis yang telah dibuat di tingkat perusahaan.

3. **RG3 Membuat Keputusan Bisnis sadar Risiko.**

   Bertujuan untuk memastikan bahwa keputusan organisasi mempertimbangkan berbagai peluang dan konsekuensi yang timbul dari ketergantungan pada TI untuk mencapai tujuan.

Tabel 2.1 *Risk Governance (RG) Detailed Maturity Model (Part 1)*

Risk Governance (RG) Detailed Maturity Model (Part 1)			
	Awareness and Communication	**Responsibility and Accountability**	**Goal Setting and Measurement**
0	The enterprise does not recognise the need to consider the business impact from IT risk. Decisions involving IT risk taking tend to be based on lack of information or incorrect information. There is no awareness of external requirements for IT risk management and integration with enterprise risk management.		
1	There is an emerging understanding that IT risk is important and needs to be managed, but it is viewed as a technical issue and the business primarily considers the downside of IT risk. Any IT risk identification criteria vary widely across the enterprise and the IT organisation. IT risk issues are primarily communicated by assurance groups (e.g., internal audit). Minimal structure and basis for discussion of IT risk concepts exist. Senior managers and IT executives struggle with IT risk language.	By default, IT is accountable for problem management, availability, system access, etc. Ownership of IT risk in the context of business services and processes is not defined. There is no consideration of business accountability and responsibility for proactive IT risk management. No linkage to an individual performance measurement and reward programme exists. There is no business expectation of value from including IT executives in risk decisions.	Risk appetite and tolerance are considered only during episodic risk assessments. Investments are focused on externally imposed requirements and expectations. Reporting is compliance-driven and focused on remediation of issues identified by assurance groups and external parties.
2	There is an awareness of the need to actively manage IT risk, but the focus is on technical compliance with no anticipation of value added. Some localised IT understanding of risk/reward exists. Senior managers and IT executives are developing a common language for IT risk, but IT risk discussions across silos may be impaired by competing business unit and function-specific risk language.	There are emerging leaders for IT risk management within silos who assume responsibility and are usually held accountable, even if this is not formally agreed. The enterprise risk committee charter covers IT risk, but IT has minimal representation. Performance targets are tied to meeting external reporting requirements and minimising negative findings. Roles are only partially defined and contain overlaps (e.g., risk evaluation overlaps with risk response, IT implementers are empowered to prescribe and opine). There is confusion about responsibility for integrating IT risk management with operations and enterprise risk management. When problems occur, a culture of blame tends to exist.	Risk tolerance is set locally and may be difficult to aggregate. Investments are focused on specific risk issues within functional and business silos (e.g., security, business continuity, operations). Regular manual reporting of IT risk management activities is directed to local IT management.
3	IT people generally understand how IT-related failures or events impact enterprise objectives and cause direct or indirect loss to the enterprise, while business people generally understand how IT-related failures or events can affect key services and processes. IT risk management is viewed as a business issue and both the downside and upside of IT risk are recognised. IT risk strategies and plans are communicated by management. IT risk discussions are based on a defined language/taxonomy. Enterprise-level information on risk and opportunity is shared.	There is a designated leader for IT risk across the enterprise who is engaged with the enterprise risk committee, where IT risk is in scope and discussed. The business understands how IT fits in the enterprise-wide, or portfolio view, risk perspective. The IT risk leader has a strong relationship with the CFO and is regularly consulted during portfolio management and budgeting activities. The IT risk leader has sufficient stature to effectively challenge business decisions involving IT risk. IT risk roles are clearly defined and contain minimal overlap. Process responsibility and accountability are defined and process owners have been identified. Performance measures are tied to providing business value in addition to meeting external requirements.	Enterprise risk tolerance is derived from local tolerances, and IT risk management activities are being aligned across the enterprise. Investments are being made against common risk issues although they may not address the root cause in all cases. Risk appetite and tolerance are applied during system design, implementation, and steady state, and during major organisational changes. Regular reporting of IT risk management process outcomes is directed to IT management.
4	Risk culture is analysed and reported. The business understands IT risk/reward. IT risk management is viewed as a business enabler, and both the downside and upside of IT risk are understood. The IT risk language spoken by senior executives is blending and aligning with corporate risk language. IT risk discussions are a normal part of executive decision making.	The designated leader for IT risk across the enterprise is fully engaged with the enterprise risk committee, which expects value from including IT in decisions. The IT department's role in operational risk management and the broader enterprise risk management is well understood. Integrated risk management is embedded in strategic planning and business operations. All identified IT risk issues have a nominated owner, and responsibility and accountability are accepted. Senior business management and IT management together determine the acceptable level of risk the enterprise will tolerate. A reward culture that motivates positive action is in place.	The board defines risk appetite and tolerance for all departments, including IT risk. Risk tolerance may be refined by the enterprise risk committee or an IT risk council. Risk portfolio views are dynamic, and risk tolerance is evaluated based on different views. Better investment decisions result from enterprise-wide visibility into costs, IT risk issues and benefits/rewards. Opportunities associated with risk are part of the risk plan's expected outcomes. Investments are balanced against a portfolio view of risk and address the root cause. Regular reporting of business outcomes related to IT risk management is made to business management.
5	Senior executives make a point of considering all aspects of IT risk in their decisions. The enterprise views integrated risk management as a source of business value.	The IT risk leader is considered a trusted advisor during design, implementation and steady-state operations. Executive sponsorship is strong, and the tone from the top has embedded integrated risk management into the enterprise culture. Roles and responsibilities are process-driven, with cross-functional teams collaborating. Accountability for risk management to help achieve objectives is embedded in all processes, support functions, business lines and geographies. The IT department is a major player in business line operational risk efforts and enterprise-wide risk efforts.	Strategic objectives are based on an executive-level understanding of IT-related business threats, risk scenarios and competitive opportunities. The enterprise employs robust business analytics to measures the effectiveness of managing uncertainties and seizing risky opportunities.

Sumber: ITGI (2008)

Tabel 2.2 *Risk Governance (RG) Detailed Maturity Model (Part 2)*

Risk Governance (RG) Detailed Maturity Model (Part 2)			
	Policies, Standards and Procedures	**Skills and Expertise**	**Tools and Automation**
0			
1	Enterprise policies and standards, which are minimal at best, may be incomplete and/or reflect only external requirements and lack defensible rationale and enforcement mechanisms. Minimal procedures for IT risk management exist. Policies and standards are not kept up to date relative to evolving business, technology or threat landscapes.	IT risk management skills may exist on an *ad hoc* basis, but they are not actively developed. Enterprise risk managers and business process owners lack IT risk understanding. IT personnel lack an understanding of the business impact of IT risk.	*Ad hoc* control-centric inventories are dispersed across desktop applications. Policies and standards exist in multiple formats. There is no workflow around incidents and risk decisions.
2	There is board-issued guidance for risk management. Policies and standards are established for functional and business silos and may not align with the board guidance and overall business risk appetite.	Minimum skill requirements, which include an awareness of IT risk, are identified for critical enterprise risk areas. Risk awareness training focuses on policy and some risk language. IT risk management training is provided in response to needs, rather than on the basis of an agreed plan, and informal training on the job occurs.	Functional and IT silo-specific inventories of risk issues exist. Key elements of risk decisions are recorded in desktop applications. Some desktop-based risk management tools may exist, but a co-ordinated approach and expected benefits from tools are lacking.
3	Formal risk categories have been identified and described in clear terms. Enterprise policies and standards reflect overall business risk appetite. Established risk policy is based on board guidance. Important issues are directed to senior management. The process, policies and procedures are defined and documented for all key IT risk management activities. Exceptions are resolved in a formal manner.	Skill requirements are defined and documented for all enterprise risk areas and include IT risk concepts. Risk awareness training includes situations and scenarios beyond specific policy and the structures and a common language for communicating risk. Enterprise risk managers and business process owners receive targeted IT training, e.g., IT for finance executives. IT personnel receive training on business activities, products, general business risk, competing risk issues and business dependency on IT. A formal training plan has been developed.	Requirements are defined for a centralized inventory of risk issues. Workflow tools are used to escalate risk issues and track decisions. Data collection tools can distinguish amongst multiple event types.
4	Enterprise policies and standards reflect business risk tolerance. Far-sighted risk scenarios consider IT risk across the enterprise. Major risk decisions fully consider the probability of both loss and reward. Standards for developing and maintaining the integrated risk management processes and procedures are adopted and followed.	Skill requirements are routinely updated for all areas, proficiency is ensured for all risk management areas and certification is encouraged. Risk awareness training is comprehensive and includes role playing and cascading and coincidental threat types and scenarios. Mature training techniques are applied according to the training plan, and knowledge sharing is encouraged. All internal IT risk management experts are involved, and the effectiveness of the training plan is evaluated.	Tools enable enterprise risk portfolio management, automation of IT risk management workflows, and monitoring of critical activities and controls. Standard tools are deployed that integrate IT risk management with ERM.
5	Enterprise policies and standards continue to reflect business risk tolerance while increasing efficiency (e.g., they are dynamically updated, they contain details for high-risk situations and flexibility for lower-risk situations). IT risk management is fully integrated into enterprise risk management processes and structures, business activities, business lines, products, and initiatives (e.g., new partnerships, service providers, mergers, acquisitions). All risk decisions are consistently based on probabilities of loss and reward. IT, internal audit, compliance, control and risk management are highly integrated and co-ordinate and report risk issues.	The enterprise formally requires continuous improvement of IT risk management skills, based on clearly defined personal and organisational goals. Training and education for IT risk management support external best practices and use of leading-edge concepts and techniques. Knowledge sharing is an enterprise culture, and knowledge-based systems are being deployed. External experts and industry leaders are used for guidance.	Real-time monitoring of events and control exceptions occurs. Policy management is automated. Automated tools enable end-to-end support of the risk management processes. Tools are being used to support improvement of the risk management process.

Sumber: ITGI (2008)

Tabel diatas menjelaskan mengenai pengukuran tingkat kematangan pada domain *Risk Governance* secara rinci yang bila dijelaskan lebih lanjut maka ukuran tingkat kematangannya adalah sebagai berikut:

1. **Level 0 – Non existent**

   Perusahaan tidak mengakui kebutuhan untuk mempertimbangkan dampak bisnis dari risiko TI. Keputusan melibatkan pengambilan risiko TI cenderung didasarkan pada kurangnya informasi atau informasi yang salah. Tidak ada kesadaran tentang persyaratan eksternal untuk manajemen risiko TI dan integrasi dengan manajemen risiko perusahaan.

2. **Level 1 - Initial**

   Ada sebuah pemahaman yang muncul bahwa risiko TI adalah penting dan perlu dikelola, tetapi dipandang sebagai masalah teknis dan bisnis terutama mempertimbangkan *downside* risiko TI. Kriteria identifikasi risiko TI bervariasi secara luas di seluruh perusahaan dan organisasi TI. TI bertanggung jawab atas manajemen masalah, ketersediaan, akses sistem dll. Risiko dan toleransi dianggap hanya selama penilaian risiko episodik. Kebijakan dan standar perusahaan sangat minim, mungkin tidak lengkap dan/atau hanya mencerminkan kebutuhan eksternal dan masih kurangnya mekanisme pelaksanaan. Keahlian manajemen risiko TI sudah ada, namun mereka tidak aktif dikembangkan.

3. **Level 2 - Repeatable**

   Adanya kesadaran akan kebutuhan untuk secara aktif mengelola risiko TI, namun fokusnya adalah pada kepatuhan teknis dengan tidak ada antisipasi nilai tambah. Adanya pemimpin untuk manajemen risiko TI yang memikul tanggung jawab dan biasanya bertanggung jawab, walaupun hal ini tidak secara resmi disepakati. Toleransi risiko diatur secara lokal. Investasi difokuskan pada isu-isu risiko spesifik pada fungsional dan bisnis (misalnya, keamanan, kelangsungan bisnis, operasi). Dewan menerbitkan panduan untuk manajemen risiko. Adanya persyaratan keterampilan minimum yang mencakup kesadaran risiko TI yang diidentifikasi untuk daerah risiko

perusahaan yang kritis. Adanya fungsional dan bagian yang spesifik yang melakukan inventarisir isu-isu risiko.

4. Level 3 - Defined

Manajemen risiko TI dipandang sebagai masalah bisnis. Ada pemimpin yang ditunjuk untuk risiko TI di seluruh perusahaan; pemimpin ini terlibat dengan komite risiko perusahaan, di mana risiko TI dalam cakupan dan pembahasan. Perusahaan memahami TI yang bagaimana yang cocok bagi perusahaan secara luas atau dari sudut pandang portofolio dan persfektif risiko. Toleransi risiko perusahaan berasal dari toleransi lokal dan kegiatan manajemen risiko TI yang disejajarkan di seluruh perusahaan. Kategori risiko formal telah diidentifikasi dan dijelaskan dalam istilah yang jelas. Adanya pelatihan yang menumbuhkan kesadaran atas risiko pelatihan kesadaran termasuk situasi dan skenario di luar kebijakan yang spesifik dan terstruktur dan bahasa risiko yang umum yang memudahkan dalam mengkomunikasikan risiko. Adanya persyaratan yang ditentukan atas inventarisir isu-isu risiko terpusat. Adanya *tools* alur kerja yang digunakan untuk meningkatkan keputusan melacak isu-isu risiko.

5. Level 4 - Managed

Manajemen risiko TI dipandang sebagai *enabler* bisnis, dan terdapat pemahaman atas risiko TI. Pemimpin yang ditujukan untuk risiko TI di seluruh perusahaan sepenuhnya terlibat dengan komite risiko perusahaan, yang mengharapkan nilai dari TI termasuk dalam keputusan. Departemen TI berperan dalam manajemen risiko operasional dan manajemen risiko perusahaan yang lebih luas dipahami dengan baik. Dewan mendefinisikan selera risiko dan toleransi untuk semua departemen, termasuk risiko TI. Kebijakan dan standar perusahaan mencerminkan toleransi risiko bisnis. Berpandangan jauh terhadap skenario risiko dengan mempertimbangkan risiko TI di perusahaan. Keputusan risiko utama sepenuhnya mempertimbangkan kemungkinan kerugian dan kemungkinan *reward*. Persyaratan keterampilan secara rutin diperbarui untuk semua bidang, kemahiran terjamin untuk semua area manajemen risiko. Mengaktifkan portofolio manajemen risiko

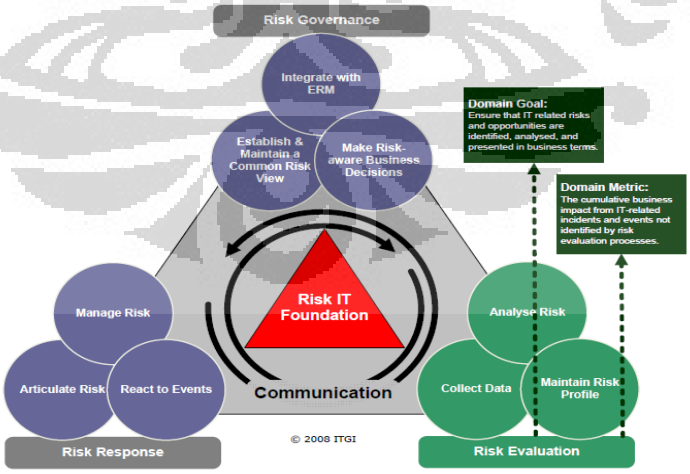
perusahaan, otomatisasi alur kerja manajemen risiko TI, dan pemantauan kegiatan kritis dan kontrol.

6. Level 5 - Optimised

Eksekutif senior mempertimbangkan semua aspek risiko IT dalam keputusannya. Pemimpin Risiko TI dianggap sebagai penasihat terpercaya selama perancangan, implementasi dan operasi dalam kondisi yang mapan. Departemen TI memiliki peranan yang utama atas upaya pengelolaan risiko TI perusahaan secara luas. Tujuan strategis didasarkan pada pemahaman tingkat eksekutif TI terkait dengan ancaman bisnis, risiko skenario dan peluang kompetitif. Kebijakan dan standar perusahaan mencerminkan toleransi risiko bisnis sambil meningkatkan efisiensi. Perusahaan secara resmi membutuhkan peningkatan keterampilan manajemen risiko TI secara kontinyu. Adanya pengecualian *real-time monitoring* kegiatan dan kontrol, seperti halnya otomasi kebijakan manajemen.

2.8.2 Domain- Evaluasi Risiko (RE)

Domain ini memastikan bahwa risiko dan peluang terkait TI telah diidentifikasi, dianalisis dan dilaporkan ke manajemen.



Gambar 2.6 Domain- Evaluasi Risiko (RE)

Sumber: ITGI (2008)

1. **RE1 Mengumpulkan data**

   Mengidentifikasi data yang relevan yang memungkinkan identifikasi, analisis dan pelaporan terkait risiko TI lebih efektif.

2. **RE2 Analisis Risiko**

   Mengembangkan informasi yang berguna untuk mendukung keputusan risiko yang memperhitungkan relevansi bisnis dari faktor risiko (misalnya, ancaman, kerentanan, nilai, kewajiban).

3. **RE3 Menjaga Profil Risiko**

   Menjaga up-to-date dan kelengkapan inventarisasi risiko yang dikenal dan atributnya (misalnya, frekuensi yang diharapkan, dampak potensial, disposisi), sumber daya TI, kemampuan, dan kontrol seperti yang dipahami dalam konteks produk bisnis, jasa, dan proses.

Tabel 2.3 *Risk Evaluate (RE) Detailed Maturity Model (Part 1)*

Risk Evaluation (RE) Detailed Maturity Model (Part 1)			
	Awareness and Communication	**Responsibility and Accountability**	**Goal Setting and Measurement**
0	The enterprise does not recognise the need to understand how IT-related events and conditions (risk factors) may affect its performance. A complete lack of data forces assumptions about key aspects of the risk environment during decision making and ongoing operations. There is no awareness of external requirements to evaluate IT risk.		
1	Recognition of the need for risk evaluation is emerging; however, there is minimal understanding of the business environment and the associated threats end events that may affect performance. There is minimal feedback to decision makers regarding the effect risk decisions have on the risk condition and the business condition. The identification and analysis of IT risk is based on 'gut feel' rather than in the context of business activities and may be perceived as producing unfounded worst-case scenarios.	By default, IT is accountable for risk evaluation. No performance measurement and reward programme exists to support individual responsibility for identifying how much risk exists.	Current IT risk information and mitigation options are inferred from episodic assessments.
2	Worst-case loss scenarios are the focus of discussions, although the driving factors for those scenarios may not be understood. Some feedback is provided to decision makers regarding the effect IT risk decisions have on the business condition. There are localised taxonomies used as a basis for discussion of IT risk analysis concepts.	Individuals assume responsibility for both risk evaluation and risk response. There is confusion about enterprise-wide risk evaluation responsibilities. When problems occur, a culture of blame tends to exist.	Some planned risk analysis occurs, but practitioners make major assumptions about the contributing factors for risk. Some goal setting for data collection and analysis occurs but is not tracked with key metrics.
3	There is an emerging understanding of risk fundamentals. Gaps between IT-related risk and opportunity and overall risk appetite are being recognised. Risk analysis discussions are based on a defined language/taxonomy. Decision makers are provided regular qualitative feedback regarding the effect IT-related risk decisions have on the business condition. Enterprise-level information regarding risk analysis practices and issues is shared.	Responsibility and accountability for key risk evaluation practices are defined and process owners have been identified. The process owner is unlikely to have full authority to exercise the responsibilities. Job descriptions consider risk evaluation responsibilities.	The capability is in place to evaluate IT risk on an enterprise-wide basis alongside other risk types. Risk information and mitigation options are based on defined procedures and meet the basic needs of decision makers. Regular reporting of IT risk evaluation process outcomes is directed to IT management. Measurement of risk evaluation processes emerges but is not consistently applied.
4	Risk analysis has been accepted as a way to better understand the enterprise's resilience and be better prepared to achieve strategic objectives. Risk identification and analysis methodologies produce structured multi-risk scenarios that are well understood by management and practitioners. Risk analysis discussions are based on defined terms. Rational estimates of loss probabilities and mitigation options are available to all stakeholders. Decision makers receive regular quantitative feedback on the effect IT-related risk decisions have on the business condition. Enterprise risk data conform to a standard model and are widely shared.	All types of risk have a nominated owner, and senior business management and IT management together determine the business relevance of risk factors. Risk evaluation response responsibility and accountability are accepted and working in a way that enables a process owner to fully discharge his/her responsibilities. A reward culture is in place that motivates positive action.	IT risk information and mitigation options are based on quantitative methods and anticipate the needs of decision makers. Management is able to monitor the risk profile. Risk evaluation efficiency and effectiveness are measured and communicated and linked to business goals and the IT strategic plan. Risk evaluation exceptions are noted by management and root cause analysis is being standardised. The acceptable degrees of error or inconsistency in risk analysis are well established. Business management receives regular reporting of business outcomes related to IT risk evaluation.
5	Decision makers enjoy transparency into IT risk and have available the best possible information about loss probabilities, emerging exposures and opportunities. The drivers of the real risks to real operations are vigorously communicated throughout the extended enterprise.	Employees at every level take direct responsibility for determining the business relevance of risk factors, e.g., threats, vulnerabilities, value, liability.	The enterprise maintains an optimal balance between the qualitative and quantitative methods that support decisions on managing uncertainties and seizing risky opportunities.

Sumber: ITGI (2008)

Tabel 2.4 *Risk Evaluate (RE) Detailed Maturity Model (Part 2)*

Risk Evaluation (RE) Detailed Maturity Model (Part 2)			
	Policies, Standards and Procedures	**Skills and Expertise**	**Tools and Automation**
0			
1	Any data collection and analysis methods are *ad hoc* and may be compliance-driven. Risk evaluation may not include all the components of risk.	IT risk analysis skills may exist on an *ad hoc* basis, but they are not actively developed. Enterprise risk managers and business process owners lack IT risk evaluation understanding. IT personnel lack the skills to determine the business relevance of risk factors. Employees desire improved data collection, analysis and profiling skills, but no inventory of risk evaluation skills exists nor is a competency model established for documenting future skill requirements.	Departments and functions maintain their own informal checklists for risk analysis within their silos.
2	Dependency analysis and scenario analysis are *ad hoc* and focus on only a limited number of business activities. Data collection, analysis and profiling methods are being used but may lack key elements and will vary across the enterprise and the IT organisation. It is difficult to normalise data across the enterprise.	Minimum skill requirements are identified for critical areas of data collection, risk analysis and risk profiling. Risk analysis training is provided in response to needs, rather than on the basis of an agreed plan, and informal training on the job occurs.	Functional and IT silo-specific risk analysis approaches and tools exist but are based on solutions developed by key individuals. Data collected in support of risk analysis are recorded in desktop applications. However, minimal distinction is made amongst threat events, vulnerability events and loss events.
3	Risk evaluation methodologies are accepted by management. Dependency analysis and scenario analysis procedures are defined and performed across multiple business activities, business lines and products. Risk analysis takes a probabilistic approach and considers threat frequency, vulnerability and loss magnitude. Risk analysis scope regularly includes existing systems and systems under design and development. The majority of risk analysis results are subject to formal peer review.	Skill requirements are defined and documented for all enterprise risk areas, with full consideration of data collection, risk analysis and profiling. Risk evaluation training includes techniques beyond minimum policy and common tools to determine the business relevance of risk factors. Enterprise risk managers and business process owners receive targeted IT risk analysis training. Skill requirements are defined and documented for all areas of risk evaluation. A formal training plan for risk evaluation has been developed. Data are available regarding the movement of critical risk evaluation skills and competencies.	Data collection tools generally adhere to defined standards and distinguish amongst threat events, vulnerability events and loss events. Some centralised tools with standardised evaluation criteria of frequency, impact and control effectiveness are in place. Prototypes of workflow have been established to embed risk probabilities into decision-making procedures.
4	Data collection, dependency analysis and scenario analysis procedures are defined and performed across multiple risk types, business activities, business lines and products. All risk analysis results are subject to formal peer review and the root cause of quality issues is investigated.	Skill requirements are routinely updated for all areas of risk evaluation, proficiency is ensured for all critical areas and certification is encouraged. The enterprise is addressing the longer-term development needs of staff with high potential in risk evaluation and related skills. Mature IT risk analysis training techniques are applied according to the training plan, and knowledge sharing is encouraged. All internal IT evaluation experts are involved, and the effectiveness of the training plan is evaluated.	Risk analysis tools are implemented according to a standardised plan, and some have been integrated with other related tools. Risk evaluation tools are being used in main areas to automate critical activities in support of data collection, risk analysis and profiling.
5	Risk evaluation activities are based on a broad and deep set of IT risk scenarios that integrate all business activities, business lines, products and known risk types. The root cause of risk is consistently understood and always used as the basis for risk response decisions. Peer review of risk analysis results and of other key risk evaluation practices is subject to rigorous root cause analysis, and actions are always taken to improve the results.	The enterprise formally requires continuous improvement of data collection, risk analysis, and profiling skills, based on clearly defined personal and organisational goals.	Real-time data are collected on threat events, vulnerability events, loss events and discovery of risk factors. Automated tools enable end-to-end support and improvement of risk evaluation efforts.

Sumber: ITGI (2008)

Tabel diatas menjelaskan mengenai pengukuran tingkat kematangan pada domain *Risk Evaluate* secara rinci yang bila dijelaskan lebih lanjut maka ukuran tingkat kematangannya adalah sebagai berikut:

1. **Level 0 – Non existent**

   Perusahaan tidak mengakui kebutuhan untuk memahami bagaimana TI-terkait peristiwa dan kondisi (risiko faktor) dapat mempengaruhi kinerjanya. Kurangnya data yang lengkap dari asumsi kekuatan tentang aspek kunci dari lingkungan risiko selama pengambilan keputusan dan operasi yang sedang berlangsung. Tidak ada kesadaran kebutuhan eksternal untuk mengevaluasi risiko TI.

2. **Level 1 - Initial**

   Pengakuan kebutuhan untuk evaluasi risiko yang muncul, namun, ada pemahaman minimal mengenai lingkungan bisnis dan ancaman terkait peristiwa yang mungkin mempengaruhi kinerja. Dengan standar, TI bertanggung jawab untuk evaluasi risiko. Informasi risiko TI saat ini dan pilihan mitigasi disimpulkan dari penilaian episodik. Setiap pengumpulan data dan metode analisis yang *ad hoc* dari pemicu kepatuhan. Keterampilan analisis risiko TI mungkin ada pada dasarnya, tetapi tidak aktif dikembangkan.

3. **Level 2 - Repeatable**

   Adanya diskusi mengenai skenario kerugian terburuk, meskipun faktor pendorong untuk skenario tidak dapat dipahami. Individu bertanggung jawab atas evaluasi risiko dan respon risiko. Adanya perencanaan analisis atas risiko yang terjadi, tetapi praktisi membuat asumsi tentang faktor risiko yang berkontribusi. Ketergantungan dan analisis skenario hanya terfokus terbatas pada sejumlah kegiatan usaha. Persyaratan keterampilan minimum diidentifikasi untuk daerah-daerah kritis data pengumpulan, analisis risiko dan profil risiko. Fungsional dan pendekatan analisis risiko TI secara spesifik dan adanya *tools* tetapi didasarkan pada solusi yang dikembangkan oleh individu-individu tertentu.

4. **Level 3 - Defined**

   Ada pemahaman mengenai dasar-dasar risiko. Kesenjangan antara TI terkait risiko dan peluang risiko keseluruhan sudah diakui. Tanggung jawab dan akuntabilitas untuk praktek evaluasi risiko didefinisikan dan pemilik proses telah diidentifikasi. Kemampuan dalam mengevaluasi risiko TI secara bersamaan pada perusahaan secara keseluruhan atas jenis risiko lainnya. Ketergantungan analisis dan skenario prosedur analisis didefinisikan dan dilakukan pada beberapa kegiatan usaha, lini bisnis dan produk. Persyaratan keterampilan didefinisikan dan didokumentasikan untuk semua area risiko perusahaan, dengan pertimbangan pada pengumpulan data, analisis dan profil risiko. Alat pengumpulan data umumnya mengikuti standar yang ditetapkan dan dapat membedakan antara peristiwa ancaman, kerentanan dan peristiwa kerugian.

5. **Level 4 - Managed**

   Analisis risiko telah diterima sebagai cara untuk lebih memahami ketahanan perusahaan dan menjadi lebih baik agar siap untuk mencapai tujuan strategis. Semua jenis risiko memiliki pemilik yang dinominasikan, manajemen bisnis senior dan manajemen TI bersama-sama menentukan relevansi faktor risiko bisnis. Efisiensi dan efektivitas evaluasi risiko diukur dan dikomunikasikan dan dihubungkan dengan tujuan bisnis dan rencana TI strategis. Risiko pengecualian evaluasi dicatat oleh manajemen berdasarkan standar analisis. Semua hasil analisis risiko dilakukan *peer review* formal, dan dilakukan penyelidikan kualitas atas akar penyebab masalah. Perusahaan menangani kebutuhan peningkatan kemampuan staf dalam yang memiliki potensi yang tinggi dalam evaluasi risiko. Adanya alat analisis risiko yang dilaksanakan sesuai dengan rencana standar, dan beberapa telah terintegrasi dengan alat-alat terkait lainnya.

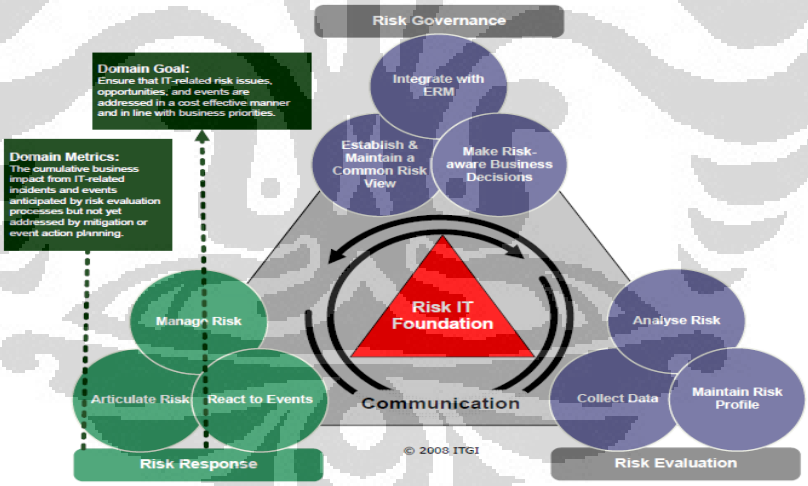
6. **Level 5 - Optimised**

   Adanya transfaransi atas risiko TI dari para pembuat keputusan dan juga telah tersedia informasi tentang probabilitas kerugian, pemaparan dan peluang yang muncul. Pemicu risiko nyata untuk operasi riil telah dikomunikasikan ke

seluruh perusahaan. Karyawan di setiap tingkat mengambil tanggung jawab langsung untuk menentukan relevansi faktor risiko bisnis. Perusahaan mempertahankan keseimbangan optimal antara metode kualitatif dan kuantitatif yang mendukung keputusan dalam mengelola ketidakpastian dan menangkap peluang berisiko. Kegiatan evaluasi risiko didasarkan pada skenario risiko TI secara luas dan mendalam yang mengintegrasikan semua kegiatan bisnis, lini bisnis, produk dan jenis risiko yang dapat dikenali. Perusahaan secara resmi membutuhkan perbaikan terus-menerus pengumpulan data, analisis dan keterampilan profil risiko. Alat otomatis memungkinkan dukungan *end-to-end* dan upaya perbaikan evaluasi risiko.

2.8.3 Domain-Respon Risiko (RR)

Domain ini bertujuan memastikan bahwa isu-isu risiko terkait TI, peluang, dan peristiwa telah ditangani dengan cara yang efektif dan sesuai dengan prioritas bisnis.



