AUDIT SISTEM INFORMASI PENJUALAN TUNAI DENGAN PENDEKATAN RESIKO DAN PENGAWASAN: STUDY KASUS PADA PT PKJ

Iwan Kurniawan Widjaya

Computerized Accounting Department, School of Information Systems, Binus University
Jl. K.H. Syahdan No. 9, Palmerah, Jakarta Barat 11480
iwankw@binus.ac.id

ABSTRACT

This research was conducted based on the evaluation about the performance of Sales information system in current system in PT PKJ. General control and application control had contributed in reducing any risk that migh occur in daily operations. Some recommendations had been submitted to the management in order to prevent any fraud or leak in any financial control. To improve the security and control in every process in sales and operational, system should have a proper control in input and output. Standarizations must be implemented in every step in applications to reduce the treats and vulnerabilities. This research can be used as a model for small medium company to grow better with proper control using optimalization of Information System and Technology in every aspect in the management.

Keywords: *evaluations, information system, sales by cash*

ABSTRAK

Tujuan penelitian adalah untuk mengevaluasi dan mengetahui sejauh mana sistem informasi penjualan tunai yang sedang berjalan (pengendalian umum dan pengendalian aplikasi) mampu menekan segala resiko yang muncul pada tingkat yang masih diterima oleh perusahaan. Selain itu, penelitian ini bertujuan untuk mengusulkan beberapa rekomendasi yang berguna bagi perusahaan untuk meminimalisasi setiap resiko yang ada pada saat ini dan yang akan terjadi dikemudian harinya. Simpulan yang dapat diambil yaitu setiap pengendalian seperti pengendalian keamanan, operasional, pengendalian boundary, pengendalian input serta output, belum sepenuhnya berjalan dengan baik dan kurang memenuhi standar yang ada yang dijadikan ukuran dalam penentuan setiap tahapan yang diterapkan dalam perusahaan. Sehingga sudah sebaiknya perusahaan memperbaiki dan menambahkan setiap kekurangan yang ada sehingga tidak mengalami gangguan maupun ancaman yang berasal baik dari dalam maupun dari luar perusahaan.

Kata kunci: *evaluasi, sistem informasi, penjualan tunai*

PENDAHULUAN

Seiring dengan kemajuan teknologi digital, perkembangan sistem informasi yang sangat pesat menyebabkan terjadinya persaingan antar perusahaan. Perkembangan ilmu pengetahuan teknologi berisikan kemudahan-kemudahan dalam melakukan aktifitas berupa pekerjaan-pekerjaan yang ringan maupun pekerjaan rumit dalam perusahaan. Kehadiran teknologi ini dimaksudkan untuk mencapai hasil yang lebih baik dengan efisien dan efektivitas yang lebih tinggi. Hasil suatu informasi yang diperoleh akan sangat memuaskan, berguna, dan bermanfaat bagi perusahaan yang menggunakannya apabila pengolahan data dan informasi dilakukan secara tepat dan efisien. Hasil informasi seperti ini dibutuhkan bagi setiap perusahaan atau instansi, seperti pada PT PKJ yang bergerak di bidang penjualan keramik. Strategi sistem informasi penjualan tunai merupakan suatu strategi dalam menjalani suatu proses penjualan ketika timbul pesanan dari klien terhadap produk yang dijual oleh perusahaan tersebut. Sistem informasi penjualan merupakan hal yang penting bagi manajer penjualan untuk menangani segala macam transaksi penjualan. Sistem informasi penjualan memerlukan pengendalian karena memiliki resiko kesalahan dan kecurangan yang terjadi seperti kesalahan pencatatan dan kegagalan memelihara kerahasian. Masalah tersebut dapat menimbulkan dampak kerugian baik financial maupun non-finansial.

