BAB 2
LANDASAN TEORI

2.1 Teori Umum

2.1.1 Pengertian Evaluasi

Menurut Wirawan (2011) evaluasi adalah riset untuk mengumpulkan, menganalisis, dan menyajikan informasi, yang bermanfaat mengenai objek evaluasi, menilainya dengan membandingkan dengan indikator evaluasi dan hasilnya di pergunakan untuk mengambil keputusan mengenai objek evaluasi.

Menurut Dalkir (2009) evaluasi merupakan memiliki arti bahwa evaluasi mampu menilai kualitas informasi, tetapi juga untuk menentukan relevansinya dengan beberapa pertanyaan atau suatu masalah.

Menurut Husni, Tandra, & Anugrah (2010) evaluasi adalah suatu proses untuk menyediakan informasi mengenai hasil penilaian atas permasalahan yang ditemukan.

2.1.2 Pengertian Data

Data adalah fakta yang belum diolah dan dapat berbentuk angka atau pernyataan. Fakta tersebut diperlukan bagi perusahaan untuk dimasukkan ke dalam prosedur guna memastikan data yang telah dicatat. Misalnya, untuk memastikan operator *call center* yang memasukkan kode pos dari setiap pelanggan, operator dapat menulis dalam catatan dan melakukan cek validasi untuk memeriksa data dari para pelanggan apakah telah dimasukkan ke dalam sistem (Hardcastle, 2011).

Komponen pencatatan data untuk informasi di seluruh negara adalah: transmisi, pengolahan, dan penyimpanan. Kategori tersebut menambah pemakaian dari data konvensional, yang biasanya berhubungan dengan *database*, namun penggunaannya tidak selengkap informasi yang diolah oleh suatu perusahaan modern (Whitman & Mattord, 2010).

2.1.3 Pengertian Sistem

Suatu sistem dapat di definisikan sebagai kumpulan komponen yang saling bekerja sama untuk mencapai suatu tujuan. Tujuan dari sistem adalah untuk menerima masukan (*input)* data dan menghasilkan suatu keluaran (*output).* Pada pembahasan sebelumnya mengenai definisi data dan informasi, proses transformasi digunakan untuk menjelaskan bagaimana data diubah menjadi informasi. Tidak setiap sistem hanya memiliki satu tujuan, pada umumnya suatu sistem terdiri dari *subsystem* dengan *subgoals.* Seluruh bagian sistem memberikan kontribusi untuk memenuhi tujuan sistem secara keseluruhan. Misalnya bagian keuangan, bagian operasional, dan bagian pemasaran, bagian-bagian tersebut harus saling bekerja sama untuk mencapai tujuan

perusahaan secara keseluruhan. Suatu sistem yang digunakan perusahaan, dijadikan sebagai penerima *input* yang diproses, sehingga menghasilkan keluaran (*output)* berupa informasi. Dalam pemantauan suatu sistem, dibutuhkan timbal balik (*feedback).* Selain itu, *control* harus dilakukan untuk memperbaiki masalah yang terjadi dan memastikan bahwa tujuan dari sistem tersebut dapat terpenuhi. Oleh sebab itu, ada lima komponen dari suatu sistem, yaitu *input*, *process*, *output, feedback, and control*" (Hardcastle, 2011).

2.1.4 Pengertian Sistem Informasi

Menurut Hall (2013), sistem informasi merupakan serangkaian prosedur formal di mana data dikumpulkan, disimpan, diproses menjadi informasi, dan didistribusikan kepada pengguna. Sedangkan menurut Cegielski (2013),sistem informasi adalah mengumpulkan, memproses, menyimpan, menganalisis, dan menyebarkan informasi untuk tujuan tertentu. Tujuan sistem informasi adalah untuk mendapatkan informasi yang tepat kepada orang yang tepat, pada waktu yang tepat, dalam jumlah yang tepat, dan dalam format yang tepat.Sistem informasi dimaksudkan untuk memberikan informasi yang berguna, kita perlu membedakan antara informasi dan dua istilah yang terkait erat: data dan pengetahuan.

Terdapat 6 komponen dalam sistem informasi, yaitu :

- Perangkat Keras
- Perangkat Lunak
- Database

- Jaringan
- Kebijakan
- Manusia

Jadi dapat ditarik kesimpulan bahwa sistem informasi adalah serangkaian prosedur formal di mana data dikumpulkan, disimpan, dianalisis, dan diproses menjadi informasi yang dapat disebarkan untuk tujuan tertentu.

2.1.5 Pengertian Sistem Informasi Akuntansi

Menurut Bodnar dan Hopwood (2010) Sebuah Sistem Informasi Akuntansi adalah kumpulan sumber daya, seperti orang dan peralatan, yang dirancang untuk mengubah data keuangan dan lainnya menjadi informasi.

Menurut Turner & Weickgenannt (2013) Sistem Informasi Akuntansi terdiri dari proses, prosedur, dan sistem yang menangkap data akuntansi dari proses bisnis; merekam data akuntansi dalam rekaman yang sesuai, memproses data akuntansi secara rinci dengan mengelompokan, meringkas konsolidasi, dan melaporkan data akuntansi yang diringkas ke pengguna internal dan eksternal.

2.1.6 Definisi Pengendalian Internal

Menurut Rama & Jones (2008),pengendalian internal(internal control) adalah suatu proses, yang dipengaruhi oleh dewan direksi entitas,manajemen, dan personel lainnya, yang dirancang untuk memberikan kepastian yang beralasan terkait dengan pencapaian sasaran kategori sebagai berikut : efektifitas dan efisiensi operasi,keandalan pelaporan keuangan,dan ketaatan terhadap hukum dan peraturan yang berlaku.

Menurut Gondodiyoto (2009) yang mengutip dari Information System Audit and Control Association (ISACA, dalam Cangemi 2003) menyatakan bahwa internal control adalah :

Dapat didefinisikan sebagai Kebijakan, prosedur, praktek dan struktur organisasi desain untuk memberikan jaminan yang wajar bahwa tujuan

bisnis akan dicapai dan bahwa peristiwa yang tidak diinginkan dapat dicegah, atau terdeteksi, dan dikoreksi.

Gondodiyoto (2009) yang mengutip dari *The Institute of Internal Auditors* (IIA) adalah : audit dapat diartikan sebagai sikap dan tindakan manajemen dan dewan mengenai siginifikan pengendalian dalam organisasi. Lingkungan pengendalian memberikan disiplin dan struktur untuk pencapaian tujuan utama dari sistem pengendalian internal. Lingkungan pengendalian mencakup unsur- unsur berikut: integritas dan nilai-nilai etika, filosofi manajemen dan gaya operasi, struktur organisasi, tugas wewenang dan tanggung jawab, kebijakan.

