BAB 2

Landasan Teori

2.1 Teori Umum

Dalam sub bab ini akan dijelaskan mengenai teori-teori umum yang diperlukan sebagai pedoman penerapan audit sistem informasi yang baik digunakan sebagai dasar pembahasan.

2.1.1 Pengertian Sistem

Menurut MC.Leod (2001, p11), sistem adalah sekelompok element yang terintegrasi dengan maksud yang sama untuk mencapai suatu tujuan.

Menurut Mulyadi (2001, p1-3), setiap sistem dibuat untuk menangani sesuatu yang berulang kali atau yang secara rutin terjadi. Sistem pada dasarnya adalah sekelompok unsur yang berhubungan erat satu dengan yang lainnya berfungsi bersama-sama untuk mencapai tujuan tertentu, dari definisi tersebut dapat diuraikan lebih lanjut tentang sistem berikut :

1. Setiap sistem terdiri dari unsur-unsur, unsur-unsur tersebut terdiri dari subsistem yang lebih kecil, yang terdiri pula dari kelompok unsur yang membentuk subsistem tersebut
2. Unsur-unsur tersebut merupakan bagian terpadu sistem yang bersangkutan, unsur-unsur sistem tersebut berhubungan erat satu dengan yang lainnya. Sifat dan kerja sama antar unsur dari sistem tersebut mempunyai bentuk tertentu.
3. Unsur sistem tersebut bekerjasama untuk mencapai suatu tujuan.

4. Suatu sistem merupakan bagian dari sistem yang lain yang lebih besar.

Jadi dapat disimpulkan bahwa sistem adalah unsur-unsur yang saling bergabung untuk mencapai suatu tujuan tertentu menangani suatu yang terjadi secara rutin, berhubungan erat satu dengan yang lainnya dan merupakan bagian dari sistem lain yang lebih besar.

2.1.2 Pengertian informasi

Menurut MC Leod (2001, p4) informasi adalah jenis utama sumber daya yang tersedia bagi manager.

Menurut Hall yang telah di terjemahkan oleh Teguh (2001,p14), informasi bukan sekedar fakta yang diproses dalam suatu laporan formal. Informasi memungkinkan para pemakainnya melakukan tindakan yang menyelesaikan konflik, mengurangi ketidakpastian, dan melakukan keputusan. Ada tiga jenis syarat yang harus dipenuhi agar suatu informasi dapat dikatakan mempunyai kualitas tinggi, yaitu:

a. Akurat

   Informasi harus bebas dari kesalahan-kesalahan dan harus jelas mencerminkan maksudnya sehingga menimbulkan banyak gangguan yang dapat merubah merusak informasi.

b. Tepat waktu

   Informasi yang datang pada penerima tidak boleh terlambat. Sebab informasi yang terlambat menjadi tidak bernilai lagi karena informasi merupakan landasan dalam pengambilan keputusan.

c. Relevan

Informasi tersebut harus mempunyai manfaat bagi para pemakai

Dari definisi diatas dapat disimpulkan bahwa informasi adalah data-data yang telah diproses,dan merupakan suatu sumber daya yang dapat digunakan untuk mencapai tujuan.

2.1.3 Pengertian sistem informasi

Menurut James A.O'brien (2006,p5) sistem informasi dapat merupakan kombinasi teratur apapun dari orang-orang, hardware, software, jaringan komunikasi, dan sumber daya data yang mengumpulkan, mengubah, dan menyebarkan informasi dalam sebuah organisasi.

Menurut Hall yang telah di terjemahkan oleh jusuf (2001,p7), sistem informasi adalah sebuah rangkaian prosedur formal dimana data dikumpulkan, diproses menjadi informasi dan didistribusikan kepada para pemakai.

Menurut Muchtar (1999,p3), sistem informasi adalah suatu pengorganisasian peralatan untuk mengumpulkan, meng-*input*, memproses, menyimpan, mengatur, mengontrol, dan melaporkan informasi untuk pencapaian tujuan perusahaan.

Berdasarkan definisi-definisi diatas dapat di simpulkan bahwa sistem informasi adalah serangkaian prosedur yang saling berhubungan satu sama lain serta bersama-sama menjalankan fungsi dan memiliki tugas masing-masing guna mengumpulkan, memproses, menyimpan, dan mendistribusikan informasi dalam rangka mencapai tujuan perusahaan.

2.1.4 Pengertian sistem informasi penjualan

Berdasarkan Standard Akuntansi Keuangan mendefinisikan, “penjualan barang meliputi barang yang diproduksi perusahaan untuk dijual dan barang yang dibeli untuk dijual kembali seperti barang dagang yang dibeli pengecer atau tanah properti lain yang dibeli untuk dijual kembali”.

Menurut Swastha (1999,p8), “penjualan merupakan suatu ilmu atau seni untuk mempengaruhi pribadi, yang dilakukan oleh penjualan untuk mengajak orang lain agar bersedia membeli barang atau jasa yang ditawarkan”.

Menurut sidharta(1996,p46) sistem penjualan adalah struktur interaksi antar manusia, peralatan metode-metode, dan kontrol-kontrol yang disusun untuk mencapai tujuan tertentu dalam menyediakan aliran informasi yang mendukung :

a. Rutinitas kerja dalam bagian order penjualan, bagian kredit, dan bagian pengiriman.
b. Pembuatan keputusan untuk personil-personil yang mengatur fungsi penjualan dan fungsi pemasaran.