Menyadari pentingnya kegiatan evaluasi bagi perusahaan dan segala kemungkinan yang akan terjadi, kami tertarik untuk memaparkan evaluasi yang berfokus pada permasalahan informasi penjualan. Kami berusaha mengangkat beberapa aspek penting yang terdapat pada bagian penjualan di PT PKJ. Oleh karena luasnya sistem informasi yang diterapkan dalam perusahaan, dilakukan pembatasan ruang lingkup, yaitu pada sistem penjualan tunai yang sedang berjalan pada PT PKJ. Ruang lingkup yang dibahas meliputi: (1) pengendalian umum berupa pengendalian manajemen keamanan dan pengendalian manajemen operasional; (2) pengendalian aplikasi berupa pengendalian *boundary*, pengendalian *input*, serta pengendalian *output*; (3) sistem penjualan tunai mulai dari pemesanan barang oleh pelanggan/customer sampai pembuatan laporan penjualan; (4) sistem kemanan yang digunakan pada sistem informasi penjualan.

Tujuan yang ingin dicapai antara lain: (1) memahami proses sistem informasi penjualan tunai pada PT PKJ; (2) mengidentifikasi masalah-masalah sistem informasi penjualan tunai yang mungkin timbul/ terjadi pada PT PKJ; (3) mengevaluasi masalah-masalah sistem informasi penjualan tunai yang sudah diidentifikasi terlebih dahulu; (4) mengidentifikasi resiko pada sistem informasi penjualan PT PKJ; (5) mengeidentifikasi ancaman-ancaman yang mengintai pada sistem informasi penjualan PT PKJ. Bagi perusahaan, hasil penelitian ini akan memberikan masukan yang berguna untuk memperbaiki kekurangan ataupun kesalahan yang mungkin terdapat pada sistem informasi penjualan yang mereka implementasikan. Manfaat lainnya adalah meningkatkan integritas kerahasian data perusahan dan meningkatkan efisiensi kinerja perusahaan.

METODE

Penelitian ini dengan menggunakan metode penelitian lapangan tentang semua hal yang berhubungan dengan sistem informasi penjualan dan pengendalian hal-hal teknis, seperti komputer, jaringan, *server*, dsb. Dan juga beberapa karyawan sebagai pengguna sistem akan dimintai keterangan soal penggunaan sistem ini. Penelitian yang dilakukan dengan cara mengadakan survei atau penelitian secara langsung ke perusahaan untuk dapat mencari tahu darimana masalah itu timbul.

Metode Penilaian Resiko

Resiko adalah suatu umpan balik negatif yang timbul dari suatu kegiatan dengan tingkat probabilitas berbeda untuk setiap kegiatan. Pada dasarnya resiko dari suatu kegiatan tidak dapat dihilangkan akan tetapi dapat diperkecil dampaknya terhadap hasil suatu kegiatan. Proses menganalisis serta memperkirakan timbulnya suatu resiko dalam suatu kegiatan disebut sebagai manajemen resiko. Untuk menentukan kemungkinan resiko yang timbul selama proses pengembangan teknologi informasi berlangsung, diperlukan analisis beberapa kemungkinan yang timbul dari pengembangan teknologi informasi tersebut. Metode penilaian resiko menurut Bastian (2007) terdiri dari beberapa langkah.

Langkah 1: Menentukan Karakterisasi Sistem

Pada langkah pertama ini batasan suatu sistem yang akan dikembangan di identifikasikan, meliputi perangkat keras, perangkat lunak, sistem antarmuka, data dan informasi, sumber daya manusia yang mendukung sistem IT, tujuan dari sistem, sistem dan data kritis, serta sistem dan data sensitif. Beberapa hal tambahan yang dapat diklasifikasikan pada karakteristik sistem selain hal tersebut di atas seperti bentuk dari arsitektur keamanan sistem, kebijakan yang dibuat dalam penanganan keamanan sistem informasi, bentuk topologi jaringan komputer yang dimiliki oleh organisasi tersebut, Manajemen pengawasan yang dipakai pada sistem TI di organisasi tersebut, dan hal lain yang berhubungan dengan masalah keamanan seputar penerapan Teknologi Informasi di organisasi yang bermaksud mengembangkan sistem informasi (Sarnom, 2009).