2.1.7 Pengertian *Data Analysis*

Data yang dikumpulkan dalam bentuk mentah, biasanya tidak cukup untuk menentukan efektivitas dari sistem yang ada atau penilaian persyaratan untuk sistem baru. Langkah berikutnya yang dilakukan, adalah untuk memanipulasi data yang dikumpulkan, sehingga anggota tim pengembangan yang berpartisipasi dalam analisa sistem dapat menggunakan data tersebut. Manipulasi ini disebut dengan proses analisa data (*data analysis*). Data dan pemodelan kegiatan, yang menggunakan diagram aliran data (*data flows diagram*), serta diagram hubungan entitas (*entity relationship diagram*), berguna selama analisa data (*data analysis*) untuk menunjukkan arus data dan hubungan antara berbagai objek, asosiasi, dan kegiatan. Alat umum lainnya dan teknik untuk analisa data yang ada yaitu aplikasi *flowchart*, grafik *grid*, *CASE tools*, dan pendekatan berorientasi objek(M.Stair & George, 2010).

2.1.8 Pengertian *Overview Activity Diagram*

Overview Activity Diagram menyajikan suatu pandangan tingkat tinggi dari proses bisnis dengan mendokumentasikan kejadian - kejadian penting, urutan kejadian-kejadian penting, dan aliran informasi antar kejadian (Rama & Jones, 2008).

2.1.9 Pengertian *Detailed Activity Diagram*

Detailed Activity Diagram menunjukkan informasi mengenai aktivitas dalam suatu kejadian spesifik. Untuk membuat *detailed activity diagram,* kita

perlu mengidentifikasi aktivitas individu dalam setiap kejadian (Rama & Jones, 2008).

2.1.10 Pengertian Resiko

Resiko adalah kemungkinan terjadinya suatu kerentanan yang dikaitkan dengan nilai atas aset informasi (Whitman & Mattord, 2010).

2.1.11 Komponen Risiko

Menurut Arens (2012), komponen risiko adalah sebagai berikut:

1. Risiko Deteksi yang Direncanakan (Planned Detection Risk) Risiko bahwa bukti audit untuk segmen akan gagal mendeteksi salah saji yang melebihi toleransi.

2. Risiko Audit yang Dapat Diterima (Acceptable Audit Risk) Ukuran tentang kesediaan auditor untuk menerima bahwa laporan keuangan mungkin disalahsajikan secara material setelah audit selesai dan pendapat wajar tanpa pengecualian telah dikeluarkan.

3. Risiko Inheren (Inherent Risk) 20 Ukuran penilaian auditor tentang kemungkinan bahwa ada salah saji yang material dalam suatu segmen sebelum mempertimbangkan keefektifan pengendalian internal.

4. Risiko Pengendalian (Control Risk) Ukuran penilaian auditor mengenai kemungkinan bahwa salah saji melampaui jumlah yang dapat ditoleransi dalam suatu segmen tidak akan tecegah atau terdeteksi oleh pengendalian internal klien.

2.1.12 Upaya Penanggulangan Risiko

Menurut Yasa (2013), tindakan yang dilakukan untuk mengurangi risiko yang muncul disebut mitigasi penanganan risiko (risk mitigation). Tindakan yang dapat dilakukan dalam menangani risiko yaitu :

1. Menahan Risiko (Risk Retention) Tindakan ini dilakukan karena dampak dari suatu kejadian yang merugikan masih dapat diterima (acceptable).

2. Mengurangi Risiko (Risk Reduction) Mengurangi risiko dilakukan dengan mempelajari secara mendalam risiko tersebut, dan melakukan usaha-usaha pencegahan pada sumber risiko atau mengkombinasikan usaha agar risiko yang diterima tidak terjadi secara simultan.

3. Memindahkan Risiko (Risk Transfer) Dilakukan dengan cara mengansuransikan risiko baik sebagian atau seluruhnya kepada pihak lain.

4. Menghindari Risiko (Risk Avoidance) Dilakukan dengan menghindari aktivitas yang tingkat kerugiannya tinggi.

2.1.13 Teori *Rich Picture*

Menurut penelitian dari Stenlund dalam *Using Grounded Theory Methodology and Rich Picture Diagrams in Analyzing Value Creation in Houses of Culture Projects in Sweden* (2010), *rich picture* adalah alat yang sesuai untuk menganalisa berbagai pembentukan proses bisnis yang kompleks.

2.2 Teori Khusus

2.2.1 Pengertian Penjualan

Menurut Reeve, Warren, & Duchac (2012) arti bahwa penjualan adalah jumlah total biaya pelanggan untuk barang dagangan yang di jual termasuk penjualan tunai dan penjualan pada akun.

Menurut Arif &Wibowo (2008), Penjualan tunai adalah penjualan barang dagang dengan menerima pembayaran kas atau tunai secara langsung dari pelanggan pada saat terjadinya penjualan. Sedangkan Penjualan Kredit adalah penjualan barang dagang dengan kesepakatan antara pembeli dan penjual pada saat transaksi, yaitu pembayaran akan dilakukan pada waktu yang akan datang.

Menurut Bodnar dalam Puspitawati dan Anggadini (2011), penjualan adalah suatu usaha yang terpadu untuk mengembangkan rencana-rencana strategis yang diarahkan pada usaha pemuasan kebutuhan dan keinginan pemebeli, guna mendapatkan penjualan yang menghasilkan laba. Penjualan merupakan sumber hidup suatu perusahaan, karena dari penjualan dapat diperoleh laba serta suatu usaha memikat konsumen yang diusahakan untuk mengetahui daya tarik mereka sehingga dapat mengetahui hasil produk yang dihasikan. Selain itu, aktivitas

penjualan kredit biasanya dilakukan dengan cara pelanggan / *customer* melakukan *order* pemesanan penjualan terlebih dahulu.

2.2.2 Peranan Sistem Pengendalian Internal

Berdasarkan hasil dari studi pustaka melalui mencari dan memahami jurnal terkait peranan sistem pengendalian internal, maka penulis mengutip dari (Kusumadianti, 2011), Pengendalian Internal sangat diperlukan setiap organisasi baik sektor publik maupun organisasi bisnis. Salah satu tujuan dari pengendalian internal adalah untuk mengamankan harta kekayaan organisasi. Umumnya persediaan merupakan aktiva yang banyak dijadikan objek kecurangan. Potensi kehilangan persediaan akan semakin besar jika jumlah dan jenis persediaan semakin banyak sementara pengendalian internal kurang diterapkan.

2.2.3 *Facilitated Risk Analysis and Asessment Process* (FRAAP)

Proses penilaian dan analisa resiko yang difasilitasi (FRAAP) telah dikembangkan sebagai suatu proses yang efisien dan disiplin untuk memastikan bahwa keamanan informasi dan resiko relatif dalam operasi bisnis di analisa dan di dokumentasikan. FRAAP dibagi menjadi tiga tahap: *Pre*-FRAAP *meeting,* FRAAP *session,* dan *Post*-FRAAP. Tim akan bekerja sama untuk mengidentifikasi potensi ancaman terhadap kerahasiaan, ketersediaan, integritas, dan sumber daya informasi. Proses penilaian dan analisa resiko yang difasilitasi (FRAAP), telah dikembangkan sebagai suatu proses yang efisien dan teratur, serta digunakan untuk memastikan bahwa resiko yang terkait dengan keamanan informasi proses bisnis, telah di analisa dan di dokumentasikan. Pada berjalannya proses tersebut, melibatkan analisa suatu sistem aplikasi yang saling terkait(Peltier, 2014).