Menurut Mulyadi (2001,p210), penjualan kredit adalah penjualan yang di laksanakan oleh perusahaan dengan cara mengirimkan barang sesuai dengan *order* yang diterima dari pembeli untuk jangka waktu tertentu dan perusahaan mempunyai tagihan kepada pembeli tersebut.

Menurut Hall (2001,p58), mayoritas penjualan bisnis dilakukan atas dasar kredit dan melibatkan tugas-tugas seperti penyiapan pesanan penjualan, pemberian kredit, pengiriman produk kepada pelanggan, dan pencatatan transaksi dalam akun.

Berdasarkan definisi-definisi diatas dapat disimpulkan bahwa Sistem informasi penjualan merupakan sekumpulan data penjualan yang telah diproses menjadi informasi penjualan yang berguna dan didistribusikan kepada para pemakainnya untuk mencapai tujuan tertentu. Dalam penjualan kredit,jika order dari pelanggan telah terpenuhi dengan pengiriman barang atau jasa, untuk jangka waktu tertentu perusahaan memiliki piutang kepada pelanggannya.

2.1.4.1 Jenis-jenis penjualan

Menurut Mulyadi (2001, p202), kegiatan penjualan barang dan jasa dapat dibedakan menjadi 2 jenis:

1. Kegiatan penjualan kredit

   didalam transaksi penjualan kredit, jika *order* dari pelanggan telah dipenuhi dengan pengiriman barang atau penyerahan jasa, untuk jangka waktu tertentu perusahaan memiliki piutang kepada pelanggan.

2. Kegiatan penjualan tunai

   didalam transaksi penjualan tunai, barang atau jasa baru dierahkan oleh perusahaan kepada pembeli jika perusahaan telah menerima kas dari pembeli.

2.1.4.2 Fungsi-fungsi yang terkait sistem penjualan kredit

Menurut Mulyadi (2001, p211), fungsi yang terkait dalam sistem penjualan kredit adalah :

A. Fungsi penjualan

fungsi ini bertanggung jawab untuk menerima order dari pembeli, meng-*edit* order dari pelanggan untuk menambahkan informasi yang belum ada pada surat order tersebut (seperti spesifikasi barang dan rute pengiriman), meminta otorisasi kredit, menentukan tanggal pengiriman dan dari gudang mana barang akan dikirim dan mengisi surat order pengiriman.

B. Fungsi kredit

fungsi ini berada dibawah fungsi keuangan yang dalam transaksi penjualan kredit, bertanggung jawab untuk meneliti status kredit pelanggan dan memberikan otorisasi pemberian kredit kepada pelanggan.

C. Fungsi gudang

fungsi ini bertanggung jawab untuk menyimpan barang dan menyiapkan barang yang dipesan oleh pelanggan, serta menyerahkan barang ke fungsi pengiriman.

D. Fungsi pengiriman

fungsi ini bertanggung jawab untuk menyerahkan barang atas dasar surat order pengiriman yang diterimanya dari fungsi penjualan.

E. Fungsi penagihan

fungsi ini bertanggung jawab untuk membuat dan mengirimkan

faktur penjualan kepada pelanggan serta menyediakan copy faktur bagi kepentingan pencatatan transaksi penjualan oleh fungsi akuntansi.

F. Fungsi akuntansi

fungsi ini bertanggung jawab untuk mencatat piutang yang yang timbul dari transaksi penjualan kredit dan membuat serta mengirimkan pernyataan piutang kepada debitur, serta membuat laporan penjualan.

2.1.4.3 Fungsi-fungsi yang terkait sistem penjualan tunai

Menurut Mulyadi (2001, p 462), fungsi yang terkait didalam sistem informasi penjualan tunai :

A. Fungsi penjualan

   fungsi ini bertanggung jawab untuk menerima order dari pembeli, mengisi faktur penjualan tunai, dan menyerahkan faktur tersebut kepada pembeli untuk kepentingan pembayaran harga barang ke fungsi kas.

B. Fungsi kas

   fungsi ini bertanggung jawab sebagai penerima kas dari pembeli.

C. Fungsi gudang

   fungsi ini bertanggung jawab untuk menyiapkan barang yang dipesan oleh pembeli, serta menyerahkan barang tersebut ke fungsi pengiriman.

D. Fungsi pengiriman

   fungsi ini bertanggung jawab untuk membungkus barang dan menyerahkan barang yang telah dibayar harganya kepada pembeli.

E. Fungsi akuntansi

fungsi ini bertanggung jawab sebagai pencatat transaksi penjualan dan penerimaan kas dan membuat laporan penerimaan kas.

2.1.5 Pengertian Audit

Menurut Arens dan Loebbecke yang diterjemahkan oleh Jusuf,A.A. (1997,p1), *auditing* adalah proses pengumpulan dan pengevaluasian bahan bukti tentang informasi yang dapat diukur mengenai suatu entitas ekonomi yang dilakukan seorang yang kompeten dan *independent* untuk dapat menentukan dan melaporkan kesesuaian informasi dimaksud dengan kriteria-kriteria yang telah di tetapkan.