Langkah 2: Mengidentifikasikan Ancaman-ancaman

Ancaman adalah aksi yang terjadi baik dari dalam sistem maupun dari luar sistem yang dapat mengganggu keseimbangan sistem informasi. Timbulnya ancaman dapat dipicu oleh suatu kondisi dari sumber ancaman. Sumber ancaman dapat muncul dari kegiatan pengolahan informasi yang berasal dari 3 hal utama, yaitu (1) ancaman alam; (2) ancaman manusia, dan (3) ancaman lingkungan. Ancaman yang berasal dari manusia memiliki karakteristik tersendiri, serta memiliki alasan tersendiri dalam melakukan gangguan terhadap sistem informasi yang ada.

Adapun alasan yang timbul dari ancaman manusia yang dapat mempengaruhi kinerja sistem aplikasi dapat didefinisikan dalam Tabel 1 berikut:

Tabel 1 Ancaman dan Pengaruhnya terhadap Kinerja Sistem Aplikasi

Sumber ancaman	Alasan	Aksi yang timbul
Hacker, Cracker	- Tantangan - Ego - Memberontak	- Hacking - Social engineering - Gangguan sistem - Akses terhadap sistem
Kriminal	- Perusakan informasi - Penyingkapan informasi secara illegal - Keuntungan moneter - Merubah data	- Tindak kriminal - Perbuatan curang - Penyuapan - *Spoofing* - Intrusi atas sistem
Teroris	- Surat kaleng - Perusakan - Peledakan - Balas dendam	- Bom/teror - Perang informasi - Penyerangan sistem - Penembusan atas sistem - *Tampering* sistem

Mata-mata	- Persaingan usaha - Mata-mata ekonomi	- Pencurian informasi - *Social engineering* - Penembusan atas sistem
Orang dalam organisasi	- Keingintahuan - Ego - Mata-mata - Kelalaian kerja	- Surat kaleng - Sabotase atas sistem - Bug sistem - Pencurian/penipuan - Perubahan data - Virus - Penyalahgunaan komputer

Langkah 3: Identifikasi Kelemahan

Cacat atau kelemahan dari suatu sistem adalah suatu kesalahan yang tidak terdeteksi yang mungkin timbul pada saat mendesain, menetapkan prosedur, mengimplementasikan maupun kelemahan atas sistem kontrol yang ada sehingga memicu tindakan pelanggaran oleh sumber ancaman yang mencoba menyusup terhadap sistem tersebut.

Penerapan metode proaktif atau tersedianya karyawan yang bertugas untuk melakukan sistem tes dapat dipakai untuk mencek kelemahan sistem secara efisien, yang tergantung pada keberadaan sumber daya atau kondisi IT yang bersifat kritis. Metode tes yang diterapkan dapat berbentuk: (1) penggunaan tool yang menscan kelemahan sistem secara automatis; (2) adanya evaluasi dan sekuriti tes (ST&E), atau (3) melakukan penetrasi tes.

Tools digunakan untuk mencek kelemahan sistem diterapkan pada grup perusahaan dengan kelengkapan jaringan komputer yang memadai, untuk memindai beberapa servis sistem yang disinyalir lemah, seperti: diperbolehkannya *anonymous* FTP, *automatic send mail*, dll). Strategi ST&E merupakan metode tes yang diterapkan pada saat proses penilaian atas resiko dilakukan. Metode ini diterapkan saat pengembangan dan eksekusi atas Sistem Informasi berjalan yaitu pada bagian *test plan*. Kegunaan dari metode ini adalah untuk melihat efektifitas dari kontrol atas sekuriti dari sistem IT terimplementasikan dalam kondisi sistem beroperasi. Penetrasi tes merupakan metode yang digunakan sebagai pelengkap dalam memeriksa kontrol atas sekuriti dan menjamin tidak adanya masalah sekuriti yang mungkin timbul pada sistem IT.

Bentuk keluaran yang timbul pada langkah ketiga ini memungkinkan pihak penilai resiko mendapatkan daftar dari kelemahan sistem yang dapat dianggap sebagai potensi dari sumber ancaman di kemudian hari.