2.2.3.1 Tahapan FRAAP Pertama: *Pre*-FRAAP *Meeting*

Pre-FRAAP *meeting* menjadi kunci bagi keberhasilan suatu proyek. Pertemuan biasanya dijadwalkan selama 90 menit, dan dilaksanakan dikantor klien. Pertemuan harus dihadiri oleh manajer bisnis, pimpinan pengembangan proyek, fasilitator, dan juru tulis. Pada pertemuan ini akan disampaikan enam kunci pada satu jam pertemuan, diantaranya:

1. ***Prescreening results*** **-** Hasil dari *pre screening* dapat mengubah kebutuhan untuk melakukan penilaian resiko.
2. ***Scope Statement*** **-** Pimpinan proyek dan manajer bisnis diharuskan membuat lingkup pernyataan untuk ditinjau kembali.
3. ***Visual Diagram*** **-** Visual diagram ini digunakan untuk melihat kembali gambaran proses dalam FRAAP, selama sesi FRAAP dilakukan, suatu tim akan diperkenalkan dengan suatu proses awal, hingga proses selesai. Penggunaan diagram visual atau model arus informasi di dalam FRAAP merupakan hal yang baik. *The neural-linguistic programming* berisikan tentang bagaimana cara orang (*people*) mempelajari suatu hal. Dalam proses ini di identifikasikan 3 hal.
    - *Auditory* - Suatu tim harus mendengarkan dan memahami pernyataan laporan ruang lingkup yang telah disampaikan oleh pemilik.
    - *Mechanical* - Pada tipe pembelajaran ini, tim harus menulis dan mendokumentasikan hal-hal yang akan dipelajari.
    - *Visual* - Dalam hal ini, melihat gambar atau diagram diperlukan untuk memahami hal yang sedang di bahas, orang - orang yang mempelajari metode ini, biasanya memiliki papan tulis dikantor dan sering menggunakannya. Diagram visual digunakan untuk membantu orang - orang dalam memahami hal apa saja yang sedang ditinjau.
4. ***Establish The*** **FRAAP** ***team*** - Tim FRAAP terdiri dari 15 sampai 30 orang anggota, pembentukan tim FRAAP tersebut dilakukan untuk mendukung proses bisnis dan infrastruktur di dalam perusahaan.
5. ***Meeting mechanics*** - Suatu pertemuan yang dihadiri oleh manajer dari unit bisnis, dari pertemuan ini diharapkan menghasilkan penjadwalan tempat, dan pengaturan waktu dalam melakukan penilaian resiko. Pertemuan yang membahas tentang penilaian resiko adalah tanggung jawab pemilik. Pemilik dibantu oleh fasilitator dalam menyelesaikan tugas ini. Dalam hal ini tidak di bahas mengenai keamanan sistem informasi, manajemen proyek, audit, atau pertemuan manajemen resiko. Hal yang di bahas adalah mengenai pertemuan antara pemilik bisnis, dan

orang yang bertanggung jawab untuk mengatur penjadwalan tempat, serta memberikan informasi waktu pertemuan kepada anggota tim.

6. ***Agreement on definitions*** - Bagian *FRAAP* ini membahas mengenai kesepakatan definisi dan unsur - unsur dari FRAAP, yaitu integritas, kerahasiaan, ketersediaan" (Peltier, 2014).

2.2.3.2 Tahapan FRAAP kedua: FRAAP *Session*

"Setelah tahapan FRAAP dilakukan bersama - sama, laporan terhadap aset perusahaan yang telah dibahas tim, harus dipertanggung jawabkan oleh bagian eksekutif bisnis di perusahaan. Laporan tersebut akan membantu anggota tim untuk memahami alasan mengapa mereka diminta untuk menjadi bagian dari FRAAP, dan bagaimana manajemen senior menilai betapa pentingnya penilaian resiko. Ketika pembahasan FRAAP selesai, fasilitator akan memberikan informasi mengenai jadwal pertemuan untuk tim. Fasilitator akan menjelaskan mengenai FRAAP pada tim. Hal tersebut akan mencakup diskusi tentang hasil yang diharapkan dari setiap tahapan proses FRAAP. Tim akan mengidentifikasi ancaman terhadap aset yang dilaporkan. Dengan menggunakan rumus probabilitas dan pengukuran dampak, tim tersebut akan menilai tingkat resiko untuk setiap ancaman. Dari pengukuran resiko tersebut, akan dihasilkan penentuan pengambilan tindakan *control* untuk mengurangi intensitas resiko. Sesi FRAAP dibagi menjadi dua tahap, tahap yang pertama umumnya dilakukan pertemuan yang akan dijadwalkan selama empat jam, pertemuan tersebut dihadiri oleh anggota tim dengan jumlah 15 sampai 25 orang. Sejumlah lembaga pemerintah telah mengubah lamanya waktu pertemuan hingga tiga hari, pada sektor bisnis dan instansi pemerintah, pertemuan selama empat jam membahas mengenai kontribusi dari tim terhadap proses bisnis pada perusahaan. Pembahasan pada tahap pertama adalah:

- Identifikasi ancaman.
- Penilaian Tingkatan resiko.
- Dokumentasi kemungkinan *control*.

Setelah penyampaian secara keseluruhan telah lengkap, maka sistem untuk pengguna dan beberapa infrastruktur dari area bisnis sudah dapat dipahami.

Anggota tim akan menyelesaikan sesi FRAAP tahap kedua, dengan tiga hal yang akan disampaikan:

- *Control* harus diidentifikasi pada seluruh tempat di perusahaan.
- Ketika ditemukan resiko dengan dampak yang luas bagi perusahaan, pemilik perusahaan harus segera mengambil tindakan untuk menanggulangi resiko tersebut.
- Setiap tindakan *control* yang dipilih, merupakan tanggung jawab dari tim yang melaksanakan tindakan *control* tersebut" (Peltier, 2014).

2.2.3.2.1 Pembahasan pada FRAAP *Session*: Identifikasi Ancaman

"Tim akan diberikan waktu 3 - 15 menit untuk mengidentifikasi dan membuat catatan mengenai ancaman yang menjadi perhatian. Fasilitator akan mengitari ruangan untuk menayakan dan membuat catatan dari setiap anggota tim mengenai ancaman yang dapat terjadi. Banyak dari anggota tim yang menuliskan lebih dari satu ancaman yang dapat terjadi, namun fasilitator hanya akan mengambil satu catatan ancaman dari setiap anggota dan beralih kepada anggota selanjutnya. Hal ini dilakukan oleh fasilitator dalam upaya melibatkan seluruh partisipasi dari anggota tim. Proses tersebut akan terus berlanjut sampai seluruh anggota tim telah memberikan kontribusinya dalam proses identifikasi ancaman tersebut (yaitu sampai tidak ada lagi ancaman yang dapat dipikirkan oleh anggota tim). Selama dua putaran pertama, seluruh anggota tim akan berpartisipasi. Namun dalam setiap kemajuan putaran, jumlah anggota tim berikut ancaman yang dituliskan akan semakin berkurang. Ketika hanya tinggal sedikit dari anggota tim yang dapat merespon dan menuliskan ancaman yang mungkin terjadi, fasilitator dapat menanyakan ancaman - ancaman yang mungkin terjadi kepada anggota tim lain, yang tentunya masih memiliki ide tentang ancaman apa saja yang mungkin dapat terjadi. Jika anggota tim tidak memiliki ide lagi, tidak berarti anggota tim yang bersangkutan keluar dari kegiatan identifikasi ancaman tersebut. Anggota tim dapat kembali kedalam sesi identifikasi ancaman tersebut, ketika ide tentang ancaman yang mungkin terjadi muncul dalam benak anggota tim yang bersangkutan, dan menuliskan ancaman yang dipikirkan ketika tiba gilirannya kembali. Sangat disarankan

bagi anggota tim untuk memiliki pena dan kertas dalam upaya menuliskan dengan cepat apa saja ide yang muncul. Ketika semua ancaman telah diposting, tim akan diberikan waktu istirahat 15 menit untuk melakukan 3 aktivitas penting, yaitu:

- Memeriksa catatan ancaman yang telah dikumpulkan
- Meninjau kembali catatan ancaman
- Membersihkan catatan ancaman yang ada

Di dalam kegiatan istirahat tersebut, tim melakukan kegiatan peninjauan kembali catatan ancaman pada elemen tertentu dan menghapus duplikasi catatan ancaman yang ada. Jika terdapat kesamaan pada catatan ancaman namun kemunculannya didalam dua elemen berbeda, yaitu elemen integritas atau elemen kerahasiaan, maka hal tersebut tidak dianggap sebagai duplikasi catatan ancaman. Suatu catatan ancaman dianggap duplikasi jika muncul dua kali didalam satu elemen saja. Proses pembersihan catatan ancaman tersebut dilakukan dalam waktu sekitar 15 menit saja" (Peltier, 2014).

2.2.3.2.2 Pembahasan pada FRAAP *Session*: Penilaian Tingkatan Resiko

"Penilaian tingkatan resiko yang dihasilkan oleh ancaman, merupakan tugas terpenting dan tersulit didalam proses penilaian resiko. Semua kegiatan lain yang mengikuti, akan tergantung pada hasil yang dilakukan oleh tim di dalan fase ini. Agar sukses, tim harus mengerti apa yang telah dilakukan dan peringatan apa saja mengenai ancaman yang telah diterapkan. Dalam contoh ini, tim akan memeriksa tiap ancaman tanpa disertai dengan *control* ditempat. Peringatan seperti ini biasanya diterapkan untuk penilaian resiko yang dilakukan terhadap aset - aset infrastruktur. Penilaian resiko tersebut mencakup atas jaringan, lingkungan proses operasi, metodologi pengembangan aplikasi, pengendalian keamanan informasi, atau platform.

Tabel 2.1 Contoh Kertas Kerja FRAAP setelah Ancaman di Identifikasi (Peltier, 2014)

Nomor Ancaman	Ancaman	Tinjauan Elemen	Tingkatan Resiko	Kemungkinan Pengendalian
1.	Informasi diakes	*Integrity*		

	oleh personil yang tidak memiliki akses			
2.	Ketidakjelasan atau tidak adanya versi atas informasi	*Integrity*		
3.	*Database* dapat rusak oleh kegagalan *hardware* atau *software* yang buruk	*Integrity*		
4.	Data dapat rusak akibat transaksi yang tidak lengkap	*Integrity*		
5.	Kemampuan untuk mengubah data dalam transit dan kemudian mengubahnya kembali untuk menutupi aktivitas	*Integrity*		
6.	Sebuah kegagalan untuk melaporkan masalah integritas	*Integrity*		
7.	Proses yang dijalankan tidak	*Integrity*		

	lengkap atau kegagalan untuk menjalankan suatu proses yang bisa merusak data			
8.	Kurang lengkapnya proses internal dalam membuat dan mengontrol, serta mengelola data di seluruh fungsi	*Integrity*		
9.	Tidak adanya pemberitahuan mengenai masalah integritas	*Integrity*		
10.	Informasi yang digunakan pada konteks yang salah	*Integrity*		

Tim akan mempertimbangkan setiap ancaman yang ada, dan akan memeriksa ancaman tersebut, berdasarkan pada kemungkinan bahwa ancaman akan terjadi dengan menggunakan definisi seperti di Tabel 2.2.

Tabel 2.2 Contoh Defnisi Probabilitas FRAAP (Peltier, 2014)

Istilah	Definisi
Kemungkinan (Probabilitas)	Kesempatan atas peristiwa yang dapat terjadi, atau suatu nilai kerugian spesifik yang dapat terjadi di dalam aktivitas
Tinggi	Sangat mungkin bahwa ancaman dapat terjadi pada tahun depan
Sedang	Mungkin saja ancaman dapat terjadi pada tahun depan
Rendah	Sangat tidak mungkin ancaman dapat terjadi pada tahun depan

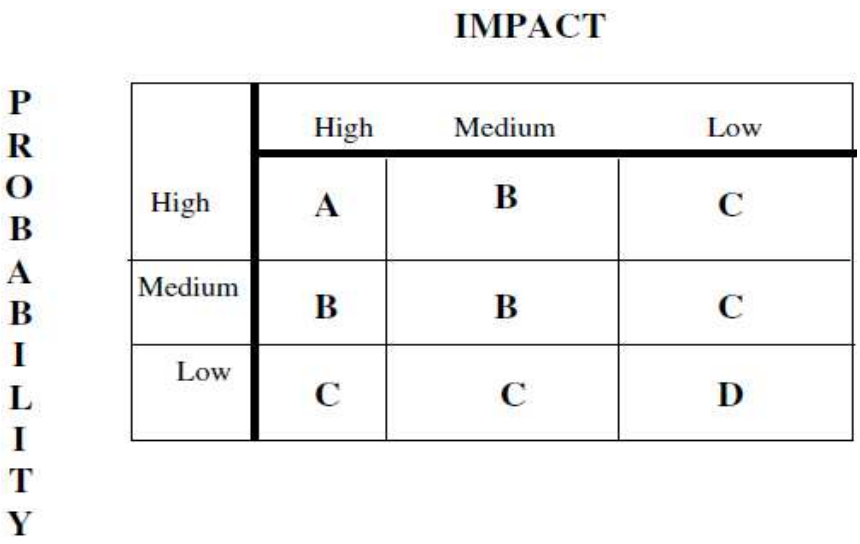
Tim akan membahas seberapa besar kemungkinan ancaman yang terjadi selama jangka waktu tertentu. Kelompok yang memiliki masalah terberat dalam pembahasan ancaman yang terjadi, namun tidak disertai dengan adanya pilihan *control* ditempat, akan menjadi kelompok yang memiliki pengetahuan mendalam mengenai pilihan *control* yang ada. Biasanya, ini akan menjadi administrasi jaringan, administrasi *database*, perubahan *control*, atau keamanan informasi. Menguji ancaman dengan cara tersebut, memungkinkan organisasi dalam menetapkan dasar atas resiko.