Menurut Mulyadi (2002,p9), *Auditing* adalah suatu proses sistematis untuk memperoleh dan mengevaluasi bukti secara obyektif mengenai pernyataan-pernyataan tentang kegiatan dan kejadian ekonomi dengan tujuan untuk menetapkan tingkat kesesuaian antara pernyataan-pernyataan dengan criteria-kriteria yang telah ditetapkan, serta penyampaian hasil-hasilnya kepada pemakai yang berkepentingan.

Menurut Mulyadi (2002,p30), *auditing* digolongkan menjadi 3 golongan:

1. Audit laporan keuangan

   Audit yang dilakukan oleh *auditor independent* terhadap laporan keuangan disajikan oleh kliennya untuk menyatakan pendapat mengenai kewajaran laporan keuangan tersebut.

2. Audit kepatuhan

Audit yang bertujuan untuk menentukan apakah yang di *audit* sesuai dengan kondisi atau peraturan tertentu.

3. Audit operasional

Memiliki tujuan untuk mengevaluasi efektifitas dan efisiensi kinerja, mengidentifikasi kesempatan untuk peningkatan dan membuat rekomendasi untuk perbaikan atau tindakan lebih lanjut.

Berdasarkan definisi-definisi diatas dapat disimpulkan bahwa Audit adalah suatu kegiatan untuk memeriksa dengan cara mengumpulkan bukti-bukti dan mengevaluasinya berdasarkan standard yang ada, kemudian akan menghasilkan laporan yang independent mengenai kesesuaian kegiatan atas kejadian yang diperiksa.

2.1.6 Struktur organisasi

Menurut James L. Gibson (1990) Tujuan dari srtuktur organisasi adalah mengendalikan perilaku, menyalurkan dan mengarahkan perilaku untuk mencapai apa yang dianggap menjadi tujuan dari organisasi.

Struktur bertautan dengan hubungan yang relatif pasti yang terdapat diantara pekerjaan-pekerjaan dalam organisasi. Hubungan ini timbul dari keputusan berikut :

1. Pembagian pekerjaan. Seluruh tugas unit dipecah dalam beberapa pekerjaan yang lebih kecil yang berurutan. Yaitu tugas dibagi-bagi diantara orang-orang dalam unit tersebut.

2. Pekerjaan individual digabungkan dan dikelompokan jadi satu. Ditentukan dasar umum untuk mencarikan alasan bagi pengelompokan ini, hal ini menyangkut departementelisasi.
3. Ukuran yang tepat bagikelompok yang melapor kepada satu atasan harus ditentukan, ini menyangkut masalah rentang kendali.
4. Wewenang dibagikan diantara pekerjaan atau kelompok pekerjaan ini merupakan masalah delegasi.

2.1.7 Pengendalian Fungsi IT

Menurut James E. Hunton (2004, p106) kategori-kategori utama yang harus dikontrol dalam fungsi TI meliputi keamanan *input,*proses,*output,* database, *backup* dan *recovery*. Setiap kategori harus dikontrol untuk meminimalisasi bisnis dan risiko audit. Ketika menilai kontrol fungsi audit, penting bagi IT auditor untuk menilai apakah kontrol risiko masih dalam batas yang biasa ditoleransi. Atau kontrol yang harus ditingkatkan atau diturunkan untuk mendapatkan level yang diterima.

2.1.7.1 *Security Controls*

Manager TI bertanggung jawab atau menjamin bahwa infrastrukstur komputer sudah aman dari ancaman *internal* dan *eksternal*. Sebuah infrastuktur dapat mempengaruhi risiko bisnis dan risiko audit secara signifikan. Kita dapat menilai keamanan melalu 2 cara yaitu *physical* dan *logical security*.

2.1.7.1.1 *Physical Security*

Keamanan fisik berfokus kepada menjaga fasilitas, komputer, alat-alat komunikasi dan aspek-aspek terlihat lainnya dari infrastruktur komputer aman dari ancaman-ancaman. Mengacu pada kontrol fasilitas akses keamanan adalah hal utama yang harus diperhatikan. Jadi hanya orang-orang yang memiliki otorisasi yang diperbolehkan untuk mengakses fasilitas dan pengunjung harus ditemani utnuk orang yang memiliki otorisasi untuk mengakses pengamanan akses dapat dilakukan dengan berbagai cara seperti *security guard*, kunci dan gembok, *card reader, finger print reader* dan lain-lain. Dan sebagai tambahan jendela,ventilasi keluar dan akses keluar lainnya harus diamankan dengan menggunakan palang seperti *safety glass* dan lain-lain.

Langkah selanjutnya dalam membuat sistem keamanan adalah dengan meng-*install* mekanisme pengawasan tentang siapa yang masuk,menggunkan dan meninggalkan fasilitas. Contohnya satpam berjaga-jaga di area fasilitas, penggunaan video kamera di berbagai tempat dan penggunaan alarm di titik akses.