Langkah 4: Analisis Pengawasan

Tujuan yang diharapkan pada langkah ini adalah untuk menganalisis penerapan kontrol yang telah diimplementasikan atau yang direncanakan. Bagi organisasi langkah ini perlu untuk meminimalisasi atau bahkan mengeliminasi probabilitas kemungkinan yang timbul dari sumber ancaman atau potensi kelemahan atas sistem.

Langkah 5: Menerapkan Beberapa Kemungkinan

Pada langkah ini, semua skalabilitas kemungkinan yang mungkin timbul dari kelemahan sistem didefinisikan. Terdapat beberapa faktor yang perlu dipertimbangkan dalam upaya mendefinisikan skalabilitas seperti: (1) motif dan kapabilitas dari sumber ancaman; (2) kelemahan bawaan dari sistem; (3) eksistensi dan efektifitas kontrol yang di terapkan.

Adapun level skalabilitas dari ancaman menurut Sarnom (2009) dapat di definisikan dalam empat kategori.

Pertama adalah *catastrophic*. Pada level ini tingkat ancaman dapat dikategorikan sangat merusak, di mana sumber ancaman memiliki motif besar saat melakukan kegiatannya. Dampak yang ditimbulkan dari tingkat ini dapat membuat sistem tidak berfungsi sama sekali.

Kedua adalah *critical*. Level ini dapat dikategorikan cukup membuat merusak sistem IT, akan tetapi penggunaan kontrol yang diterapkan pada sistem telah dapat menahan kondisi kerusakan sehingga tidak menyebabkan kerusakan yang besar pada sistem.

Ketiga adalah *marginal*. Pada level ini kontrol keamanan mampu mendeteksi sumber ancaman yang menyerang sistem IT, walau tingkat kerusakan pada sistem masih terjadi akan tetapi masih dapat di perbaiki dan dikembalikan kepada kondisi semula.

Keempat adalah *negligible.* Pada level ini sumber ancaman tidak dapat mempengaruhi sistem, di mana kontrol atas sistem sangat mampu mengantisipasi adanya kemungkinan ancaman yang dapat mengganggu sistem.

Langkah 6 Analisis dampak

Analisis dampak merupakan langkah untuk menentukan besaran dari resiko yang memberi dampak terhadap sistem secara keseluruhan. Penilaian atas dampak yang terjadi pada sistem berbeda-beda di mana nilai dari dampak sangat tergantung pada: (1) tujuan sistem IT tersebut saat di kembangkan; (2) kondisi sistem dan data yang bersifat kritis, apakah dikategorikan penting atau tidak; (3) sistem dan data yang bersifat sensitif.

Langkah 7: Tahap Penentuan Resiko

Dalam tahap ini, dampak resiko didefinisikan dalam bentuk matriks sehingga resiko dapat terukur. Bentuk dari matriks tersebut dapat berupa matriks 4 x 4, 5 x 5 yang tergantung dari bentuk ancaman dan dampak yang di timbulkan.

Probabilitas dari setiap ancaman dan dampak yang ditimbulkan dibuat dalam suatu skala misalkan probabilitas yang timbul dari suatu ancaman pada langkah ke 5 di skalakan dalam nilai 1.0 untuk tingkat *catastrophic*; 0,7 untuk tingkat *critical*; 0,4 untuk tingkat *marginal* dan 0,1 untuk tingkat *negligible*.

Terdapat 3 proses dalam manajemen resiko IT menurut Weber (1999). Pertama adalah p**roses** identifikasi resiko (*risk identification*). Identifikasi risiko merupakan suatu proses yang secara sistematis dan terus menerus dilakukan untuk mengidentifikasi kemungkinan timbulnya risiko atau kerugian terhadap kekayaan, hutang, dan personil perusahaan. Proses identifikasi risiko ini mungkin adalah proses yang terpenting, karena dari proses inilah, semua risiko yang ada atau yang mungkin terjadi pada suatu proyek, harus diidentifikasi. Kedua adalah proses pengurangan resiko (*risk mitigation*). Strategi di dalam melakukan pengurangan resiko misalnya dengan menerima resiko (*risk assumption*), mencegah terjadinya resiko (*risk avoidance*), membatasi level resiko (*risk limitation*), atau mentransfer resiko (*risk transference*). Proses terakhir adalah evaluasi resiko (*risk evaluation*). Pada proses ini dilakukan evaluasi apakah pendekatan manajemen resiko yang diterapkan sudah sesuai. Kemudian dilakukan penilaian resiko kembali untuk memastikan keberadaan resiko yang teridentifikasi maupun resiko yang belum teridentifikasi.