Setelah dikalkulasi, tim dapat memeriksa *control* yang ada untuk menentukan seberapa efektif *control* tersebut dalam mengurangi resiko. Ketika Anda memfasilitasi proses ini, maka anda harus mengingatkan orang - orang IT untuk terus berpartisipasi dan memberikan kontribusinnya dalam kegiatan ini. Dalam contoh ini, setelah kemungkinan telah ditetapkan, tim akan menentukan dampak dari ancaman yang terjadi, namun tanpa disertai penetapan atas pengendalian. Tim akan menggunakan definisi dampak seperti yang pada Tabel 2.3.

Tabel 2.3 Contoh Definisi Dampak FRAAP (Peltier, 2014)

Istilah	Definisi
Dampak	Sebuah ukuran besarnya kerugian atau kerusakan pada nilai suatuaset
Tinggi	Seluruh misi atau bisnis terkena dampak
Sedang	Kerugian terbatas pada unit bisnis tunggal atau tujuan
Rendah	Bisnis berjalan seperi biasa

Setelah menetapkan tingkatan dampak dan probabilitas/kemungkinan, tim akan melihat matriks tingkat resiko (Gambar 2.1) dan menetapkan tingkatan resiko dari ancaman tersebut.



Gambar 2.1 Matriks Tingkatan Resiko FRAAP (Peltier, 2014)

A – Tindakan korektif harus diimplementasikan

B – Tindakan korektif sebaiknya diimplementasikan

C – Memerlukan pemantauan

D – Tidak ada tindakan yang diperlukan saat ini

Seperti dalam matriks yang telah kita teliti tersebut, tim akan melihat di mana tingkat probabilitas dan tingkat dampak berpotongan, lalu memasukkan informasi ini ke dalam kertas kerja FRAAP (Tabel 2.4).

Tabel 2.4 Contoh Kertas Kerja FRAAP

Setelah Penetapan Tingkatan Resiko (Peltier, 2014)

Nomor Ancaman	**Ancaman**	**Tinjauan Elemen**	**Tingkatan Resiko**	**Kemungkinan *Control***
1.	Informasi diakes oleh personil yang tidak memiliki akses	*Integrity*	B	
2.	Ketidakjelasan atau tidak adanya versi atas informasi	*Integrity*	B	
3.	*Database* dapat rusak oleh kegagalan *hardware* atau *software* yang buruk	*Integrity*	D	
4.	Data dapat rusak akibat transaksi yang tidak lengkap	*Integrity*	C	
5.	Kemampuan untuk mengubah data dalam transit dan kemudian mengubahnya kembali untuk menutupi aktivitas	*Integrity*	C	
6.	Sebuah kegagalan untuk melaporkan masalah integritas	*Integrity*	A	

7.	Proses yang dijalankan tidak lengkap atau kegagalan untuk menjalankan suatu proses yang bisa merusak data	*Integrity*	B	
8.	Kurang lengkapnya proses internal dalam membuat dan mengontrol, serta mengelola data di seluruh fungsi	*Integrity*	A	
9.	Tidak adanya pemberitahuan mengenai masalah integritas	*Integrity*	A	
10.	Informasi yang digunakan pada konteks yang salah	*Integrity*	B	

Dalam bab berikutnya akan diadakan pemeriksaan mengenai variasi pada tema FRAAP, dan akan diteliti bagaimana FRAAP dapat digunakan, berikut dengan kontrol yang akan diimplementasikan. Untuk saat ini, penetapan atas tingkatan resiko yang dilakukan, didasarkan pada konsep bahwa tidak ada *control* yang diimplementasikan atau yang dijalankan.

2.2.3.2.3 Pembahasan pada FRAAP *Session*: Seleksi atas *Control*

"Proses terakhir dalam sesi FRAAP adalah mengidentifikasi *control* untuk ancaman - ancaman dengan tingkatan risiko tinggi. Dalam contoh yang telah dibuat, ancaman diketahui memiliki tingkatan resiko A atau B. Daftar sampel atas *control* terhadap ancaman yang ada, harus dikirim ke seluruh anggota tim, berikut dengan pemberitahuan pertemuan yang dijadwalkan, dan

salinan atas daftar tersebut harus tersedia bagi tim selama sesi FRAAP ini berlangsung. Selama langkah ini berlangsung, tim penilaian resiko akan menentukan *control* keamanan mana yang dapat mengurangi tingkatan resiko atas ancaman ke tingkat yang lebih dapat diterima. Sebagai contoh, akan digunakan satu set *control* berdasarkan organisasi teknologi informasi yang mendukung proses bisnis. Ada 34 *control* yang dapat tim pilih dari (Tabel 2.5). Memilih *control* yang sempurna tidak perlu dilakukan pada saat ini. Ingat, karena salah satu tujuan dari penilaian resiko adalah untuk mencatat semua alternatif yang dipertimbangkan dalam mengurangi tingkat resiko dari ancaman yang ada" (Peltier, 2014).

Tabel 2.5 Contoh Organisasi Teknologi Informasi yang Mendukung Proses Bisnis (Peltier, 2014)

Nomor *Control*	**Group TI**	***Descriptor***	**Definisi**
1.	Pengendalian Operasi	*Backup*	Persyaratan *backup* akan ditentukan dan dikomunikasikan dengan operasi, termasuk notifikasi elektronik atas *backup* yang telah selesai, dapat dikirim kepada administrator sistem aplikasi, Operasi akan diminta untuk menguji prosedur *backup*.
2.	Pengendalian Operasi	Rencana Pemulihan	Pengembangan, dokumen, dan pengetesan prosedur pemulihan, dirancang untuk memastikan bahwa aplikasi dan informasi dapat dipulihkan dari resiko, menggunakan prosedur *backup* yang telah dibuat, dalam kejadian yang dapat merugikan.
3.	Pengendalian Operasi	Analisa Resiko	Melakukan analisa resiko guna menentukan tingkat ancaman, dan mengidentifikasi kemungkinan

			perlindungan atau kontrol.
4.	Pengendalian Operasi	*Antivirus*	1. Memastikan administrator LAN (*Local Area Network*) telah menerapkan *antivirus* standar perusahaan pada seluruh komputer. 2. Pelatihan dan kesadaran dari teknik pencegahan terhadap virus, akan diterapkan dalam program proteksi informasi organisasi.
5.	Pengendalian Operasi	Depedensi Antarmuka	Sistem yang membutuhkan informasi, akan diidentifikasi dan dikomunikasikan dengan proses operasi, dalam upaya penekanan dampak atas kesalahan aplikasi.
6.	Pengendalian Operasi	Pemeliharaan	Persyaratan waktu untuk pemeliharaan teknis akan diteliti dan permintaan untuk penyesuaian akan dikomunikasikan kepada pihak manajemen.
7.	Pengendalian Operasi	*Service Level Agreement*	Menetapkan perjanjian tingkatan layanan (*Service Level Agreement*), untuk menetapkan tingkat harapan dari para pelanggan, dan jaminan dari operasi pendukung yang ada.
8.	Pengendalian Operasi	Pemeliharaan	Menetapkan perjanjian bagi pemasok dan pemeliharaan, untuk memfasilitasi status operasional berkelanjutan dari aplikasi.
9.	Pengendalian Operasi	Manajemen perubahan	*Control* migrasi produksi, seperti proses pencarian dan penghapusan data, untuk memastikan penyimpanan data bersih.
10.	Pengendalian Operasi	Analisa Dampak	Analisa dampak bisnis formal yang akan dilakukan untuk menentukan nilai kritis