Gambar 2.7 Domain-Respon Risiko (RR)
Sumber: ITGI (2008)

1. **RR1 Artikulasikan Risiko**

   Memastikan bahwa informasi tentang keadaan sebenarnya dari eksposur yang berkaitan dengan IT dan kesempatan yang tersedia pada waktu yang tepat dan kepada orang yang tepat untuk respon yang tepat.

2. **RR2 Mengelola Risiko TI**

   Memastikan bahwa langkah-langkah untuk menangkap peluang strategis dan mengurangi risiko TI ke tingkat yang dapat diterima dikelola sebagai portofolio.

3. **RR3 Menanggapi peristiwa**

   Memastikan bahwa langkah-langkah untuk segera menangkap peluang atau membatasi besarnya kerugian dari peristiwa yang berkaitan dengan IT telah diaktifkan secara tepat waktu dan efektif.

Tabel 2.5 *Risk Response (RR) Detailed Maturity Model (Part 1)*

Risk Response (RR) Detailed Maturity Model (Part 1)			
	Awareness and Communication	**Responsibility and Accountability**	**Goal Setting and Measurement**
0	The enterprise does not recognise the need to manage IT risk issues and exposures to the business and its operations. No crisis communication processes are in place. No monitoring of internal control exists. There is no awareness of external requirements to deploy controls, capabilities and resources to limit the frequency and impact (loss magnitude) of IT-related events.		
1	Recognition of the need for risk response is emerging, but it is viewed as limited to risk avoidance, meeting compliance requirements and transfer through insurance. There is minimal individual awareness of threats and what to do when they materialise. There is minimal communication around detection and response to events and risk responses in line with business priorities.	There is minimal accountability for ensuring that reasonable risk response measures are in place and reflect the threat environment and asset values. Individuals assume responsibility for both risk evaluation and risk response.	IT-related events and conditions that could affect day-to-day operations are occasionally discussed at management meetings but specific risk responses are not considered. Control deficiencies are discussed in a reactive mode and are difficult to define. Minimal management information exists to help detect events in a timely manner and compare responses with business priorities.
2	There is growing awareness of the need to respond to risk, as evidenced by the introduction of strategies beyond avoidance, such as reduction, sharing or acceptance in the context of risk appetite and tolerance. There is individual awareness of threats and points of contact for direction when they materialise. IT risk response issues are communicated by management, but IT risk response discussions may be impaired by competing business unit-specific risk language.	There is an emerging leader for IT risk response who assumes responsibility for mitigating risk and helping to manage the impact of events. The leader is usually held accountable, even if this is not formally agreed. Overall, there is confusion about responsibility for risk response. When problems occur, a culture of blame tends to exist.	Control deficiencies may be identified but they are not remediated in timely manner. Some risk response goal setting occurs but it may not be focused on the real risk to real operations.
3	IT and business executives can explain their top three IT risk issues (i.e., combinations of control, value and threat conditions that impose a noteworthy level of risk) and the steps they are taking to respond, in line with risk appetite and tolerance. Across the enterprise there is individual understanding of business-impacting threats and the specific actions to take if the business threat materialises. Employees are aware of their responsibility for control activities. There is a common understanding of the need to enact risk response measures. IT risk strategies and plans are communicated by management. IT risk response discussions are based on a defined language/taxonomy. Enterprise-level information on risk response is shared.	Responsibility and accountability for key risk response practices are defined and process owners have been identified. The process owner is unlikely to have full authority to exercise his/her responsibilities. Job descriptions consider risk response responsibilities.	Control deficiencies are identified and remediated in a timely manner. Unacceptable tolerance and mitigation are reported to the appropriate manager. Risk appetite and tolerance are applied during the development of IT risk mitigation and event action plans. Regular reporting of IT risk response process outcomes is directed to IT management.
4	Management is advised on changes in the business and IT environment that could significantly affect the IT risk scenarios. There is both individual and organisational understanding of the full requirements for responding to risk. Risk response discussions are based on defined terms. Enterprise risk response information conforms to a standard model and is widely shared.	Senior business management and IT management together determine whether a risk condition exceeds define risk tolerances. Risk mitigation and response responsibility and accountability are accepted and working in a way that enables a process owner to fully discharge his/her responsibilities. A reward culture is in place that motivates positive action.	Efficiency and effectiveness of risk response are measured and communicated, and linked to business goals and the IT strategic plan The operating effect of control activities is evaluated on a periodic basis and the process is adequately documented. Regular reporting is made to business management of the business outcomes related to IT risk response process.
5	The extended enterprise is well aware of the full requirements and the strategies and plans in place for responding to risk. The responses to real risks to real operations are vigorously communicated throughout the extended enterprise.	Employees at every level take direct responsibility for responding to risk. The enterprise as whole collaborates with external entities to respond to common and pandemic risk issues.	The enterprise measures the effectiveness of risk response efforts both internally and in collaboration with external entities.

Tabel 2.6 *Risk Response (RE) Detailed Maturity Model (Part 2)*

Risk Response (RR) Detailed Maturity Model (Part 2)			
	Policies, Standards and Procedures	**Skills and Expertise**	**Tools and Automation**
0			
1	IT controls exist but are based on compliance requirements, vary widely in relation to risk and operate in isolated silos.	A lack of skills and competency for risk response may force the enterprise to accept risk beyond tolerance levels when value propositions are particularly compelling. IT risk articulation, mitigation and crisis management skills may exist in silos but they are not actively developed. Enterprise risk managers and business process owners lack IT risk response understanding. IT personnel lack the project management and crisis management skills critical for risk mitigation programmes and minimising the impact of risk events. Employees desire improved risk response skills, but no inventory of these skills exists nor is there an established competency model for documenting future skill requirements.	Technical security tools are deployed in a haphazard manner that is generally unrelated to risk, impact and cost-effectiveness. Some control-centric inventory and incident logging tools may exist; usage is based on standard desktop applications.
2	Risk mitigation processes are starting to be implemented where IT risk issues are identified.	Minimum skill requirements are identified for critical areas of risk articulation, mitigation and crisis management. Risk response training is provided in response to tactical needs, rather than on the basis of an agreed plan, and informal training occurs on the job.	Common approaches to the use of risk mitigation and response tools exist but are based on solutions developed by key individuals.
3	An enterprise-wide risk response policy defines when and how to respond to risk. A process to address a key IT risk issue is usually instituted once it is identified.	Job descriptions include expectations for risk response. Employees are periodically trained in IT-related threats, risk scenarios, and controls relevant to their roles and responsibilities. Skill requirements are defined and documented for all enterprise risk areas, with full consideration of IT risk articulation, mitigation and crisis management. Risk response training includes techniques beyond minimum policies and common tools for project management and crisis management. Enterprise risk managers and business process owners receive targeted IT risk response training. Skill requirements are defined and documented for all areas of risk response. A formal training plan for risk response has been developed. Data are available regarding the movement of critical risk response skills and competencies.	A plan has been defined for the use and standardisation of tools to automate certain risk mitigation activities, such as user provisioning.
4	There are streamlined mechanisms for reporting risk incidents upward to senior management without delay or 'spin'. All aspects of the risk response process are documented and quantitatively managed. Standards for developing and maintaining the processes and procedures are adopted and followed.	Skill requirements are routinely updated for all risk response areas, including risk articulation, risk mitigation, reacting to events and seizing opportunities. Proficiency is ensured for all critical areas, and certification is encouraged. Mature training techniques are applied according to the training plan, and knowledge sharing is encouraged. All internal domain risk response experts are involved, and the effectiveness of the training plan is evaluated. The enterprise is addressing the longer-term development needs of staff with high potential in risk response (e.g., project management, crisis management) and related skills.	Tools are being used in main areas to enable enterprise risk portfolio management and to monitor critical controls, capabilities and resources.
5	The full range of risk response strategies is holistically applied and, where fully justified, cost-effective controls mitigate exposure to risk on a continuing basis. Process documentation is evolved to automated workflows. Processes, policies and procedures are standardised and integrated to enable end-to-end risk response and improvement.	The enterprise formally requires continuous improvement of risk response skills (e.g., risk articulation, mitigation, crisis management) based on clearly defined personal and organisational goals. There are frequent reminders and discussions of IT-related threats, risk scenarios, controls and progress toward meeting key risk response goals.	Real-time monitoring of emerging risk factors and events with standard tools occurs. Technology is leveraged to its fullest extent to document processes; identify gaps; and evaluate the effectiveness of risk-based controls, capabilities, and resources. The enterprise employs advanced risk response technologies to intelligently take on additional risk and seize competitive opportunities.

Sumber: ITGI (2008)

Tabel diatas menjelaskan mengenai pengukuran tingkat kematangan pada domain *Risk Response* secara rinci yang bila dijelaskan lebih lanjut maka ukuran tingkat kematangannya adalah sebagai berikut:

1. **Level 0 – Non existent**

   Perusahaan tidak mengenali kebutuhan untuk mengelola isu-isu dan eksposur risiko TI ke bisnis dan operasinya. Tidak ada krisis proses komunikasi. Tidak ada pemantauan pengendalian internal. Tidak ada kesadaran tentang persyaratan eksternal untuk menyebarkan kontrol, kemampuan dan sumber daya untuk membatasi frekuensi dan dampak (besarnya kerugian).

2. **Level 1 - Initial**

   Pengakuan kebutuhan untuk respon risiko muncul, tetapi dipandang terbatas pada risiko penghindaran, memenuhi persyaratan kepatuhan dan transfer melalui asuransi. Ada minimal kesadaran individu atas ancaman dan apa yang harus dilakukan ketika terjadi.

   Ada komunikasi yang minim atas deteksi dan respon terhadap peristiwa dan respon risiko sejalan dengan prioritas bisnis. Ada akuntabilitas yang minimal untuk memastikan bahwa risiko yang masuk akal atas respon tindakan yang ada dan mencerminkan ancaman terhadap lingkungan dan nilai aset. Individu bertanggung jawab untuk risiko baik evaluasi maupun respon risiko. Peristiwa terkait TI dan kondisi yang dapat mempengaruhi sehari-hari operasi kadang-kadang dibahas pada pertemuan manajemen, tetapi tanggapan risiko spesifik tidak dipertimbangkan. Kekurangan kontrol dibahas dalam modus reaktif dan sulit untuk didefinisikan. Informasi manajemen sangat minim untuk membantu mendeteksi peristiwa secara tepat waktu dan membandingkan tanggapan dengan prioritas bisnis.

3. **Level 2 - Repeatable**

   Adanya kesadaran kebutuhan untuk menanggapi risiko, sebagaimana dibuktikan oleh strategi *preventif*, seperti pengurangan, pembagian atau penerimaan dalam konteks toleransi risiko. Ada kesadaran individu atas ancaman dan adanya indikasi ketika risiko itu terjadi. Adanya respon atas isu

risiko TI yang disampaikan oleh manajemen., tetapi pembahasan ini terbentur oleh adanya konflik kepentingan maupun budaya kerja yang tidak. Ada pemimpin yang muncul untuk respon risiko TI yang bertanggung jawab untuk mitigasi risiko dan membantu mengelola dampak peristiwa. Secara keseluruhan, ada kebingungan tentang tanggung jawab atas respon risiko. Ketika terjadi masalah, budaya saling menyalahkan cenderung ada. Kekurangan kontrol dapat diidentifikasi namun mereka tidak dapat menangani secara tepat waktu.

4. **Level 3 - Defined**

Departemen TI dan eksekutif perusahaan dapat menjelaskan atas tiga isu risiko TI (yaitu, kombinasi kontrol,nilai dan ancaman kondisi yang memaksakan patut diperhatikan tingkat risikonya) dan langkah-langkah untuk menanggapi, sesuai dengan selera risiko dan toleransi. Di seluruh perusahaan ada pemahaman tentang ancaman berdampak pada bisnis dan tindakan spesifik yang dilakukan jika ancaman bisnis terjadi. Karyawan menyadari tanggung jawab mereka untuk kegiatan pengendalian. Ada pemahaman umum tentang kebutuhan untuk memberlakukan tindakan respon risiko.

Tanggung jawab dan akuntabilitas praktek penanggulangan risiko didefinisikan dan pemilik proses telah diidentifikasi. Pemilik proses tidak memiliki kewenangan penuh untuk melaksanakan tanggung jawabnya. Deskripsi pekerjaan mempertimbangkan tanggung jawab respon risiko. Kekurangan kontrol diidentifikasi dan ditangani secara tepat waktu. Toleransi tidak dapat diterima dan mitigasi dilaporkan kepada manajer yang tepat. Selera risiko dan toleransi diterapkan selama pengembangan mitigasi risiko TI dan rencana tindakan. Pelaporan hasil proses respon risiko TI diarahkan ke manajemen TI.

5. **Level 4 - Managed**

Manajemen disarankan pada perubahan dalam bisnis dan lingkungan TI yang dapat secara signifikan mempengaruhi skenario risiko TI. Ada pemahaman yang baik dari individu dan organisasi mengenai persyaratan untuk menanggapi risiko. Informasi respon risiko perusahaan sesuai dengan model

standar. Senior manajemen bisnis dan manajemen TI bersama-sama menentukan apakah kondisi risiko melebihi toleransi risiko. Mitigasi risiko dan respon tanggung jawab dan akuntabilitas yang diterima dan bekerja dengan cara yang memungkinkan pemilik proses untuk sepenuhnya bertanggungjawab. Adanya budaya imbalan untuk memotivasi tindakan positif. Efisiensi dan efektivitas respon risiko diukur dan dikomunikasikan, dan terkait untuk tujuan bisnis dan rencana strategis TI. Efek operasi kegiatan kontrol dievaluasi secara periodik dan didokumentasikan secara memadai. Pelaporan secara rutin dibuat untuk pengelolaan hasil bisnis terkait dengan TI proses respon risiko.

6. **Level 5 - Optimised**

Perusahaan secara luas sangat menyadari penuh persyaratan dan strategi dan rencana untuk menanggapi risiko. Respon terhadap risiko untuk operasi riil dikomunikasikan dengan penuh semangat ke seluruh level perusahaan. Karyawan di setiap tingkatan bertanggung jawab langsung untuk menanggapi risiko. Perusahaan secara keseluruhan bekerja sama dengan entitas eksternal untuk merespon isu-isu risiko umum dan pandemi. Perusahaan mengukur efektivitas upaya respon risiko baik secara internal maupun dalam kolaborasi dengan entitas eksternal.

Dalam penelitian ini, setiap risiko yang baru di identifikasi untuk setiap *risk scenario* akan mengambil COBIT *control practices* yang menurut Risk IT dapat memitigasi risiko-risiko dalam *risk scenario* tersebut. Usulan kontrol tersebut tetap diajukan dengan melihat control mana yang dapat diimplementasikan PT. Radiant Utama Interinsco, Tbk.

BAB III

GAMBARAN PERUSAHAAN

Bab 3 membahas tentang gambaran profil PT Radiant Utama Interinsco Tbk sebagai objek penelitian karya akhir ini dan metodologi penelitian yang dipergunakan. Gambaran mengenai latar belakang organisasi antara lain visi, misi, struktur organisasi, dan kebijakan *IT Governance* yang diterapkan saat ini.

3.1 Sejarah Singkat Perusahaan

Didirikan pada tanggal 22 Agustus 1984, PT Radiant Utama Interinsco Tbk (RUIS) memfokuskan diri pada penyediaan jasa teknis penunjang untuk Industri Minyak dan Gas mulai dari hulu hingga ke hilir, serta industri terkait lainnya. Di bidang Inspeksi dan Sertifikasi, RUIS memperoleh akreditasi sebagai badan Inspeksi dan Sertifikasi resmi dari beberapa instansi berwenang seperti: Direktorat Jenderal Minyak dan Gas Bumi; Direktorat Jenderal Mineral, Batubara, dan Panas Bumi; Direktorat Jenderal Listrik dan Pemanfaatan Energi; serta Departemen Tenaga Kerja dan Transmigrasi. Pada tahun 2008, perusahaan memasuki bisnis hulu migas dengan mengakuisisi 100% kepemilikan pada Radiant Bukit Barisan yang memiliki 51% kepemilikan atas blok migas South West Bukit Barisan di Sumatera Barat.

Pada tahun 2010, melalui anak perusahaan, PT Supraco Indonesia, membentuk konsorsium dengan Tata Power dan Origin Energy dalam mengembangkan potensi panas bumi di Indonesia. Sertifikat ISO 9001:2008, 14001:2004, dan OHSAS 18001:2007 menunjukkan komitmen kuat perusahaan dalam menjaga kualitas dan keunggulan jasa yang diberikan termasuk komitmen terhadap Kesehatan dan Keselamatan Kerja dalam Sistem Manajemen RUI. Perusahaan mencatatkan sahamnya di Bursa Efek Indonesia pada 12 Juli 2006 dan memiliki dua anak perusahaan yaitu: PT Radiant Tunas Interinsco dan PT Supraco Indonesia

VISI:

"Menjadi sebuah perusahaan yang unggul melalui orang-orang profesional, struktur keuangan yang solid, pertumbuhan berkelanjutan, kepuasan pelanggan"

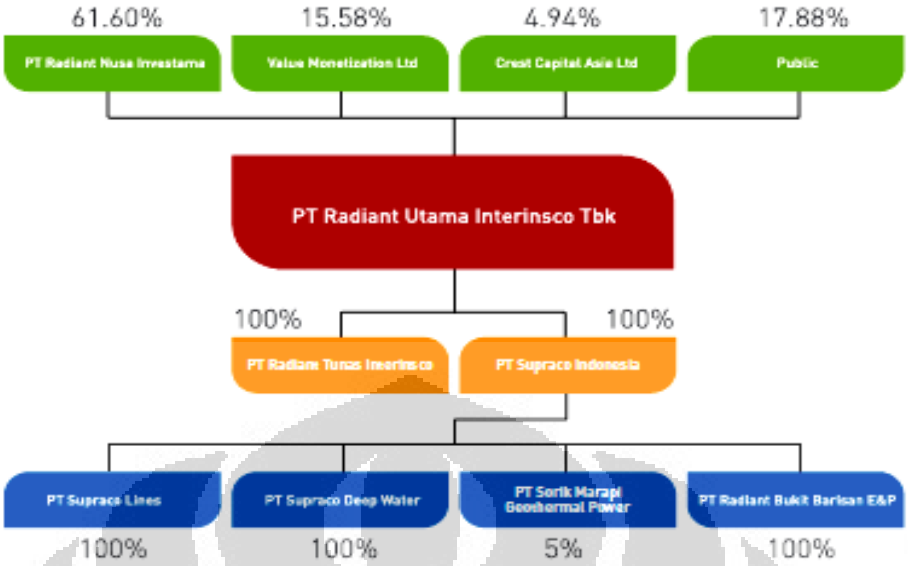
MISI:

"Untuk memberikan pelayanan teknis dan manajemen profesional standar internasional terutama untuk industri minyak dan gas mendukung."

3.2 Kegiatan Usaha Perusahaan

Segmen bisnis perusahaan meliputi penyediaan layanan teknis seperti jasa pendukung minyak & gas dari hulu ke hilir dan industri terkait lainnya, termasuk penyediaan fasilitas eksplorasi lepas pantai, fasilitas produksi lepas pantai, jasa inspeksi dan sertifikasi serta perdagangan umum. Saat ini, PT Radiant Utama Interinsco dengan dua anak perusahaan yaitu PT Supraco Indonesia dan PT Radiant Tunas Interinsco bergerak di segmen bisnis, seperti:

- Layanan NDT (Nondestructive Test) & Oil Country Tubular Goods
- Layanan Inspeksi & Sertifikasi, Blasting & Coating
- Layanan Konstruksi, Operasi & Pemeliharaan
- Layanan lepas pantai
- Jasa Lainnya, seperti Pelatihan Teknis, Penilaian Dampak Lingkungan, dll



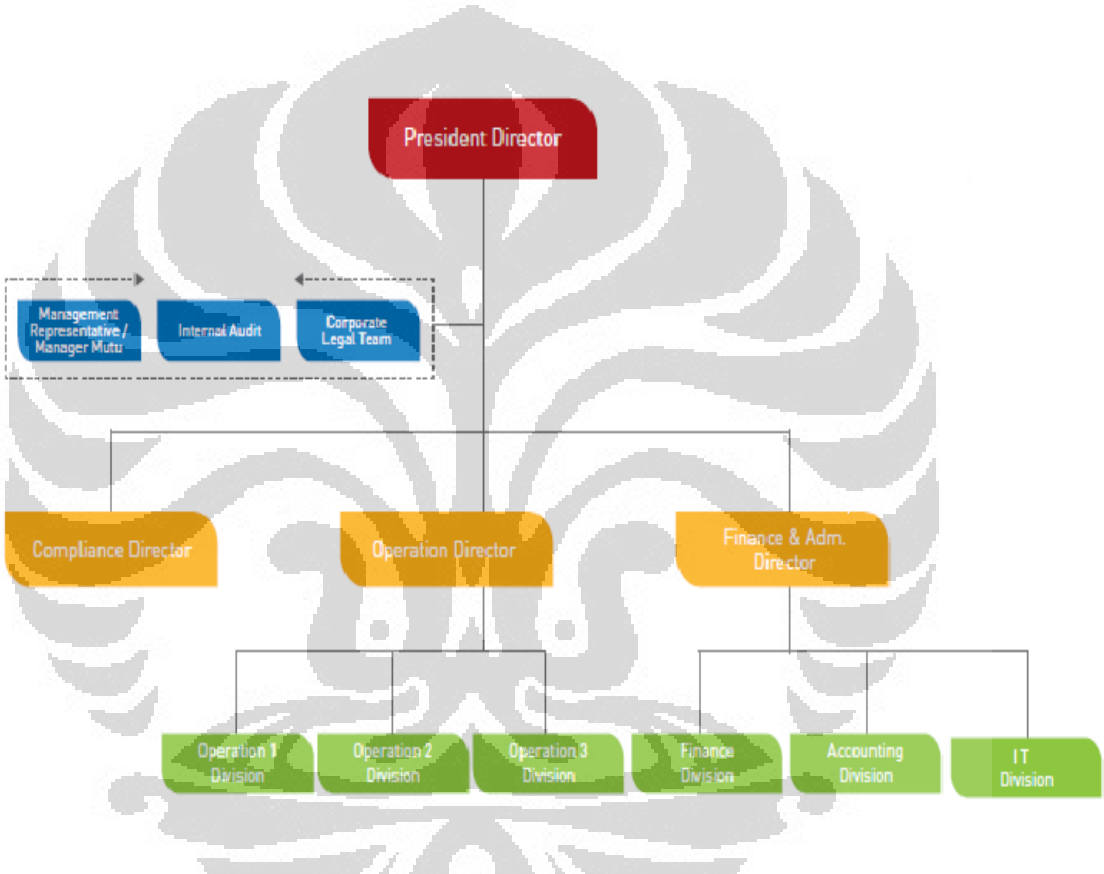
Gambar 3.1 Struktur Perusahaan
Sumber: Company Profile PT Radiant Utama Interinsco (2010)

Ditahun 2010 harga saham PT Radiant Utama Interinsco Tbk (RUIS) mencapai harga tertinggi di level Rp 310 per saham pada bulan Maret dan harga terendah di level Rp 160 per saham pada bulan Juni 2010. Saham RUIS ditutup pada harga Rp 200 per saham di akhir tahun 2010 atau terjadi peningkatan sebesar 5.8% dari harga di awal tahun. Namun volume perdagangan di tahun 2010 sangat rendah. Hal ini menunjukkan bahwa para pemegang saham masih meyakini potensi yang dimiliki perusahaan untuk berkembang di masa depan.

3.3 Manajemen dan Struktur Organisasi Perusahaan

Pengendalian Internal perusahaan ditujukan untuk melindungi kepentingan para pemegang saham dan *stakeholder* lainnya dengan cara memastikan operasional perusahaan berjalan efektif dan efisien, memastikan laporan keuangan perusahaan dapat diyakini kebenarannya, melindungi aktiva perusahaan, dan memastikan perusahaan mematuhi peraturan perundang-undangan yang berlaku. Untuk memastikan hal-hal tersebut di atas perusahaan secara terus menerus melakukan perbaikan-perbaikan di segala bidang, meningkatkan kualitas, dan menilai pelaksanaannya secara reguler. Hasil penilaian tersebut dilaporkan kepada

Direksi, dan tindak lanjut atas pemeriksaan tersebut dimonitor secara berkala. Dalam pelaksanaan pengendalian internal, internal audit melakukan evaluasi efektivitas dan kecukupan kontrol yang dijalankan oleh Perusahaan / anak-anak Perusahaan / Unit kerja, mengevaluasi efektivitas dan kecukupan manajemen risiko yang dijalankan Perusahaan, dan mengevaluasi efektivitas dan kecukupan penilaian Perusahaan atas Tata Kelola perusahaan dan kesinambungannya. Pemeriksaan ini dilaksanakan secara periodik dalam setahun.



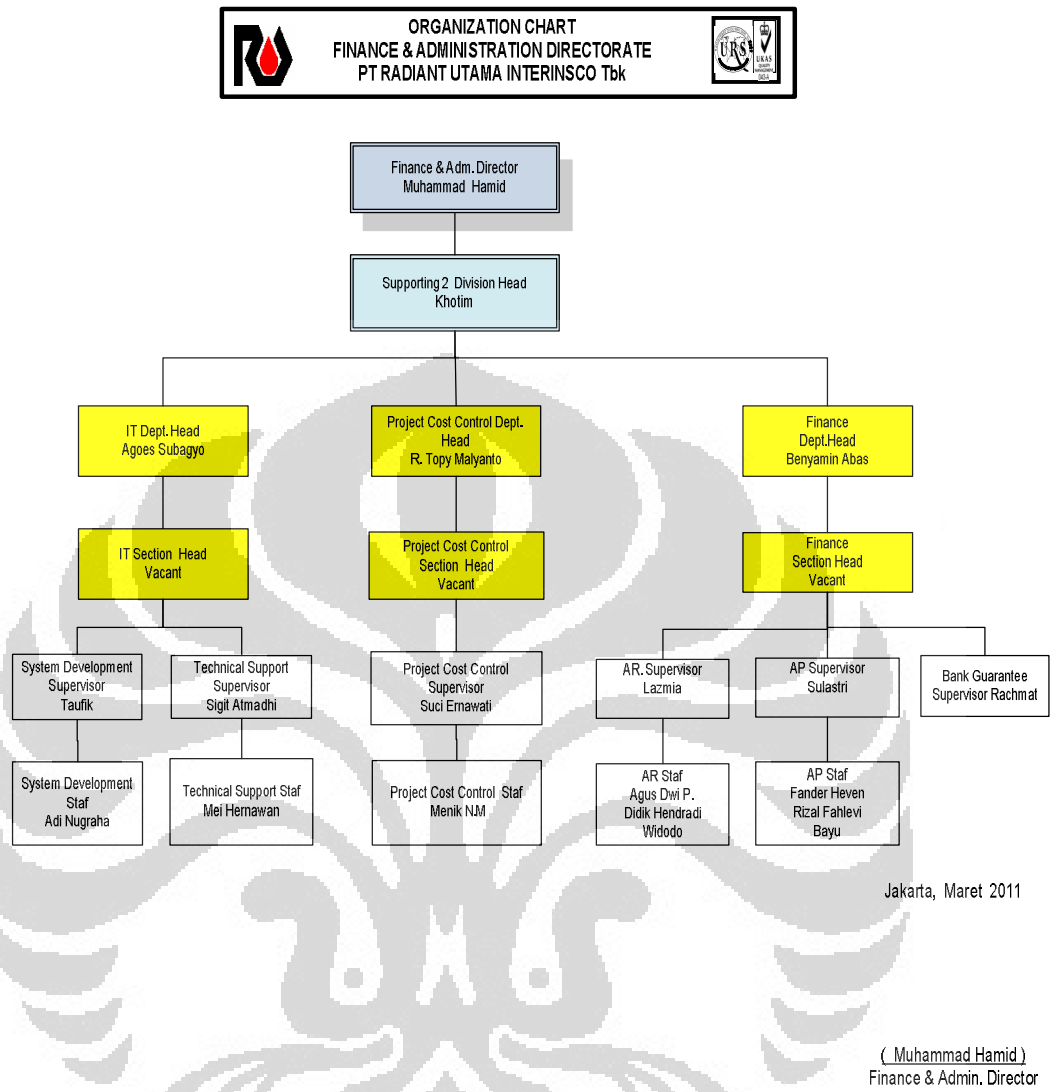
Gambar 3.2. Struktur Organisasi Perusahaan
Sumber: Company Profile PT Radiant Utama Interinsco (2010)

Dalam mengelola risiko, Direksi dibantu oleh Komite Audit untuk menyiapkan kebijakan manajemen risiko perusahaan, melaksanakan dan mengawasi penerapan manajemen risiko; memastikan bahwa risiko dari setiap proyek baik yang sedang maupun yang akan berjalan terkendali dengan baik; mengkaji proses manajemen risiko yang telah berjalan, memberikan laporan dan masukan kepada Dewan Komisaris.

3.4 Infrastruktur Teknologi Informasi Perusahaan

Infrastruktur teknologi informasi telah menjadi alat yang dapat mempengaruhi kemampuan perusahaan untuk mencapai keunggulan bersaing sehingga menjadikan penggunaan infrastruktur teknologi informasi sebagai kebutuhan strategi yang merupakan kunci yang memungkinkan implementasi dari sistem inovasi, mengurangi biaya, meningkatkan *bargaining power*, mendefinisikan kembali dan meningkatkan pelayanan dan memungkinkan perusahaan untuk menawarkan produk-produk baru. Selain itu, infrastruktur teknologi informasi dibutuhkan oleh perusahaan agar dapat mengalami perubahan-perubahan gradual untuk mendapatkan keuntungan dengan adanya teknologi baru dan efisiensi. Infrastruktur teknologi informasi juga dibutuhkan untuk mengadakan perubahan-perubahan proses bisnis guna memenuhi kebutuhan strategi saat ini dan untuk memenuhi kebutuhan konsumen.

Infrastruktur teknologi informasi merupakan pondasi dasar dari kapabilitas teknologi informasi. Kapabilitas teknologi informasi ini meliputi *internal technical* (*equipment*, *software* dan *cabling*) maupun *human expertise* yang dibutuhkan untuk memberikan pelayanan yang dapat dipercaya. Infrastruktur teknologi informasi pada PT. Radiant Utama Interinsco Tbk, sebagaimana pada umumnya di perusahaan lain. Divisi TI perusahaan dipimpin oleh seorang manajer TI dibawah Direktorat *Finance & Administration* yang terbagi atas dua sub bagian yaitu *System Development & Technical Support*. Yang dapat dilihat dalam gambar berikut ini.



Gambar 3.3. Struktur Organisasi Divisi TI
Sumber: Company Profile PT Radiant Utama Interinsco (2010)

Divisi TI perusahaan membangun dan mengembangkan program aplikasi RUI 204 dengan menggunakan DBMS Oracle. RUI 204 terdiri dari program aplikasi yang menunjang kegiatan operasional perusahaan diantaranya marketing, operasional cabang, keuangan, manajemen aset dan program penunjang lainnya yang terintegrasi namun untuk program aplikasi akuntansi dan HRD masih menggunakan program aplikasi yang tidak terintegrasi dengan program aplikasi yang dikembangkan perusahaan. Pengembangan program RUI 204 ini diharapkan dapat memenuhi kebutuhan kegiatan operasional perusahaan dengan mempertimbangkan efektivitas maupun efisiensi baik waktu maupun biaya. RUI 204 digunakan terpusat, dimana semua data tersimpan di *server* kantor pusat yang dapat diakses oleh kantor cabang dimanapun dalam bertransaksi

secara online. Dengan semakin berkembangnya PT. Radiant Utama Interinsco dan kebutuhan akan komunikasi data yang cepat antara kantor pusat dan kantor-kantor cabang, maka saat ini dirasakan perlunya pengembangan jaringan komputer. Pengembangan jaringan ini menjadikan jaringan komputer kantor-kantor cabang menjadi bagian dari jaringan komputer Radiant Utama Interinsco. Salah satu solusi untuk memudahkannya komunikasi data antara kantor cabang dengan kantor pusat di Jakarta adalah menggunakan *OpenVPN*.