2.1.7.1.2 *Logical security*

Secara umum bagian yang paling penting dari infrastuktur komputer adalah bagian yang tidak terlihat meliputi data koorporat dan software komputer.(aplikasi *user*, sistem, *network*, sistem komunikasi dan operating sistem). Bagian-bagian ini

dikenal sebagai komponen *logical* dari infrastuktur. Bagian dari sistemselain komponen logika di jaga via *physical* kontrol jadi setiap orang yang ingin menggunakan data dan software harus memakai ID dan *password* dan berdasarkan ID dan *password* tersebut maka dapat ditentukan aplikasi-aplikasi apa sajakah yang dapat dijalankan dan informasi apa saja yang dapat dilihat. Untuk sistem berbasis internet biasanya menggunakan firewall, jadi hanya orang-orang tertentu yang dapat meng-upload dan menggunakan data.

2.1.7.2 *Information control*

Proses mengumpulkan, memproses, dan mendistribusikan informasi dapat diklasifikasikan menjadi aktifitas, *input*, proses, *output*. Dalam setiap aktivitas, pengawasan diperlukan untuk menjamin integritas dan keakuratan dari informasi. Sebagai tambahan perusahaan harus membuat *backup* dari informasi dan proses. Risiko audit sangat tinggi jika *internal control* rendah, proses *input*-proses-*output* tidak efisien.

2.1.7.2.1 *Input control*

Auditor SI harus melihat apakah perusahaan sudah mengikuti prosedur-prosedur tertulis mengenai otorisasi, pengesahan dan *input* transaksi akun.

2.1.7.2.2 *Output control*

Akses ke *auto control* harus dikontrol sehingga informasi yang diminta dapat dilihat oleh pihak yang berkepentingan jika

output yang diminta ditampilkan dilayar komputer maka layar harus ditempatkan ditempat yang aman dari pihak-pihak yang tidak berkepentingan. Pada perusahaan biasanya *output* berbentuk *hard copy*, jadi hasil *hard copy* harus diamankan

2.1.7.3 *Continuity control*

Resiko bisnis yang paling utama terkait dengan bisnis IT adalah terganggunnya aktivitas bisnis dikarenakan kesalahan komputer. Oleh karena itu, perusahaan mempersiapkan diri untuk menghadapi hal-hal tersebut sehingga jika terjadi kesalahan proses bisnis tidak atau terlalu terganggu.

2.1.7.3.1 *Backup control*

Sangat penting bagi perusahaan untuk membangun strategi *backup* jika tidak maka seluruh data dapat hilang jika terjadi kesalahan ada beberapa hal yang harus diperhatikan yaitu :

- waktu pemulihan
- biaya

Semakin cepat waktu pemulihan maka semakin tinggi biaya yang dikeluarkan. Ada 2 jenis *backup* yaitu data dan *hardware,* data *backup* harus mempertimbangkan volume transaksi *technical support,* lokasi penyimpanan, *redudansi hardware-hardware backup* jika salah satu atau beberapa komponen hardware terganggu, maka sistem dan proses bisnis akan terganggu jika terjadi mati listrik.

2.1.7.4 *Disaster discovery control*

Perusahaan tidak dapat menunggu sampai bencana terjadi dan baru memikirkan apa yang harus dilakukan. Mereka harus proaktif bukan reaktif. Perusahaan harus merencanakan sebelum bencana terjadi dan mengetes secara periodik rencananya. Manajer IT harus menentukan risiko-risiko apa sajakah yang dapat terjadi dan apa yang harus dilakukan. Setelah itu harus membuat rencana perbaikan sistem.

2.1.8 Instrumen penelitian

2.1.8.1 Observasi

Menurut Indrianto dan Supomo (1999,p157), observasi yaitu proses pencatatan pola perilaku subjek (orang) obyek (benda), atau kejadian yang sistematik tanpa adanya pertanyaan atau komunikasi dengan individu yang diteliti. Tipe-tipe observasi dibagi menjadi :

1. Observasi langsung, yaitu observasi langsung yang dilakukan oleh peneliti
2. Observasi mekanik, yaitu observasi yang dilakukan dengan bantuan peralatan mekanik seperti (kamera, video, mesing hitung)

2.1.8.2 Wawancara

Menurut Indrianto dan Supomo (1999,p152-154), wawancara merupakan teknik pengumpulan data dalam metode survey yang

menggunakan pertanyaan secara lisan kepada subjek penelitian. Teknik wawancara dapat dilakukan dengan 2 cara:

1. Wawancara tatap muka, yaitu metode pengumpulan data primer dapat dilakukan dengan cara komunikasi langsung tatap muka antara penanya dengan responden yang menjawab pertanyann secara lisan.
2. Wawancara dengan telepon, yaitu pertanyaan peneliti dan jawaban responden (wawancara) dapat juga dilakukan melalui telepon.

2.1.8.3 Kuesioner

Menurut Singarimbun (1995, p175-186) dalam survey penggunaan kuesioner merupakan hal yang pokok untuk pengumpulan data. Jenis-jenis kuesioner berdasarkan jenis pertanyaan dibagimenjadi :

1. Pertanyann tertutup, yaitu jawaban sudah ditentukan sehingga *responden* tidak diberi kesempatan memberi jawaban lain.
2. Pertanayaan terbuka, yaitu jawaban tidak ditentukan oleh peneliti sehingga *responden* bebas memberikan jawaban
3. Pertanyaan kombinasi terbuka dan tertutup, yaitu jawaban sudah ditentukan tapi disusul dengan pertanyaan terbuka.
4. Pertanyaan semi terbuka, yaitu jawaban sudah disusun tetapi ada kemungkinan tambahan jawaban.