		Bisnis	relatif dari suatu aset dengan aset lainnya.
11.	Pengendalian Operasi	*Backup*	Pelatihan *backup* bagi sistem administrator akan dilakukan beserta rotasi tugas, untuk memastikan efektifitas dari program pelatihan yang telah dilakukan.
12.	Pengendalian Operasi	*Backup*	Program kesadaran keamanan bagi para karyawan harus diterapkan, diperbaharui, dan setidaknya dilaksanakan setiap tahun.
13.	Pengendalian Operasi	Rencana Pemulihan	Menerapkan mekanisme untuk membatasi informasi kepada jaringan tertentu atau terhadap lokasi fisik yang ditetapkan.
14.	Pengendalian Operasi	Analisa Resiko	Menerapkan otentikasi pengguna, (seperti *firewalls, dial-in controls, secure ID*) untuk membatasi hak akses bagi yang tidak memiliki kewenangan dalam mengakses suatu informasi di dalam sistem.
15.	Pengendalian Aplikasi	Pengendalian Aplikasi	Merancang dan mengimplementasikan *control* aplikasi (pemeriksaan data yang masuk, melakukan validasi, indikator alarm, menilai *password* yang *invalid*) untuk menjamin integritas, kerahasiaan, dan ketersediaan informasi pada aplikasi.
16.	Pengendalian Aplikasi	Pengujian Penerimaan	Pengembangan prosedur pengetesan, yang harus dilakukan selama pengembangan aplikasi dijalankan, dan dalam proses modifikasi aplikasi yang

			diikuti dengan partisipasi dari pengguna (*system user*).
17.	Pengendalian Aplikasi	Pelatihan	Mengimplementasikan *User Programs* (evaluasi kinerja pengguna), yang dirancang untuk mendorong kepatuhan terhadap kebijakan dan prosedur yang ada, guna memastikan pemanfaatan yang tepat dari penggunaan aplikasi.
18.	Pengendalian Aplikasi	Pelatihan	Pengembang aplikasi akan menyediakan dokumentasi, bimbingan, dan dukungan kepada staf operasional dalam mekanisme pelaksanaan, untuk memastikan keamanan transfer informasi antara aplikasi.
19.	Pengendalian Aplikasi	Strategi Korektif	Tim pengembang akan mengembangkan strategi korektif seperti pemrosesan ulang, dan kebutuhan revisi atas aplikasi.
20.	Pengendalian Keamanan	Kebijakan	Mengembangkan kebijakan serta prosedur, untuk membatasi hak akses dan operasi sesuai dengan kebutuhan bisnis.
21.	Pengendalian Keamanan	Pelatihan (*user training*)	*User Training* yang dilakukan, mencakup dokumentasi tata cara penggunaan yang tepat dari aplikasi.Contohnya seperti pentingnya menjaga kerahasiaan atas akun pribadi, nilai *password*, beserta penekanan atas pentingnya menjaga informasi.
22.	Pengendalian Keamanan	*Review*	Menerapkan mekanisme untuk memantau, melaporkan, dan kebutuhan atas kegiatan audit, seperti pengecekan berkala atas validitas *User-ID*, untuk

			memverifikasi kebutuhan bisnis.
23.	Pengendalian Keamanan	Klasifikasi Aset	Aset yang sedang ditinjau (*review*), akan diklasifikasikan dengan kebijakan perusahaan, standar, dan prosedur klasifikasi aset.
24.	Pengendalian Keamanan	Pengendalian Akses	Mekanisme untuk melindungi *database* dari akses yang tidak sah, dan modifikasi yang dilakukan dari luar aplikasi, akan ditentukan dan dilaksanakan.
25.	Pengendalian Keamanan	Dukungan Manajemen	Meminta dukungan manajemen untuk menjamin kerja sama dan koordinasi dari berbagai unit bisnis.
26.	Pengendalian Keamanan	Hak Milik	Proses yang dilakukan untuk memastikan hak aset atas perusahaan telah dilindungi, dan menjamin perusahaan dalam memenuhi perjanjian lisensi.
27.	Pengendalian Keamanan	Kesadaran Keamanan	Menerapkan mekanisme *control* akses untuk mencegah akses yang tidak sah terhadap informasi. Mekanisme ini akan mencakup kemampuan dalam mendeteksi, *logging,* dan pelaporan jika ada upaya penerobosan keamanan informasi.
28.	Pengendalian Keamanan	Pengendalian Akses	Menerapkan mekanisme enkripsi (*data, end to end*) untuk mencegah akses tidak sah, yang berguna melindungi integritas dan kerahasiaan informasi.
29.	Pengendalian Keamanan	Pengendalian Akses	Mengikuti proses perubahan manajemen yang dirancang untuk memfasilitasi pendekatan struktural dari modifikasi aplikasi, guna memastikan ketepatan

			atas langkah dan tindakan pencegahan yang diterapkan. Modifikasi darurat harus disertakan dalam proses ini.
30.	Pengendalian Keamanan	Pengendalian Akses	Prosedur pengendalian yang diterapkan untuk melakukan *review* proses *sistem log* oleh pihak ketiga secara *independen,* bertujuan untuk menganalisa kegiatan *sistem update* yang dilakukan.
31.	Pengendalian Keamanan	Pengendalian Akses	Melakukan konsultasi dengan manajemen fasilitas, guna memfasilitasi kegiatan implementasi *control* keamanan fisik, yang dirancang untuk melindungi informasi, *software*, *hardware*, yang dibutuhkan oleh sistem.
32.	Pengendalian Sistem	Manajemen Perubahan	Persyaratan *backup* akan ditentukan dan dikomunikasikan dengan operasi, termasuk permintaan mengenai notifikasi elektronik *backup* yang telah diselesaikan, harus dikirim ke administrator sistem aplikasi. Operasi akan diminta untuk menguji prosedur *backup* tersebut.
33.	Pengendalian Sistem	*Log* Sistem *Monitor*	Pengembangan, dokumen, dan pengetesan prosedur pemulihan, dirancang untuk memastikan bahwa aplikasi dan informasi dapat dipulihkan dari resiko, menggunakan prosedur *backup* yang telah dibuat, dalam kejadian yang dapat merugikan.
34.	Keamanan Fisik	Keamanan Fisik	Melakukan analisa resiko guna menentukan tingkat ancaman, dan mengidentifikasi kemungkinan perlindungan atau *control*.

Tim akan menetukan *control* dari ancaman yang memiliki tingkatan resiko tinggi (ancaman dengan tingkat A atau B). Ancaman dengan tingkatan resiko C hanya akan dipantau, sedangkan ancaman dengan resiko tingkatan D tidak memerlukan tindakan tertentu. (Tabel 2.6). Semua *control* yang mungkin harus dimasukkan ke dalam kertas kerja FRAAP.