Dengan penggunaan openvpn ini maka jaringan kantor cabang dapat terhubung ke jaringan kantor pusat sebagai bagian dari jaringan komputer lokal kantor pusat dalam satu segmen jaringan tersendiri, sehingga komunikasi data dan penggunaan aplikasi yang dibutuhkan untuk menunjang operasional perusahaan dapat dilakukan terpusat dan terintegrasi.

Kebutuhan komunikasi data antara kantor pusat dengan kantor-kantor cabang dan fasilitas kepada karyawan yang berlokasi di luar kantor agar dapat tetap tersambung ke jaringan di kantor dengan tetap terjaga kemanan jaringannya, RUIS menggunakan *Open Virtual Private Network* (VPN). Dengan *Open* VPN, koneksi bersifat *private* dan aman meskipun menggunakan jaringan internet. Keuntungan dengan menggunakan *service OpenVPN* ini adalah:

1. Akses global ke jaringan Radiant Utama Interinsco melalui internet.
2. Kemudahan mengakses *resources* yang berada di dalam jaringan Radiant Utama Interinsco yang tidak dapat diakses dari luar Radiant Utama Interinsco secara langsung.
3. Keamanan dalam transfer data karena adanya enkripsi data.
4. Keamanan jaringan sebab hanya user yang telah melewati proses autentikasi dan autorisasi saja yang dapat menggunakan *service VPN*.

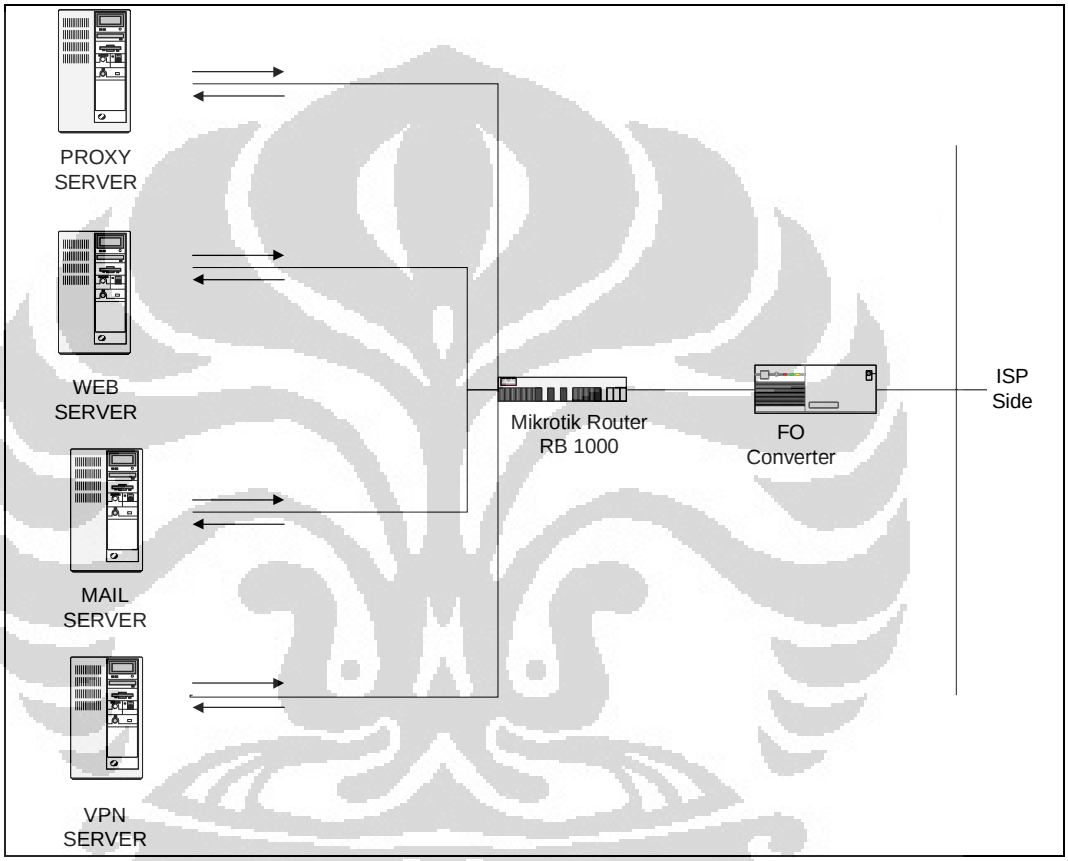
Hal-hal yang harus diperhatian dalam menggunakan *Open VPN*:

1. Perhatian yang serius pada keamanan jaringan publik (*internet*), dalam hal ini yang harus diperhatikan adalah konfigurasi *firewall* pada server
2. Sangat tergantung pada faktor-faktor terjadi di internet yang terkadang berada di luar kendali pihak perusahaan.

Ada dua sisi yang harus dipersiapkan untuk membuat koenksi menggunakan *OpenVPN* ini, yaitu di kantor pusat sebagai server untuk seluruh jaringan yang masuk dan sisi client baik itu di kantor cabang maupun client lainnya yang berada diluar kantor yang akan

terhubung ke kantor pusat *(user mobile)*. Perangkat penunjang dalam komunikasi data di RUIS diantaranya adalah:

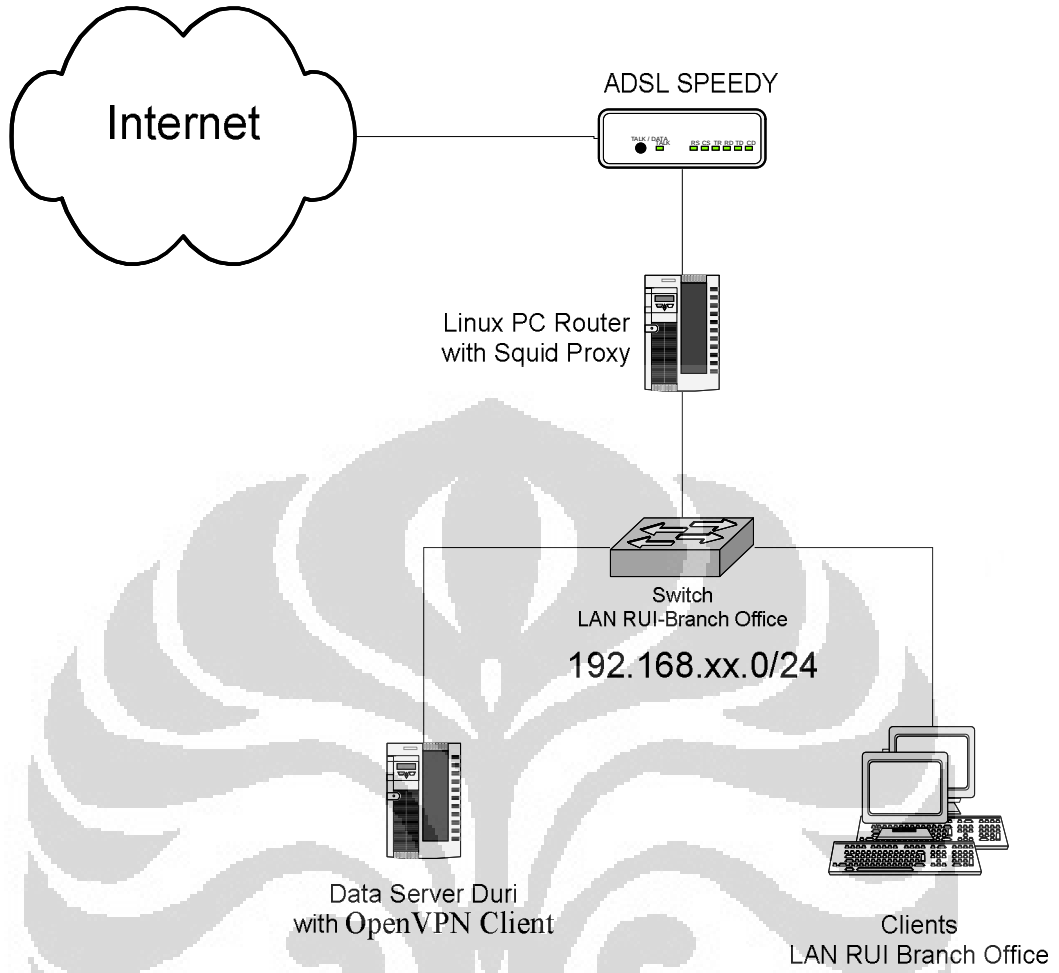
1. **Koneksi internet,** koneksi internet yang digunakan di kantor pusat Radiant Utama Interinsco adalah koneksi fiber optic sebesar 1 MB, dan bandwidth yang digunakan untuk koneksi *OpenVPN* ini sebesar 512 kbps.



Gambar 3.4 Skema koneksi Internet Head Office

Sumber: PT Radiant Utama Interinsco (2010)

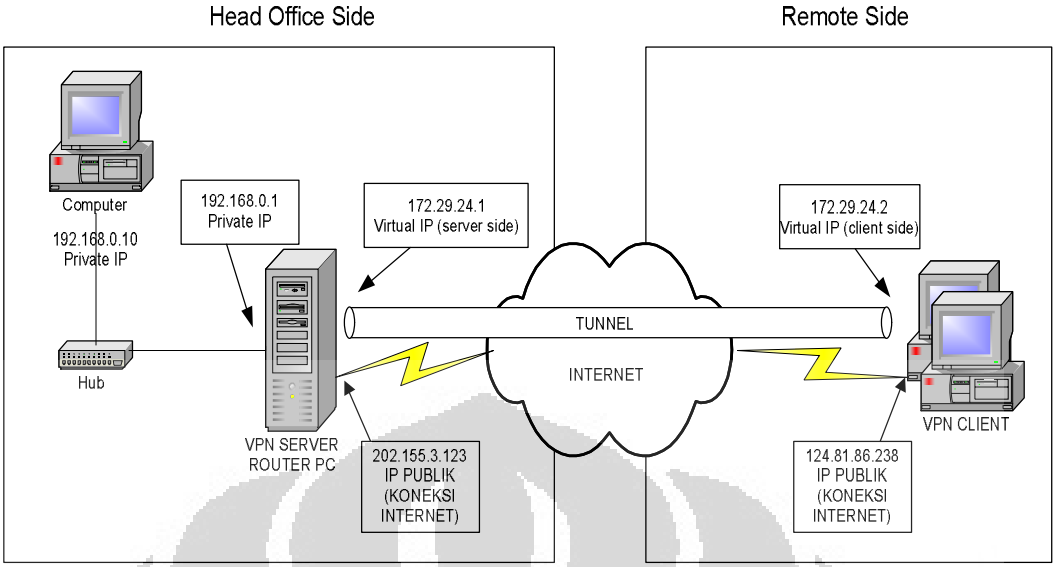
Untuk koneksi internet yang digunakan di kantor cabang, yang berada di kota Balikpapan, Bontang, Batam, Palembang, Cilegon, Cirebon, Duri dan Surabaya menggunakan koneksi Speedy ADSL unlimited dari telkom.



Gambar 3.5 Skema jaringan di kantor cabang

Sumber: PT Radiant Utama Interinsco (2010)

2. **Server,** adalah sebuah aplikasi VPN server side yang terinstall di server dengan system operasi linux yang berbasis router dan firewall. Fungsi router pada server ini adalah mengendalikan lalu lintas jaringan antara jaringan internet dengan ip publik, jaringan VPN dan jaringan lokal. Sedangkan firewall adalah metode untuk memproteksi antara satu jaringan dengan jaringan yang lain.



Gambar 3.6 Skema OpenVPN PT. Radiant Utama Interinsco

Sumber: PT Radiant Utama Interinsco (2010)

Dalam perencanaan penanggulan risiko atas terjadinya bencana yang dapat mengancam kelangsungan hidup perusahaan, RUIS telah membangun sebuah pusat penyimpanan data perusahaan yang terpisah dari gedung tempat perusahaan beroperasi yang lebih dikenal dengan istilah *Disaster Recovery Center*. Hal ini menggambarkan fleksibilitas teknologi informasi perusahaan. Fleksibilitas memberikan organisasi kemampuan untuk mengontrol lingkungan di luar organisasi secara efektif yang merupakan sumber potensial untuk mencapai posisi persaingan yang baik. Disamping itu, fleksibilitas infrastruktur ini menentukan kemampuan dari perusahaan untuk cepat dan peka menanggapi perubahan-perubahan dari luar, dimana hal ini penting bagi inovasi.

BAB IV

ANALISIS DAN PEMBAHASAN HASIL PENELITIAN

Bab ini berisi tentang analisis dan pembahasan yang dilakukan oleh penulis terhadap hasil audit sistem informasi dengan menggunakan kerangka kerja *Risk IT*.

4.1 Audit Sistem Informasi Menggunakan Kerangka Kerja Risk IT

Berikut adalah hasil pengukuran penerapan tata kelola Teknologi informasi di RUIS dengan menggunakan kerangka kerja *Risk IT*. Pengukuran tersebut berdasarkan analisis hasil wawancara yang telah dilakukan penulis dan dilengkapi dengan data-data pendukung lainnya. Wawancara dilakukan kepada beberapa pihak yang dipandang terkait dengan proses dan kegiatan operasional teknologi informasi yaitu:

1. MIS/IT Manager
2. Internal Audit Manager
3. Internal Audit Supervisor (System Analyst)
4. Risk Management Manager

Analisis dilakukan dengan cara menarik kesimpulan mengenai praktik yang terkait pengelolaan risiko TI di RUIS dengan membuat RACI *chart*. Implementasi RACI *chart* di RUIS yang disusun berdasarkan data struktur organisasi dan dilengkapi dengan hasil wawancara yang dilakukan kepada pihak-pihak terkait. Selanjutnya analisis untuk masing-masing tahapan proses yang terdapat dalam ketiga elemen kerangka kerja *Risk IT* yaitu: *Risk Governance, Risk Evaluate, Risk Response.* Dengan cara melihat praktik tujuan aktivitas dan tujuan proses ada di RUIS serta melakukan penentuan tingkat kematangan melalui metrik aktivitas dan metrik proses berdasarkan fakta yang terjadi di RUIS.

4.2. Pemaparan Hasil Penelitian

4.2.1. RACI *Chart*

Seperti yang telah dijelaskan dalam Bab 2 Tinjauan Pustaka, RACI *Chart* adalah tabel yang memperlihatkan bagaimana pembagian peran dan tanggung jawab atas pengelolaan risiko TI di dalam perusahaan, yaitu dengan melihat siapa (*who*) yang bertugas (*role*) atau memiliki tanggug jawab (*responsibility*) atau apa (*what*) yang dilaksanakan dalam setiap prosesnya. Dalam hal ini, RACI chart RUIS dipisahkan menjadi bagian Direksi, Dept *Risk Management*, Dept TI, Dept Internal Audit, SDM, *Finance & Accounting* dan *Operational*. Direksi adalah perwujudan dari fungsi jajaran dewan direksi yang ada di RUIS, Risk Management adalah perwujudan fungsi dari Dept *Risk Management* RUIS, TI adalah perwujudan dari fungsi departemen TI RUIS, Internal Audit adalah perwujudan dari fungsi departemen Internal Audit RUIS, SDM adalah perwujudan dari fungsi departemen SDM RUIS, *Finance & Accounting* adalah perwujudan dari fungsi departemen *Finance & Accounting* dan O*perational* adalah perwujudan dari fungsi operasional perusahaan.

Gambar 4.1 adalah salah satu contoh gambar RACI *chart* yang tertera didalam kerangka kerja *Risk IT* yang dikeluarkan oleh ITGI, yaitu RACI *chart* bagian *Risk Governance* (RG) untuk proses RG 1 Membangun dan memelihara risiko secara umum, pada bagian ini terdapat delapan aktivitas yang terkait, yaitu: Mengembangkan kerangka manajemen risiko TI perusahaan secara spesifik; Mengembangkan metode manajemen risiko TI; Lakukan penilaian risiko TI perusahaan secara keseluruhan; Mengusulkan ambang batas toleransi risiko TI; Menyetujui toleransi risiko TI; Selaraskan pernyataan kebijakan dan standar dengan toleransi risiko TI; Mempromosikan budaya sadar risiko TI; Mempromosikan komunikasi yang efektif dari risiko IT.

RACI Chart

Key Activities \ Roles	Board	CEO	CRO	CIO	CFO	Enterprise Risk Committee	Business Management	Business Process Owner	Risk Control Functions	HR	Compliance and Audit
RG1.1 Develop an enterprise-specific IT risk management framework.	A	R	R	R	C	I	R	I	C	I	C
RG1.2 Develop IT risk management methods.	C	C	A	R	C	I	C	C	C	I	C
RG1.3 Perform an enterprise-wide IT risk assessment.	I	A	R	R	C	I	R	C	R	C	C
RG1.4 Propose IT risk tolerance thresholds.	I	I	C	R	C	I	A	C	C		C
RG1.5 Approve IT risk tolerance.	A	C	C	C	C	R	C	C	C	C	C
RG1.6 Align policy and standards statements with IT risk tolerance.		I	A	R	I	C	R	I	C	R	I
RG1.7 Promote an IT risk-aware culture.	A	R	R	R	R	R	R	R	R	R	R
RG1.8 Promote effective communication of IT risk.	A	R	R	I	I	R	I	I	I	I	C

A RACI chart identifies who is Responsible, Accountable, Consulted and/or Informed.

Gambar 4.1 RACI chart RG 1

Sumber: ITGI (2008)

Tabel 4.1 adalah tabel yang menjelaskan mengenai salah satu contoh implementasi RACI *chart* di RUIS, yaitu bagian RG 1 Membangun dan Memelihara Risiko secara Umum yang ada pada kerangka kerja Risk IT. RACI *chart* ini disusun berdasarkan data struktur organisasi yang salah satu contohnya adalah seperti tertera pada gambar 4.1 dengan dilengkapi oleh hasil wawancara yang dilakukan kepada pihak-pihak terkait.

RACI *chart* dari proses lainnya yang ada di dalam kerangka kerja *Risk IT*, baik proses yang terdapat di dalam bagian *Risk Governance* (RG) yaitu RG2 dan RG3, ataupun bagian *Risk Evaluate* (RE) yaitu: RE1, RE2 dan RE3 dan bagian *Risk Response* (RR) yaitu: RR1, RR2 dan RR3 dapat dilihat dalam lampiran 1, sementara implementasi RACI *chart* di RUIS untuk semua proses yang ada pada bagian RG, RE maupun RR dalam kerangka kerja *Risk IT* dapat dilihat di dalam lampiran 2.

Tabel 4.1 RACI Chart RG 1 di RUIS

Role								
Key Activities		Board	Risk Manajemen	Dept TI	Internal Audit	SDM	Acctg & Finance	Operasional
Risk Governance								
RG1 Establish and Maintain a Common Risk View Risk Governance								
RG1.1	Develop an enterprise-specific IT risk management framework. Mengembangkan kerangka manajemen risiko IT perusahaan secara spesifik.	A	C	R	I			
RG1.2	Develop IT risk management methods. Mengembangkan metode manajemen risiko TI.	C	C	R	C			
RG1.3	Perform an enterprise-wide IT risk assessment. Lakukan penilaian risiko TI perusahaan secara luas.	I	C	R	R			
RG1.4	Propose IT risk tolerance thresholds. Mengusulkan ambang batas toleransi risiko TI.	I	C	R	C			
RG1.5	Approve IT risk tolerance. Menyetujui toleransi risiko TI.	A	C	C	I			
RG1.6	Align policy and standards statements with IT risk tolerance. Sesuaikan pernyataan kebijakan dan standar dengan toleransi risiko TI.		R	R	C			
RG1.7	Promote an IT risk-aware culture. Mempromosikan budaya sadar risiko TI	A	R	R	I			
RG1.8	Promote effective communication of IT risk. Mempromosikan komunikasi yang efektif dari risiko IT.	A	R	R	I			

4.2.2 Tujuan dan Metrik Kerangka Kerja Risk IT

Selain RACI *chart*, kerangka kerja Risk IT, juga memberikan panduan tujuan dan metrik sebagai alat bantu dalam menganalisis tingkat penerapan tata kelola TI didalam sebuah perusahaan. Tujuan dan metrik tersebut dikembangkan menjadi dasar pengukuran tingkat kematangan tata kelola TI suatu perusahaan.

Gambar 4.2 menggambarkan salah satu gambar tujuan dan metrik yang ada di dalam kerangka kerja *Risk IT*, yaitu untuk bagian RG 1 Membangun dan memelihara risiko secara umum.

Tujuan dan metrik kerangka kerja risk IT dari proses lainnya yang ada di dalam kerangka kerja risk IT baik proses yang terdapat di dalam bagian RG, RE, ataupun RR dapat dilihat di dalam lampiran 3, sementara implementasi pengukuran dengan *detail maturity model* untuk semua proses yang ada pada bagian RG, RE maupun RR dalam kerangka kerja Risk IT yang terjadi di RUIS dapat dilihat di dalam tabel 4.2, tabel 4.3 dan tabel 4.4.

Goals and Metrics

Activity Goals	Process Goal	RG Goal
• Develop an enterprise-specific IT risk management framework. • Develop IT risk management methods. • Perform an enterprise-wide IT risk assessment. • Propose IT risk tolerance thresholds. • Approve IT risk tolerance. • Align policy and standards statements with IT risk tolerance. • Promote an IT risk-aware culture. • Promote effective communication of IT risk.	• Ensure that risk management activities align with the enterprise's objective capacity for IT-related loss and leadership's subjective tolerance of it.	• Ensure that IT risk management practices are embedded in the enterprise, enabling the enterprise to secure optimal risk-adjusted return.
Activity Metrics	**Process Metrics**	**RG Metrics**
• Existence of a defined and documented IT risk management framework • Degree of completeness of the IT risk management framework • Percentage of the IT risk management framework covered by defined methods • Percentage of IT risk management structures and activities set up vs. planned • Frequency of enterprise-wide IT risk assessments • Level of executive participation in enterprise-wide IT risk assessments (e.g., attend in person, send a subordinate, receive report) • Number of out-of-cycle enterprise-wide IT risk assessments • Number of aligned policies to which intended audience has signed adherence • Extent to which risk management communications and training are targeted to specific roles and responsibilities	• Number of known executive-level risk tolerance violations not subjected to disciplinary action (enforcement of policy) • Number of IT-related events with business impact in which a failure to escalate was a factor in event occurrence and/or the loss magnitude (e.g., the risk manager did not know or there was an impaired cultural ability to escalate) • Number of policies in force with one or more statements contradicting a related risk tolerance (alignment of IT policies with tolerance) • Number of IT risk issues that exceed risk tolerance	• The degree to which the strategic use of IT in leveraging enterprise resources reduces overall enterprise risk • Percentage of staff trained in critical risk management techniques (e.g., standard risk analysis techniques, crisis management, project management, skills of people [audit, etc.] to detect when something IT-related is amiss)

Gambar 4.2 Tujuan dan Metrik RG 1

Sumber: ITGI (2008)

Tabel 4.2 Pengukuran *Risk Governance (RG) Detailed Maturity Model*

	Key Activities	Awareness and Communication	Responsibility and Accountability	Goal Setting and Measurement	Policies, Standards and Procedures	Skills and Expertise	Tools and Automation	Tingkat Kematangan
Risk Governance								**2,15**
RG1 Establish and Maintain a Common Risk View Risk Governance								
RG1.1	Develop an enterprise-specific IT risk management framework. Mengembangkan kerangka manajemen risiko IT perusahaan secara spesifik.	■						2
RG1.2	Develop IT risk management methods. Mengembangkan metode manajemen risiko TI.	■						2
RG1.3	Perform an enterprise-wide IT risk assessment. Lakukan penilaian risiko TI perusahaan secara luas.				■			2
RG1.4	Propose IT risk tolerance thresholds. Mengusulkan ambang batas toleransi risiko TI.				■			2
RG1.5	Approve IT risk tolerance. Menyetujui toleransi risiko TI.				■			3
RG1.6	Align policy and standards statements with IT risk tolerance. Sesuaikan pernyataan kebijakan dan standar dengan toleransi risiko TI.				■			2
RG1.7	Promote an IT risk-aware culture Mempromosikan budaya sadar risiko TI	■						3
RG1.8	Promote effective communication of IT risk. Mempromosikan komunikasi yang efektif dari risiko IT.	■						2
	Total Rata-rata Tingkat Kematangan RG1							**2,25**
RG2 Integrate with ERM								
RG2.1	Establish enterprise-wide accountability for managing IT risk. Membangun akuntabilitas perusahaan secara luas untuk mengelola risiko TI.		■					3
RG2.2	Establish accountability for IT risk issues. Membangun akuntabilitas untuk isu-isu risiko TI.		■					3
RG2.3	Co-ordinate IT risk strategy and business risk strategy. Mengkoordinasikan startegi risiko IT dan strategi risiko bisnis.					■		2
RG2.4	Adapt IT risk management practices to organisational risk management practices. Adaptasikan praktik manajemen risiko IT untuk praktek manajemen risiko organisasi.					■		2
RG2.5	Provide adequate resources for IT risk management. Menyediakan sumber daya yang memadai untuk manajemen risiko TI.					■		1
	Total Rata-rata Tingkat Kematangan RG2							**2,20**
RG3 Make Risk-aware Business Decisions								
RG3.1	Gain management buy-in for the IT risk analysis approach.						■	1
RG3.2	Approve IT risk analysis results. Menyetujui hasil analisis risiko TI.						■	3
RG3.3	Embed IT risk considerations into strategic business decision making. Melekatkan pertimbangan risiko IT ke dalam pengambilan keputusan bisnis strategis.			■				3
RG3.4	Accept IT risk. Terima risiko TI.			■				2
RG3.5	Prioritise IT risk response activities. Prioritaskan respon kegiatan risiko IT .			■				2
RG3.6	Track key IT risk decisions Melacak keputusan utama risiko TI						■	1
	Total Rata-rata Tingkat Kematangan RG3							**2,00**

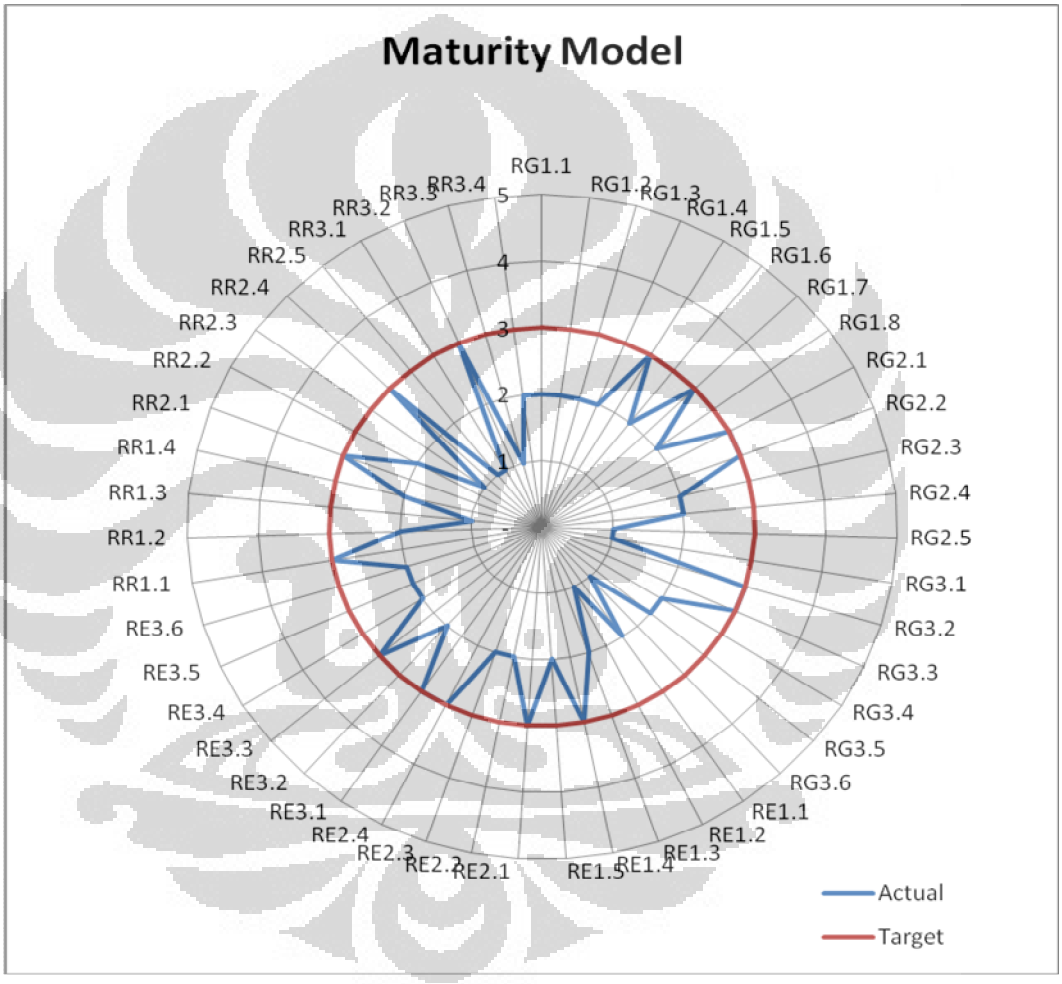
Tabel 4.3 Pengukuran *Risk Evaluate (RE) Detailed Maturity Model*

Key Activities		Awareness and Communication	Responsibility and Accountability	Goal Setting and Measurement	Policies, Standards and Procedures	Skills and Expertise	Tools and Automation	Tingkat Kematangan
Risk Evaluation								**2,28**
RE1 Collect Data								
RE1.1	Establish and maintain a model for data collection. Membangun dan memelihara sebuah model untuk pengumpulan data.							2
RE1.2	Collect data on the external environment. Mengumpulkan data pada lingkungan eksternal.							1
RE1.3	Collect timely event, incident, problem and loss data. Kumpulkan data yang tepat waktu atas peristiwa, insiden, masalah dan kerugian.							2
RE1.4	Identify risk factors. Mengidentifikasi faktor risiko.							3
RE1.5	Organise historical IT risk data. Mengorganisir data historis risiko TI.							2
	Total Rata-rata Tingkat Kematangan RE1							**2,00**
RE2 Analyse Risk								
RE2.1	Define IT risk analysis scope. Tentukan lingkup analisis risiko TI.							3
RE2.2	Estimate IT risk to and from critical products, services, processes and IT resources. Perkiraan risiko TI ke dan dari produk , jasa, proses dan sumber daya TI yang kritis.							2
RE2.3	Identify risk response options. Identifikasi opsi respon risiko.							2
RE2.4	Perform a peer review of IT risk analysis results. Melakukan peer review hasil analisis risiko TI.							3
	Total Rata-rata Tingkat Kematangan RE2							**2,50**
RE3 Maintain Risk Profile								
RE3.1	Map IT resources to business processes. Memetakan sumber daya TI untuk proses bisnis.							3
RE3.2	Determine the business criticality of IT resources. Tentukan kekritisan bisnis atas sumber daya TI.							2
RE3.3	Understand IT capabilities. Memahami kemampuan IT.							3
RE3.4	Connect threat types and business impact categories. Hubungkan jenis ancaman dengan kategori dampak bisnis.							2
RE3.5	Maintain the IT risk register and IT risk map. Menjaga daftar risiko TI dan peta risiko TI.							2
RE3.6	Design and communicate IT risk indicators. Desain dan mengkomunikasikan indikator risiko TI.							2
	Total Rata-rata Tingkat Kematangan RE3							**2,33**