2.1.9 Visi dan Misi

Menurut Ir.Hendro (2006), visi adalah pandangan tujuan dan imajinasi seorang pemilik (owner) atau pemimpin bisnis tentang perusahaan baik bentuk, posisi, letak, arah atau sosoknya di dalam peta persaingan bisnis yang sedang digeluti untuk beberapa tahun yang akan datang. Sedangkan misi adalah tujuan bisnis secara jangka panjang,yaitu lebih dari 10 tahun hingga kita "tahu apa tujuan bisnis kita dan mau diapakan bisnis kita ini.

2.1.10 Pendekatan risiko

Menurut Arens dan Loebbecke yang diterjemahkan oleh Amir Abdi Jusuf (1995,p.222) risiko berarti bahwa auditor menerima suatu tingkat ketidakpastian tertentu dalam pelaksanaan audit. Menurut Amin (2005,p.79) risiko dibagi jadi 3 macam. Yaitu :

1. *Control risk (*risiko pengendalian) risiko bahwa suatu salah saji material yang dapat terjadi dalam suatu asersi tidak dapat dicegah atau ditemukan secara tepat waktu oleh kebijakan atau prosedur struktur pengendalian intern suatu perusahaan
2. *Detection risk* (risiko deteksi) risiko bahwa auditor tidak dapat menemukan salah saji material dalam suatu asersi
3. *Inherent risk* (risiko bawaan) kerentanan suatu asersi terhadap salah saji material dengan asumsi tidak ada kebijakan atau prosedur struktur pengendalain intern yang berkaitan.

2.1.11 Teori Proses Bisnis

Definisi Proses adalah serangkaian langkah sistematis, atau tahapan yang jelas dan dapat ditempuh berulangkali, untuk mencapai hasil yang diinginkan. Jika ditempuh, setiap tahapan itu secara konsisten mengarah pada hasil yang diinginkan.

Sumber **:** http://kakilimasubang.wordpress.com/2008/07/09/definisi-proses/

Definisi Bisnis : adalah suatu organisasi yang menjual barang atau jasa kepada konsumen atau bisnis lainnya, untuk mendapatkan laba

Sumber : http://id.wikipedia.org/wiki/Bisnis

Menurut Dasaratha V. Rama (2006,p.22-23) Proses bisnis merupakan seperangkat aktifitas yang dilakukan oleh suatu bisnis untuk memperoleh, menghasilkan,serta menjual barang dan jasa. Satu cara penting untuk mempelajari proses bisnis perusahaan adalah dengan berfokus pada siklus transaksi. Siklus transaksi mengelompokkan kejadian terkait yang pada umumnya terjadi dalam suatu urutan tertentu. Proses bisnis dapat disusun menjadi tiga siklus transaksi utama :

1. Siklus pemerolehan/pembelian

   Mengacu pada proses pembelian barang dan jasa.

2. Siklus konversi

   Mengacu pada proses mengubahsumber daya yang diperoleh menjadi barang-barang dan jasa. Siklus konversi memiliki sifat yang kompleks.

3. Siklus pendapatan

   Mengacu pada proses menyediakan barang dan jasa untuk pelanggan.

Proses Bisnis adalah Sekumpulan tugas atau aktivitas untuk mencapai tujuan yang diselesaikan baik secara berurut atau paralel, oleh manusia atau sistem, baik di luar atau di dalam organisasi .

2.1.12 Identifikasi risiko IT

Menurut James E. Hunton (2004.p.48-51) *Bisnis enterprises* menghadapi beberapa resiko, termasuk bisnis, audit, *security, continuity risks*.

2.1.12.1 *Business risk*

Risiko bisnis merupakan kemungkinan bahwa suatu organisasi tidak akan mencapai tujuan bisnis. Faktor *eksternal* dan *internal* dapat berpengaruh terjadinya risiko bisnis. Untuk mengerti fakta-fakta risiko bisnis suatu organisasi, pertama-tama auditor harus lebih mengenal rencana strategi organisasi. Secara garis besar rencana organisasi harus memiliki jangka waktu yang pendek (3-5 tahun). Bersamaan dengan strategi dan tujuan, karyawan akan mengetahui misi dari organisasi.

2.1.12.2 *Audit risk*

Risiko audit merupakan kemungkinan bahwa auditor *external* organisasi melakukan kesalahan ketika mengeluarkan pendapat yang menjadi bukti untuk suatu kewajaran pada laporan keuangan atau seorang auditor IT gagal untuk menemukan kesalahan atau kecurangan bahan tersebut. Risiko audit sebenarnya

merupakan kombinasi dari risiko, yaitu termasuk *inherent risk, control risk, and detection risk*.

2.1.12.3 *Security risk*

Risiko keamanan IT merupakan risiko yang berhubungan dengan data akses dan integritas. Akses yang tidak diizinkan untuk mengakses data yang mungkin berbentuk *logical* maupun *physical* data. Memungkinkan seorang pengguna lalai untuk mematikan komputer setelah selesai bekerja. Banyak risiko yang berhubungan dengan *physical* dan *logical* akses yang tidak diberikan izin.