Tabel 2.6 Contoh Kertas Kerja FRAAP
dengan *Control* Yang di Identifikasi (Peltier, 2014)

Nomor Ancaman	**Ancaman**	**Tinjauan Elemen**	**Tingkatan Resiko**	**Kemungkinan *Control***
1.	Informasi diakes oleh personil yang tidak memiliki akses	*Integrity*	B	3, 5, 6, 11, 12, 16
2.	Ketidakjelasan atau tidak adanya versi atas informasi	*Integrity*	B	9, 13, 26
3.	*Database* rusak oleh kegagalan *hardware* atau *software* buruk	*Integrity*	D	
4.	Data dapat rusak akibat transaksi yang tidak lengkap	*Integrity*	C	
5.	Kemampuan untuk mengubah data dalam transit	*Integrity*	C	

	dan kemudian mengubahnya kembali untuk menutupi aktivitas			
6.	Sebuah kegagalan untuk melaporkan masalah integritas	*Integrity*	A	7, 11-13, 20. 21
7.	Proses yang dijalankan tidak lengkap atau kegagalan untuk menjalankan suatu proses yang bisa merusak data	*Integrity*	B	1, 2, 12-15, 18, 20, 21, 25
8.	Kurang lengkapnya proses internal dalam membuat dan mengontrol, serta mengelola data di seluruh fungsi	*Integrity*	A	7, 13, 17, 20, 23, 25
9.	Tidak adanya pemberitahuan mengenai	*Integrity*	A	7, 13, 26

	masalah integritas			
10.	Informasi yang digunakan pada konteks yang salah	*Integrity*	B	11, 12, 19

- Ancaman telah di identifikasi
- Tingkatan atas resiko telah ditetapkan
- Kemungkinan *control* telah di identifikasi

"Tim FRAAP tidak akan menghilangkan setiap ancaman yang ada. Manajemen yang mempunyai tugas untuk menentukan setiap ancaman yang ada, beserta *control* dari setiap ancaman yang harus di identifikasi. Pada dasarnya, Tim FRAAP dibentuk untuk membantu manajemen dalam membuat keputusan bisnis terkait dengan informasi" (Peltier, 2014).

2.2.3.3 Tahapan FRAAP Ketiga: *Post*-FRAAP

"Pada fase FRAAP ini, laporan yang dihasilkan berisikan mengenai penilaian resiko, dan bagaimana tindakan manajemen yang diambil sesuai dengan kebutuhan. Selama fase ini, fasilitator dan pemilik akan bekerja sama untuk membuat perencanaan penilaian resiko. Rencana ini mencakup tahapan sesi FRAAP 1 dan 2

Identifikasi ancaman:

- Tingkatan resiko
- Catatan kemungkinan *control*
- Identifikasi *control* yang ada
- *Control* terhadap ancaman terbuka
- Pihak yang bertanggung jawab atau dokumentasi perusahaan

Informasi tersebut akan dikombinasikan dengan pemeriksaan *control* biaya, dan laporan akhir akan muncul. *Post*-FRAAP memiliki tiga hal yang akan disampaikan:

- Penetapan waktu dalam pengambilan tindakan *control*

- Ringkasan laporan manajemen
- Halaman petunjuk *control*" (Peltier, 2014).

2.2.3.3.1 Rencana Tindakan (*Action Plan*)

Ketika sesi FRAAP tahap kedua telah selesai, maka informasi setelah sesi FRAAP ada pada tabel 2.7.

Tabel 2.7 Contoh Kertas Kerja ke-4 dalam Sesi FRAAP (Peltier, 2014)

Nomor Ancaman	**Ancaman**	**Kemungkinan *Control***	**Tingkat Resiko**	***Control* yang berjalan atau pemilihan *Control***	**Tanggung Jawab *Control***
1	Informasi yang di akses oleh pihak yang tidak berwenang	3,5,6,11, 12,16	B		Pemilik
2	Informasi yang tidak jelas	9,13,26	B		*Control* Produksi
3	*Database* yang rusak akibat kesalahan pada *hardware* atau *software*		D		
4	Data yang rusak akibat transaksi yang tidak lengkap		C		
5	Kemampuan mengubah data saat dilakukan pemindahan		C		

	data				
6	Kesalahan laporan	7, 11, 12, 13,20,21	A		
7	Proses yang dijalankan tidak selesai, sehingga bisa merusak data	1,2	B	Merancang dan mengimplementasikan aplikasi *control* untuk memastikan integritas, kerahasiaan, dan ketersediaan informasi aplikasi	Pengembangan aplikasi
8	kurangnya proses internal untuk membuat dan mengontrol, dan mengelola data di seluruh fungsi	7,13,17, 20,23,25	A	Memperoleh tingkat pelayanan untuk menetapkan jaminan bagi pelanggan dalam mendukung operasional	Operasi TI
9	Tidak ada pemberitahuan tentang masalah *Integrity*	7,13,26	A	Suatu program keamanan bagi karyawan telah diimplementasikan dan diperbarui, dan diperkenalkan kepada	Selesai

				karyawan	
10	Informasi yang digunakan tidak sesuai	11,12,19	B	Suatu program keamanan bagi karyawan telah di jalankan kepada karyawan	Selesai

Tabel 2.8 Contoh Rencana Tindakan FRAAP

(*Action Plan)* (Peltier, 2014)

Nomor Ancaman	Level Resiko	Tindakan yang dipilih oleh Pemilik	Tanggung Jawab Kelompok	Tanggal	Komentar Tambahan
1	B	ACF2 telah diterapkan dan dilakukan akses kontrol bagi pihak yang berwenang	Pemilik dan perlindungan informasi	7/15/2004	
2	B	Melakukan perubahan pada prosedur manajemen yang diterapkan	Operasi	Selesai	
3	D				
4	C				
5	C				

6	A	Penjadwalan pelatihan karyawan	HR	8/15/2004	
7	B	SLA cadangan yang ditinjau melalui operasi yang berjalan	Pemilik dan operasi	7/31/2004	
8	A	Penyedia layanan SLA yang akan diterapkan	Pemilik	8/20/2004	
9	A	Penyedia layanan SLA yang akan diterapkan	Pemilik	8/20/2004	
10	B	Melatih pengguna dalam menggunakan data	Pemilik, keamanan informasi	9/28/2004	

Pada Tabel 2.8 tersebut, berisikan hal - hal mengenai informasi yang digunakan untuk menyelesaikan perencanaan tindakan, atau yang biasa disebut dengan rencana aksi (*action plan*) yang merupakan tahapan dari *Post*-FRAAP.

2.2.3.3.2 *Cross-Reference Report*

Pengendalian digunakan untuk mengukur dampak resiko yang di identifikasi, contoh pengukuran tingkat resiko tersebut terdapat pada tabel berikut.