Tabel 4.4 Pengukuran *Risk Response (RR) Detailed Maturity Model*

Key Activities		Awareness and Communication	Responsibility and Accountability	Goal Setting and Measurement	Policies, Standards and Procedures	Skills and Expertise	Tools and Automation	Tingkat Kematangan
Risk Response								**1,92**
RR1 Articulate Risk								
RR1.1	Report IT risk analysis results. Laporan hasil analisis risiko TI.							3
RR1.2	Report IT risk management activities and state of compliance. Laporan kegiatan manajemen risiko TI dan laporan kepatuhan.							2
RR1.3	Interpret external IT assessment findings. Menafsirkan temuan penilaian eksternal TI.							1
RR1.4	Identify IT-related opportunities. Mengidentifikasi peluang yang berkaitan dengan TI.							2
	Total Rata-rata Tingkat Kematangan RR1							**2,00**
RR2 Manage IT Risk								
RR2.1	Inventory controls, capabilities and resources. Inventarisasi kontrol, kemampuan dan sumber daya.							3
RR2.2	Monitor operational alignment with risk tolerance thresholds. Memantau keselarasan operasional dengan batas toleransi risiko.							2
RR2.3	Respond to discovered risk exposure and opportunity Menanggapi eksposur dan peluang risiko yang ditemukan							1
RR2.4	Implement controls. Melaksanakan kontrol.							3
RR2.5	Report on IT risk action plan progress. Laporan atas progress perencanaan tindakan risiko TI.							1
	Total Rata-rata Tingkat Kematangan RR2							**2,00**
RR3 React to Events								
RR3.1	Maintain incident response plans. Menjaga rencana atas respon insiden.							1
RR3.2	Monitor IT risk. Memantau risiko TI.							3
RR3.3	Initiate incident response plans. Memulai rencana respon insiden.							1
RR3.4	Conduct post-mortem reviews of IT-related incidents. Melakukan post-mortem review dari insiden terkait TI.							2
	Total Rata-rata Tingkat Kematangan RR3							**1,75**

Skor hasil pengukuran ini diperoleh dari rata-rata tingkat kematangan untuk setiap domain. Skor tersebut merupakan hasil analisis penulis berdasarkan hasil wawancara dengan responden kemudian *plotting* ke kerangka kerja *Risk IT* (lampiran 4) dan mengidentifikasikan berada pada tingkat kematangan yang manakah setiap proses dan aktivitas yang ada di perusahaan saat ini berdasarkan pengukuran dengan *Maturity Model*. Hasil pengukuran tersebut dapat digambarkan dalam diagram berikut:

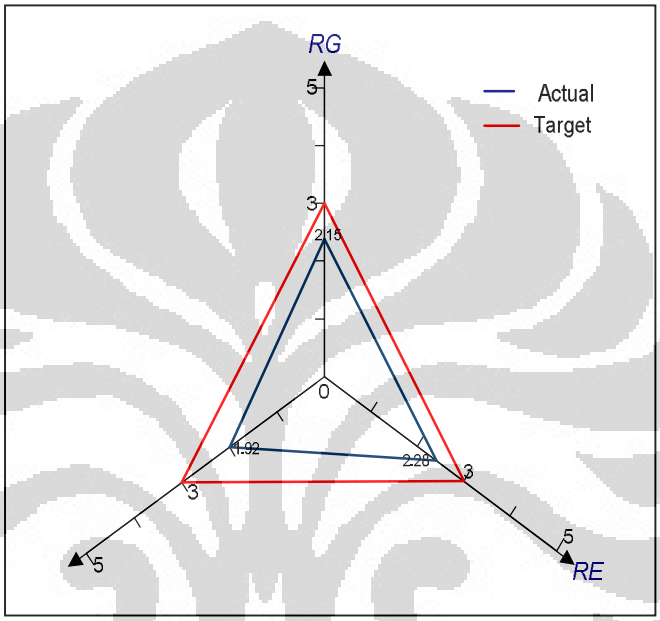


Gambar 4.3 Diagram Maturity Model

4.3 Hasil pengukuran tingkat kematangan dengan menggunakan kerangka kerja Risk IT pada RUIS

Hasil pengukuran tingkat kematangan dengan menggunakan kerangka kerja risk IT pada RUIS adalah seperti ditunjukan dalam tabel diatas, dapat dilihat bahwa pada bagian *Risk Governance* (tabel 4.2), RUIS memperoleh skor tingkat

kematangan sebesar 2,15. Sementara pada bagian *Risk Evaluate* (tabel 4.3), tingkat kematangan 2,28, dan pada bagian *Risk Response* (tabel 4.4), tingkat kematangan RUIS adalah sebesar 1,92, sehingga hasil total pengukuran tingkat kematangan menggunakan kerangka kerja *risk IT* pada RUIS adalah sebesar 2,09 yang menunjukan bahwa tingkat kematangan RUIS saat ini berada pada level 2. Tingkat kematangan untuk masing-masing domain dapat digambarkan dalam diagram triangle seperti pada gambar 4.4 dibawah ini.



Gambar 4.4 Diagram Triangle

Dengan demikian, RUIS saat ini berada pada tahap *repeatable* dan menuju tahap *defined process*. Pada tahap ini perusahaan dinyatakan sudah mulai menerapkan manajemen risiko TI, namun belum optimal. Proses manajemen risiko TI diperusahaan sudah ada namun belum mengikuti standar baku, dan mulai mencapai tahap ketika semua proses yang dijalankan perusahaan sudah terdokumentasi dan dikomunikasikan dengan baik. Namun, pada tahap ini praktik manajemen yang ada di dalam perusahaan belum dapat menghitung dan mengoptimalkan fungsi manajemen risiko TI terhadap bisnis yang diperkirakan dapat menciptakan nilai tambah bagi pengelolaan TI dan proses bisnis perusahaan dimasa yang akan datang.

Jika dirinci lebih lanjut, hasil penerapan tingkat kematangan untuk masing-masing komponen yang ada dalam kerangka kerja *Risk IT* di RUIS adalah sbb:

1. Risk Governance (RG)

Pada bagian ini, RUIS memperoleh skor tingkat kematangan sebesar 2,15. Skor ini diperoleh dari rata-rata tingkat kematangan RG1 sebesar 2,25, RG2 sebesar 2,20 dan RG3 sebesar 2,00. Skor ini menunjukkan bahwa untuk bagian RG, tata kelola TI RUIS juga berada pada posisi *Repeatable* dengan kondisi sebagai berikut (ITGI 2008):

a. Adanya kesadaran akan kebutuhan untuk secara aktif mengelola risiko TI, namun fokusnya adalah pada kepatuhan teknis dengan tidak ada antisipasi nilai tambah.
b. Adanya pemimpin untuk manajemen risiko TI yang memikul tanggung jawab dan biasanya bertanggung jawab, walaupun hal ini tidak secara resmi disepakati.
c. Toleransi risiko diatur secara lokal.
d. Investasi difokuskan pada isu-isu risiko spesifik pada fungsional dan bisnis (misalnya, keamanan, kelangsungan bisnis, operasi).
e. Dewan menerbitkan panduan untuk manajemen risiko.
f. Adanya persyaratan keterampilan minimum yang mencakup kesadaran risiko TI yang diidentifikasi untuk daerah risiko perusahaan yang kritis.
g. Adanya fungsional dan bagian yang spesifik yang melakukan inventarisir isu-isu risiko.

Kondisi yang ada di RUIS terkait dengan praktik pengelolaan Risiko TI dengan menggunakan kerangka kerja *Risk IT* untuk bagian RG antara lain adalah sudah adanya konsep manajemen risiko TI dan telah memulai untuk mengembangkan prosedur terkait pengelolaan risiko TI. Pada bagian RG1 dapat diketahui, kerangka manajemen risiko TI di RUIS sudah ada namun belum terdokumentasi. Penilaian risiko telah dilakukan namun masih terbatas pada pembenahan kontrol sistem. Batasan toleransi atas risiko TI sudah ada namun belum didefinisikan secara jelas, sehingga sulit untuk di implementasikan dan dikomunikasikan. Manajemen berusaha menyelaraskan kebijakan yang ada saat ini namun karena budaya kerja yang sudah tercipta selama ini menjadi hambatan dalam proses menjalankan pengelolaan risiko TI perusahaan. Adanya kesadaran pentingnya pengelolaan risiko TI, namun hal ini terhambat karena kurangnya

SDM manajemen risiko. Manajemen risiko TI belum didefinisikan secara spesifik, saat ini pengelolaan risiko TI masih terbatas pada area tertentu pada proses bisnis perusahaan.

Pada bagian RG2, RUIS memperoleh skor tingkat kematangan sebesar 2,20. Dengan kondisi sebagai berikut, RUIS telah menugaskan analis sistem sebagai penanggung jawab dalam proses pembenahan kontrol atas sistem perusahaan. Dalam praktiknya, penerapan manajemen risiko TI belum dilakukan secara maksimal, karena belum terdefinisi secara spesifik dan tidak ada prosedur yang baku dalam penerapan manajemen risiko TI di perusahaan. Manajemen risiko TI masih terfokus pada masalah teknis. SDM dalam manajemen risiko TI masih belum memadai. Pemetaan tanggung jawab atas kontrol dan pengelolaan risiko TI sudah dilakukan untuk mengantisipasi tumpang tindih dalam menjalankan fungsi kontrol. Pelatihan manajemen risiko TI belum dilakukan. Belum ada pengukuran secara kuantitatif atas pengeluaran operasional manajemen. Rapat yang membahas masalah TI sering dilakukan. Belum ada keselarasan antara tujuan organisasi dan Risiko TI.

Pada bagian RG3, RUIS memperoleh skor kematangan sebesar 2,00. Batasan toleransi risiko TI belum didefinisikan dan dikomunikasikan ke tingkat pelaksana. Belum ada prosedur pengukuran baku atas pengelolaan risiko TI. Setiap risiko yang terjadi didokumentasikan namun tindak lanjutnya belum dilakukan karena keterbatasan SDM. Hasil analisis atas pengelolaan risiko TI dijadikan dasar oleh manajemen dalam pengambilan keputusan manajemen dan dapat memudahkan identifikasi dan tindakan yang akan dilakukan ketika terjadi risiko TI.

Dari kondisi diatas dapat disimpulkan bahwa dalam praktiknya perusahaan telah menyadari adanya risiko terkait TI di perusahaan, oleh karena itu manajemen melakukan analisis atas sistem yang ada secara bertahap melakukan pembenahan atas kontrol-kontrol yang dinilai lemah. Manajemen telah memiliki konsep pengelolaan risiko TI namun belum didokumentasikan secara baku sehingga sulit untuk mengkomunikasikan ke seluruh pemangku kepentingan atas TI. Identifikasi risiko masih terbatas pada isu-isu spesifik saja dan menanggapinya secara parsial saja (tidak menyeluruh), hal ini disebabkan karena tidak adanya batasan toleransi yang didefinisikan dengan jelas dan tertulis. RUIS melakukan

investasi dalam menanggulangi risiko yang terjadi, namun masih penanggulangan dari segi teknis saja misalnya pembelian *hardware* (*server backup*) sebagai antisipasi terjadinya bencana. Sedangkan dari sisi proses bisnisnya masih banyak potensi-potensi kerugian karena tidak dikelolanya risiko secara cermat dan komprehensif. Masih lemahnya pengelolaan risiko TI di RUIS karena masih terbatasnya SDM yang memiliki keahlian dalam manajemen risiko TI.

Untuk mencapai tahap *Defined,* RUIS sebaiknya:

1. Mendefinisikan manajemen risiko TI secara jelas dan mendokumentasikannya sehingga mudah dikomunikasikan keseluruh tingkat pelaksana dan menjadi acuan dalam pengelolaan risiko TI di perusahaan. Hal ini dapat dilakukan dengan cara merumuskan setiap risiko yang teridentifikasi dan mendokumentasikannya yaitu dengan menjadikan kebijakan manajemen sehingga memiliki kekuatan dalam penerapannya di perusahaan

2. Menumbuhkan kesadaran atas risiko yaitu dengan memberikan pelatihan terkait manajemen risiko TI termasuk situasi dan skenario di luar kebijakan yang spesifik dan terstruktur

3. Mengembangkan bahasa risiko yang umum yang memudahkan dalam mengkomunikasikan risiko. Hal ini dapat dilakukan dengan membuat definisi-definisi risiko yang ada dalam setiap proses dan aktivitas yang ada di perusahaan sesuai dengan bahasa yang mudah dimengerti dan bersifat umum.

4. Mengembangkan *tools* alur kerja yang digunakan untuk meningkatkan keputusan melacak isu-isu risiko yaitu dengan melakukan observasi atas aktivitas terkait risiko TI yang kemudian disusun alur proses kerja yang sesuai kerangka manajemen risiko TI sehingga dapat meminimalisir risiko TI yang terjadi.

2. Risk Evaluate (RE)

Pada bagian ini, RUIS memperoleh skor tingkat kematangan sebesar 2,28. Skor ini diperoleh dari rata-rata tingkat kematangan metrik aktivitas dan metrik

proses RE1 sebesar 2,00, RE2 sebesar 2,50, dan RE3 sebesar 2,33. Skor ini juga menunjukkan bahwa bagian RE, tata kelola TI RUIS juga berada pada posisi *Repeatable* dengan kondisi sebagai berikut (ITGI 2008) :

a. Adanya diskusi mengenai skenario kerugian terburuk, meskipun faktor pendorong untuk skenario tidak dapat dipahami.
b. Individu bertanggung jawab untuk kedua evaluasi risiko dan respon risiko. Beberapa analisis risiko direncanakan terjadi, tetapi praktisi membuat asumsi tentang faktor risiko yang berkontribusi.
c. Ketergantungan dan analisis skenario hanya terfokus terbatas pada sejumlah kegiatan usaha.
d. Persyaratan keterampilan minimum diidentifikasi untuk daerah-daerah kritis data pengumpulan, analisis risiko dan profil risiko.
e. Fungsional dan pendekatan analisis risiko TI secara spesifik dan adanya *tools* tetapi didasarkan pada solusi yang dikembangkan oleh individu tertentu

Pada bagian RE1, terdapat kondisi-kondisi yaitu belum ada standar pengumpulan data yang baku dan sesuai dengan konsep manajemen risiko TI, pengumpulan data bersumber pada data internal saja, tidak ada data dari pihak eksternal yang digunakan sebagai bahan pembanding analisis. Pengumpulan data dilakukan dengan observasi, wawancara dan review laporan hasil audit internal Perusahaan sudah melakukan identifikasi terhadap faktor risiko yang ada dan menjadikan prioritas dalam pembenahan sistem yang telah didokumentasikan oleh Departemen TI perusahaan dengan lengkap.

Pada bagian RE2, praktik yang dilakukan yaitu dalam analisis risiko TI, manajemen telah mengidentifikasi dan menentukan lingkup analisis yang masih fokus pada isu-isu teknis dan risiko yang paling kritis dan baru terbatas pada proses bisnis yang berisiko menimbulkan kerugian finansial tanpa adanya standar yang baku. Adanya keterbatasan SDM dan kurangnya pelatihan manajemen risiko TI mempengaruhi hasil analisis atas risiko TI yang ada di perusahaan. Manajemen sudah memperkirakan risiko yang terjadi berdasarkan data historis dan hasil analisis namun belum terdokumentasi dengan jelas dan konsisten. RUIS sudah melakukan identifikasi atas kemungkinan risiko yang terjadi namun

perencanaan penanggulangannya masih dalam lingkup teknis. Setiap hasil analisis direview keakuratannya sebelum dibahas dan dipresentasikan dalam rapat manajemen.

Pada bagian RE3, praktik yang dilakukan RUIS yaitu sudah ada pemetaan sumber daya TI terhadap proses bisnis perusahaan, karena RUIS memandang TI sebagai kebutuhan yang sangat penting dalam operasional perusahaan. RUIS memahami kemampuan dan keterbatasan TI perusahaan, oleh karena itu secara kontinyu dilakukan pembenahan atas kontrol dan sistem yang ada. Belum dilakukan pengukuran secara spesifik atas ancaman yang terjadi dengan dampak bisnis yang akan dihadapi. Konsep pemikiran manajemen risiko TI belum didokumentasikan dan didefinisikan secara jelas, sehingga belum dapat dikomunikasikan secara jelas dan meyeluruh kepada stakeholder.

Dari kondisi diatas dapat disimpulkan bahwa RUIS telah melakukan analisis atas pengelolaan TI perusahaan, namun masih terbatas pada area tertentu yang menjadi prioritas berdasarkan tingkat urgensi dan risiko yang paling kritis dan baru terbatas pada proses bisnis yang berisiko menimbulkan kerugian finansial yang potensial. Mekanisme analisis didasarkan atas asumsi individu tanpa menggunakan standar analisis yang baku, sehingga seringkali analisis keluar dari lingkup yang ditetapkan. Analisis dilakukan oleh seorang analis dimana masih memiliki keterbatasan karena kurangnya pelatihan atas manajemen risiko TI, sehingga analisis masih berfokus pada proses kontrol yang ada pada perusahaan dan melakukan pembenahan atas kelemahan dan risiko yang mugkin timbul terkait TI.

Untuk mencapai tahap *Defined,* RUIS harus:

1. Mendefinisikan scenario dan prosedur analisis atas seluruh kegiatan usaha perusahaan secara keseluruhan. Yaitu dengan mendokumentasikan dan menjadikan scenario dan prosedur analisis yang telah dilakukan menjadi sebuah kebijakan sehingga dapat dijadikan panduan dalam melakukan analisis atas risiko TI dikemudian hari.
2. Menetapkan persyaratan keterampilan yang didefinisikan dan didokumentasikan untuk semua area risiko perusahaan, dengan pertimbangan pada pengumpulan data, analisis dan profil risiko. Dapat

dicapai dengan memberikan pelatihan manajemen risiko TI khususnya prosedur analisis yang sesuai dengan standar yang baku.

3. Mengembangkan alat pengumpulan data yang sesuai standar yang ditetapkan dan dapat membedakan antara peristiwa ancaman, kerentanan dan peristiwa kerugian.

3. Risk Response (RR)

Pada bagian ini, RUIS memperoleh skor tingkat kematangan sebesar 1,92. Skor ini diperoleh dari rata-rata tingkat kematangan masing-masing proses RR1 sebesar 2,00, RR2 sebesar 2,00, dan RR3 sebesar 1,75. Skor ini juga menunjukkan bahwa bagian RR, tata kelola TI RUIS juga berada pada posisi *Initial* dengan kondisi sebagai berikut (ITGI 2008) :

1. Pengakuan kebutuhan untuk respon risiko muncul, tetapi dipandang terbatas pada risiko penghindaran, memenuhi persyaratan kepatuhan dan transfer melalui asuransi.
2. Ada kesadaran individu atas ancaman dan apa yang harus dilakukan ketika terjadi risiko.
3. Komunikasi yang minim atas deteksi dan respon terhadap peristiwa dan respon risiko sejalan dengan prioritas bisnis.
4. Akuntabilitas yang minimal untuk memastikan bahwa risiko yang masuk akal atas respon tindakan yang ada dan mencerminkan ancaman terhadap lingkungan dan nilai aset. Individu bertanggung jawab untuk risiko baik evaluasi maupun respon risiko.
5. Peristiwa terkait TI dan kondisi yang dapat mempengaruhi operasi sehari-hari kadang-kadang dibahas pada pertemuan manajemen, tetapi tanggapan risiko secara spesifik tidak dipertimbangkan.
6. Kekurangan kontrol dibahas dalam modus reaktif dan sulit untuk didefinisikan.
7. Informasi manajemen sangat minim untuk membantu mendeteksi peristiwa secara tepat waktu dan membandingkan tanggapan dengan prioritas bisnis.

Pada bagian RR1 dalam praktiknya RUIS telah melaporkan hasil analisis TI ke direksi, biasanya direksi memberikan tanggapan dengan memberi arahan dan

masukan atas temuan yang dibahas dalam rapat. Penilaian risiko TI dilakukan oleh internal perusahaan. Masih sering terjadi risiko TI yang mengganggu kegiatan operasional perusahaan, namun belum ada respon yang memusakan atas risiko yang terjadi.

Pada bagian RR2, RUIS sudah memetakan kelemahan kontrol yang ada, kemampuan dan keterbatasan sumber daya, oleh karena itu RUIS telah memperkirakan risiko apa saja yang akan dihadapi dan seberapa besar dampaknya terhadap kegiatan operasional perusahaan. Pelaksanaan atas kontrol tersebut belum optimal kerana terbentur adanya konflik kepentingan, keterbatasan SDM dan budaya kerja yang belum selaras dengan kebijakan perusahaan dan manajemen risiko TI.

Pada bagian RR3 dapat diketahui di RUIS belum ada perencanaan atas respon peristiwa terkait risiko TI, respon bersifat reaktif yaitu dilakukan jika risiko tersebut terjadi. Pemantauan atas risiko TI dilakukan secara kontinyu, namun karena adanya keterbatasan SDM dan belum adanya keselarasan antara kebijakan perusahaan dan konsep manajemen risiko TI menyebabkan pemantauan atas risiko TI belum optimal. Setiap risiko yang terjadi didokumentasikan oleh Departemen TI namun tidak ada tindak lanjut atas permasalahan tersebut.

Dari kondisi diatas dapat disimpulkan bahwa RUIS, telah ada kesadaran perusahaan untuk menanggapi risiko yang terjadi dan memetakan risiko yang mungkin terjadi, hal ini dapat dilihat adanya rekomendasi dan solusi atas hasil analisis pengelolaan TI yang berupa pembenahan kontrol maupun perbaikan sistem secara bertahap. Dalam menanggapi risiko, perusahaan belum menggunakan standar baku penanggulangan risiko TI dan tidak ada pengukuran secara kuantitatif atas respon risiko yang dilakukan. Atas risiko yang terjadi, dilakukan dokumentasi secara lengkap namun tidak ada upaya tindak lanjutnya. Respon atas risiko belum didefinisikan dan dikomunikasikan ke tingkat pelaksana sehingga respon atas risiko yang terjadi sifatnya reaktif dan masih kurang dari yang diharapkan. Selain itu budaya kerja yang sudah tercipta sulit untuk mengimplementasikan manajemen risiko terkait TI.

Untuk mencapai tahap *Repeatable,* RUIS harus:

1. Mengembangkan pemahaman tentang ancaman berdampak pada bisnis dan tindakan spesifik yang dilakukan jika ancaman bisnis terjadi. Pengembangan pemahaman ini dapat dilakukan dengan memberikan dan mensosialisasikan pengetahuan mengenai dampak dari risiko TI yang terjadi sehingga setiap karyawan menyadari pentingnya mengelola risiko TI.
2. Membudayakan kesadaran tanggung jawab karyawan untuk kegiatan pengendalian sehingga tumbuh pemahaman umum tentang kebutuhan untuk memberlakukan tindakan respon risiko.
3. Batasan toleransi yang tidak dapat diterima dan mitigasi dilaporkan kepada manajer yang tepat. Batasan toleransi ini harus didefinisikan yaitu dengan mensosialisasikannya ke semua pelaksana setiapa risiko yang teridentifikasi beserta dampak yang ditimbulkannya.
4. Mengembangkan mitigasi risiko TI dan rencana tindakan. Pelaporan hasil proses respon risiko TI diarahkan ke manajemen TI. Hal ini dilakukan secara kontinyu oleh departemen TI perusahaan berdasarkan risiko yang sudah ditetapkan dan membuat perencanaan penanggulangannya.

BAB V
KESIMPULAN DAN REKOMENDASI

Bab 5 merupakan bagian penutup berupa kesimpulan dari hasil penelitian dan rekomendasi yang dapat diberikan kepada PT. Radiant Utama Interinsco, Tbk dalam penerapan audit sistem informasi dengan menggunakan kerangka kerja *Risk IT*.

5.1 Kesimpulan

5.1.1 Penerapan Tata Kelola TI di RUIS

Berdasarkan hasil penelitian, dapat disimpulkan bahwa saat ini belum ada konsep tertulis yang menyatakan bahwa RUIS telah menerapkan manajemen risiko TI di dalam perusahaan. Namun secara tidak langsung RUIS telah menerapkan pengelolaan risiko TI perusahaan. RUIS menyadari pentingnya mengelola risiko terkait TI yang dapat dilihat dengan adanya pembenahan kontrol atas sistem aplikasi secara bertahap yang dilakukan oleh analis sistem yang merupakan bagian dari Divisi Internal Audit perusahaan. Pimpinan perusahaan sangat *concern* atas perkembangan dan pembenahan pengelolan TI meskipun saat ini dalam struktur perusahaan belum ada Direktur TI namun fungsi dan tugasnya sudah didefinisikan yang saat ini berada di Direktur Keuangan dan Administrasi sebagai penanggung jawab atas pengelolaan TI perusahaan.

Di RUIS terlihat bahwa telah ada konsep yang menunjukkan kesadaran tentang pentingnya pengelolaan risiko TI dan adanya pemahaman mengenai keterkaitan antara kegiatan operasional perusahaan dengan risiko terkait TI. Namun konsep tersebut belum didokumentasikan dengan jelas sehingga sulit untuk dikomunikasikan ke seluruh pemilik kepentingan atas TI. Analisis yang dilakukan pun belum menggunakan standar analisis dan alat pengukuran atas analisis yang baku. Pembahasan mengenai pengelolaan risiko TI cukup sering dilakukan yang biasanya di picu oleh adanya temuan audit internal, hasil analisis sistem maupun terjadinya kegagalan terkait TI. Hasil rapat ini selalu dikomunikasikan ke tingkat pelaksana dengan tujuan untuk membudayakan kesadaran atas risiko TI dan respon atas risiko yang terjadi.

5.1.2 Kesimpulan Hasil Pengukuran Tingkat Kematangan dengan Menggunakan Kerangka Kerja Risk IT pada RUIS

Berdasarkan hasil pengukuran tingkat kematangan dengan menggunakan kerangka kerja risk IT pada RUIS dapat dilihat bahwa RUIS memperoleh tingkat kematangan sebesar 2,09 yang menunjukkan bahwa tingkat kematangan RUIS saat ini berada pada level 2 yaitu berada pada tahapan *Repeatable* dan menuju tahap *Defined Process*. Hasil ini diperoleh dari pengukuran tingkat kematangan untuk bagian RG sebesar 2,15, RE sebesar 2,28, dan RR 1,92. Perusahaan dinyatakan sudah menerapkan pengelolaan risiko TI, namun belum optimal. Proses yang ada diperusahaan sudah menunjukkan penerapan pengelolaan risiko yang selaras dengan konsep manajemen risiko yang baku, dan mulai mencapai tahap ketika semua proses yang dijalankan perusahaan sudah didokumetasikan dan dikomunikasikan dengan baik. Untuk mengoptimalkan pengelolaan risiko terkait TI, RUIS harus melakukan pengukuran dan analisis atas risiko TI dengan standar yang baku.

Jika dilihat dari perolehan skor untuk masing-masing bagian yang ada di kerangka kerja *Risk IT* maka untuk bagian RG memperoleh skor tingkat kematangan sebesar 2,15. Skor ini diperoleh dari rata-rata tingkat kematangan proses RG 1 sebesar 2,25, RG 2 sebesar 2,20 dan RG 3 sebesar 2,00. Skor ini menunjukkan bahwa untuk bagian RG, tata kelola TI RUIS berada pada posisi *Repeatable*. Sementara untuk bagian RE memperoleh skor tingkat kematangan sebesar 2,28. Skor ini diperoleh dari rata-rata tingkat kematangan proses RE 1 sebesar 2,00, RE 2 sebesar 2,50, dan RE 3 sebesar 2,33. Skor ini juga menunjukkan bahwa bagian RE, tata kelola TI RUIS saat ini berada pada tingkat *Repeatable*. Untuk bagian yang terakhir yaitu RR, RUIS memperoleh skor tingkat kematangan sebesar 1,92. Skor ini diperoleh dari rata-rata tingkat kematangan proses RR 1 sebesar 2,00, RR 2 sebesar 2,00, dan RR 3 sebesar 1,75. Skor ini menunjukkan bahwa bagian RR, tata kelola TI RUIS saat ini berada pada tingkat *Initial.*

5.2 Rekomendasi

Untuk meningkatkan kualitas tata kelola TI pada RUIS, rekomendasi yang dapat diberikan adalah sebagai berikut:

1. Sebaiknya RUIS mendokumentasikan konsep pengelolaan risiko TI dan menjadikannya standar yang baku sehingga dapat dijadikan acuan dalam setiap proses yang terkait dengan TI di perusahaan.
2. Sebaiknya RUIS mulai memasukkan posisi Direktur TI ke dalam struktur organisasi perusahaan, sehingga Departemen TI dapat lebih meningkatkan perannya di dalam perusahaandalam upaya mencapai tujuan perusahaan.
3. RUIS sebaiknya meningkatkan pelatihan terkait pengelolaan risiko TI agar SDM RUIS memiliki keahlian dan keterampilan dalam mengelola risiko TI.
4. Terkait dengan hasil pengukuran tingkat kematangan, terlihat bahwa RUIS memiliki kelemahan pada semua bagian, baik RG,RE maupun RR.

Untuk meningkatkan tingkat kematangan pengelolaan risiko TI dari tahapan *Repeatable* ke tahapan *Defined Process*, sebaiknya RUIS mulai mendokumentasikan dengan jelas semua proses yang terkait dengan pengelolaan risiko TI, termasuk hal-hal teknis. Selain itu, meningkatkan kemampuan SDM yang terlibat langsung dalam pengelolaan risiko TI dengan memberikan pelatihan-pelatihan terkait pengelolaan risiko TI agar kinerja pengelolaan risiko TI lebih efektif dan tepat sasaran. Penulis juga merekomendasikan agar RUIS mulai membuat suatu prosedur yang baku dan lengkap mengenai pengelolaan risiko TI mulai dari perencanaan, evaluasi dan penanggulangan atas risiko yang terjadi. Sehingga jika dikemudian hari terjadi suatu masalah terkait risiko TI, maka pihak-pihak terkait tinggal mengikuti prosedur yang telah ditetapkan sebelumnya.

5.3 Keterbatasan Penelitian

Dalam pelaksanaan penelitian ini, penulis memiliki kelemahan dan keterbatasan antara lain:

1. Keterbatasan data, berkenaan adanya dokumen dan informasi yang dianggap rahasia oleh perusahaan.
2. Pengukuran tingkat kematangan berdasarkan analisis penulis, sehingga cenderung subjektif.

Daftar Pustaka

Alvin A, Arens, James K.Loebbecke, *Auditing*, Edisi Indonesia, Jakarta, (2003).

Arens, Elder, Beasley, *Auditing and Asssurance Services* Ninth Edition. Prentice Hall, (2003)

Boynton, Johnson, Kell, *Modern Auditing*. Seventh Edition. John Wiley & Sons, Inc., (2003)

Dan M. Guy, C. Wayne Alderman, Alan J. Winters, *"Auditing"*. Fifth Edition. Alih Bahasa Erlangga Jakarta, 2002)

Effendi, Muh. Arief, Risk Based Internal Auditing Rubrik "Audit Isu", *Majalah Media Akuntansi* No. 32 Edisi April 2003

Information Sistem Audit and Control Association (ISACA), *IS Standards, Guidelines and Procedures for Auditing and Control Professionals*, http://www.isaca.org., (2003).