Jenis-jenis Ancaman

Di dalam dunia Teknologi dan Informasi yang makin canggih dan berkembang saat ini pastinya banyak sekali jenis-jenis ancaman (*threats*) yang dapat dilakukan melalui penggunaan Tekhnologi Informasi, karena semakin majunya teknologi, maka semakin banyak juga ancaman-ancaman (threats) yang berkembang di dunia saat ini. Berikut adalah ancaman yang sering terjadi dalam penggunaan IT:

Virus

Virus merupakan program komputer yang dapat menggandakan atau menyalin dirinya sendiri dan menyebar dengan cara menyisipkan salinan dirinya ke dalam program atau dokumen lain. Virus komputer dapat dianalogikan dengan virus biologis yang menyebar dengan cara menyisipkan dirinya sendiri ke sel makhluk hidup. Virus komputer dapat merusak (misalnya dengan merusak data pada dokumen), membuat pengguna komputer merasa terganggu, maupun tidak menimbulkan efek sama sekali. Ada beberapa cara virus menyebar, yaitu melalui disket atau CD, email, dan *file* yang diunduh dari Internet

Beberapa jenis virus di antaranya: (1) *worm* – menduplikatkan dirinya sendiri pada *harddisk*. Worm membuat *harddisk* menjadi penuh akan *worm* itu. Jenis-jenis worm seperti WANK, Code Red, Sapphire (Slammer), Blaster, Sasser, dan lain-lain; (2) Trojan – mengambil data pada komputer yang telah terinfeksi dan mengirimkannya pada pembuat trojan itu sendiri; (3) *Brain* – virus pertama untuk bergerak dari satu PC IBM ke PC yang lain. *Brain* menginfeksi sektor *boot* dari media penyimpanan diformat dengan tabel alokasi *file* DOS (FAT) sistem *file*; (4) Michelangelo **–** eksekusi *file* menimpa catatan kritis pada *boot disk*; (5) Melissa **–** makro dalam dokumen Word yang dilampirkan ke pesan email; (6) Backdoor – hamper sama dengan trojan. Namun, Backdoor biasanya menyerupai *file* yang baik-baik saja, misalnya game; (7) Spyware – virus yang memantau komputer yang terinfeksi; (8) Rogue – merupakan program yang meniru program antivirus dan menampilkan aktivitas layaknya antivirus normal, dan memberikan peringatan-peringatan palsu tentang adanya virus. Tujuannya adalah agar pengguna membeli dan mengaktivasi program antivirus palsu itu dan mendatangkan uang bagi pembuat virus rogue tersebut. Rogue Juga dapat membuka celah keamanan dalam komputer guna mendatangkan virus lain; (9) Rootkit – virus yang bekerja menyerupai kerja sistem komputer yang biasa saja; (10) Polymorphic virus – gemar beubah-ubah agar tidak dapat terdeteksi; (11) metamorphic virus – mengubah pengkodeannya sendiri agar lebih sulit dideteksi.

Cara menangani virus komputer adalah dengan menggunakan perangkat lunak antivirus. Berikut adalah beberapa antivirus yang sering digunakan: Avast!, AVG Anti-Virus, eTrust, McAfee Anti-Virus dan McAfee Virus Scan, Kaspersky Antivirus, SMADAV, dll.

Hacker

Hacker adalah orang yang mempelajari, menganalisis, memodifikasi, menerobos masuk ke dalam komputer dan jaringan komputer, baik untuk keuntungan atau dimotivasi oleh tantangan.