Risiko ini meningkat bersamaan dengan *integrasi* sistem informasi dan *remote akses capability.*

2.1.12.4 *Continuity risk*

Risiko berkelanjutan termasuk risiko yang berhubungan dengan sistem informasi yang ada dan *backup* and *recovery*. Ketersediaan yang ada tertuju pada keamanan yang menjamin suatu sistem informasi selalu dapat diakses oleh pengguna. Prosedur *Backup* and *recovery* menjamin bahwa dalam kasus ganguan yang berkelanjutan, prosedur tersedia untuk menyimpan data dan kegiatan operasional. *Backup* data dan *recovery* data dapat dilakukan berdasarkan besar atau kecilnya suatau organisasi, jika organisasi semakin besar maka biaya dan kesilitan semakin besar. Organisasi yang tidak terlalu besar cukup dengan disket atau CD untuk back up datanya. Sedangkan perusahaan yang besardapat dengan menyewa server untuk back up dan recovery data.

2.1.13 Teori Overview Activity Diagram

Menyajikan suatu pandangan tingkat tinggi dari proses bisnis dengan mendokumetasikan kejadian-kejadian penting, urutan kejadian-kejaidian ini, dan aliran informasi antar kejadian.

Simbol-simbol diagram Activity :

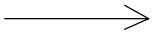
1. Lingkaran penuh

 memulai suatu proses dalam suatu diagram aktivitas

2. Segiempat panjang

kejadian, aktivitas atau pemicu

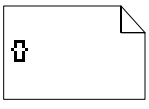
3. Garis tidak terputus

 urutan dari suatu kejadian atau aktivitas yang keberikutnya

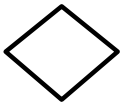
4. Garis putus-putus

 alur informasi antar kejadian

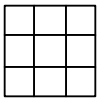
5. Dokumen

 menunjukkan dokumen sumber atau laporan

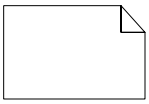
6. Berlian

 sebuah cabang

7. Tabel

 suatu file computer darimana data bisa dibaca atau direkam selama kejadian bisnis

8. Catatan

 memberikan acuan bagi pembaca pada diagram atau dokumen lain untuk perinciannya.

9. Mata banteng

 akhir dari suatu proses.

Gambar 2.1

Simbol-simbol diagram activity

Sumber : Dasaratha V. Rama/Frederick L. Jones (Sistem Informasi Akuntansi, 2006), p111

2.2 Teori khusus

Dalam sub bab ini akan dijelaskan mengenai teori-teori khusus yang mendukung dalam sistem informasi penjualaan kredit yang digunakan sebagai dasar pembahasan.

2.2.1 Pengertian audit sistem informasi

Menurut James E. Hunton (2004,p.13) audit sistem informasi adalah mengenai pengendalaian risiko yang berhubungan dengan sistem informasi. Audit sistem merupakan ilmu yang terus bertumbuh, teknologi selalu berubah dan terus menigkat mempengaruhi bisnis dan perusahaan. Kebutuhan akan *auditing* selalu penting untuk meningkat, dalam beberapa tahun ini untuk mengawasi masalah yang berpusat pada kebutuhan untuk mengawasi akuntasi (keuangan) dan kekeliruannya. Jadi jika teknologi informasi menjadi lebih *complex* dan *pervasive*, dan jika kebutuhan untuk auditing meningkat, maka IT auditors akan sanagat banyak dibutuhkan.

Menurut Weber (1999,p.10) audit sistem informasi adalah proses pengumpulan dan pengevaluasian bukti-bukti untuk memutuskan apakah dengan adanya sistem pengamanan asset yang berbasis computer dan pemeliharaan integritas data, data dapat mendukung perusahaan untuk mencapai tujuannya secara efektif dan penggunaan sumber daya secara eifisien, serta mengetahui apakah suatu perusahaan memiliki pengendalian intern yang memadai. Jadi dapat disimpulkan bahwa audit sistem

informasi adalah proses pengumpulan dan pengevaluasian bukti-bukti serta pengkajian ulang pengendalian intern untuk mencapai tujuan perusahaan secara efektif dan penggunaan sumber daya yang efisien.

2.2.2 Peranan auditor dalam proses audit

Menurut James E. Hunton (2004,p.6) :

1. Mengembangkan apa yang diinginkan *client* dan melaksanakan persiapan audit. Dalam hal ini auditor IT mengevaluasi kerumitan pada IT dalam perusahaan.
2. Pemngembangan perencanaan audit. Dalam hal ini auditor IT bekerja dengan auditor keuangan untuk mengembangkan perencanaan audit.
3. Evaluasi pada sistem *internal control*. Dalam hal ini auditor IT dan auditor keuangan bersama-sama mengevaluasi sistem *internal control*.
4. Memberikan kepercayaan pada pengendalian internal. Dalam hal ini auditor IT dan auditor keuangan bersama-sama memberikan kepercayaan kepada individu dalam pengendalian intern.
5. Melakukan pengujian *substantive*. Dalam hal ini auditor IT memungkinkan melakukan suatu analisis data or (CAAT) secara rutin untuk mendukung auditor keuangan.