Information Sistem Audit and Control Association (ISACA), *Risk IT Practitioner Guide*, (2009)

IT Governance Institute, *Executive Summary*, COBIT 4th Edition, (2008)

IT Governance Institute, *The Risk IT Framework*, (2009)

Pri Heriyanto. 2002. Menuju Audit Yang Efektif Dan Efisien. *Majalah Pemeriksa No. 86 page 45-47*., (2002)

Risk IT - the New Framework for Managing IT Related Business Risks, By Paul Williams on January 4, http://bit.ly/5mGt2k, (12 Oktober 2011)

Richard W. Houston, Michael F. Peters, Jamie H. Pratt. The Audit Risk Model, Business Risk and Audit Planning Decisions. *The Accounting Review Journal*. Volume 74. (Juli 1999)

PT. Radiant Utama Interinsco (Tbk) , Annual Report (2010)

Soekrisno Agoes, *Auditing (Pemeriksaan Akuntan) Oleh KAP*. Edisi Tiga. LPFEUI Jakarta. (2004)

Schneider, Laura , Information Technology Audit http://jobsearchtech.about.com/od/historyoftechindustry/g/IT Audit.htm, (15 Januari 2011)

Weber, Ron, *Information Sistems Control and Audit*, The University of Queensland, Prentice Hall, (2000)

Lampiran 1

RACI *chart* dalam Kerangka Kerja *Risk IT*

MANAGEMENT GUIDELINES—RG1

RACI Chart

Key Activities \ Roles	Board	CEO	CRO	CIO	CFO	Enterprise Risk Committee	Business Management	Business Process Owner	Risk Control Functions	HR	Compliance and Audit
RG1.1 Develop an enterprise-specific IT risk management framework.	A	R	R	R	C	I	R	I	C	I	C
RG1.2 Develop IT risk management methods.	C	C	A	R	C	I	C	C	C	I	C
RG1.3 Perform an enterprise-wide IT risk assessment.	I	A	R	R	C	I	R	C	R	C	C
RG1.4 Propose IT risk tolerance thresholds.	I	I	C	R	C	I	A	C	C		C
RG1.5 Approve IT risk tolerance.	A	C	C	C	C	R	C	C	C	C	C
RG1.6 Align policy and standards statements with IT risk tolerance.		I	A	R	I	C	R	I	C	R	I
RG1.7 Promote an IT risk-aware culture.	A	R	R	R	R	R	R	R	R	R	R
RG1.8 Promote effective communication of IT risk.	A	R	R	I	I	R	I	I	I	I	C

A RACI chart identifies who is Responsible, Accountable, Consulted and/or Informed.

MANAGEMENT GUIDELINES—RG2

RACI Chart

Key Activities \ Roles	Board	CEO	CRO	CIO	CFO	Enterprise Risk Committee	Business Management	Business Process Owner	Risk Control Functions	HR	Compliance and Audit
RG2.1 Establish enterprise-wide accountability for managing IT risk.	A	R	R	C		I			C		C
RG2.2 Establish accountability for IT risk issues.	I	A	R	R		I	I	R	R		C
RG2.3 Co-ordinate IT risk strategy and business risk strategy.	I	A	C	R	C	C	R	C	C	C	I
RG2.4 Adapt IT risk management practices to organisational risk management practices.			C	A/R	C	I	C	C	R	C	C
RG2.5 Provide adequate resources for IT risk management.	A	R	C	R		I	C	R	C		

A RACI chart identifies who is Responsible, Accountable, Consulted and/or Informed.

MANAGEMENT GUIDELINES—RG3

RACI Chart

Key Activities \ Roles	Board	CEO	CRO	CIO	CFO	Enterprise Risk Committee	Business Management	Business Process Owner	Risk Control Functions	HR	Compliance and Audit
RG3.1 Gain management buy-in for the IT risk analysis approach.		C	A/R	R	C	C	C	C	R	C	C
RG3.2 Approve IT risk analysis results.		I	R	C	C	A	I	R	I	I	I
RG3.3 Embed IT risk considerations into strategic business decision making.	I	C	C	A/R	C	C	C	C	R	C	I
RG3.4 Accept IT risk.	I	I	C	R	C	R	A	R	C		I
RG3.5 Prioritise IT risk response activities.		I	A	R	I	C	C	R	R		I
RG3.6 Track key IT risk decisions.		I	A	R	I	I	I	R	R	I	I

A RACI chart identifies who is Responsible, Accountable, Consulted and/or Informed.

MANAGEMENT GUIDELINES—RE1

RACI Chart

Key Activities \ Roles	Board	CEO	CRO	CIO	CFO	Enterprise Risk Committee	Business Management	Business Process Owner	Risk Control Functions	HR	Compliance and Audit
RE1.1 Establish and maintain a model for data collection.	I	I	A/R	C	C	C	C	C	C		C
RE1.2 Collect data on the external environment.		I	A/R	C	I	I	C	I	I	I	C
RE1.3 Collect timely event, incident, problem and loss data.		I	A	R	C	I		C	C		I
RE1.4 Identify risk factors.			A	R	I	I	C	C	R	C	C
RE1.5 Organise historical IT risk data.		I	A	C	C	I	C	R	R	I	I

A RACI chart identifies who is Responsible, Accountable, Consulted and/or Informed.

MANAGEMENT GUIDELINES—RE2

RACI Chart

Key Activities \ Roles	Board	CEO	CRO	CIO	CFO	Enterprise Risk Committee	Business Management	Business Process Owner	Risk Control Functions	HR	Compliance and Audit
RE2.1 Define IT risk analysis scope.		I	R	C	I	C	A	R	C		C
RE2.2 Estimate IT risk to and from critical products, services, processes and IT resources.		I	R	C	C	I	A/R	R	R		C
RE2.3 Identify risk response options.			C	C	C	R	A	R	R		I
RE2.4 Perform a peer review of IT risk analysis results.			A/R				I		I		

A RACI chart identifies who is Responsible, Accountable, Consulted and/or Informed.

MANAGEMENT GUIDELINES—RE3

RACI Chart

Key Activities \ Roles	Board	CEO	CRO	CIO	CFO	Enterprise Risk Committee	Business Management	Business Process Owner	Risk Control Functions	HR	Compliance and Audit
RE3.1 Map IT resources to business processes.			I	R			A	R	C		I
RE3.2 Determine the business criticality of IT resources.		C		R		C	A	R			I
RE3.3 Understand IT capabilities.			C	A/R				C	C		I
RE3.4 Connect threat types and business impact categories.			C	R	I	C	C	A	R		C
RE3.5 Maintain the IT risk register and IT risk map.		I	A	R	I	I	I	R/C	C		I
RE3.6 Design and communicate IT risk indicators.			A	I			R	C	R	C	C

A RACI chart identifies who is Responsible, Accountable, Consulted and/or Informed.

MANAGEMENT GUIDELINES—RR1

RACI Chart

Key Activities \ Roles	Board	CEO	CRO	CIO	CFO	Enterprise Risk Committee	Business Management	Business Process Owner	Risk Control Functions	HR	Compliance and Audit
RR1.1 Report IT risk analysis results.		I	R	C	C	C	A	R	R	C	I
RR1.2 Report IT risk management activities and state of compliance.	I	I	C	R	I	A	I	I	I	I	C
RR1.3 Interpret external IT assessment findings.	I	I	A/R	R	I	I	I		C	I	C
RR1.4 Identify IT-related opportunities.		I	I	R	I	I	A	R	R	I	I

A RACI chart identifies who is Responsible, Accountable, Consulted and/or Informed.

MANAGEMENT GUIDELINES—RR2

RACI Chart

Key Activities \ Roles	Board	CEO	CRO	CIO	CFO	Enterprise Risk Committee	Business Management	Business Process Owner	Risk Control Functions	HR	Compliance and Audit
RR2.1 Inventory controls, capabilities and resources.		I	A/R	C	I	I	C	C	R		C
RR2.2 Monitor operational alignment with risk tolerance thresholds.			C	C		I	A	R	R		C
RR2.3 Respond to discovered risk exposure and opportunity.	I	A	C	R	C	I	R	C	C	C	
RR2.4 Implement controls.	I	A	C	R	C	I	R	C	C	C	I
RR2.5 Report on IT risk action plan progress.	I	I	I	R	I	I	I	A	R	I	I

A RACI chart identifies who is Responsible, Accountable, Consulted and/or Informed.

MANAGEMENT GUIDELINES—RR3

RACI Chart

Key Activities \ Roles	Board	CEO	CRO	CIO	CFO	Enterprise Risk Committee	Business Management	Business Process Owner	Risk Control Functions	HR	Compliance and Audit
RR3.1 Maintain incident response plans.	I	I	I	R	C	I	I	A	R	I	I
RR3.2 Monitor IT risk.			C	I	I	I	I	A	R		R
RR3.3 Initiate incident response plans.	I	I	I	I	I	I	R	A	R	C	I
RR3.4 Conduct post-mortem reviews of IT-related incidents.	I	I	A/R	R	C	I	C	C	R	C	I

A RACI chart identifies who is Responsible, Accountable, Consulted and/or Informed.

Lampiran 2

Penerapan RACI *Chart* di RUIS

Role								
Key Activities		**Board**	**Manajemen**	**Dept TI**	**Internal Audit**	**SDM**	**Akntg & Finance**	**Operasional**
Risk Governance								
RG1 Establish and Maintain a Common Risk View Risk Governance								
RG1.1	Develop an enterprise-specific IT risk management framework. Mengembangkan kerangka manajemen risiko IT perusahaan secara spesifik.	A	C	R	I			
RG1.2	Develop IT risk management methods. Mengembangkan metode manajemen risiko TI.	C	C	R	C			
RG1.3	Perform an enterprise-wide IT risk assessment. Lakukan penilaian risiko TI perusahaan secara luas.	I	C	R	R			
RG1.4	Propose IT risk tolerance thresholds. Mengusulkan ambang batas toleransi risiko TI.	I	C	R	C			
RG1.5	Approve IT risk tolerance. Menyetujui toleransi risiko TI.	A	C	C	I			
RG1.6	Align policy and standards statements with IT risk tolerance. Sesuaikan pernyataan kebijakan dan standar dengan toleransi risiko TI.		R	R	C			
RG1.7	Promote an IT risk-aware culture Mempromosikan budaya sadar risiko TI	A	R	R	I			
RG1.8	Promote effective communication of IT risk. Mempromosikan komunikasi yang efektif dari risiko IT.	A	R	R	I			
RG2 Integrate with ERM								
RG2.1	Establish enterprise-wide accountability for managing IT risk. Membangun akuntabilitas perusahaan secara luas untuk mengelola risiko TI.	A	R	R	R			
RG2.2	Establish accountability for IT risk issues. Membangun akuntabilitas untuk isu-isu risiko TI.	A	R	R	C			
RG2.3	Co-ordinate IT risk strategy and business risk strategy. Mengkoordinasikan startegi risiko IT dan strategi risiko bisnis.	I	R	R	R			
RG2.4	Adapt IT risk management practices to organisational risk management practices. Adaptasikan praktik manajemen risiko IT untuk praktek manajemen risiko organisasi.	I	R	R	I			
RG2.5	Provide adequate resources for IT risk management. Menyediakan sumber daya yang memadai untuk manajemen risiko TI.	A	C	R	I			

Key Activities		Board	Risk Manajemen	Dept TI	Audit	SDM	Finance	Operasional
Risk Governance								
RG3 Make Risk-aware Business Decisions								
RG3.1	Gain management buy-in for the IT risk analysis approach.							
RG3.2	Approve IT risk analysis results. Menyetujui hasil analisis risiko TI.		I	I	C			
RG3.3	Embed IT risk considerations into strategic business decision making. Melekatkan pertimbangan risiko IT ke dalam pengambilan keputusan bisnis strategis.	I	C	R	C			
RG3.4	Accept IT risk. Terima risiko TI.	A	C	R	I			
RG3.5	Prioritise IT risk response activities. Prioritaskan respon kegiatan risiko IT .	I	C	R	C			
RG3.6	Track key IT risk decisions Melacak keputusan utama risiko TI	I	C	R	R			

Key Activities		Board	Risk Manajemen	Dept TI	Internal Audit	SDM	Finance	Operasional
Risk Evaluation								
RE1 Collect Data								
RE1.1	Establish and maintain a model for data collection. Membangun dan memelihara sebuah model untuk pengumpulan data.	I	R	R	C			
RE1.2	Collect data on the external environment. Mengumpulkan data pada lingkungan eksternal.		R	R	R			
RE1.3	Collect timely event, incident, problem and loss data. Kumpulkan data yang tepat waktu atas peristiwa, insiden, masalah dan kerugian.		R	R	I			
RE1.4	Identify risk factors. Mengidentifikasi faktor risiko.	C	R	I	C			
RE1.5	Organise historical IT risk data. Mengorganisir data historis risiko TI.		R	I	C			

Key Activities		Board	Risk Manajemen	Dept TI	Internal Audit	SDM	Finance	Operasional
Risk Evaluation								
RE2 Analyse Risk								
RE2.1	Define IT risk analysis scope. Tentukan lingkup analisis risiko TI.	C	R	C	C			
RE2.2	Estimate IT risk to and from critical products, services, processes and IT resources. Perkiraan risiko TI ke dan dari produk , jasa, proses dan sumber daya TI yang kritis.		R	R	R			
RE2.3	Identify risk response options. Identifikasi opsi respon risiko.		R	C	R			
RE2.4	Perform a peer review of IT risk analysis results. Melakukan peer review hasil analisis risiko TI.		R	R	R			
RE3 Maintain Risk Profile								
RE3.1	Map IT resources to business processes. Memetakan sumber daya TI untuk proses bisnis.	C	A	R	I			
RE3.2	Determine the business criticality of IT resources. Tentukan kekritisan bisnis atas sumber daya TI.		A	R	C			
RE3.3	Understand IT capabilities. Memahami kemampuan IT.		R	C	I			
RE3.4	Connect threat types and business impact categories. Hubungkan jenis ancaman dengan kategori dampak bisnis.		R	R	C			
RE3.5	Maintain the IT risk register and IT risk map. Menjaga daftar risiko TI dan peta risiko TI.		R	R	C			
RE3.6	Design and communicate IT risk indicators. Desain dan mengkomunikasikan indikator risiko TI.	A	R	C	I			

Key Activities		Board	Manajemen	Dept TI	Internal Audit	SDM	Finance	Operasional
Risk Response								
RR1 Articulate Risk								
RR1.1	Report IT risk analysis results. Laporan hasil analisis risiko TI.	I	R	R	C			
RR1.2	Report IT risk management activities and state of compliance. Laporan kegiatan manajemen risiko TI dan laporan kepatuhan.	I	R	I	C			
RR1.3	Interpret external IT assessment findings. Menafsirkan temuan penilaian eksternal TI.							
RR1.4	Identify IT-related opportunities. Mengidentifikasi peluang yang berkaitan dengan IT.	I	R	C	R			
RR2 Manage IT Risk								
RR2.1	Inventory controls, capabilities and resources. Inventarisasi kontrol, kemampuan dan sumber daya.		A	R	I			
RR2.2	Monitor operational alignment with risk tolerance thresholds. Memantau keselarasan operasional dengan batas toleransi risiko.	I	R	R	I			
RR2.3	Respond to discovered risk exposure and opportunity		R	R	I			
RR2.4	Implement controls. Melaksanakan kontrol.	I	R	R	R			
RR2.5	Report on IT risk action plan progress. Laporan atas progress perencanaan tindakan risiko TI.	C	A	R	I			
RR3 React to Events								
RR3.1	Maintain incident response plans. Menjaga rencana atas respon insiden.	I	R	R	I			
RR3.2	Monitor IT risk. Memantau risiko TI.	I	C	R	R			
RR3.3	Initiate incident response plans. Memulai rencana respon insiden.	C	R	I	C			
RR3.4	Conduct post-mortem reviews of IT-related incidents. Melakukan post-mortem review dari insiden terkait TI.	I	R	C	C			

Lampiran 3

Tujuan dan Metrik Kerangka Kerja *Risk IT*

Enterprise Risk: Identify, Govern and Manage IT Risk, The Risk IT Framework Exposure Draft

RG1 Establish and Maintain a Common Risk View Risk Governance

Goals and Metrics

Activity Goals	Process Goal	RG Goal
• Develop an enterprise-specific IT risk management framework. • Develop IT risk management methods. • Perform an enterprise-wide IT risk assessment. • Propose IT risk tolerance thresholds. • Approve IT risk tolerance. • Align policy and standards statements with IT risk tolerance. • Promote an IT risk-aware culture. • Promote effective communication of IT risk.	• Ensure that risk management activities align with the enterprise's objective capacity for IT-related loss and leadership's subjective tolerance of it.	• Ensure that IT risk management practices are embedded in the enterprise, enabling the enterprise to secure optimal risk-adjusted return.
Activity Metrics	**Process Metrics**	**RG Metrics**
• Existence of a defined and documented IT risk management framework • Degree of completeness of the IT risk management framework • Percentage of the IT risk management framework covered by defined methods • Percentage of IT risk management structures and activities set up vs. planned • Frequency of enterprise-wide IT risk assessments • Level of executive participation in enterprise-wide IT risk assessments (e.g., attend in person, send a subordinate, receive report) • Number of out-of-cycle enterprise-wide IT risk assessments • Number of aligned policies to which intended audience has signed adherence • Extent to which risk management communications and training are targeted to specific roles and responsibilities	• Number of known executive-level risk tolerance violations not subjected to disciplinary action (enforcement of policy) • Number of IT-related events with business impact in which a failure to escalate was a factor in event occurrence and/or the loss magnitude (e.g., the risk manager did not know or there was an impaired cultural ability to escalate) • Number of policies in force with one or more statements contradicting a related risk tolerance (alignment of IT policies with tolerance) • Number of IT risk issues that exceed risk tolerance	• The degree to which the strategic use of IT in leveraging enterprise resources reduces overall enterprise risk • Percentage of staff trained in critical risk management techniques (e.g., standard risk analysis techniques, crisis management, project management, skills of people [audit, etc.] to detect when something IT-related is amiss)

Enterprise Risk: Identify, Govern and Manage IT Risk, The Risk IT Framework Exposure Draft

RG2 Integrate with ERM — Risk Governance

Goals and Metrics

Activity Goals	Process Goal	RG Goal
• Establish enterprise-wide accountability for managing IT risk. • Establish accountability for IT risk issues. • Co-ordinate IT risk strategy and business risk strategy. • Adapt IT risk management practices to organisational risk management practices. • Provide adequate resources for IT risk management.	• Integrate the IT risk strategy and operations with the business strategic risk decisions that have been made at the enterprise level.	• Ensure that IT risk management practices are embedded in the enterprise, enabling the enterprise to secure optimal risk-adjusted return.
Activity Metrics	**Process Metrics**	**RG Metrics**
• Percentage of employees whose performance metrics and rewards reflect risk management objectives • An alignment score related to RACI regarding the ranking of actions to take (e.g., percentage of key IT risk-related accountabilities accepted by business and IT personnel) • Number of different risk reports provided to the board; extent of integration of reporting on IT risk • Percentage of IT risk practices adapted to ERM organisational expectations • Percent of IT risk management action plans approved for implementation • Percentage of core ERM activities with embedded IT risk considerations • Number of different issue management processes and platforms • Extent to which budgets are allocated based on risk significance (e.g., per risk assessment results) • Number of open positions in the risk management staff	• Percentage of business executives and managers who have received training on the enterprise's reliance on and usage of IT, the related risk, IT risk strategy and framework • Percentage of IT risk management operational expenditures that have direct traceability to business risk strategy • Percentage of business projects that consider IT risk • Percentage of core ERM activities that consider IT risk • Frequency of IT risk as an agenda item for the executive committee • Extent of alignment between organisational objectives and IT risk management objectives • Extent of overlap of risk management activities performed by business units, risk and control functions, and internal audit	• The degree to which the strategic use of IT in leveraging enterprise resources reduces overall enterprise risk • Percentage of staff trained in critical risk management techniques (e.g., standard risk analysis techniques, crisis management, project management, skills of people [audit, etc.] to detect when something IT related is amiss)

Enterprise Risk: Identify, Govern and Manage IT Risk, The Risk IT Framework Exposure Draft

RG3 Make Risk-aware Business Decisions — Risk Governance

Goals and Metrics

Activity Goals	Process Goal	RG Goal
• Gain management buy-in for the IT risk analysis approach. • Approve IT risk analysis results. • Embed IT risk considerations into strategic business decision making. • Accept IT risk. • Prioritise IT risk response activities. • Track key IT risk decisions.	• Ensure that organisational decisions consider the full range of opportunities and consequences arising from reliance on IT for success.	• Ensure that IT risk management practices are embedded in the enterprise, enabling the enterprise to secure optimal risk-adjusted return.
Activity Metrics	**Process Metrics**	**RG Metrics**
• Percentage of business decisions that should have considered IT risk but did not • Number and size of adverse events/losses arising out of risk acceptance decision, including opportunity losses • Percentage of accepted IT risks with a complete set of supporting documentation • Number of prioritised risk response activities • Percentage of IT risk issues for which the expected reduction in frequency and magnitude is tracked	• Value of failed projects due to issues not identified during the decision-making process (e.g., was the risk presented on the risk log? Was it estimated properly? Was there follow-through on it?) • Number of key management decisions made without the availability of a relevant risk analysis report • Percentage of decisions (or indecision) leading to IT-related loss revisited for lessons learned • Cycle time from the discovery of a control deficiency (e.g., vulnerability event) to a risk acceptance decision • Cycle time from reported policy exceptions to a decision on their disposition	• The degree to which the strategic use of IT in leveraging enterprise resources reduces overall enterprise risk • Percentage of staff trained in critical risk management techniques (e.g., standard risk analysis techniques, crisis management, project management, skills of people [audit, etc.] to detect when something IT-related is amiss)

Enterprise Risk: Identify, Govern and Manage IT Risk, The Risk IT Framework Exposure Draft

RE1 Collect Data — Risk Evaluation

Goals and Metrics

Activity Goals	Process Goal	RE Goal
• Establish and maintain a model for data collection. • Collect data on the external environment. • Collect timely event, incident, problem and loss data. • Identify risk factors. • Organise historical IT risk data.	• Identify relevant data to enable effective IT-related risk identification, analysis and reporting.	• Ensure that IT-related risks and opportunities are identified, analysed and presented in business terms.
Activity Metrics	**Process Metrics**	**RE Metrics**
• Existence of a defined and documented risk-related data collection model • Number of sources used for data collection • Completeness of event data against established standards (e.g., affected assets, impact data, threat community, actions). This includes both discrete event data (e.g., control 'yes' or 'no') and continuous data (e.g., ongoing stream data on server response time). • Number of data items for which the contributing factors have been identified • Completeness of historical data across the top classes of IT risk	• Number of loss events with key characteristics not captured in some form of repository • Degree to which collected data supports reporting of trends and scenario analysis • The degree of visibility and recognition into the control state provided by data collection • The degree of visibility and recognition into the threat landscape provided by data collection	• The cumulative business impact from IT-related incidents and events not identified by risk evaluation processes

Enterprise Risk: Identify, Govern and Manage IT Risk, The Risk IT Framework Exposure Draft

RE2 Analyse Risk — Risk Evaluation

Goals and Metrics

Activity Goals	Process Goal	Domain Goal
• Define IT risk analysis scope. • Estimate IT risk to and from critical products, services, processes and IT resources. • Identify risk response options. • Perform a peer review of IT risk analysis results.	• Develop useful information to support risk decisions that take into account the business relevance of risk factors (e.g., threats, vulnerabilities, value, liability).	• Ensure that IT-related risks and opportunities are identified, analysed and presented in business terms.
Activity Metrics	**Process Metrics**	**Domain Metrics**
• Percentage of time analyses are substantiated by later experience or testing (accuracy) • Percentage of time peer review finds no significant logical, calculation or incompleteness errors (defensibility) • Percentage of time parallel assessments on the same scenarios performed by different analysts get the same results (consistency) • Percentage of time analyses are performed by trained analysts (higher-level metric related to accuracy, defensibility and consistency) • A 'satisfaction index' over risk analysis reporting (e.g., the percentage of favourable satisfaction survey responses from business executives regarding the readability, usefulness and accuracy of risk analysis reports) • Ratio of cumulative actual losses to expected loss magnitude	• Percentage of risks for which the probable frequency of occurrence and the probable magnitude of the business impact are measured within the scope • Percentage of highly ranked assets, targets and resources reviewed for the effect of known operational controls • Percentage of risk analysis undergoing peer review before being sent to management	• The cumulative business impact from IT-related incidents and events not identified by risk evaluation processes

Enterprise Risk: Identify, Govern and Manage IT Risk, The Risk IT Framework Exposure Draft

RE3 Maintain Risk Profile — Risk Evaluation

Goals and Metrics

Activity Goals	Process Goal	RE Goal
• Map IT resources to business processes. • Determine the business criticality of IT resources. • Understand IT capabilities. • Connect threat types and business impact categories. • Maintain the IT risk register and IT risk map. • Design and communicate IT risk indicators.	• Maintain an up-to-date and complete inventory of known risks and attributes (e.g., expected frequency, potential impact, disposition), IT resources, capabilities, and controls as understood in the context of business products, services, and processes.	• Ensure that IT-related risks and opportunities are identified, analysed and presented in business terms.
Activity Metrics	**Process Metrics**	**RE Metrics**
• Percentage of key business activities with a dependency linkage to supporting IT resources and IT infrastructure resources • Percentage of the critical elements of the IT portfolio covered by risk triggers and thresholds • Number of realised events with business impact not detected by a trigger mechanism	• Number of approved risk analysis results not yet incorporated into the risk profile • Percentage of critical business services not covered by risk analysis • Completeness of key risk data attributes across the IT risk register	• The cumulative business impact from IT-related incidents and events not identified by risk evaluation processes

Risk IT Framework

RR1 Articulate Risk — Risk Response

Goals and Metrics

Activity Goals	Process Goal	RR Goal
• Report IT risk analysis results. • Report IT risk management activities and state of compliance. • Interpret external IT assessment findings. • Identify IT-related opportunities.	• Ensure that information on the true state of IT-related exposures and opportunities is made available in a timely manner and to the right people for appropriate response.	• Ensure that IT-related risk issues, opportunities and events are addressed in a cost-effective manner and in line with business priorities.
Activity Metrics	**Process Metrics**	**RR Metrics**
• Percentage of risk analysis reports accepted on initial delivery • Frequency of risk management activity reporting • Number of IT-related events with business impact not previously reported as an IT risk • Number of IT risk issues identified by outside parties yet to be interpreted and mapped into risk profile	• Percentage of risk issues inappropriately distributed too high or too low in the organisational hierarchy (and consequently sent up or down the chain of command for decision) • The number of IT-related events with business impact not earlier reported as an IT risk • Percentage of critical IT assets covered by monitoring activities (detectability) • Timeliness of reports on IT exposures relative to the next expected threat or loss event • Potential business impact of exposures (as agreed by management) discovered by assurance groups	• The cumulative business impact from IT-related incidents and events anticipated by risk evaluation processes but not yet addressed by mitigation or event action planning

MANAGEMENT GUIDELINES—RR2

Goals and Metrics

Activity Goals	Process Goal	RR Goal
• Inventory controls, capabilities and resources. • Monitor operational alignment with risk tolerance thresholds. • Respond to discovered risk exposure and opportunity. • Implement controls. • Report on IT risk action plan progress.	• Ensure that measures for seizing strategic opportunities and reducing IT risk to an acceptable level are managed as a portfolio.	• Ensure that IT-related risk issues, opportunities and events are addressed in a cost-effective manner and in line with business priorities.
Activity Metrics	**Process Metrics**	**RR Metrics**
• Percentage of controls that are directly related to maintaining the defined risk tolerance • Percentage of IT risk issues exceeding defined risk tolerance for which action plans have been established (alternatively, percentage of mitigation plans that have not been developed) • Number and value of missed IT-related opportunities	• Satisfaction of the risk owner regarding mitigation project outcomes • Percentage of risk mitigation plans executed on time (per management's decision, set date) • Percentage of unaccepted IT risk issues without mitigation plans developed • Percentage of unaccepted IT risk issues with action plan developed • Amount of investment spent on risk mitigation efforts that are later cancelled	• The cumulative business impact from IT-related incidents and events anticipated by risk evaluation processes but not yet addressed by mitigation or event action planning

Enterprise Risk: Identify, Govern and Manage IT Risk, The Risk IT Framework Exposure Draft

RR3 React to Events — **Risk Response**

Goals and Metrics

Activity Goals	Process Goal	RR Goal
• Maintain incident response plans. • Monitor IT risk. • Initiate incident response plans. • Conduct post-mortem reviews of IT-related incidents.	• Ensure that measures for seizing immediate opportunities or limiting the magnitude of loss from IT-related events are activated in a timely manner and are effective.	• Ensure that IT-related risk issues, opportunities and events are addressed in a cost-effective manner and in line with business priorities.
Activity Metrics	**Process Metrics**	**RR Metrics**
• Percentage of incident response plans past their next required review date • Number of incident response plans with unresolved quality issues • Percentage of incidents with business impact not subject to a post-mortem review	• Number of events with business impact due to delayed incident response plan execution • Number of incident response plans without an accountable owner • Timeliness of enacting incident response plans • Percentage of incident response plan past their next required review date • Percentage of incident response plans with one or more open issues regarding their quality and/or dissemination	• The cumulative business impact from IT-related incidents and events anticipated by risk evaluation processes but not yet addressed by mitigation or event action planning

Lampiran 4

Plotting Hasil Wawancara ke Kerangka Kerja *Risk IT*

Risk Governance
Tujuan Aktivitas RG 1 ***Establish and Maintain a Common Risk View Risk Governance***

<table>
<tr><th>Tujuan Aktivitas Risk IT</th><th>Fakta Di Perusahaan</th></tr>
<tr><td>Develop an enterprise-specific IT risk management framework.</td><td rowspan="6">Kerangka manajemen risiko TI sudah ada namun belum terdokumentasi. Direksi sangat concern terhadap perkembangan dan permasalahan terkait TI. Manajemen risiko TI sudah menjadi konsep dan target utama perusahaan dalam upayanya mengembangkan dan mengintegrasikan sumber daya TI perusahaan , karena system yang ada saat ini belum terintegrasi dan masih banyak nya kelemahan seperti, ketidak akuratan, output yang belum dapat memenuhi kebutuhan user.sebagai langkah pembenahan atas system yang ada secara berkesinambungan system ini dibenahi dari sisi control dan fungsi nya agar lebih maksimal yaitu dengan mengembangkan dan mendevelop system yang sesuai kebutuhan perusahaan. Manajemen juga sudah membuat pemetaan yg jelas dalam hal pengelolaan TI perusahaan.</td></tr>
<tr><td>Mengembangkan kerangka kerja manajemen risiko TI perusahaan secara spesifik .</td></tr>
<tr><td>Develop IT risk management methods.</td></tr>
<tr><td>Mengembangkan metode manajemen risiko TI.</td></tr>
<tr><td>Perform an enterprise-wide IT risk assessment.</td></tr>
<tr><td>Lakukan penilaian risiko TI perusahaan secara luas.</td></tr>
<tr><td>Propose IT risk tolerance thresholds.</td><td rowspan="10">Batasan toleransi atas resiko TI yang dapat diterima sudah ada dalam konsep pemikiran manajemen namun belum didokumentasikan dan didefinisikan secara jelas, sehingga belum dapat dikomunikasikan secara jelas dan meyeluruh kepada stakeholder. hasil dari analisis TI perusahaan juga memberikan masukan bagi manajemen dalam menentukan batasan toleransi resiko yang ada maupun dalam pengambilan keputusan terkait TI.</td></tr>
<tr><td>Mengusulkan batas toleransi risiko TI.</td></tr>
<tr><td>Approve IT risk tolerance.</td></tr>
<tr><td>Menyetujui toleransi risiko TI.</td></tr>
<tr><td>Align policy and standards statements with IT risk tolerance.</td></tr>
<tr><td>Sejajarkan pernyataan kebijakan dan standar dengan toleransi risiko TI.</td></tr>
<tr><td>Promote an IT risk-aware culture.</td></tr>
<tr><td>Mempromosikan budaya sadar risiko TI.</td></tr>
<tr><td>Promote effective communication of IT risk.</td></tr>
<tr><td>Mempromosikan komunikasi efektif risiko TI.</td></tr>
</table>

Metrik Aktivitas RG 1 ***Establish and Maintain a Common Risk View Risk Governance***

Metrik Aktivitas RG 1	**Fakta Diperusahaan**
Existence of a defined and documented IT risk management framework	**Kerangka manajemen risiko TI sudah ada namun belum terdokumentasi.** Direksi sangat concern terhadap perkembangan dan permasalahan terkait TI. **Manajemen risiko TI sudah menjadi konsep dan target utama perusahaan dalam upayanya mengembangkan dan mengintegrasikan sumber daya TI perusahaan** , karena system yang ada saat ini belum terintegrasi dan masih banyak nya kelemahan seperti, ketidak akuratan, output yang belum dapat memenuhi kebutuhan user.
Adanya kerangka kerja manajemen risiko TI yang didefinisikan dan didokumentasikan	
Degree of completeness of the IT risk management framework	**Kerangka manajemen risiko TI disusun berdasarkan asumsi dan pemahaman yang masih terbatas pada lingkup teknikal saja** sehingga penilaian atas risiko TI belum dilakukan secara luas di perusahaan
Tingkat kelengkapan kerangka manajemen risiko TI	
Percentage of the IT risk management framework covered by defined methods	**Perusahaan belum mendefinisikan secara spesifik manajemen risiko T**I karena masih concern terhadap pembenahan atas kontrol sistem secara keseluruhan
Persentase dari kerangka manajemen risiko TI yeng telah tercakup oleh metode yang telah didefinisikan	
Percentage of IT risk management structures and activities set up vs planned	Analis sistem berfungsi juga sebagai QC atas pengelolaan TI di perusahaan dan melakukan analisa resiko-resiko yang mungkin terjadi yang mengakibatkan kerugian yang **dilakukan secara kontinyu sesuai dengan skala prioritasnya**. Selain itu Analis juga bertugas menganalisa antara kesesuaian kebijakan terkait TI dengan pelaksanaan maupun dengan prosedur yang sudah ada.
Persentase struktur manajemen risiko TI dan kegiatan yang diatur vs direncanakan	
Frequency of enterprise-wide IT risk assessments	Analis sistem berfungsi juga sebagai QC atas pengelolaan TI di perusahaan dan melakukan analisa resiko-resiko yang mungkin terjadi yang mengakibatkan kerugian yang **dilakukan secara kontinyu sesuai dengan skala prioritasnya**. Selain itu Analis juga bertugas menganalisa antara kesesuaian kebijakan terkait TI dengan pelaksanaan maupun dengan prosedur yang sudah ada.
Frekuensi penilaian risiko TI perusahaan secara luas	
Level of executive participation in enterprise-wide IT risk assessments (e.g., attend in person, send a subordinate, receive report)	Dalam menilai dan mengidentifikasi risiko, **manajemen (Direksi) menugaskan analis sistem (Dept Internal Audit) yang langsung bertanggung jawab ke Direksi** dalam hal pelaporan atas aktivitasnya
Tingkat partisipasi eksekutif di perusahaan secara luas atas penilaian risiko TI (misalnya, menghadiri secara pribadi, mengirim bawahan, menerima laporan)	
Number of out-of-cycle enterprisewide IT risk assessments	Tidak ada pengukuran secara kuantitatif atas penilaian risiko TI secara spesifik
Jumlah penilaian risiko TI yang keluar dari siklus perusahaan secara luas	
Number of aligned policies to which intended audience has signed adherence	**Manajemen berusaha menyelaraskan konsep manajemen risiko TI dengan kebijakan yang ada** saat ini dengan mempertimbangkan kondisi dan budaya kerja yang sudah tercipta
Jumlah kebijakan yang selaras dimana audiens telah menandatangani kepatuhan	
Extent to which risk management communications and training are targeted to specific roles and responsibilities	**Manajemen risiko perusahaan belum dapat mengkomunikasikan dan memberikan pelatihan terkait risiko TI secara spesifik**, hal ini karena masih kurang memadainya SDM manajemen risiko yang ada diperusahaan.
Sejauh mana komunikasi manajemen risiko dan pelatihan yang ditargetkan untuk peran dan tanggung jawab yang spesifik.	