White hacker atau White Hacker Community, adalah individu atau sekelompok orang atau komunitas yang mengunakan hacking untuk kepentingan dan bertujuan yang positif serta untuk mencari celah keamanan suatu sistem maupun suatu perangkat lunak serta memperbaiki celah keamanan yang ditemukan tersebut (atau menginformasikan celah keamanan yang ditemukan kepada pemilik system tersebut). Berani menampakkan dirinya secara terang-terangan, ada struktur organisasi yang jelas dan tanggung jawab ada pada masing-masing personal pelakunya maupun pada organisasi serta mau berbagi ilmu/ *sharing* pengalaman dengan publik.

Black Hacker atau Black Hacker Community, adalah individu atau sekelompok orang atau komunitas yang mengunakan hacking untuk kepentingan pribadi dan bertujuan merusak, mencuri data atau informasi, mengunakan *carding* untuk keuntungan pribadi, serta merugikan orang lain, tidak berani menampakkan dirinya secara terang-terangan dan tanggung jawab ada pada masing-masing personal pelakunya. Serta lebih menyukai gaya hidup individual dari pada bermasyarakat.

Blue Hat adalah Personal atau sekelompok orang/ komunitas yang mengunakan *hacking* sebagai *security advisor*.

Pencurian Identitas

Menurut Hasabudin, (2007) pemahaman atas pencurian identitas adalah penyalahgunaan identitas orang lain untuk mengambil tindakan yang diizinkan pemilik, seperti menarik dana, transfer uang, mendapatkan akses ke dokumen informasi atau masalah di bawah identitas korban.

HASIL DAN PEMBAHASAN

Proses Bisnis PT PKJ

PT PKJ mengawali usahanya pada tahun 1970-an berupa toko material dan bangunan yang berlokasi di Kalimantan. Pada tahun 1980-an, salah satu produsen keramik di Indonesia menawarkan keramik reject secara gratis dengan alasan barang-barang tersebut tidak ada peminatnya dan sangat menyita tempat. Sementara jika dibuang dibutuhkan biaya yang cukup besar. Setelah melihat barang yang dimaksud, beliau bersedia menampungnya. Sesampainya di gudang kemenangan keramik-keramik tersebut dibersihkan dari kotoran-kotoran yang menempel (bahkan harus sampai disikat karena sudah terlalu lama sehingga berlumut). Kemudian dipotong dan diikat. Selanjutnya, keramik-keramik tersebut disusun didepan toko untuk dipasarkan. Respon masyarakat pada saat itu cukup baik sehingga keramik tersebut terjual habis dengan harga jual yang cukup layak.

Dengan melihat hal tersebut, tim cikal bakal PT PKJ merasakan bahwa peluang bisnis produk keramik di Indonesia di masa mendatang dinilai akan terus meningkat. Maka mereka mendatangi produsen keramik *reject* yang dimaksud dan menyatakan bahwa mereka sudah berhasil mejual keramik yang diberikan dengan hasil sekian dan bermaksud membayar senilai 50% dari total nilai uang yang ia peroleh. Pihak produsen menolak uang yang dimaksud karena awal pemberian keramik *reject* dimaksud diberikan secara cuma-cuma dan juga sudah merasa sangat dibantu karena barang-barang tersebut dapat terjual habis dan tidak menyita banyak tempat di pabriknya.

Pada tahun 1993, PT PKJ didirikan untuk memasarkan seluruh produk yang dihasilkan dengan total dealer sejumlah dari 60 dealer yang tersebar hampir di seluruh propinsi di Indonesia dengan masing-masing dealer memiliki 100-200 subdealer, sehingga total pelanggan PT PKJ saat ini sudah lebih dari 6000 sub-dealer.

Berbagai macam produk sudah bisa dihasilkan dan berhasil didistribusikan ke seluruh pasar Indonesia seta ke beberapa mancanegara. Mulai dari produk ukuran kecil gingga ke ukuran besar, mulai dari yang bercorak sederhana hingga yang kompleks pembuatannya. Kesadaran pengguna keramik sesuai dengan spesifikasi juga sudah mulai diterapkan oleh pengguna keramik di Indonesia. Sehingga boleh dikatakan bahwa pasar bahan bangunan keramik di Indonesia sudah dewasa dan sudah dapat menyesuaikan dengan tren pasar maupun tren gaya hidup modern sekarang ini.