Tabel 2.9 Contoh kertas kerja *Cross-Reference* (Peltier, 2014)

Nomor *Control*	Deskripsi *Control*	Nomor Ancaman	Ancaman	Gambaran elemen	Tingkat Resiko
19	Menerapkan program bagi pengguna yang dirancang agar pengguna mematuhi kebijakan dan prosedur untuk memastikan aplikasi dimanfaatkan dengan baik				
		10	Penyalahgunaan informasi	INT	B
		13	Data diperbarui secara internal tetapi tidak dibuat secara eksternal	INT	B
		17	Keamanan dan otorisasi prosedur yang tidak dijalankan dengan baik, sehingga memproses bisnis	INT	A
		19	Membuat perubahan,	INT	B

			namun belum terlatih dalam keputusan		
		20	Publikasi informasi oleh pihak yang tidak memiliki otorisasi	INT	B
		21	Informasi yang dirubah tidak sah	INT	B
		24	Menyalah gunakan prosedur keamanan	CON	B
		32	Penyimpanan informasi penting yang tidak pasti tempat penyimpanan nya	CON	B
		33	Kurang data	CON	B

2.2.3.4 Tahap Pengambilanm Kesimpulan

Setelah penetapan pengendalian telah dipilih, rencana pelaksanaan harus mengidentifikasi siapa yang akan menerapkan *control* dan waktu pelaksanaan nya. Jika pemilik memutuskan untuk menerima resiko, maka tindakan ini harus diidentifikasi dalam rencana pelaksanaan dan ringkasan laporan manajemen. Unsur terakhir dari dokumentasi penilaian resiko dengan menggunakan metode FRAAP adalah *cross-reference*. Mengidentifikasi

ancaman dan memilih *control* merupakan hal yang penting, tetapi unsur yang paling penting dalam proses penilaian resiko yang efektif adalah membangun tingkatan resiko. Sebelum setiap perusahaan dapat memutuskan apa yang harus dilakukan, perusahaan harus memiliki gambaran yang jelas tentang masalahnya. Ketika tingkat resiko harus ditentukan, hal tersebut menjadi poin penting bagi tim untuk memahami ancaman yang akan dinilai.

Selain itu karena pada metode FRAAP staff non teknis atau non keamanan dapat terlibat dan juga melibatkan manajer operasional sehingga hasilnya dapat secara langsung terkait dengan strategi bisnis. Gambaran analisa pengukuran risiko TI nya juga mengacu kepada pendapat ahli yang dalam hal ini adalah manajer sebagai perwakilan perusahaan yang memahami risiko dan proses TI yang berlangsung.

2.2.3.5 Penelitian Sebelumnya

2.2.3.5.1 FRAAP

Menurut thariq dalam penelitian ini dilakukan penelitian terhadap besarnya resiko – resiko dalam implementasi pada PT Abc untuk menentukan analysis resiko serta mengidentifikasi dan ancaman yang ada.dari penelitian tersebut kemudian keluar hasil dari identifikasi risiko mengenai:

1. Kehilangan informasi akibat kesalahan pada proses input data.
2. Kesalahan klasifikasi informasi.
3. Kerusakan Hardware akibat SDM yang kurang terlatih.
4. Menentukan bagaimana resiko yang ada dapat dikontrol atau dikurangi.

Sebelum pembangunan FRAAP analysis resiko sering di anggap sebagai tugas utama yang dibutuhkan perusahaan dan memakan waktu yang panjang untuk menyelesaikan dan mempresentasikan anggran item yang besar dan biaya yang efektif dengan menggunakan FRAAP diharapkan analysis resiko dilakukan dalam hitungan hari bukan mingguan atau bulanan sehingga analisis resiko bukan merupakan kendala.

Tujuan Penelitian mengidentifikasi dan mengukur resiko,memprioritaskan factor resiko yang ditemukan dan menentukan bagaimana resiko yang ada dapat dikontrol atau dikurangi.serta menerapkan Teknologi Informasi untuk mendukung untuk

menjalankan proses bisnis dengan cukup baik mengacu pada resiko yang telah di identifikasi serta perbaikan dalam mengelola resiko.

2.2.3.5.2 Penjualan

Menurut lira pada penelitian audit sistem informasi penjualan atas aktivitas penjualan barang dagang, apakah dalam sistem informasi penjualan di perusahaan terdapat masalah dan bagaimana cara mendeteksi dan mencegah masalah yang ada. Penelitian yang dimaksud, yaitu dengan tujuan untuk kelancaran kegiatan operasional perusahaan.

Tujuan pemeriksaan operasional atas fungsi penjualan dan piutang dagang pada PT Kimia Farma T&D yaitu:

1. Untuk menilai apakah pelaksanaan kegiatan penjualan telah terlaksana sesuai dengan kebijakan dan prosedur yang telah ditetapkan perusahaan.
2. Untuk mendeteksi kelemahan dalam kegiatan penjualan
3. memberikan rekomendasi perbaikan yang diperlukan dan kelancaran kegiatan yang sedang berjalan.
4. Menghasilkan output yang yang ada.

Maka dalam audit sistem informasi penjualan pada PT KFTD dapat disimpulkan :

Pertama,Untuk Menilai Kegiatan Operasional penjualan terlaksana sesuai kebijakan dalam melaksanakan audit operasional diperlukan persiapan dan perencanaan yang baik untuk mendapatkan hasil yang maksimal sehingga pada akhirnya dapat mengatasi masalah yang dihadapi oleh perusahaan.

Kedua,untuk mendeteksi kelemahan dalam kegiatan penjualan terlebih dahulu mengadakan perencanaan untuk menganalisis kegiatan tersebut berjalan dengan baik atau mengidentifikasi perencanaan yang merupakan penyusunan strategi menyeluruh mengenai tindakan yang akan dilakukan dan ruang lingkup kegiatan penjualan.

Ketiga Untuk memulai suatu audit, rekomendasi perbaikan yang dilakukan seperti oleh seorang auditor harus terlebih dahulu mengadakan perencanaan

audit. Perencanaan audit merupakan penyusunan strategi menyeluruh mengenai tindakan yang akan dilakukan dan ruang lingkup audit. Luas sempitnya ruang lingkup audit operasional akan tergantung pengendalian intern. Semakin baik pengendalian intern di suatu perusahaan semakin sempit pula ruang lingkup audit operasional yang perlu diteliti auditor, begitu sebaliknya.

Keempat, Setiap pengiriman barang yang dilakukan oleh PT KIMIA FARMA T&D kepada para langganan atau customernya selalu didukung oleh surat jalan atau dokumen pengiriman lainnya. Dalam pengriman barang tersebut, perusahaan selalu memberikan nomor urut cetak terhadap semua dokumen (kwitansi, surat jalan, dan sebagainya). Nomor urut cetak yang diberikan oleh perusahaan terhadap semua dokumen (kwintansi, surat jalan, dan dokumen pendukung lainnya), yang berhubungan dengan proses penjualan kredit kepada langganan atau customernya, selalu diperiksa oleh bagian fungsi administrasi penjualan dan piutang dagang yang dijabat oleh kepala TU, dengan tujuan untuk membuat laporan penjualan/PD dan menghindari adanya penyimpangan yang dilakukan oleh pihak-pihak yang tidak bertanggung jawab.menggunakan faktur penjualan sebagai dasar untuk penjualan dan membuat surat jalan. Dan memberikan nomor urut cetak terhadap semua faktur penjualan kredit dan penjualan tunai, dengan melakukan pemisahan terhadap kedua faktur tersebut. Setelah semua dokumen atas terjadinya suatu penjualan terkumpul diserahkan kepada bagian fungsi administrasi Inkasso, untuk juga diserahkan kepada bagian TU (Juru Tagih).