Tujuan Proses RG 1 ***Establish and Maintain a Common Risk View Risk Governance***

Tujuan Proses RG 1	**Fakta di perusahaan**
Ensure that risk management activities align with the enterprise's objective capacity for IT-related loss and leadership's subjective tolerance of it.	**Belum selaras** karena keterbatasan SDM TI maupun budaya kerja TI, **konsep risk manajemen TI masih belum terdokumentasi** sehingga untuk implementasinya sulit dilakukan karena **tidak dapat dikomunikasikannya konsep risk manajemen TI** tersebut ke seluruh pihak yang berkepentingan atas TI.
Pastikan bahwa kegiatan manajemen risiko sejalan dengan kapasitas tujuan perusahaan untuk TI terkait kerugian dan toleransi subjektif pemimpin atas toleransi ini.	

Metrik Proses RG 1 ***Establish and Maintain a Common Risk View Risk Governance***

Metrik Proses RG 1	**Fakta Diperusahaan**
Number of known executive level risk tolerance violations not subjected to disciplinary action (enforcement of policy)	**Pelanggaran batas toleransi terkait resiko Ti yang ada cukup sering terjadi**, hal ini dikarenakan oleh kelemahan system aplikasi yang ada. Contohnya adalah ketika terjadi suatu masalah terkait angka ataupun jumlah maka, user bisa langsung menghubungi dept TI untuk segera mengkoreksi secara langsung pada database(tidak sesuai dengan prosedur perbaikan yang benar). Sehingga **manajemen megeluarkan satu kebijakan terkait hal ini dengan mengharuskan dept TI mencatat/mendokumentasikan setiap ada perbaikan yang tidak sesuai prosedur dengan terlebih dahulu mendapatkan persetujuan dari direksi**, kebijakan ini menjadi *win-win solution* atas permasalahan yang timbul sehingga setiap penyimpangan dapat dipertanggung jawabkan dan historis penyimpangan dapat menjadi acuan dan bahan dalam hal evaluasi dan perbaikan system aplikasi perusahaan.
Jumlah pelanggaran toleransi risiko yang diketahui level eksekutif yang tidak dikenai tindakan disipliner (penegakan kebijakan)	
Number of IT-related events with business impact in which a failure to escalate was a factor in event occurrence and/or the loss magnitude and/or the loss magnitude (e.g., the risk manager did not know or there was an impaired cultural ability to escalate)	
Jumlah peristiwa terkait TI dengan dampak bisnis di mana kegagalan yang meningkat merupakan faktor dalam terjadinya peristiwa dan /atau besarnya kerugian (misalnya, manajer risiko tidak tahu atau ada gangguan kemampuan budaya untuk meningkat)	
Number of policies in force with one or more statements contradicting a related risk tolerance (alignment of IT policies with tolerance)	**Kebijakan yang bertentangan dengan toleransi risiko masih ada namun tidak terlalu banyak**, karena seiring dengan proses pembenahan yang dilakukan saat ini lambat laun diselaraskan dengan toleransi risiko yang ditetapkan
Jumlah kebijakan yang berlaku dengan satu atau lebih pernyataan yang bertentangan dengan toleransi risiko yang terkait (keselarasan kebijakan TI dengan toleransi)	
Number of IT risk issues that exceed risk tolerance	**Risiko terkait TI yang terjadi saat ini masih dalam batas wajar**, belum pernah terjadi risiko yang menimbulkan dampak yang potensial bagi kegiatan perusahaan
Jumlah isu risiko TI yang melebihi toleransi risiko	

Tujuan Aktivitas RG 2 *Integrate with ERM*

Tujuan Aktivitas Risk IT	**Fakta Di Perusahaan**
Establish enterprise-wide accountability for managing IT risk.	Perusahaan menerapkan prinsip kehati-hatian dalam kegiatannya. **Selalu memperhitungkan segala aspek risiko dalam mengambil keputusan** operasional maupun kebijakan-kebijakan yag berlaku umum dalam perusahaan. **Perusahaan memahami risiko dengan mengawasi 7 aspek perusahaan**, yaitu risiko dari proses marketing, risiko dari proses operasional, risiko dari proses IT, risiko dari proses legal, risiko dari proses audit internal, dan risiko dari proses pengelolan SDM
Membangun akuntabilitas perusahaan secara luas untuk mengelola risiko TI.	
Establish accountability for IT risk issues.	
Membangun akuntabilitas untuk isu-isu risiko TI.	
Co-ordinate IT risk strategy and business risk strategy.	**Risiko TI melekat pada business *process capture* yang akurat, disertai pelekatan fungsi-fungsi control terhadap tiap-tiap risiko** yang mungkin timbul ditiap bisnis proses tersebut. Namun dalam prosesnya pengawasan terhadap pelaksanaan fungsi-fungsi kontrol tersebut masih **terdapat keterbatasan SDM** dalam mengelola risiko terkait TI.
Mengkoordinasikan strategi risiko TI dengan strategi risiko bisnis.	
Adapt IT risk management practices to organisational risk management practices.	
Mengadaptasikan praktik manajemen risiko IT untuk praktek manajemen risiko organisasi.	
Provide adequate resources for IT risk management.	
Menyediakan sumber daya yang memadai untuk manajemen risiko TI.	

Metrik Aktivitas RG 2 *Integrate with ERM*

Metrik Aktivitas Risk IT	Fakta Diperusahaan
Percentage of employees whose performance metrics and rewards reflect risk management objectives	Dalam menilai dan mengidentifikasi risiko, **manajemen menugaskan analis sistem yang langsung bertanggung jawab ke Direksi dalam hal pelaporan atas aktivitasnya**. Analis sistem berfungsi juga sebagai QC atas pengelolaan TI di perusahaan dan melakukan analisa resiko-resiko yang mungkin terjadi yang mengakibatkan kerugian yang dilakukan secara kontinyu sesuai dengan skala prioritasnya.
Persentase karyawan yamg matrik kinerja dan *rewards nya* mencerminkan tujuan manajemen risiko	
An alignment score related to RACI regarding the ranking of actions to take (e.g., percentage of key IT risk-related accountabilities accepted by business and IT personnel)	Dalam hal terjadinya resiko terkait TI, **manajer TI sebagai penanggung jawab dalam pengelolaan TI perusahaan memberikan laporan ke direksi terkait permasalahan yang terjadi dan memberikan laporan progress penyelesaian atas masalah tersebut.**
Menilai keselarasan yang dihubungkan dengan RACI berdasarkan peringkat dalam mengambil tindakan (misalnya, persentase utama risiko TI terkait akuntabilitas yang diterima oleh bisnis dan personil TI)	
Number of different risk reports provided to the board; extent of integration of reporting on IT risk	Laporan hasil analisa yang dilaporkan ke direksi berisi mengenai permasalahan yang terjadi, dampaknya, dan memberikan rekomendasi atas permasalahan yang terjadi. **Sejauh ini laporan hasil analisa sangat mendukung dalam pengambilan keputusan manajemen**
Jumlah perbedaan laporan risiko yang disajikan kepada dewan; sejauh mana tingkat integrasi pelaporan risiko TI	
Percentage of IT risk practices adapted to ERM organisational expectations	Dalam penerapannya, **praktek risiko TI masih belum maksimal**, hal ini disebabkan masih lemahnya infrastruktur dalam mendukung pengelolaan risiko TI
Persentase praktek risiko TI yang diadaptasikan dengan ERM sesuai harapan organisasi	
Percent of IT risk management action plans approved for implementation	**Tindakan manajemen risiko TI dilakukan ketika terjadi risiko TI itu sendiri**, hal ini yang menyebabkan terlambatnya penanganan atas risiko yang terjadi
Persentase dari perencanaan tindakan manajemen risiko TI yang disetujui untuk diimplemetasikan	
Percentage of core ERM activities with embedded IT risk considerations	**Risiko TI melekat pada business *process capture* yang akurat, disertai pelekatan fungsi-fungsi control terhadap tiap-tiap risiko** yang mungkin timbul **ditiap bisnis proses** tersebut. Namun dalam prosesnya pengawasan terhadap pelaksanaan fungsi-fungsi kontrol tersebut masih **terdapat keterbatasan SDM** dalam mengelola risiko terkait TI.
Persentase kegiatan inti ERM dengan pertimbangan risiko TI yang melekat	
Number of different issue management processes and platforms	Tidak ada pengukuran secara kuantitatif atas aktivitas ini
Jumlah isu proses manajemen yang berbeda dengan platform	
Extent to which budgets are allocated based on risk significance (e.g., per risk assessment results)	Perusahaan sangat tergantung terhadap TI dalam menunjang kegiatan operasional perusahaan yang didukung dengan infrastruktur TI yang cukup memadai baik SDM maupun perangkat TI lainnya. **Jumlah SDM TI saat ini masih cukup** dalam menunjang dan melayani kegiatan operasional perusahaan, sedangkan untuk infrastruktur penunjang lainnya disesuaikan dengan kebutuhan perusahaan dengan **mempertimbangkan cost & benefit nya.**
Sejauh mana anggaran dialokasikan berdasarkan signifikansi risiko (misalnya, per hasil penilaian resiko)	
Number of open positions in the risk management staff	
Jumlah posisi yang dibutuhkan di staf manajemen risiko	

Tujuan Proses RG 2 *Integrate with ERM*

Tujuan Proses	**Fakta di perusahaan**
Integrate the IT risk strategy and operations with the business strategic risk decisions that have been made at the enterprise level.	**Risiko dipertimbangkan dengan menimbang magnitude risk nya menciptakan toleransi risiko yang dapat diterima perusahaan**.Pengecualian diberikan dengan syarat-syarat yang ketat, dan peningkatan awareness terhadap risiko yang melekat.
Mengintegrasikan strategi dan kegiatan risiko TI dengan keputusan risiko bisnis strategis yang telah dibuat di tingkat perusahaan.	

Metrik Proses RG 2 *Integrate with ERM*

Metrik Proses Risk IT	**Fakta Diperusahaan**
Percentage of business executives and managers who have received training on the enterprise's reliance on and usage of IT, the related risk, IT risk strategy and framework	**Pelatihan yang dilaksanakan perusahaan dalam pengelolaan risiko TI masih kurang diminati,** hal ini dapat terlihat dari jumlah kehadiran level manajer perusahaan dengan mengirim bawahannya sebagai penggantinya
Persentase eksekutif perusahaan dan manajer yang telah menerima pelatihan di perusahaan yang memiliki ketergantungan pada dan penggunaan TI, terkait risiko , strategi risiko TI dan kerangkanya	
Percentage of IT risk management operational expenditures that have direct traceability to business risk strategy	**Tidak ada pengukuran terkait pengeluaran operasional manajemen risiko TI** yang dapat ditelusuri secara langsung ke strategi risiko bisnis
Persentase pengeluaran operasional manajemen risiko TI yang dapat ditelusuri secara langsung ke strategi risiko bisnis	
Percentage of business projects that consider IT risk	**Risiko dipertimbangkan dengan menimbang *magnitude risk*** nya menciptakan toleransi risiko yang dapat diterima perusahaan.Pengecualian diberikan dengan syarat-syarat yang ketat, dan peningkatan awareness terhadap risiko yang melekat.
Persentase proyek bisnis yang mempertimbangkan risiko TI	
Percentage of core ERM activities that consider IT risk	
Persentase kegiatan ERM inti yang mempertimbangkan risiko TI	
Frequency of IT risk as an agenda item for the executive committee	Laporan hasil analisa TI dilaporkan ke direksi, biasanya direksi memberikan tanggapan dengan memberi arahan dan masukan atas temuan yang dibahas dalam rapat manajemen. **Rapat yg membahas masalah TI cukup sering dilakukan yg dihadiri oleh manajemen**, hal ini sebagai bukti keseriusan manajemen dalam pengelolaan TI di perusahaan
Frekuensi risiko TI sebagai item agenda untuk komite eksekutif	
Extent of alignment between organisational objectives and IT risk management objectives	**Belum selaras karena budaya kerja yang tertanam masih dirasakan kurangnya kesadaran atas resiko terkait TI** dan sistem aplikasi yang masih dalam tahap pengembangan.
Tingkat keselarasan antara tujuan organisasi dan tujuan pengelolaan risiko TI	
Extent of overlap of risk management activities performed by business units, risk and control functions, and internal audit	**Manajemen telah memetakan fungsi kontrol atas risiko** maupun penyimpangan yang mungkin terjadi, **sehingga tidak terjadi tumpang tindih dalam menjalankan fungsinya masing-masing**
Tingkat tumpang tindih kegiatan manajemen risiko yang dilakukan oleh unit-unit bisnis, fungsi risiko dan kontrol, dan internal audit.	

Tujuan Aktivitas RG 3 *Make Risk-aware Business Decisions*

Tujuan Aktivitas Risk IT	**Fakta Di Perusahaan**
Gain management buy-in for the IT risk analysis approach.	**Risiko dipertimbangkan dengan menimbang *magnitude risk*** nya **menciptakan toleransi risiko yang dapat diterima** perusahaan.Pengecualian diberikan dengan syarat-syarat yang ketat, dan peningkatan awareness terhadap risiko yang melekat.
Keuntungan manajemen buy-in untuk pendekatan analisis risiko TI.	
Approve IT risk analysis results.	
Menyetujui hasil analisis risiko TI.	
Embed IT risk considerations into strategic business decision making.	
Melekatkan pertimbangan risiko TI ke dalam pengambilan keputusan bisnis strategis.	
Accept IT risk.	
Menerima risiko TI.	
Prioritise IT risk response activities.	**Manajemen telah memetakan fungsi kontrol atas risiko** maupun penyimpangan yang mungkin terjadi, sehingga tidak terjadi tumpang tindih dalam menjalankan fungsinya masing-masing
Memprioritaskan kegiatan respon risiko TI	
Track key IT risk decisions	
Melacak keputusan resiko TI utama	

Metrik Aktivitas RG 3 *Make Risk-aware Business Decisions*

Metrik Aktivitas Risk IT	**Fakta Diperusahaan**
Percentage of business decisions that should have considered IT risk but did not	Ya, Keputusan manajeman atas resiko TI didukung oleh laporan hasil analisa, namun **ada beberapa yang tidak didukung oleh laporan hasil analisa.**
Persentase keputusan bisnis yang seharusnya dianggap risiko TI tetapi tidak	
Number and size of adverse events/losses arising out of risk acceptance decision, including opportunity losses	Tidak ditemukan adanya kerugian yang disebabkan oleh pengambilan keputusan penerimaan batas toleransi risiko TI yang **mengakibatkan kerugian perusahaan dari sisi keuangan namun dari sisi waktu dan kesempatan ada tapi tidak cukup potensial**
Jumlah dan ukuran kejadian kerugian yang timbul dari keputusan penerimaan risiko, termasuk kerugian kesempatan	
Percentage of accepted IT risks with a complete set of supporting documentation	Dalam memutuskan batasan toleransi risiko TI yang dapat diterima atau tidak, **manajemen mendasarkan keputusannya dari hasil analisa dan data historis sebagai data pendukung pengambilan keputusan**
Persentase menerima risiko TI dengan satu set lengkap dokumentasi pendukung	
Number of prioritised risk response activities	kegiatan **penanggulangan atas risiko TI yang terjadi cukup sering dilakukan** karena masih lemahnya pengelolaan sistem maupun infrastruktur TI perusahaan
Jumlah kegiatan penanggulangan risiko diprioritaskan	
Percentage of IT risk issues for which the expected reduction in frequency and magnitude is tracked	Dengan menganalisa isu-isu risiko yang ada**, diharapkan dapat mengurangi terjadinya risiko terkait kegagalan TI**
Persentase isu-isu risiko TI yang diharapkan mengurangi frekuensi dan magnitudonya yang dapat dilacak	

Tujuan Proses RG 3 *Make Risk-aware Business Decisions*

Tujuan Proses	**Fakta di perusahaan**
Ensure that organisational decisions consider the full range of opportunities and consequences arising from reliance on IT for success.	**Manajemen cukup mengetahui masalah atas resiko yang timbul yang melewati batasan toleransi**. Direksi sudah memiliki perencanaan atas permasalahan yang terjadi walaupun belum terdokumentasi. **Direksi mengkategorikan resiko yang ada menjadi dua yaitu resiko yang terdeteksi dan resiko yang tidak terdeteksi**. Untuk risiko yang terdeteksi direksi memiliki perencanaan penanggulangan nya sedangkan yg tdk terdeteksi dijadikan sebuah bahan evaluasi yang biasanya diangkat ke meja rapat. Dalam pembahasan terkait risiko TI biasanya dihadiri oleh level manajer atau stafnya.
Memastikan bahwa keputusan organisasi mempertimbangkan berbagai peluang dan konsekuensi yang timbul dari ketergantungan pada TI untuk mencapai tujuan	

Metrik Proses RG 3 *Make Risk-aware Business Decisions*

Metrik Proses Risk IT	**Fakta Diperusahaan**
Value of failed projects due to issues not identified during the decision-making process (e.g., was the risk presented on the risk log? Was it estimated properly?Was there follow-through on it?)	**Tidak ditemukan adanya kerugian yang disebabkan oleh pengambilan keputusan penerimaan batas toleransi risiko TI yang mengakibatkan kerugian perusahaan** dari sisi keuangan namun dari sisi waktu dan kesempatan ada tapi tidak cukup potensial
Nilai proyek-proyek gagal karena masalah tidak diidentifikasi selama proses pengambilan keputusan (misalnya, adalah resiko disajikan pada log risiko? Apakah itu diperkirakan dengan benar? Apakah ada tindak lanjut di atasnya?)	
Number of key management decisions made without the availability of a relevant risk analysis report	Ya, Keputusan manajeman atas resiko TI didukung oleh laporan hasil analisa, namun **ada beberapa yang tidak didukung oleh laporan hasil analisa.**
Jumlah keputusan manajemen kunci dibuat tanpa ketersediaan laporan analisis risiko yang relevan	
Percentage of decisions (or indecision) leading to IT-related loss revisited for lessons learned	Dept TI mendokumentasikan setiap risiko yang terjadi dalam form IT service request dengan lengkap namun **atas peristiwa tersebut tidak dilakukan review dan ditindak lanjuti**, sehingga peristiwa ini akan terulang kembali dimasa yang akan datang
Persentase keputusan (atau keraguan) mengarah ke kerugian terkait TI ditinjau kembali untuk pelajaran	
Cycle time from the discovery of a control deficiency (e.g., vulnerability event) to a risk acceptance decision	**Tidak ditemukan pengukuran yang baku atas jangka waktu yang diperlukan** dari menemukan kelemahan kontrol ke penerimaan risiko
Waktu yang diperlukan dari menemukan kelemahan kontrol (misalnya, kerentanan peristiwa) ke keputusan penerimaan risiko	
Cycle time from reported policy exceptions to a decision on their disposition	**Tidak ditemukan pengukuran yang baku atas jangka waktu yang diperlukan** dari pengecualian kebijakan yang dilaporkan ke keputusan disposisi mereka
Waktu yang diperlukan dari pengecualian kebijakan yang dilaporkan ke keputusan disposisi mereka	

Risk Evaluate

Tujuan Aktivitas RE 1 *Collect Data*

Tujuan Aktivitas Risk IT	**Fakta Di Perusahaan**
Establish and maintain a model for data collection.	Dalam **menganalisa resiko TI dilakukan observasi terhadap aktivitas terkait TI**, yang dapat **dilakukan dengan cara wawancara, review catatan atas masalah yang terjadi, review hasil temuan internal audit.** Data sumber identifikasi resiko TI didapatkan dari user dan pihak internal TI perusahaan
Membangun dan mempertahankan model untuk pengumpulan data.	
Collect data on the external environment.	
Mengumpulkan data pada lingkungan eksternal.	
Collect timely event, incident, problem and loss data.	Sudah, kesemuanya **dilakukan sebelum proyek dimulai**. Bahkan untuk **proyek yang bernilai tertentu perlu mendapat persetujuan komite di *Holding* perusahaan untuk dianalisa risiko dan tingkat kontrolnya, identifikasi biaya dan manfaat proyek tersebut.**
Mengumpulkan data yang tepat waktu acara, insiden, masalah dan kerugian.	
Identify risk factors.	
Mengidentifikasi faktor risiko.	
Organise historical IT risk data.	
Mengorganisir data risiko historis TI.	

Metrik Aktivitas RE 1 *Collect Data*

Metrik Aktivitas Risk IT	**Fakta Diperusahaan**
Existence of a defined and documented risk-related data collection model	Dalam menganalisa resiko TI dilakukan **observasi terhadap aktivitas terkait TI**, yang dapat dilakukan dengan cara **wawancara, review catatan atas masalah yang terjadi, review hasil temuan internal audit**, **data sumber identifikasi resiko TI didapatkan dari user dan pihak internal TI** perusahaan
Adanya model pengumpulan data terkait risiko didefinisikan dan didokumentasikan	
Number of sources used for data collection	
Jumlah sumber yang digunakan untuk pengumpulan data	
Completeness of event data against established standards (e.g., affected assets, impact data, threat community, actions). This includes both discrete event data (e.g., control 'yes' or 'no') and continuous data (e.g., ongoing stream data on server response time).	**Dept TI mendokumentasikan setiap risiko yang terjadi dalam form IT service request dengan lengkap** namun atas peristiwa tersebut tidak dilakukan review dan ditindak lanjuti, sehingga peristiwa ini akan terulang kembali dimasa yang akan datang
Kelengkapan data peristiwa terhadap standar yang ditetapkan (misalnya, aset yang terkena dampak, data dampak, komunitas ancaman, tindakan). Ini mencakup baik data kejadian diskrit (misalnya, kontrol 'ya' atau 'tidak') dan data kontinu (misalnya, aliran data yang sedang berlangsung pada waktu respon server).	
Number of data items for which the contributing factors have been identified	Data atas risiko yang teridentifikasi terdokumentasi dengan lengkap di Dept TI sehingga memudahkan proses analisa
Jumlah item data di mana faktor telah diidentifikasi	
Completeness of historical data across the top classes of IT risk	
Kelengkapan data historis di kelas atas risiko TI	

Tujuan Proses RE 1 *Collect Data*

Tujuan Proses	**Fakta di perusahaan**
Identify relevant data to enable effective IT-related risk identification, analysis and reporting.	Dalam menganalisa resiko TI d**ilakukan observasi terhadap aktivitas terkait TI, yang dapat dilakukan dengan cara wawancara, review catatan atas masalah yang terjadi, review hasil temuan internal audit**, data sumber identifikasi resiko TI didapatkan dari user dan pihak internal TI perusahaan
Mengidentifikasi data yang relevan untuk memungkinkan efektif terkait TI identifikasi risiko, analisis dan pelaporan.	

Metrik Proses RE 1 *Collect Data*

Metrik Proses Risk IT	**Fakta Diperusahaan**
Number of loss events with key characteristics not captured in some form of repository	Peristiwa yang menimbulkan k**erugian yang tidak terdeteksi sebelumnya cukup sering terjadi**, hal ini disebabkan oleh lemahnya sistem
Jumlah peristiwa kerugian dengan karakteristik utama yang tidak tertangkap dalam beberapa bentuk repositori	
Degree to which collected data supports reporting of trends and scenario analysis	**Data historis atas resiko yg timbul sudah tercatat dan cukup lengkap**, karena setiap kali ada permasalahan terkait TI yang terjadi tercatat dalam form IT service request
Tingkat data yang dikumpulkan yang dapat mendukung pelaporan analisis tren dan skenario	
The degree of visibility and recognition into the control state provided by data collection	Ada, Dept TI sudah melakukan dokumentasi dalam mengatasi permasalahan yang ada namun belum diimplementasikan dengan sempurna**. Dokumentasi ini menjadi dasar historis dalam perencanaan penanggulangan permasalahan yang terjadi terkait resiko IT**
Tingkat visibilitas dan pengakuan atas kontrol yang dihasilkan pengumpulan data	
The degree of visibility and recognition into the threat landscape provided by data collection	
Tingkat visibilitas dan pengakuan ke lanskap ancaman yang dihasilkan dari data yang terkumpul	

Tujuan Aktivitas RE 2 *Analyse Risk*

Tujuan Aktivitas Risk IT	**Fakta Di Perusahaan**
Define IT risk analysis scope.	Pencatatan data historical **atas peristiwa/kesalahan yang terjadi, melihat dampak dan frekuensinya, peristiwa yang berdampak terbesar dan berfrekuensi tinggi** merupakan pengkategorian risiko tinggi dan perlu **penanganan untuk mitigasi risikonya**.
Tentukan lingkup analisis risiko TI.	
Estimate IT risk to and from critical products, services, processes and IT resources.	
Perkiraan risiko TI ke dan dari produk kritis, jasa, proses dan sumber daya TI.	
Identify risk response options.	
Mengidentifikasi opsi-opsi risiko respon.	
Perform a peer review of IT risk analysis results.	
Melakukan peer review TI hasil analisis risiko.	

Metrik Aktivitas RE 2 *Analyse Risk*

Metrik Aktivitas Risk IT	**Fakta Diperusahaan**
Percentage of time analyses are substantiated by later experience or testing (accuracy)	**Belum pernah dilakukan pengukuran atas waktu yang dibutuhkan** dalam melakukan pengujian atas akurasi hasil analisa
Persentase waktu analisis yang didukung oleh pengalaman atau pengujian (akurasi) sebelumnya	
Percentage of time peer review finds no significant logical, calculation or incompleteness errors (defensibility)	Pengujian atas system **hanya menguji keakuratan kalkulasinya, cukup informative atau tidak bagi user**. Lebih ke interface dan hasil antara input dan output
Persentase waktu *peer review yang* tidak signifikan menemukan *Error logical* , kalkulasi atau kesalahan ketidaklengkapan (defensibility)	
Percentage of time parallel assessments on the same scenarios performed by different analysts get the same results (consistency)	**Belum pernah dilakukan analisa atas risiko TI perusahaan oleh pihak eksternal**
Persentase waktu penilaian paralel pada skenario yang sama yang dilakukan oleh analis yang berbeda dengan hasil yang sama (konsistensi)	
Percentage of time analyses are performed by trained analysts (higher-level metric related to accuracy, defensibility and consistency)	Belum pernah dilakukan analisis oleh *trained analysts*
Persentase waktu aalisis yang dilakukan oleh analis	
A ‘satisfaction index’ over risk analysis reporting (e.g., the percentage of favourable satisfaction survey responses from business executives regarding the readability, usefulness and accuracy of risk analysis reports)	**Manajemen cukup puas atas hasil laporan analisa yang dilaporkan**
Sebuah 'indeks kepuasan' atas analisis pelaporan resiko (misalnya, persentase tanggapan survei kepuasan baik dari eksekutif bisnis tentang pembacaan, kegunaan dan akurasi laporan analisis risiko)	
Ratio of cumulative actual losses to expected loss magnitude	Kemampuan TI Saat ini cukup **berkontribusi dalam menahan terjadinya kerugian perusahaan**, seperti control waktu terhadap invoicing, nyata-nyata memberi manfaat terhadap penghematan cost of money
Rasio kerugian aktual kumulatif untuk besarnya kerugian yang diperkirakan	

Tujuan Proses RE 2 *Analyse Risk*

Tujuan Proses	**Fakta di perusahaan**
Develop useful information to support risk decisions that take into account the business relevance of risk factors (e.g., threats, vulnerabilities, value, liability).	**Laporan analisis risiko dijadikan sebagai input untuk mitigasi risiko itu sendiri, serta pertimbangan penempatan control yang tepat, dengan selalu mengukur probabilitas risiko terbesar** ditangani dengan lebih berhati-hati, tingkat kesalahan yang tinggi dihadapi dengan pemberian control bertahap/berlapis
Mengembangkan informasi yang berguna untuk mendukung keputusan risiko yang memperhitungkan relevansi bisnis dari faktor risiko (misalnya, ancaman, kerentanan, nilai, kewajiban).	