Proses bisnis yang digambarkan adalah proses bisnis dalam penjualan tunai. Proses bisnis tersebut adalah sebagai berikut:

Konsumen datang untuk membeli barang dan dilayani oleh bagian marketing. Ketika konsumen sudah dapat barang yang ingin dibeli, bagian marketing membuat SO lalu diberikan untuk konsumen tersebut. Kemudian, konsumen membayar biayanya ke bagian kasir dengan menunjukkan SO yang telah dibuat oleh bagian marketing. Kasir menerima pembayaran dari konsumen, lalu kasir membuat struk pembayaran sebanyak tiga rangkap: (1) struk asli diberikan untuk konsumen; (2) rangkap warna merah untuk kasir; (3) rangkap warna hijau untuk CS sebagai bukti pengambilan barang dari gudang yang telah ditempel tanda lunas.

Lalu konsumen pulang dengan membawa struk pembayaran asli untuk bukti pembelian barang pada saat barang dikirim. Kemudian CS membuat DO dari struk pembayaran untuk diserahkan ke bagian gudang untuk mengambil barang. Lalu barang diambil untuk diperiksa dahulu lalu disiapkan untuk dikirim ke konsumen.

Setelah itu, CS membuat surat jalan tiga rangkap untuk dibawa supir ke konsumen. Lalu surat jalan dicocokkan dengan barang yang akan dikirim. Setelah barang dan surat jalan siap dikirim, supir tersebut mengirim barang ke konsumen yang telah membeli barang tersebut.

Setelah barang diterima, konsumen menunjukkan struk pembayaran sebagai bukti pembelian barang. Lalu konsumen menandatangani surat jalan. Surat jalan asli diserahkan kepada konsumen. Dua rangkap sisanya dibawa kembali oleh supir untuk diserahkan kepada CS.

Setelah kembali ke kantor, supir menyerahkan surat jalan dua rangkap sisanya kepada bagian CS. Satu rangkap pertama di buat arsip oleh CS tersebut. Satu arsip lagi diserahkan kepada *Accounting division* untuk diarsip.

Pada sore hari bagian kasir membuat laporan penjualan atau omset dari penjualan pada hari itu. Rincian laporan tersebut adalah jumlah keseluruhan dari uang kas, ditambah kartu kredit, ditambah debit, ditambah transfer, ditambah pelunasan, lalu dikurangi dengan penjualan sisa ditempat sama dengan netto penjualan. Laporan tersebut nantinya akan diserahkan kepada head *cashier* beserta bukti struk penjualan atau faktur penjualan pada hari itu untuk diperiksa atau diteliti. Setalah diteliti laporan tersebut diserahkan ke manager untuk bukti penjualan pada hari itu, dan manager melakukan pengecekkan hasil laporan seminggu sekali.

Pada sistem tersebut setiap orang bisa mengakses sistem informasi penjualan tersebut jadi tidak ada batasan pengendalian di mana hanya orang tertentu yang bisa mengakses sistem informasi bagian pembelian bisa menggunakan aplikasi yang sama tanpa harus *login* terlebih dahulu dan hanya menggunakan No. Id sesuai dengan bagiannya, itu dilakukan supaya pekerjaan lebih cepat selesai dan *update* dari hari-ke hari, karena sistem tersebut hanya untuk bagian penjualan dan pembelian sehingga diluar bagian tersebut tidak akan bisa mengaksesnya, dan yang bisa melihat hasilnya hanya pihak atasan yang bisa mengakses hasilnya.

Secara ringkas proses penjualan tunai dituangkan pada *event table* berikut (Tabel 3).