6. Melakukan pemeriksaan kerja pokok persoalan pada laporan audit. Dalan hal ini auditor IT memeriksa laporan dan membuat laporan untuk menejer dengan memberikan rekomendasi.
7. Meminpin tindak lanjut kerja.dalma hal ini auditor IT berkerja dengan manajer dan auditor dalam tindak lanjut kerjaan.

2.2.3 Struktur perencanaan audit

menurut Richard Cascarino (2007,p.93) struktur perencanaan audit sebagai berikut :

1. Mempersiapkan melakukan *survey*. Bertujuan untuk memperoleh pengertian awal dari operasi audit dan untuk berkumpul mempersiapkan bukti-bukti untuk perencanaan audit lebih lanjut.
2. Analisa dan gambaran pengendalian *internal*. Dari mempersiapkan *survey* audit harus memiliki pengertian yang baik mengenai bisnis dan control objective pada area yang diperiksa.
3. *Expanded Test*. Dalam menetukan struktur *internal control* dapat sangat efektive,biasanya besar perluasan audit akan sangat diperlukan.
4. *Findings* and *recommendations*, yaitu berdasarkan kerja lapangan auditor akan menemukan perkembangan dan

keputusan yang diubah, jika ada keperluan untiuk meningkatkan *internal control.*

5. *Report production*, yaitu membuat laporan audit termasuk dokumentasi dan komunikasi dari hasil akhir audit.
6. *Follow – up*, yaitu menindak lanjuti *recommendations* yang sudah diberikan.
7. *Audit evaluation*, yaitu bagian akhir dari audit yang menghubungkan untuk pembuatan evaluasi oleh auditor sendiri.

2.2.4. Tahapan-tahapan audit

Menurut Jamees E. Hunton (2004, p208) tahapan-tahapan audit meliputi :

2.2.4.1 Planning

Dalam melakukan audit tahap pertama meliputi perencanaan. Hal ini berarti harus menentukan risiko-risiko apa saja yang dapat timbul, menjalin hubungan dengan klien, membiasakan diri dengan lingkungan dan menentukan staff-staff audit. Menurut ISACA standart 050.010 tahap-tahap planning adalah :

1. menentukan batasan dan tujuan audit
2. melakukan penilaian awal yang relevan
3. mengumpulkan pengetahuan tentang organisasi, bisnis proses, keuangan, risiko bawaan dan *environmental issues*
4. mengidentifikasikan pihak luar (seperti outsourcing)

5. membangun program audit yang berisi prosedur-prosedur audit yang akan dilakukan selama proses audit
6. membuat rencana audit yang akan dilakukan selama audit
7. mengumpulkan dokumen proses audit meliputi rencana audit, program audit dan dokumentasi lainnya yang penting untuk memberikan pengertian tentang bisnis klien.

2.2.4.2 Penilaian resiko/*what can go wrong*

Banyak auditor saat ini menggunakan pendekatan *risk-bassed* audit untuk melakukan audit. Dalam jenis audit ini penilaian resiko seputar pertanyaan "*what can go wrong*" jadi auditor SI fokus pertama kali dalam menentukan proses penting untuk melakukan audit. Hal ini membuat auditor untuk menentukan risiko-risiko apa sajakah yang harus dilakukan.

2.2.4.3 *The audit program*

Tak ada standart audit untuk IT audit karena prosedur audit harus disesuaikan dengan hardware dan software yang dipakai, arsitektur jaringan dan topologi dan lingkungan sistem. Program audit umum meliputi komponen-komponen :

1. Lingkup audit
2. Tujuan audit
3. Prosedur audit
4. Detail administrasi seperti perencanaan dan pelaporan

2.2.4.4 Mengumpulkan bukti

Temuan audit dan kesimpulan harus di*support* oleh analisis dan *interpretasi* yang tepat dari bukti-bukti yang ada. Menemukan bukti adalah kunci dari audit sebagaimana ini menyediakan dasar dari opini audit yang dibentuk. ISACA guidline 060.020.030 mengidentifikasikan beberapa tipe bukti yang akan dikumpulkan auditor SI meliputi:

1. Proses observasi dan keberadaan dari komponen-komponen fisik seperti operasi-operasi komputer dan prosedur *backup*
2. Bukti dokumentari seperti program *change logs*, sistem akses *logs* dan tabel otorisasi
3. *Representasi* atau perwakilan seperti flowchart, naratif, dan prosedur tertulis
4. Analisis seperti prosedur CAATs yang berjalan

2.2.4.5 *Forming conclusion*

Setelah semua bukti audit dikumpulkan maka tugas selanjutnya dari auditor adalah untuk mengevaluasi bukit-bukti dan mengambi kesimpulan tentang apakah tujuan audit tercapai dan proses audit berjalan sesuai prosedur atau tidak. Auditor juga dapat mengidentifikasi kondisi-kondisi yang dapat dilaporkan.