Metrik Proses RE 2 *Analyse Risk*

Metrik Proses Risk IT	**Fakta Diperusahaan**
Percentage of risks for which the probable frequency of occurrence and the probable magnitude of the business impact are measured within the scope	**Perkiraan kemungkinan frekuensi kejadian** dan besarnya dampak bisnis dan perkiraan jumlah maksimum kerusakan yang dapat diderita yaitu dengan **menggunakan acuan *historical record***
Persentase risiko yang kemungkinan frekuensi kejadian dan besarnya kemungkinan dampak bisnis yang dapat diukur dalam lingkup	
Percentage of highly ranked assets, targets and resources reviewed for the effect of known operational controls	**Belum ditemukan pengukuran atas pengendalian operasional yang diketahui**
Persentase aset yang berperingkat tinggi, target dan sumber daya direview untuk mengetahui dampak pengendalian operasional dikenal	
Percentage of risk analysis undergoing peer review before being sent to management	Hasil analisa risiko selalu **dilakukan review dan pengujian keakuratannya sebelum disampaikan/dilaporkan ke manajemen**
Persentase analisis risiko menjalani peer review sebelum dikirim ke manajemen	

Tujuan Aktivitas RE 3 *Maintain Risk Profile*

Tujuan Aktivitas Risk IT	**Fakta Di Perusahaan**
Map IT resources to business processes.	Pemetaan risiko dalam lingkup asset dan trigger TI **dilakukan dengan memetakan setiap proses yang terlibat dalam pengelolaan asset TI**, lalu dilakukan **review atas proses tersebut**, **bagian-bagian mana yang mengandung risiko tertentu, dikombinasikan dengan *incident record* untuk membantu pengukuran jenis risiko tinggi/rendah.**
Memetakan sumber daya TI untuk proses bisnis.	
Determine the business criticality of IT resources.	
Tentukan kekritisan bisnis sumber daya TI.	
Understand IT capabilities.	
Memahami kemampuan IT.	
Connect threat types and business impact categories.	
Hubungkan jenis ancaman dan kategori dampak bisnis.	
Maintain the IT risk register and IT risk map.	
Menjaga daftar risiko TI dan peta risiko TI.	
Design and communicate IT risk indicators.	Batasan toleransi atas resiko TI yang dapat diterima sudah ada dalam konsep pemikiran manajemen namun **belum didokumentasikan dan didefinisikan secara jelas, sehingga belum dapat dikomunikasikan secara jelas dan meyeluruh** kepada stakeholder.
mendesain dan mengkomunikasikan indikator risiko TI.	

Metrik Aktivitas RE 3 *Maintain Risk Profile*

Metrik Aktivitas Risk IT	**Fakta Diperusahaan**
Percentage of key business activities with a dependency linkage to supporting IT resources and IT infrastructure resources	**Perusahaan sangat tergantung terhadap TI dalam menunjang kegiatan operasional** perusahaan yang didukung dengan infrastruktur TI yang cukup memadai baik SDM maupun perangkat TI lainnya
Persentase kegiatan bisnis utama dengan hubungan ketergantungan untuk mendukung sumber daya TI dan sumber daya infrastruktur TI	
Percentage of the critical elements of the IT portfolio covered by risk triggers and thresholds	**Tidak ditemukan pengukuran atas elemen-elemen penting dari portofolio TI**
Persentase dari elemen-elemen penting dari portofolio TI di*cover* oleh pemicu dan ambang risiko	
Number of realised events with business impact not detected by a trigger mechanism	Peristiwa yang terjadi yang mempengaruhi proses bisnis terkait TI yang tidak terdeteksi dan teridentifikasi sebelumnya **cukup sering terjadi namun masih dalam batas wajar**
Jumlah kejadian diwujudkan dengan dampak bisnis tidak terdeteksi oleh mekanisme pemicu	

Tujuan Proses RE 3 *Maintain Risk Profile*

Tujuan Proses	**Fakta di perusahaan**
Maintain an up-to-date and complete inventory of known risks and attributes (e.g., expected frequency, potential impact, disposition), IT resources, capabilities, and controls as understood in the context of business products, services, and processes.	**Pencatatan data historical atas peristiwa/kesalahan yang terjadi, melihat dampak dan frekuensinya**, peristiwa yang berdampak terbesar dan berfrekuensi tinggi merupakan pengkategorian risiko tinggi dan perlu penanganan untuk mitigasi risikonya.
Menjaga up-to-date dan kelengkapan inventarisir risiko yang dikenal dan atributnya (misalnya, frekuensi yang diharapkan, dampak potensial, disposisi), sumber daya TI, kemampuan, dan kontrol seperti yang dipahami dalam konteks produk bisnis, jasa, dan proses.	

Metrik Proses RE 3 *Maintain Risk Profile*

Metrik Proses Risk IT	**Fakta Diperusahaan**
Number of approved risk analysis results not yet incorporated into the risk profile	**Setiap risiko yang berhasil diidentifikasi didokumentasikan untuk selanjutnya dikategorikan kedalam beberapa kategori** untuk penanganan mitigasi risikonya
Jumlah hasil analisis risiko yang disetujui belum dimasukkan ke dalam profil risiko	
Percentage of critical business services not covered by risk analysis	Peristiwa yang terjadi yang mempengaruhi proses bisnis terkait TI yang tidak terdeteksi dan teridentifikasi sebelumnya **cukup sering terjadi namun masih dalam batas wajar**
Persentase layanan bisnis penting yang tidak tercakup oleh analisis risiko	
Completeness of key risk data attributes across the IT risk register	**Daftar risiko sudah ada** namun blm terdokumentasi secara lengkap, resiko dikategorikan menjadi 3 macam kategori yaitu Major, Middle dan Minor
Kelengkapan atribut data utama risiko di seluruh daftar risiko TI	

Risk Response

Tujuan Aktivitas RR 1 *Articulate Risk*

Tujuan Aktivitas Risk IT	**Fakta Di Perusahaan**
Report IT risk analysis results.	**Laporan hasil analisa TI dilaporkan ke direksi, biasanya direksi memberikan tanggapan dengan memberi arahan dan masukan atas temuan yang dibahas dalam rapat manajemen**. Rapat yg membahas masalah TI cukup sering dilakukan yg dihadiri oleh level manajemen, hal ini sebagai bukti keseriusan manajemen dalam pengelolaan TI di perusahaan
Laporan hasil analisis risiko TI.	
Report IT risk management activities and state of compliance.	
Laporan kegiatan manajemen risiko TI dan kepatuhan.	
Interpret external IT assessment findings.	
Menafsirkan temuan penilaian eksternal TI.	
Identify IT-related opportunities.	
Mengidentifikasi peluang yang berkaitan dengan IT.	

Metrik Aktivitas RR 1 *Articulate Risk*

Metrik Aktivitas Risk IT	**Fakta Diperusahaan**
Percentage of risk analysis reports accepted on initial delivery	Laporan hasil analisa TI dilaporkan ke direksi, **biasanya direksi memberikan tanggapan dengan memberi arahan dan masukan atas temuan** yang dibahas dalam rapat manajemen. **Rapat yg membahas masalah TI cukup sering dilakukan yg dihadiri oleh level manajemen**, hal ini sebagai bukti keseriusan manajemen dalam pengelolaan TI di perusahaan
Persentase laporan analisis risiko yang diterima pada pengiriman awal	
Frequency of risk management activity reporting	
Frekuensi pelaporan aktivitas manajemen risiko	
Number of IT-related events with business impact not previously reported as an IT risk	Ada namun **frekuensinya tidak banyak**, hal ini disebabkan karena kurangnya pemahaman mengenai manajemen risiko TI
Jumlah peristiwa terkait TI dengan dampak bisnis yang sebelumnya tidak dilaporkan sebagai risiko TI	
Number of IT risk issues identified by outside parties yet to be interpreted and mapped into risk profile	**Belum pernah dilakukan analisa** terkait isu-isu risiko TI yang dilakukan **pihak eksternal perusahaan**
Jumlah isu risiko TI yang diidentifikasi oleh pihak luar masih harus ditafsirkan dan dipetakan ke dalam profil risiko	

Tujuan Proses RR 1 *Articulate Risk*

Tujuan Proses	**Fakta di perusahaan**
Ensure that information on the true state of IT-related exposures and opportunities is made available in a timely manner and to the right people for appropriate response.	Pemetaan risiko dalam lingkup asset dan trigger TI dilakukan dengan **memetakan setiap proses yang terlibat dalam pengelolaan asset TI, lalu dilakukan review atas proses tersebut, bagian-bagian mana yang mengandung risiko tertentu, dikombinasikan dengan incident record untuk membantu pengukuran jenis risiko tinggi/rendah.**
Memastikan bahwa informasi tentang keadaan sebenarnya dari eksposur yang berkaitan dengan IT dan kesempatan yang tersedia pada waktu yang tepat dan kepada orang yang tepat untuk respon yang tepat.	

Metrik Proses RR 1 *Articulate Risk*

Metrik Proses Risk IT	**Fakta Diperusahaan**
Percentage of risk issues inappropriately distributed too high or too low in the organisational hierarchy (and consequently sent up or down the chain of command for decision)	Pemetaan risiko dalam lingkup asset dan trigger TI dilakukan dengan memetakan setiap proses yang terlibat dalam pengelolaan asset TI, lalu **dilakukan review atas proses tersebut, bagian-bagian mana yang mengandung risiko tertentu, dikombinasikan dengan incident record untuk membantu pengukuran jenis risiko tinggi/rendah**.
Persentase isu-isu risiko didistribusikan tidak tepat terlalu tinggi atau terlalu rendah dalam hirarki organisasi (dan akibatnya dikirim keatas atau dibawah rantai komando untuk pengambilan keputusan)	
The number of IT-related events with business impact not earlier reported as an IT risk	Gangguan system yang terkait resiko TI **cukup sering terjadi** mulai dari gangguan yg kecil maupun yg besar. Direksi banyak mengetahui masalah TI yg terjadi baik dari hasil analisa maupun temuan internal audit dan biasanya memberikan solusi atas pelanggaran toleransi tsb.
Jumlah peristiwa terkait TI dengan dampak bisnis sebelumnya tidak dilaporkan sebagai risiko TI	
Percentage of critical IT assets covered by monitoring activities (detectability)	Sudah, **persyaratan tingkat tinggi untuk proyek-proyek atau program yang ada berdasarkan toleransi risiko** yang diharapkan **dapat mengurangi risiko yang dapat diterima** atau mengurangi tingkat kontrol yang ada, mengidentifikasi biaya, manfaat dan tanggung jawab untuk eksekusi proyek dilakukan sebelum proyek dimulai. Bahkan **untuk proyek yang bernilai tertentu perlu mendapat persetujuan komite di *Holding* perusahaan untuk dianalisa risiko dan tingkat kontrolnya, identifikasi biaya dan manfaat proyek tersebut.**
Persentase aset TI penting yang dicakup oleh kegiatan pemantauan (terdeteksi)	
Timeliness of reports on IT exposures relative to the next expected threat or loss event	Tidak ada pengukuran atas ketepatan waktu pelaporan
Ketepatan waktu laporan tentang eksposur TI relatif terhadap ekspektasi ancaman berikutnya atau peristiwa kehilangan	
Potential business impact of exposures (as agreed by management) discovered by assurance groups	**Risiko terkait TI yang terjadi saat ini masih dalam batas wajar**, belum pernah terjadi risiko yang menimbulkan dampak yang potensial bagi kegiatan perusahaan
Eksposur dampak bisnis yang potensial (sebagaimana disetujui oleh manajemen) ditemukan oleh kelompok jaminan	

Tujuan Aktivitas RR 2 *Manage IT Risk*

Tujuan Aktivitas Risk IT	**Fakta Di Perusahaan**
Inventory controls, capabilities and resources.	Sudah, **persyaratan tingkat tinggi untuk proyek-proyek atau program yang ada berdasarkan toleransi risiko** yang diharapkan **dapat mengurangi risiko yang dapat diterima** atau mengurangi tingkat kontrol yang ada, mengidentifikasi biaya, manfaat dan tanggung jawab untuk eksekusi proyek dilakukan sebelum proyek dimulai. Bahkan **untuk proyek yang bernilai tertentu perlu mendapat persetujuan komite di *Holding* perusahaan untuk dianalisa risiko dan tingkat kontrolnya, identifikasi biaya dan manfaat proyek tersebut.**
Kontrol persediaan, kemampuan dan sumber daya.	
Monitor operational alignment with risk tolerance thresholds.	
Memantau keselarasan operasional dengan batas toleransi risiko.	
Respond to discovered risk exposure and opportunity.	
Menanggapi eksposur temuan dan peluang risiko	
Implement controls.	
Melaksanakan kontrol.	
Report on IT risk action plan progress.	Ya ada, laporan hasil analisa menjadi indicator dalam mempengaruhi pengambilan keputusan manajemen terkait kebijakan risiko TI perusahaan, **report ini dibuat oleh analis dan dilaporkan kepada direksi**.
Laporan progress perencanaan tindakan risiko TI	

Metrik Aktivitas RR 2 *Manage IT Risk*

Metrik Aktivitas Risk IT	**Fakta Diperusahaan**
Percentage of controls that are directly related to maintaining the defined risk tolerance	Saat ini pembenahan dalam **pengelolaan TI terutama difokuskan pembenahan fungsi kontrol** yang ada disetiap proses bisnis perusahaan sehingga dapat meminimalisir potensi kerugian yang mungkin terjadi
Persentase kontrol yang berhubungan langsung untuk memelihara toleransi risiko yang terdefinisi	
Percentage of IT risk issues exceeding defined risk tolerance for which action plans have been established (alternatively, percentage of mitigation plans that have not been developed)	**Risiko terkait TI yang terjadi saat ini masih dalam batas wajar**, belum pernah terjadi risiko yang menimbulkan dampak yang potensial bagi kegiatan perusahaan
Persentase isu risiko TI yang melebihi toleransi risiko yang ditetapkan untuk rencana aksi yang telah ditetapkan (alternatif, persentase rencana mitigasi yang belum dikembangkan)	
Number and value of missed IT-related opportunities	Peluang **terjadinya risiko TI yang tak terhindarkan masih sering terjadi** walupun frekuensinya tidak sesering sebelum dilakukan analisa atas pengelolaan TI
Jumlah dan nilai yang tidak terjawab yang berkaitan dengan peluang TI	

Tujuan Proses RR 2 *Manage IT Risk*

Tujuan Proses	**Fakta di perusahaan**
Ensure that measures for seizing strategic opportunities and reducing IT risk to an acceptable level are managed as a portfolio.	Secara kontinyu **melakukan pemantauan terhadap efektifitas control**, pengutamaan terhadap control preventif diputuskan sebagai langkah terbijak bagi perusahaan.
Memastikan bahwa langkah-langkah untuk menangkap peluang strategis dan mengurangi risiko TI ke tingkat yang dapat diterima dikelola sebagai portofolio.	

Metrik Proses RR 2 *Manage IT Risk*

Metrik Proses Risk IT	**Fakta Diperusahaan**
Satisfaction of the risk owner regarding mitigation project outcomes	**Manajemen cukup puas atas hasil proyek mitigasi risiko**, misalnya saja pembangunan server backup sebagai antisipasi terjadinya bencana atau risiko yang dapat mengganggu kelangsungan hidup perusahaan
Kepuasan pemilik mengenai hasil proyek mitigasi risiko	
Percentage of risk mitigation plans executed on time (per management's decision, set date)	Tidak ditemukan adanya perencanaan respon insiden risiko TI secara spesifik
Persentase rencana mitigasi risiko dieksekusi pada waktunya (per keputusan manajemen, tanggal yang ditetapkan)	
Percentage of unaccepted IT risk issues without mitigation plans developed	Peluang terjadinya risiko TI yang tak terhindarkan masih terjadi walaupun frekuensinya tidak sesering sebelum dilakukan analisa atas pengelolaan TI
Persentase isu-isu risiko TI yang tidak diterima tanpa rencana pengembangan mitigasi	
Percentage of unaccepted IT risk issues with action plan developed	**Masih ada risiko TI yang terjadi** yang tidak sesuai dengan rencana tindakan yang telah disusun
Persentase isu-isu risiko TI yang tidak dapat diterima/sesuai dengan rencana tindakan yang sudah dikembangkan	
Amount of investment spent on risk mitigation efforts that are later cancelled	**Belum pernah ada investasi yang dibatalkan dalam proyek mitigasi risiko**, karena dalam setiap proyek mitigasi risiko terkait TI sudah diperhitungkan dengan akurat.
Jumlah investasi yang dihabiskan pada upaya mitigasi risiko yang kemudian dibatalkan	

Tujuan Aktivitas RR 3 *React to Events*

Tujuan Aktivitas Risk IT	**Fakta Di Perusahaan**
Maintain incident response plans.	Respon atas terjadinya resiko TI cukup cepat dan akurat dalam menanggulangi permasalahan yang terjadi terkait TI. **Dalam penanggulangan permasalahan yang terjadi sudah ada penyusunan dan pembagian tugas dalam penanggulangan TI**
Menjaga rencana respon insiden.	
Monitor IT risk.	Melakukan **pemantauan atas insiden-insiden dan mendapatkan inputan dari audit internal yang menandakan kesalahan tersebut merupakan potensi risiko dimasa yang akan dating, sehingga diperlukan langkah-langkah perbaikan.**
Memonitor risiko TI.	
Initiate incident response plans.	
Memulai rencana respon insiden .	
Conduct post-mortem reviews of IT-related incidents.	
Melakukan post-mortem review dari insiden terkait TI.	

Metrik Aktivitas RR 3 *React to Events*

Metrik Aktivitas Risk IT	**Fakta Diperusahaan**
Percentage of incident response plans past their next required review date	Tidak ditemukan adanya perencanaan respon insiden risiko TI secara spesifik
Persentase perencanaan respon insiden yang melewati tanggal review yang diperlukan	
Number of incident response plans with unresolved quality issues	Tidak ditemukan adanya perencanaan respon insiden risiko TI secara spesifik
Jumlah rencana respon insiden dengan masalah kualitas yang belum terselesaikan	
Percentage of incidents with business impact not subject to a post-mortem review	Melakukan **pemantauan atas insiden-insiden dan mendapatkan inputan dari audit internal yang menandakan kesalahan tersebut merupakan potensi risiko** dimasa yang akan datang, sehingga diperlukan langkah-langkah perbaikan.
Persentase insiden dengan dampak bisnis yang tidak tunduk pada post mortem review	

Tujuan Proses RR 3 *React to Events*

Tujuan Proses	**Fakta di perusahaan**
Ensure that measures for seizing immediate opportunities or limiting the magnitude of loss from IT-related events are activated in a timely manner and are effective.	**Dengan menyiapkan dan meminimalisir resiko sebisa mungkin.** Misalnya saja dengan membeli perangkat baik software maupun hardware untuk mencegah kerusakan pada system yang mengakibatkan kerugian yang lebih besar bagi perusahaan. **Misalnya saja dengan membangun sebuah server backup dalam hal antisipasi kerusakan system/server secara total yang disebabkan oleh bencana alam, kebakaran dsb**
Memastikan bahwa langkah-langkah untuk segera menangkap peluang atau membatasi besarnya kerugian dari peristiwa yang berkaitan dengan IT telah diaktifkan secara tepat waktu dan efektif.	

Metrik Proses RR 3 *React to Events*

Metrik Proses Risk IT	**Fakta Diperusahaan**
Number of events with business impact due to delayed incident response plan execution	Namun demikian masih **banyak terjadi kegagalan maupun gangguan yang disebabkan oleh lemahnya sistem aplikasi yang belum terintegrasi, dan budaya kerja maupun kesadaran dan partisipasi user** yang **kurang mendukung dalam upaya meminimalisir resiko** terkait TI.
Jumlah kejadian dengan dampak bisnis karena tertundanya eksekusi rencana respon insiden	
Number of incident response plans without an accountable owner	Tidak ditemukan adanya perencanaan respon insiden risiko TI secara spesifik
Jumlah rencana respon insiden tanpa pertanggung jawaban pemilik	
Timeliness of enacting incident response plans	Tidak ditemukan adanya perencanaan respon insiden risiko TI secara spesifik
Ketepatan waktu memberlakukan rencana respon insiden	
Percentage of incident response plan past their next required review date	Tidak ditemukan adanya perencanaan respon insiden risiko TI secara spesifik
Persentase rencana respon insiden yang melewati tanggal review yang diperlukan	
Percentage of incident response plans with one or more open issues regarding their quality and/or dissemination	Dengan menyiapkan dan meminimalisir resiko sebisa mungkin. Misalnya saja dengan membeli perangkat baik software maupun hardware **untuk mencegah kerusakan pada system yang mengakibatkan kerugian yang lebih besar bagi perusahaan** seperti membangun sebuah server backup dalam hal antisipasi kerusakan system/server secara total yang disebabkan oleh bencana alam, kebakaran dsb. Namun demikian **masih banyak terjadi kegagalan maupun gangguan yang disebabkan oleh lemahnya sistem aplikasi yang belum terintegrasi, dan budaya kerja maupun kesadaran** dan partisipasi user yang kurang mendukung dalam upaya meminimalisir resiko terkait TI.
Persentase rencana respon insiden dengan satu atau lebih masalah terbuka mengenai kualitas dan / atau penyebaran	

Lampiran 5

Hasil wawancara dengan bagian *Risk Management*

1. Bagaimana pandangan perusahaan terhadap prinsip-prinsip manajemen risiko dan risiko secara luas?

   Perusahaan menerapkan prinsip kehati-hatian dalam kegiatannya. Selalu memperhitungkan segala aspek risiko dalam mengambil keputusan operasional maupun kebijakan-kebijakan yag berlaku umum dalam perusahaan. Perusahaan memahami risiko dengan mengawasi 7 aspek perusahaan, yaitu risiko dari proses marketing & BD, risiko dari proses operasional, risiko dari proses IT, risiko dari proses legal, risiko dari proses audit internal, dan risiko dari proses penfelolan SDM (HR)

2. Kapan dan bagaimana perusahaan memandang risiko yang akan digunakan untuk risiko TI?

   Risiko TI melekat pada business process capture yang akurat, disertai pelekatan fungsi-fungsi control terhadap tiap-tiap risiko yang mungkin timbul ditiap bisnis proses tersebut. Namun dalam prosesnya pengawasan terhadap pelaksanaan fungsi-fungsi kontrol tersebut masih **terdapat keterbatasan SDM** dalam mengelola risiko terkait TI.
3. Mana yang Anda anggap sebagai risiko tinggi? Apakah kontrol yang efektif (yaitu, tepat waktu akurat, bermakna, dll)? Apakah ada pengecualian kontrol yang tidak tertangkap oleh sistem kontrol?

   Risiko tinggi dalam TI adalah "sistem failure" yang berdampak langsung terhadap kerugian perusahaan, seperti kehilangan asset perusahaan juga kesalahan pencatatan yang meyebabkan penggambaran kondisi keuangan perusahaan yang salah yang berakibat pada kesalahan pengambilan keputusan strategis perusahaan**. Control yang efektif adalah control yang preventif, terlepas bahwa control korektif** diperlukan, akan tetapi pencegahan terjadinya kesalahan adalah yang paling efektif, tentunya control tersebut harus tepat sasaran, tepat waktu dan akurat. **Pengecualian control diberikan hanya pada otoritas level tertentu**, dan terbatas untuk **pengambilan keputusan yang mendesak**, dengan persyaratan pemenuhan administrative akan dilengkapi kemudian.
4. Apakah sistem baru atau perubahan sistem yang signifikan direncanakan untuk sisa tahun ini, atau tahun depan?

   tidak
5. Apa saja ancaman yang paling signifikan pada sistem aplikasi perusahaan? Apakah mencakup beberapa hal berikut ini: penolakan atau gangguan dari layanan sistem, pemantauan sistem layanan yang tidak sah, pengungkapan informasi kepemilikan atau swasta, modifikasi atau kerusakan kemampuan komputer yang terkait (yaitu, kode pemrograman, jaringan, database), dan manipulasi komputer, atau komunikasi jasa yang dihasilkan dalam penipuan, kerugian finansial atau pelanggaran pidana lainnya?

- Kerugian financial
- Kerugian database

6. Apakah kapasitas dan fungsi dari Teknologi Informasi di perusahaan dapat mendukung tujuan strategis perusahaan?

Tentu saja. Dengan peningkatan kapasitas dan fungsi TI dapat meningkatkan program efisiensi dan efektivitas, serta ketergantungan bisnis man pwer supply terhadap database, menjadikan fungsi TI menjadi sangat strategis.

7. Bagaimana perusahaan menanggapi risiko TI dan meminimalkan dampak TI- terkait peristiwa?
   Dengan memberikan control yang lebih bersifat preventif dalam bisnis proses yang ada.
8. Bagaimana kemampuan TI yang ada dapat memberikan kontribusi terhadap kemampuan perusahaan untuk menahan kerugian?
   Kemampuan TI Saat inu cukup berkontribusi dalam menahan terjadinya kerugian perusahaan, seperti control waktu terhadap invoicing, nyat-nyata member manfaat terhadap penghematan cost of money.
9. Bagaimana persepsi manajemen atas pentingnya kemampuan TI terhadap kemampuan TI yang ada saat ini?
   persepsi manajemen atas pentingnya kemampuan TI terhadap kemampuan TI yang ada saat ini cukup memiliki perhatian, yaitu dapat dilihat dari pengembangan program aplikasi yang ada dalam mendukung kegiatan perusahaan
10. Apakah ambang batas toleransi risiko TI sudah sesuai dengan tujuan bisnis perusahaan sebagai dasarnya dan bandingkan antara dampak bisnis yang dapat diterima dan tidak dapat diterima?
    Sebagai langkah korektif dilakukan audit terhadap sistem, dari hasil tersebut terus menerus dilakukan perbaikan.
11. Apakah kebijakan dan standar TI sudah mencerminkan *risk appetite* dan toleransi perusahaan?
    Ya, sudah mencerminkan
12. Apakah perusahaan secara proaktif mengidentifikasi risiko dan peluang TI, yang mempertimbangkan dampak bisnis potensial?
    Ya, secara proaktif mengidentifikasi risiko dan peluang TI dilakukan sesuai kebutuhan, dalam rangka identifikasi risiko dan peluang TI
13. Bagaimanakah peran manajemen risiko perusahaan terhadap risiko IT yang muncul?
    Melakukan pemantauan atas insiden-insiden dan mendapatkan inputan dari audit internal yang menandakan kesalahan tersebut merupakan potensi risiko dimasa yang akan dating, sehingga diperlukan langkah-langkah perbaikan.
14. Bagaimana pendekatan manajemen risiko TI dalam konteks jenis risiko perusahaan lainnya?
    Pada prinsipnya tetap mengandalkan control secara preventif dalam menanggapi risiko-risiko yang terjadi diperusahaan.
15. Apakah perusahaan menetapkan peran departemen TI dalam kegiatan operasional manajemen risiko (menentukan bagaimana keterampilan manajer dan staf manajemen risiko akan dikembangkan dan dipertahankan)?
    Tidak secara spesifk
16. Apakah proses dan prosedur manajemen risiko TI sudah terdokumentasi?
    belum

17. Apakah perusahaan menetapkan anggaran dan sumber daya lain untuk kegiatan penanggulangan risiko spesifik?
    Pengelolaan risiko perusahaan disentralisasi dan tidak spesifik terhadap risiko tertentu
18. Jelaskan pada tingkat apa kualitas pengambil keputusan yang sesuai harapan dan bagaimana menafsirkan laporan analisis risiko, definisi istilah kunci (misalnya, probabilitas risiko, tingkat kesalahan, faktor risiko), dan keterbatasan yang melekat pada perkiraan yang dihasilkan dari data yang tidak lengkap dan masalah lainnya?

- Kualitas pengambilan keputusan diharapkan telah meng-*cover* control preventif dengan selalu memperhitungkan segala jenis risiko.
- Laporan analisis risiko dijadikan sebagai input untuk mitigasi risiko itu sendiri, serta pertimbangan penempatan control yang tepat, dengan selalu mengukur probabilitas risiko terbesar ditangani dengan lebih berhati-hati, tingkat kesalahan yang tinggi dihadapi dengan pemberian control bertahap/berlapis.

19. Bagaimana risiko dipertimbangkan dalam keputusan dan alasan pengecualian untuk toleransi risiko yang dibuat?

- Risiko dipertimbangkan dengan menimbang *magnitude risk* nya menciptakan toleransi risiko yang dapat diterima perusahaan.
- Pengecualian diberikan dengan syarat-syarat yang ketat, dan peningkatan *awareness* terhadap risiko yang melekat.

20. Bagaimana kebijakan perusahaan terhadap langkah-langkah mitigasi yang ada dan kontrol, kemampuan, penyebaran sumber daya, dan rencana komunikasi?
    Secara kontinyu melakukan pemantauan terhadap efektivitas control, pengutamaan terhadap control preventif diputuskan sebagai langkah terbijak bagi perusahaan.
21. Berapa banyak perubahan pada sistem aplikasi perusahaan telah diimplementasikan tahun ini (baik hardware dan software)?
    Ada beberapa.
22. Apakah pelatihan staf IT perusahaan dan dokumentasi pengguna untuk sistem aplikasi perusahaan sudah memadai?
    Cukup memadai, para staf IT dalam keseharian mengatasi trouble shooting pada sistem aplikasi perusahaan.Ada levelisasi hak akses user
23. Bagaimana menentukan faktor risiko spesifik dan kondisi yang berkontribusi pada frekuensi dan dampak peristiwa?
    Pencatatan data historical atas peristiwa/kesalahan yang terjadi, melihat dampak dan frekuensinya, peristiwa yang berdampak terbesar dan berfrekuensi tinggi merupakan pengkategorian risiko tinggi dan perlu penanganan untuk mitigasi risikoya.
24. Tentukan kondisi khusus apa yang ada atau tidak ada ketika peristiwa risiko terjadi dan bagaimana kondisi ini mungkin dapat mempengaruhi terhadap frekuensi peristiwa dan besarnya kerugian?
    Melihat kontrolnya, jikakotrolnya yang terpasang tidak dapat mencegah/mengkoreksi peristiwa tersebut, maka perlu ada review menyeluruh akan keterjadian peristiwa.
25. Apakah struktur data sesuai dengan model yang mendasari perusahaan untuk pengumpulan data, dan menyoroti faktor factor risiko untuk digunakan dalam analisis di masa depan?

Struktur data hanya berarti jika dilengkapi dengan informasi yang memadai, untuk scanning risiko di dalam analisis risiko masa depan.

26. Bagaimana pemetaan risiko dalam kekritisan yang ada dalam lingkup aset dan *Triger* TI?

    Pemetaan risiko dalam lingkup asset dan trigger TI dilakukan dengan memetakan setiap proses yang terlibat dalam pengelolaan asset TI, laludilakukan review atas proses tersebut, bagian-bagian mana yang mengandung risiko tertentu, dikombinasikan dengan *incident record* untuk membantu pengukuran jenis risiko tinggi/rendah.
27. Apakah perusahaan mengidentifikasi ancaman terhadap aset berisiko?

    Iya, terutama asset yang berfungsi vital dalam perusahaan.
28. Adakah Perkiraan kemungkinan frekuensi kejadian dan besarnya dampak bisnis dan perkiraan jumlah maksimum kerusakan yang dapat diderita?