Tabel 3 Event Table Proses Penjualan Tunai

No.	*Event*	*Internal Agent*	*Start When*	*Activity*
1.	Melayani konsumen	Marketing	Konsumen memilih barang	Membuat SO
2.	Menerima pembayaran	Kasir, *Customer Service*	Ketika konsumen menyerahkan SO	Membuat faktur penjualan tiga rangkap, menghitung pembayaran
3.	Mengambil barang di gudang	*Customer Service*, bagian gudang	Ketika faktur penjualan rangkap hijau diserahkan ke bagian CS	Mengambil barang, memeriksa barang
4.	Mengirim barang	*Customer Service*	Menerima DO	Membuat surat jalan tiga rangkap, mencocokkan barang
5.	Menyerahkan barang ke konsumen	Konsumen, supir	Ketika konsumen menunjukkan struk pembayaran	Menandatangani surat jalan, menyerahkan barang ke konsumen
6.	Menyerahkan bukti pembayaran	*Customer Service*, *Accounting division*, supir	Ketika 2 rangkap dibawa kembali ke kantor	SJ rangkap 1 diserahkan ke CS untuk arsip, rangkap dua diserahkan ke *Accouting* untuk arsip
7.	Membuat laporan penjualan	Kasir	Pada sore hari	Menghitung netto penjualan, menyerahkan ke *head cashier*, lalu diserahkan ke manajer

Keterangan:
SO: *sales order*
DO: *delivery order*

Analisis Temuan

Berdasarkan hasil temuan Audit pada PT PKJ, dapat disusun suatu hasil evaluasi yang menjadi bahan pertimbangan dan perbaikan di masa mendatang yang meliputi hal-hal sebagai berikut: (1) seharusnya sistem tersebut diberikan password bagi setiap penggunannya dan dilakukan reset empat hari sekali; (2) pembuatan *tab form* antara bagian penjualan dan pembelian menggunakan jenis aplikasi sama tetapi beda server sehingga tidak terjadi namanya tubrukan data, walaupun saat ini belum kelihatan dampaknya; (3) tidak adanya pengendalian kontrol kepada para karyawan dan juga atasan , jika sistem tersebut digunakan secara bersamaan walaupun atasan hanya mengecek hasil penjualan dan pembelian seminggu sekali; (4) sebaiknya saat memasuki aplikasi *user* harus *login* bedasarkan *User Id* yang diberikan dan *password* bisa ditentukan masing-masing; (5) memberikan batasan saat salah memasukkan password sebanyak tiga kali. Jika lebih dari itu, masa *User Id* di-block; (6) membentuk satu bagian untuk melakukan pengawasan dan *maintanance system*; (7) antara bagian penjualan dan bagian pembelian masih dalam 1 aplikasi tapi berbeda server sehingga data yang tersimpan masing-masing sehingga tidak terjadi tabrakkan data; (8) pihak manager harus melakukan *login* juga terlebih dahulu untuk melihat laporan; (9) memberikan anti virus yang sesuai sehingga, tidak akan merusak data yang ada di dalam perusahaan.

PENUTUP

Berdasarkan hasil pembahasan diatas mengenai ancaman-ancaman yang ditimbulkan dari penggunaan TI serta manajemen resiko yang dilakukan untuk mencegah dan menanggulangi resiko-resiko yang mungkin terjadi, dapat disimpulkan sebaiknya dalam membuat aplikasi dan menjalankan aplikasi *user* harus diberikan hak akses yang sesuai dengan kegiatannya masing-masing, sehingga itu akan membuat semua data yang ada di perusahaan menjadi terintegrasi dengan baik.

DAFTAR PUSTAKA

Bastian, Indra. (2007). *Audit Sector Public*. Jakarta: Salemba Empat.

Hasabudin. (2007). Peran implementasi strategi, perilaku termotovasi dan pelaksanaan sistem akuntansi terhadap pengendalian intern. *Jurnal Akuntansi/XTh. I/01/Januari/2007.*

Sarnom, Rianarto. (2009). *Audit Sistem dan Teknologi Informasi*. Surabaya: ITS Press.

Weber, R (1999). *Information System Control and Audit*. New Jersey: Prentice Hall.