2.2.4.6 *Audit Opinion*

Panduan untuk hal-hal umum yang terdapat dalam audit report yang diatur dalam ISACA guideline 070.010.010 meliputi :

1. Nama dari organisasi yang diaudit
2. Judul, tanda tangan dan tanggal
3. Penjelasan tentang tujuan audit dan apakah tujuan audit tercapai
4. Ruang lingkup audit meliputi area audit, periode pelaksanaan audit, lingkungan aplikasi atau proses yang diaudit
5. Penjabaran tentang batas ruang lingkup dimana seorang auditor dapat melakukan pekerjaan audit secara benar untuk mencapai tujuan tertentu
6. *The intended audience for the report* meliputi peraturan-peraturan dalam distribusi laporan
7. Standar-standar dan kriteria dimana auditor melakukan pekerjaan audit
8. Penjabaran detil dari temuan-temuan
9. Kesimpulan dari area-area audit yang dievaluasi, meliputi beberapa kualifikasi dan *reservasi* signifikan
10. Masukkan-masukkan untuk pembetulan atau peningkatan

11. Hal-hal yang terjadi setelah pekerjaan audit selesai dilakukan

2.2.4.7 *Following up*

Tahap akhir dari siklus audit adalah *follow up*. Setelah auditor mengkomunikasikan hasil audit kepada klien dan menyampaikan opini audit, seorang auditor akan membuat ketetapan untuk *follow up* dengan klien tentang kondisi-kondisi yang tidak dapat ditemukan selama proses audit.

2.2.5 Standar Audit Sistem Informasi

Mengacu pada ISACA (2008), standar audit sistem informasi mendefinisikan persyaratan – persyaratan yang wajib dipenuhi dalam pelaksanaan dan pelaporan atas audit sistem informasi.

Information System Audit and Control Association (ISACA) menetapkan standar audit sistem informasi, sebagai berikut:

1. *Audit Charter*

   Bahwa *audit charter* harus disetujui oleh level organisasi yang tepat dan harus memuat mengenai tujuan, tanggung jawab, otoritas, dan pertanggungjawaban dari fungsi audit sistem informasi.

2. *Independence*

Memuat mengenai pentingnya independensi professional dan independensi organisasi.

3. *Professional Ethics and Standards*

   Bahwa auditor sistem informasi harus setia pada kode

4. *Professional Competence*

   Bahwa auditor sistem informasi harus kompeten secara profesional dan selalu memelihara kompetensi profesional yang dimilikinya tersebut dengan cara mengikuti pendidikan dan pelatihan profesional secara berkelanjutan.

5. *Planning*

   Berkaitan dengan perencanaan atas cakupan audit sistem informasi, pengembangan dan pendokumentasian pendekatan audit berbasis resiko, rencana audit, program audit beserta prosedur-prosedurnya.

6. *Performance of Audit Work*

   Berkaitan dengan pengawasan terhadap staf audit sistem informasi, pengumpulan bukti audit, dan pendokumentasian atas proses audit dalam rangka mendukung temuan dan kesimpulan auditor sistem informasi.

7. *Reporting*

   Berkaitan dengan rincian keterangan dalam laporan audit yang diperlukan, penyediaan laporan audit yang dibuat pada akhir penyelesaian audit harus berdasarkan bukti yang memadai, dan bahwa laporan ketika diterbitkan harus

ditandatangani, diberi tanggal, dan didistribusikan sesuai dengan persyaratan yang terutang pada surat perjanjian.

8. *Follow-Up Activities*

   Berkaitan dengan pengevaluasian atas informasi yang relevan untuk mengetahui apakah tindakan yang semestinya telah diambil oleh pihak manajemen dalam rangka menyikapi temuan dan rekomendasi dari auditor.

9. *Irregularities and Illegal Acts*

   Berkaitan dengan pertimbangan dan prosedur-prosedur audit yang diperlukan dalam melakukan penilaian atas adanya resiko tindakan yang tidak biasa dan melanggar hukum; pentingnya surat representasi dari manajemen; pengkomunikasian mengenai temuan yang diperoleh, dan juga dokumentasi mengenai tindakan-tindakan tidak biasa dan melanggar hukum yang materil.

10. *IT Governance*

    Berkaitan dengan penilaian fungsi sistem informasi yang harus sejalan dengan misi, visi, tujuan, strategi perusahaan; penilaian terhadap hasil yang dicapai dan keefektifan penggunaan sumber daya sistem informasi serta kepatuhan terhadap hukum, kualitas informasi, dan persyaratan keamanan yang ada.

11. *Use of Risk Assessment in Audit Planning*

Berkaitan dengan penggunaan teknik penilaian resiko yang tepat atas rencana audit dan dalam penentuan prioritas untuk alokasi sumber daya audit sistem informasi yang efektif.

12. *Audit Materiality*

    Berkaitan dengan pertimbangan mengenai materialitas audit dan hubungannya terhadap resiko audit; pertimbangan mengenai kelemahan pengendalian yang berpengaruh secara materil dalam sistem informasi; dan pengungkapan mengenai hal tersebut pada laporan auditor.

13. *Using the Work of Other Experts*

    Berkaitan dengan penggunaan pekerjaan dari pakar lainnya untuk keperluan audit dan penilaian terhadap kompetensi, independensi, dan pengalaman dari pakar tersebut.

14. *Audit Evidence*

    Berkaitan dengan pengumpulan bukti audit yang memadai dan layak untuk menarik kesimpulan yang wajar dan pengevaluasian atas kecukupan bukti audit.