    Ada, Perkiraan kemungkinan frekuensi kejadian dan besarnya dampak bisnis dan perkiraan jumlah maksimum kerusakan yang dapat diderita yaitu dengan menggunakan acuan *historical record*
29. Sudahkah ditentukan persyaratan tingkat tinggi untuk proyek-proyek atau program yang ada berdasarkan toleransi risiko yang diharapkan dapat mengurangi risiko yang dapat diterima atau mengurangi tingkat kontrol yang ada, mengidentifikasi biaya, manfaat dan tanggung jawab untuk eksekusi proyek?

    Sudah, persyaratan tingkat tinggi untuk proyek-proyek atau program yang ada berdasarkan toleransi risiko yang diharapkan dapat mengurangi risiko yang dapat diterima atau mengurangi tingkat kontrol yang ada, mengidentifikasi biaya, manfaat dan tanggung jawab untuk eksekusi proyek dilakukan sebelum proyek dimulai. Bahkan untuk proyek yang bernilai tertentu perlu mendapat persetujuan komite di *Holding* perusahaanuntuk dianalisa risiko dan tingkat kontrolnya, identifikasi biaya dan manfaat proyek tersebut.
30. Sejauh mana ketergantungan kegiatan bisnis utama pada proses layanan manajemen TI dan sumber daya Infrastruktur TI (misalnya, aplikasi, middleware, server, storage, jaringan dan fasilitas fisik)?

    Cukup besar ketergantungannya terhadap infrastruktur TI, untuk mempercepat proses dan memberikan efisiensi yang diperlukan.
31. Bagaimana ketersediaan layanan TI dan sumber daya infrastruktur TI yang diperlukan untuk mempertahankan pengoperasian layanan utama dan proses bisnis?

    Cukup memadai, walaupun masih banyak ruang untuk improvisasi.
32. Apakah perusahaan melakukan review dan memperbarui kategori untuk TI terkait jenis ancaman dan dampak bisnis, dan memelihara konsistensi dengan unsur-unsur standar manajemen risiko perusahaan untuk pemetaan risiko?

    Belum, dan kemungkinan akan sangat baik jika bias diterapkan diperusahaan

Hasil wawancara dengan bagian Internal Audit / Analis Sistem

1. Apakah manajemen risiko khususnya TI sudah tersusun dan terdokumentasi?

Sudah ada namun belum terdokumentasi. Direksi sangat concern terhadap perkembangan dan permasalahan terkait TI. Manajemen risiko TI sudah menjadi konsep dan target utama perusahaan dalam upayanya mengembangkan dan mengintegrasikan sumber daya TI perusahaan, karena sistem yang ada sat ini belum terintegrasi dan masih banyak nya kelemahan seperti, ketidak akuratan, output yang belum dapat memenuhi kebutuhan user.sebagai langkah pembenahan atas sistem yang ada secara berkesinambungan sistem ini dibenahi dari sisi control dan fungsi nya agar lebih maksimal yaitu dengan mengembangkan dan mendevelop sistem yang sesuai kebutuhan perusahaan. Manajemen juga sudah membuat pemetaan yg jelas dalam hal pengelolaan TI perusahaan.

2. Apakah perusahaan sudah menyadari adanya resiko-resiko terkait TI diperusahaan?adakah batasan toleransi risiko TI yang didefinisikan?

Manajemen perusahaan sangat menyadari adanya resiko dan ancaman terkait TI diperusahaan, untuk itu sebagai fungsi Quality control atas kegiatan dan kinerja terkait TI perusahaan, manajemen menunjuk personil sebagai sistem analis yang berfungsi sebagai pengawas sekaligus pemberi masukan atas kondisi sistem yang ada saat ini.

Batasan toleransi atas resiko TI yang dapat diterima sudah ada dalam konsep pemikiran manajemen namun belum didokumentasikan dan didefinisikan secara jelas, sehingga tidak dapat dikomunikasikan secara jelas dan meyeluruh kepada stakeholder. hasil dari analisis TI perusahaan juga memberikan masukan bagi manajemen dalam menentukan batasan toleransi resiko yang ada maupun dalam pengambilan keputusan terkait TI.

3. Laporan hasil analisa dilaporkan ke mana?seberapa sering rapat yg membahas masalah It dilakukan? Apakah manajemen risiko TI sudah dikomunikasikan ke seluruh stakeholder?

   Laporan hasil analisa TI dilaporkan ke direksi, biasanya direksi memberikan tanggapan dengan memberi arahan dan masukan atas temuan yang dibahas dalam rapat manajemen. Rapat yg membahas masalah TI cukup sering dilakukan yg dihadiri oleh level manajemen, hal ini sebagai bukti keseriusan manajemen dalam pengelolaan TI di perusahaan. Manajemen risiko TI Belum dikomunikasikan ke seluruh stakeholder, karena manajemen risiko TI belum didefinisikan dan didokumentasikan secara jelas

4. Dalam hal penilaian resiko TI yg ada, seberapa sering terjadinya penyimpangan/pelanggaran dari batas toleransi ?

   Pelanggaran batas toleransi terkait resiko Ti yang ada cukup sering terjadi, hal ini dikarenakan oleh kelemahan sistem aplikasi yang ada. Contohnya adalah ketika terjadi suatu maslah terkait angka ataupun jumlah maka, user bisa langsung

menghubungi dept TI untuk segera mengkoreksi secara langsung pada database(tidak sesuai dengan prosedur perbaikan yang benar). Sehingga manajemen megeluarkan satu kebijakan terkait hal ini dengan mengharuskan dept TI mencatat/mendokumentasikan setiap ada perbaikan yang tidak sesuai prosedur dengan terlebih dahulu mendapatkan persetujuan dari direksi, kebijakan ini menjadi win-win solution atas permasalahan yang timbul sehingga setiap penyimpangan dapat dipertanggung jawabkan dan histroris penyimpangan dapat menjadi acuan dan bahan dalam hal evaluasi dan perbaikan sistem aplikasi perusahaan.

5. Seberapa sering personil TI mengikuti training?

   Training dalam hal peningkatan kemampuan teknis personil TI sudah cukup memadai dalam menunjang kinerja namun dalam hal implementasi sistem aplikasi kepada user tidak dilakukan maksimal, hanya ada training singkat saja.

   Kebanyakan improve atau membuat sistem baru/menggantikan?ada beberapa sistem baru dan kebanyakan improve sistem yg udah ada, belum pernah menggantikan sistem yang ada. Ada wacana membeli sistem baru yang terintegrasi, saat ini masih memaksimalkan sistem aplikasi yang ada.

6. Masalah gangguan sistem yg terkait resiko It seberapa sering terjadi?sejauh mana manajemen mengetahui /pelanggaran batas toleransi atas masalah sistem yg terjadi?

   Gangguan sistem yg terkait resiko It Cukup sering terjadi baik gangguan yg kecil maupun yg besar terkait IT. Direksi banyak mengetahui masalah IT yg terjadi baik dari hasil analisa dan biasanya memberikan solusi atas pelanggaran toleransi tsb.

7. Adakah kebijakan yg berbenturan dengan toleransi manajemen risiko IT?

   Ada dan frekuensinya cukup sering yang biasanya dapat diselesaikan dengan mendiskusikannya

8. Bagaimana SDM IT, apakah sudah mamadai?

   Jika dilihat dari jumlah SDM TI sudah cukup memadai namun hasil kinerjanya masih belum maksimal.

9. Apakah SOP sudah berjalan?

   Belum berjalan dengan sempurna, karena SOP masih dalam proses pembenahan.

10. Dari konsep risk manajemen It sendiri apakah sudah sesuai dgn proses bisnis yg ada?

    Belum selaras karena keterbatasan SDM TI maupun budaya kerja TI, konsep risk manajemen TI masih belum terdokumentasi sehingga untuk implementasinya sulit dilakukan karena tidak dapat dikomunikasikannya konsep risk manajemen TI tersebut ke seluruh pihak yang berkepentingan atas TI.

11. Bagaimana partisipasi level manajer dalam mengikuti training terkait TI?

    Kurang antusias mengikuti/kurangnya kesadaran mengenai pentingnya permasalahan TI di perusahaan

12. Terhadap Hasil analisis yg ada bagaimana tanggapan manajemen?

    Manajemen cukup concern dlm setiap temuan yg ada dari laporan analisa dan memberikan masukan dan solusi atas permasalahan yang ada

13. Adakah perencanaan respon terhadap terjadinya resiko TI?

    Ada, dept IT sudah melakukan dokumentasi dalam mengatasi permasalahan yang ada namun belum diimplementasikan dengan sempurna. Dokumentasi ini menjadi dasar historis dalam perencanaan penanggulangan permasalahan yang terjadi terkait resiko IT

14. Seberapa sering resiko yang timbul tidak dilaporkan kepada manajemen?

    Manajemen cukup mengetahui masalah atas resiko yang timbul yang melewati batasan toleransi, manajemen sendiri (direksi). Direksi sudah memilkik perencanaan atas permasalahn yang terjadi walaupun belum terdokumentasi. Direksi mengkategorikan resiko yang ada menjadi dua yaitu resiko yang terdeteksi dan resiko yang tidak terdeteksi. Untuk risiko yang terdeteksi direksi memiliki pernecanaan penanggulangan nya sedangkan yg tdk terdeteksi dijadikan sebuah bahan evaluasi yang biasanya diangkat ke meja meeting.

15. Untuk mengajukan improve dan developt sistem aplikasi baru memerlukan approval siapa saja?

    Manajer, KaDiv dan Direksi

16. Apakah kegagalan dalam mengembangkan sudah didokumentasikan?

    Sudah

17. Apakah Keputusan manajeman atas resiko TI didukung oleh laporan hasil analisa?

    Ya, Keputusan manajeman atas resiko TI didukung oleh laporan hasil analisa, namun ada beberapa yang tidak didukung oleh laporan hasil analisa.

18. Dalam identifikasi resiko TI darimanakah data sumber didapatkan? Adakah data historis atas resiko yg timbul?

    Dalam identifikasi resiko TI data sumber didapatkan Dari user, pihak internal TI perusahaan. Data historis atas resiko yg timbul sudah tercatat dan cukup lengkap, karena setiap kali ada permasalahn terkait TI yang terjadi tercatat dalam IT form IT service request

19. Apa Kendala dalam pengumpulan data untuk analisa resiko TI?

    Tidak ada kendala dalam pengumpulan data yang bersumber di divisi TI karena data sudah terdokumentasi dengan baik lain halnya dengan data yang bersumber dari user karena masih kurang memahami fungsi dan tanggung jawab dari analis sistem.

20. Apakah data tsb relevan dengan resiko TI yg ada?

    Cukup relevan

21. Bagaimana cakupannya dlm hal analisa secara keseluruhan atau berdasarkan prioritas? Apakah perusahaan memiliki opsi atau alternative lain dalam penanggulangan resiko yang terjadi?

    Analisa dilakukan berdasarkan skala prioritas yang dilihat mulai dari potensi kerugian keuangan yang paling potensial. Dan manajemen memiliki pilihan-pilihan alternative lainnya dengan mendiskusikan di ruang rapat bersama pihak yang berkepentingan, yang biasanya menghasilkan beberapa pilihan solusi yang win2 solution.

22. Butuh berapa lama pengujian atas sistem yg ada?

    Pengujian atas sistem hanya menguji keakuratan kalkulasinya, cukup informative atau tidak bagi user. Lebih ke interface dan hasil antara input dan output pengujian / analisa ini dilakukan sesuai dengan lingkupnya

23. Rasio kerugian estimasi dgn aktualnya?

    Rasio estimasI kerugian keuangan dgn aktualnya tidak ada namun untuk waktu dan data ada dan cukup sering atau banyak

24. Apakah user cukup memahami dan bagaimana kemampuan user dalam memahami dan menyadari resiko TI?

    User cukup mengerti dan memahami resiko terkait TI yang mungkin terjadi

25. Daftar risiko ada atau tidak? Bagaimana ancaman terjadinya resiko dikategorikan?

    Daftar risiko konsepnya sudah Ada dan namun blm terdokumentasi , resiko dikategorikan menjadi 3 macam kategori yaitu Major, Middle dan Minor

26. Seberapa ketergantungan proses bisnis perusahaan terhadap TI?apakah Anggaran IT sdh mendukung dalam pengelolaan resiko IT dalam menyediakan jumlah SDM TI maupun infrastruktur?

    Perusahaan sangat tergantung terhadap TI dalam menunjang kegiatan operasional perusahaan yang didukung dengan infrastruktur TI yang cukup memadai baik SDM maupun perangkat TI lainnya. Jumlah SDM TI saat ini masih cukup dalam menunjang

dan melayani kegiatan operasional perusahaan, sedangkan untuk infrastruktur penunjang lainnya disesuaikan dengan kebutuhan perusahaan dengan mempertimbangkan *cost & benefit* nya.

Cukup concern, namun dalam membeli sistem yang besar masih terbatas oleh budget keuangan yg ada.

27. Adakah resiko terkait TI yang terjadi tidak terdeteksi?

    Ada namun frekuensinya tidak banyak

28. Sudah pernah ada penilaian dari konsultan eksternal?

    Belum pernah

29. Jumlah resiko terkait IT yg tidak dilaporkan sblmya?

    Cukup banyak

30. Layanan IT seberapa cepat dan akurat menanggulangi masalah IT?

    Respon atas terjadinya resiko TI cukup cepat dan akurat dalam menanggulangi permasalahan yang terjadi terkait TI. Dalam penanggulangan permasalah yang terjadi sudah ada penyusunan dan pembagian tugas dalam penanggulangan TI

31. Sudah selaraskah antara batas toleransi resiko dgn strategi bisnis perusahaan?

    Sudah selaras, karena batas toleransi sendiri berfungsi menjaga dan menunjang startegi bisnis perusahaan agar tidak terjadi penyimpangan dari strategi yang sudah ditetapkan perusahaan.

32. Apakah progress dari perencanaan TI dibuat ke dalam laporan hasil analisa?

    Ya ada, laporan hasil analisa menjadi indicator dalam mempengaruhi pengambilan keputusan manajemen terkait kebijakan risiko TI perusahaan, report ini dibuat oleh analis dan dilaporkan kepada direksi.

33. Apakah ada alternative solusi dari toleransi yg ada?

    Selalu ada alternative solusi dari resiko TI yang terjadi

34. Apakah perusahaan memiliki anggaran dan perencanaan dalam investasi TI dimasa depan?

    Ya ada, disesuaikan dengan kebutuhan dan urgensinya

35. Apakah setiap resiko kegagalan terkait TI yang terjadi direview dan didokumentasikan dengan lengkap?

Atas resiko terkait TI yang terjadi sudah didokumentasikan dan dilakukan review atas masalah yang terjadi tersebut sehingga menjadi masukan bagi perbaikan sistem yang dilakukan oleh internal Divisi TI.

36. Bagaimana respon atas risiko yang terjadi atas insiden terkait TI? Apakah ada perencanaan atas respon insiden terkait TI yang terdokumentasi?

    Respon atas resiko yang terjadi cukup cepat dilakukan karena kebutuhan perusahaan atas TI sangat tinggi sehingga penanggulangan dan perbaikannya bersifat segera. Perencanaan atas respon resiko sendiri belum terdokumentasi namun sudah ada pemetaan personil yang bertanggung jawab untuk menanggulangi risiko yang terjadi.

37. Apa upaya perusahaan dalam membatasi kerugian terkait resiko Ti yang terjadi?

    Dengan menyiapkan dan meminimalisir resiko sebisa mungkin. Misalnya saja dengan membeli perangkat baik software maupun hardware untuk mencegah kerusakan pada sistem yang mengakibatkan kerugian yang lebih besar bagi perusahaan. Misalnya saja dengan membangun sebuah server backup dalam hal antisipasi kerusakan sistem/server secara total yang disebabkan oleh bancan alam, kebakaran dsb.

38. Pernahkah ada kerusakan sistem yang fatal yang mengakibatkan kehilangan data yang menimbulkan kerugian perusahaan?

    Tidak pernah ada

Hasil wawancara dengan bagian Teknologi Informasi

1. Apa yang medasari penysusunan kerangka manajemen resiko TI perusahaan?

   Kerangka manajemen risiko TI disusun berdasarkan asumsi dan pemahaman yang masih terbatas pada lingkup teknikal saja sehingga penilaian atas risiko TI belum dilakukan secara luas di perusahaan

2. Apakah perusahaan mendefinisikan secara spesifik manajemen resiko TI?

   Perusahaan belum mendefinisikan secara spesifik manajemen risiko TI karena masih concern terhadap pembenahan atas kontrol sistem secara keseluruhan

3. Siapa yang bertugas memantau dan mengawasi pengelolaan resiko TI?

   Analis sistem berfungsi juga sebagai QC atas pengelolaan TI di perusahaan dan melakukan analisa resiko-resiko yang mungkin terjadi yang mengakibatkan kerugian yang dilakukan secara kontinyu sesuai dengan skala prioritasnya. Selain itu Analis juga bertugas menganalisa antara kesesuaian kebijakan terkait TI dengan pelaksanaan maupun dengan prosedur yang sudah ada.

4. Bagaimana partisipasi manajemen terhadap pengelolaan resiko TI

   Dalam menilai dan mengidentifikasi risiko, manajemen (Direksi) menugaskan analis sistem (Dept Internal Audit) yang langsung bertanggung jawab ke Direksi dalam hal pelaporan atas aktivitasnya

5. Berapa jumlah penilaian risiko TI yang keluar dari siklus perusahaan secara luas?

   Tidak ada pengukuran secara kuantitatif atas penilaian risiko TI secara spesifik

6. Berapa jumlah kebijakan yang selaras dimana audiens telah menandatangani kepatuhan?

   Manajemen berusaha menyelaraskan konsep manajemen risiko TI dengan kebijakan yang ada saat ini dengan mempertimbangkan kondisi dan budaya kerja yang sudah tercipta

7. Sejauh mana komunikasi manajemen risiko dan pelatihan yang ditargetkan untuk peran dan tanggung jawab yang spesifik.?

   Manajemen risiko perusahaan belum dapat mengkomunikasikan dan memberikan pelatihan terkait risiko TI secara spesifik, hal ini karena masih kurang memadainya SDM manajemen risiko yang ada diperusahaan. Manajemen risiko perusahaan masih mendefinisikan risiko secara umum sedangkan untuk kontrol atas kegiatan terkait TI dilakukan oleh analis sistem

8. Apakah kegiatan manajemen risiko sejalan dengan kapasitas tujuan perusahaan untuk TI terkait kerugian dan toleransi subjektif pemimpin atas toleransi ini?

   Belum selaras karena keterbatasan SDM TI maupun budaya kerja TI, konsep risk manajemen TI masih belum terdokumentasi sehingga untuk implementasinya sulit dilakukan karena tidak dapat dikomunikasikannya konsep risk manajemen TI tersebut ke seluruh pihak yang berkepentingan atas TI.

9. Adakah kebijakan yang berlaku dengan satu atau lebih pernyataan yang bertentangan dengan toleransi risiko yang terkait (keselarasan kebijakan TI dengan toleransi)?

   Kebijakan yang bertentangan dengan toleransi risiko masih ada namun tidak terlalu banyak, karena seiring dengan proses pembenahan yang dilakukan saat ini lambat laun diselaraskan dengan toleransi risiko yang ditetapkan

10. Berapa banyak isu risiko TI yang melebihi toleransi risiko?

    Risiko terkait TI yang terjadi saat ini masih dalam batas wajar, belum pernah terjadi risiko yang menimbulkan dampak yang potensial bagi kegiatan perusahaan

11. Bagaimana pemetaan atas tanggung jawab pengelolaan resiko TI?

    Dalam menilai dan mengidentifikasi risiko, manajemen menugaskan analis sistem yang langsung bertanggung jawab ke Direksi dalam hal pelaporan atas aktivitasnya. Analis sistem berfungsi juga sebagai QC atas pengelolaan TI di perusahaan dan melakukan analisa resiko-resiko yang mungkin terjadi yang mengakibatkan kerugian yang dilakukan secara kontinyu sesuai dengan skala prioritasnya.

    Dalam hal terjadinya resiko terkait TI, manajer TI sebagai penanggung jawab dalam pengelolaan TI perusahaan memberikan laporan ke direksi terkait permasalahan yang terjadi dan memberikan laporan progress penyelesaian atas masalah tersebut.

12. Apakah penerapan risiko TI sudah memuaskan?

    Dalam penerapannya, praktek risiko TI masih belum maksimal, hal ini disebabkan masih lemahnya infrastruktur dalam mendukung pengelolaan risiko TI

13. Bagaimana respon atas terjadinya resiko TI?

    Tindakan manajemen risiko TI dilakukan ketika terjadi risiko TI itu sendiri, hal ini yang menyebabkan terlambatnya penanganan atas risiko yang terjadi

14. Sejauh mana anggaran dialokasikan berdasarkan signifikansi risiko (misalnya, per hasil penilaian resiko)?

    Perusahaan sangat tergantung terhadap TI dalam menunjang kegiatan operasional perusahaan yang didukung dengan infrastruktur TI yang cukup memadai baik SDM maupun perangkat TI lainnya. Jumlah SDM TI saat ini masih cukup dalam menunjang dan melayani kegiatan operasional perusahaan, sedangkan untuk infrastruktur penunjang lainnya disesuaikan dengan kebutuhan perusahaan dengan mempertimbangkan cost & benefit nya.

15. Seberapa sering pelatihan mengenai resiko TI dilakukan?Bagaimana partisipasi manajemen?

    Pelatihan yang dilaksanakan perusahaan dalam pengelolaan risiko TI masih kurang diminati, hal ini dapat terlihat dari jumlah kehadiran level manajer perusahaan dengan mengirim bawahannya sebagai penggantinya

16. Bagaimana pengukuran atas biaya yang dikeluarkan dalam kaitannya dengan manajemen rsisiko TI?

    Tidak ada pengukuran terkait pengeluaran operasional manajemen risiko TI yang dapat ditelusuri secara langsung ke strategi risiko bisnis

17. Apakah penerapan manajemen resiko TI sudah selaras dengan tujuan perusahaan?

    Belum selaras karena budaya kerja yang tertanam masih dirasakan kurangnya kesadaran atas resiko terkait TI dan sistem aplikasi yang masih dalam tahap pengembangan. Hal ini disebabkan belum dapat dikomunikasikannya kerangka manajemen risiko TI kepada user.

18. Apakah ada pemetaan atas fungsi control atas risiko?

    Manajemen telah memetakan fungsi kontrol atas risiko maupun penyimpangan yang mungkin terjadi, sehingga tidak terjadi tumpang tindih dalam menjalankan fungsinya masing-masing

19. Apakah hasil laporan analisa resiko TI memberi kontribusi terhadap keputusan manajemen?

    Ya, Keputusan manajeman atas resiko TI didukung oleh laporan hasil analisa, namun ada beberapa yang tidak didukung oleh laporan hasil analisa. Dalam memutuskan batasan toleransi risiko TI yang dapat diterima atau tidak, manajemen mendasarkan keputusannya dari hasil analisa dan data historis sebagai data pendukung pengambilan keputusan

20. Adakah kerugian yang timbul sebagai akibat dari kegagalan dalam menetapkan resiko TI?

    Tidak ditemukan adanya kerugian yang disebabkan oleh pengambilan keputusan penerimaan batas toleransi risiko TI yang mengakibatkan kerugian perusahaan dari sisi keuangan namun dari sisi waktu dan kesempatan ada tapi tidak cukup potensial. Dengan menganalisa isu-isu risiko yang ada, diharapkan dapat mengurangi terjadinya risiko terkait kegagalan TI, kegiatan penanggulangan atas risiko TI yang terjadi cukup sering dilakukan karena masih lemahnya pengelolaan sistem maupun infrastruktur TI perusahaan

21. Apakah ada dokumentasi atas resiko TI yang terjadi?

    Dept TI mendokumentasikan setiap risiko yang terjadi dalam form IT service request dengan lengkap namun atas peristiwa tersebut tidak dilakukan review dan ditindak lanjuti, sehingga peristiwa ini akan terulang kembali dimasa yang akan datang

22. Bagaimana identifikasi resiko dilakukan?

    Dalam menganalisa resiko TI dilakukan observasi terhadap aktivitas terkait TI, yang dapat dilakukan dengan cara wawancara, review catatan atas masalah yang terjadi, review hasil temuan internal audit. Data sumber identifikasi resiko TI didapatkan dari user dan pihak internal TI perusahaan

23. Seberapa sering resiko yang terjadi akibat dari resiko yang tidak terdeteksi?

    Peristiwa yang menimbulkan kerugian yang tidak terdeteksi sebelumnya cukup sering terjadi, hal ini disebabkan oleh lemahnya sistem

24. Adakah data histori terkait resiko TI?apakah sudah didokumentasikan dengan lengkap?

    Data historis atas resiko yg timbul sudah tercatat dan cukup lengkap, karena setiap kali ada permasalahan terkait TI yang terjadi tercatat dalam form IT service request. Pencatatan data historical atas peristiwa/kesalahan yang terjadi, melihat dampak dan frekuensinya, peristiwa yang berdampak terbesar dan berfrekuensi tinggi merupakan pengkategorian risiko tinggi dan perlu penanganan untuk mitigasi risikonya.

25. Apakah hasil analisa sudah akurat?

    Belum pernah dilakukan pengukuran atas waktu yang dibutuhkan dalam melakukan pengujian atas akurasi hasil analisa. Pengujian atas sistem hanya menguji keakuratan kalkulasinya, cukup informative atau tidak bagi user. Lebih ke interface dan hasil antara input dan output

26. Apakah sudah pernah dilakukan analisa oleh pihak eksternal perusahaan?

    Belum pernah dilakukan analisa atas risiko TI perusahaan oleh pihak eksternal

27. Bagaimana estimasi resiko TI diperhitungkan?

    Perkiraan kemungkinan frekuensi kejadian dan besarnya dampak bisnis dan perkiraan jumlah maksimum kerusakan yang dapat diderita yaitu dengan menggunakan acuan historical record

28. Apakah hasil analisa direview ulang sebelum disampaikan ke manajemen?

    Hasil analisa risiko selalu dilakukan review dan pengujian keakuratannya sebelum disampaikan/dilaporkan ke manajemen

29. Bagaimana pemetaan resiko terkait TI dilakukan?

    Pemetaan risiko dalam lingkup asset dan trigger TI dilakukan dengan memetakan setiap proses yang terlibat dalam pengelolaan asset TI, lalu dilakukan review atas proses tersebut, bagian-bagian mana yang mengandung risiko tertentu, dikombinasikan dengan incident record untuk membantu pengukuran jenis risiko tinggi/rendah.

30. Apakah resiko TI sudah dikategorikan sesuai dengan tingkatannya?

    Setiap risiko yang berhasil diidentifikasi didokumentasikan untuk selanjutnya dikategorikan kedalam beberapa kategori untuk penanganan mitigasi risikonya. Daftar

risiko sudah ada namun blm terdokumentasi secara lengkap, resiko dikategorikan menjadi 3 macam kategori yaitu Major, Middle dan Minor

31. Jumlah peristiwa terkait TI dengan dampak bisnis yang sebelumnya tidak dilaporkan sebagai risiko TI?

    Ada namun frekuensinya tidak banyak, hal ini disebabkan karena kurangnya pemahaman mengenai manajemen risiko TI

32. Seberapa banyak jumlah peristiwa terkait TI dengan dampak bisnis sebelumnya tidak dilaporkan sebagai risiko TI?

    Gangguan sistem yang terkait resiko TI cukup sering terjadi mulai dari gangguan yg kecil maupun yg besar. Direksi banyak mengetahui masalah TI yg terjadi baik dari hasil analisa maupun temuan internal audit dan biasanya memberikan solusi atas pelanggaran toleransi tsb.

33. Adakah pengukuran atas persentase ketepatan waktu pelaporan hasil analisa?

    Tidak ada pengukuran atas ketepatan waktu pelaporan

34. Apakah hasil analisa didokumentasikan? Dilaporkan ke siapa?

    Ya ada, laporan hasil analisa menjadi indicator dalam mempengaruhi pengambilan keputusan manajemen terkait kebijakan risiko TI perusahaan, report ini dibuat oleh analis dan dilaporkan kepada direksi.

35. Bagaimana lingkup analisa TI diperusahaan?

    Saat ini pembenahan dalam pengelolaan TI terutama difokuskan pembenahan fungsi kontrol yang ada disetiap proses bisnis perusahaan sehingga dapat meminimalisir potensi kerugian yang mungkin terjadi

36. Apakah perusahaan pernah mengalami kerugian yang potensial akibat dari kegagalan TI yang terjadi?

    Risiko terkait TI yang terjadi saat ini masih dalam batas wajar, belum pernah terjadi risiko yang menimbulkan dampak yang potensial bagi kegiatan perusahaan

37. Bagaimana manajemen menanggapi kinerja dalam upaya mitigasi risiko TI?

    Manajemen cukup puas atas hasil proyek mitigasi risiko, misalnya saja pembangunan server backup sebagai antisipasi terjadinya bencana atau risiko yang dapat mengganggu kelangsungan hidup perusahaan

38. Apakah perencanaan respon insiden sudah dilakukan?

    Tidak ditemukan adanya perencanaan respon insiden risiko TI secara spesifik

39. Bagaimana peluang terjadinya resiko terkait TI diperusahaan saat ini?

    Peluang terjadinya risiko TI yang tak terhindarkan masih terjadi walaupun frekuensinya tidak sesering sebelum dilakukan analisa atas pengelolaan TI

40. Apakah semua resikosudah diantisipasi, sehingga tidak ada celah atas resiko yang tidak teridentifikasi?

    Masih ada risiko TI yang terjadi yang tidak sesuai dengan rencana tindakan yang telah disusun

41. Pernahkah perusahaan membatalkan investasinya terkait mitigasi risiko TI?

    Belum pernah ada investasi yang dibatalkan dalam proyek mitigasi risiko, karena dalam setiap proyek mitigasi risiko terkait TI sudah diperhitungkan dengan akurat.

42. Apa saja upaya perusahaan dalam menjaga dan memantau terjadinya resiko?

    Melakukan pemantauan atas insiden-insiden dan mendapatkan inputan dari audit internal yang menandakan kesalahan tersebut merupakan potensi risiko dimasa yang akan datang, sehingga diperlukan langkah-langkah perbaikan.

43. Adakah pegukuran secara kuantitatif atas perencanaan respon insiden yang sudah disusun oleh perusahaan?

    Tidak ditemukan adanya perencanaan respon insiden risiko TI secara spesifik

44. Seberapa sering resiko yang terjadi merupakan sebagai dampak dari kurang tepatnya respon yang diambil?

    Respon atas resiko yang terjadi saat ini cukup memadai, namun demikian masih banyak terjadi kegagalan maupun gangguan yang disebabkan oleh lemahnya sistem aplikasi yang belum terintegrasi, dan budaya kerja maupun kesadaran dan partisipasi user yang kurang mendukung dalam upaya meminimalisir resiko terkait TI.

45. Bagaimana upaya perusahaan dalam merencanakan penanggulangan resiko terkait TI?

    Dengan menyiapkan dan meminimalisir resiko sebisa mungkin. Misalnya saja dengan membeli perangkat baik software maupun hardware untuk mencegah kerusakan pada sistem yang mengakibatkan kerugian yang lebih besar bagi perusahaan seperti membangun sebuah server backup dalam hal antisipasi kerusakan sistem/server secara total yang disebabkan oleh bencana alam, kebakaran dsb. Namun demikian masih banyak terjadi kegagalan maupun gangguan yang disebabkan oleh lemahnya sistem aplikasi yang belum terintegrasi, dan budaya kerja maupun kesadaran dan partisipasi user yang kurang mendukung dalam upaya meminimalisir resiko terkait TI.