AUDIT SISTEM INFORMASI PERSEDIAAN

Henny Hendarti (D0840), Krisna Darma Yanti (0700732593), Megawati (700732605), Henny (0700733740)
Universitas Bina Nusantara Jakarta
e-mail: henny@binus.ac.id

ABSTRAKSI

Audit sistem informasi persediaan merupakan salah satu cara untuk mengevaluasi dan mengetahui sejauh mana sistem informasi persediaan yang sedang berjalan (pengendalian manajemen dan pengendalian aplikasi) telah mampu mengcover resiko hingga pada tingkat yang dapat diterima oleh perusahaan sekaligus memberikan rekomendasi-rekomendasi konstruktif bagi perusahaan dalam rangka meminimalisasi resiko yang ada pada saat ini dan yang akan terjadi dikemudian hari. Audit ini dilakukan dengan menggunakan audit around the computer. Metode Penelitian yang digunakan adalah studi kepustakaan dengan menggali materi-materi yang bersumber dari berbagai buku dan sumber pustaka lainnya serta melakukan penelitian lapangan yang meliputi kuesioner, wawancara, observasi, dan testing aplikasi. Hasil yang dicapai dari proses audit berfokus pada kelemahan-kelemahan yang ada pada sistem dimana kelemahan-kelemahan tersebut disajikan dalam bentuk matriks resiko dan pengendalian yang terdiri dari temuan masalah, potensi resiko (Impact dan Likelihood), keandalan pengendalian yang ada (Design dan Effectiveness).

Kata kunci: *Audit, Sistem Informasi Persediaan, Pengendalian Manajemen, Pengendalian Aplikasi.*

1. PENDAHULUAN

Audit sistem informasi persediaan merupakan salah satu cara untuk mengevaluasi dan mengetahui sejauh mana sistem informasi persediaan yang sedang berjalan (pengendalian manajemen dan pengendalian aplikasi) telah mampu meng*cover* resiko hingga pada tingkat yang dapat diterima oleh perusahaan sekaligus memberikan rekomendasi-rekomendasi konstruktif bagi perusahaan dalam rangka meminimalisasi resiko yang ada pada saat ini dan yang akan terjadi dikemudian hari. Audit ini dilakukan dengan menggunakan *audit around the computer*. Metode Penelitian yang digunakan adalah studi kepustakaan dengan menggali materi-materi yang bersumber dari berbagai buku dan sumber pustaka lainnya serta melakukan penelitian lapangan yang meliputi kuesioner, wawancara, observasi, dan *testing* aplikasi. Hasil yang dicapai dari proses audit berfokus pada kelemahan-kelemahan yang ada pada sistem dimana kelemahan-kelemahan tersebut disajikan dalam bentuk matriks resiko dan pengendalian yang terdiri dari temuan masalah, potensi resiko (*Impact* dan *Likelihood*), keandalan pengendalian yang ada (*Design* dan *Effectiveness*).

2. PEMBAHASAN

Agar lebih mengarahkan topik bahasan auditnya maka penulis membatasi ruang lingkup auditnya sebagai berikut:

1. Audit yang dilakukan terhadap sistem informasi persediaan (*member kit*) yang dimulai dari proses barang masuk, proses pengeluaran barang serta proses peng*update*an data jumlah *stock* pada sistem informasi persediaan.
2. Pengendalian yang merupakan pembahasan penulis yang meliputi:
   a. Pengendalian Manajemen (*Management Control*): Pengendalian Manajemen Keamanan (*Security Management Controls*) dan Pengendalian Manajemen Operasi (*Operations Management Controls*).
   b. Pengendalian aplikasi (*Aplication control*) : Pengendalian *Boundary, Input, dan Output.*
3. Metode audit yang digunakan adalah *Audit Around the Computer*.
4. Menyajikan laporan.

Tujuan dari audit sistem informasi persediaan adalah sebagai berikut:

- Mengetahui pengendalian yang diterapkan oleh perusahaan dalam sistem persediaannya.
- Mengidentifikasi kelemahan–kelemahan dari pengendalian yang diterapkan oleh perusahaan dalam sistem persediaannya.
- Melakukan audit terhadap pengendalian sistem informasi persediaan yang sedang berjalan.
- Melakukan penilaian terhadap resiko berdasarkan kelemahan-kelemahan yang ditemukan pada pengendalian sistem informasi persediaannya.
- Membuat rekomendasi perbaikan berdasarkan kelemahan–kelemahan dan resiko yang ditemukan dari proses audit tersebut.

Adapun **manfaat** yang dapat diperoleh dari audit sistem informasi persediaan meliputi:

- Bagi auditor
  Dapat memberikan gambaran secara langsung penerapan teori–teori yang dipelajari auditor dengan praktek yang sesungguhnya.
- Bagi perusahaan
  Membantu perusahaan dalam memecahkan dan memperbaiki masalah–masalah yang sedang dihadapi perusahaan sehingga pihak perusahaan

bisa mengetahui kehandalan dan kelayakan dari sistem aplikasi dan manajemen yang sedang diimplementasi guna meningkatkan produktifitas kerja serta untuk meningkatkan keamanan, keakuratan, kelengkapan dan integritas data.

- Bagi pembaca
  Bisa mengembangkan wawasan bagi pembaca yang ingin mempelajari serta memahami lebih lanjut mengenai audit terhadap pengendalian sistem informasi persediaan.

Sistem informasi adalah gabungan dari orang–orang, perangkat keras, perangkat lunak, jaringan komunikasi, dan sumber daya data yang mengumpulkan, memproses, menyimpan, menganalisa data, dan menghasilkan informasi untuk tujuan yang spesifik. Informasi yang andal dan berkualitas harus memiliki karakteristik sebagai berikut: relevansi, lengkap, akurat, dan tepat waktu.

Menurut Arens dan Loebbecke yang diterjemahkan oleh Jusuf (1997, h.1), "*Auditing* adalah proses pengumpulan dan pengevaluasian bahan bukti audit tentang informasi yang dapat diukur mengenai suatu entitas ekonomi yang dilakukan seorang yang kompeten dan independen untuk dapat menentukan dan melaporkan kesesuaian informasi dengan kriteria-kriteria yang telah ditetapkan".

Menurut Mulyadi (2002, h.30), *auditing* dapat digolongkan menjadi tiga golongan, yaitu Audit Laporan Keuangan (*General Financial Statement Audit*), Audit Kepatuhan (*Compliance Audit*), Audit Operasional/Manajemen (*Operational*/*Management Audit*).

Arens and Loebbecke (1997, p.153-161) berpendapat bahwa, "Dalam menentukan prosedur audit mana yang akan digunakan, ada tujuh kategori bahan bukti audit yang dapat dipilih auditor yaitu: Pemeriksaan Fisik, Konfirmasi, Dokumentasi (Pemeriksaan Dokumen/*Voucing*), Pengamatan, Tanya Jawab dengan Klien, Pelaksanaan Ulang (*Reperformance*) dan Prosedur Analitis.

Menurut Cangemi (2003, p.48) dalam bukunya yang berjudul *Managing the Audit Function, "Information systems auditing is defined as any audit that encompass the review and evaluation of all aspects (or any portion) of automated information processing systems, including related non-automated processes, and the interfaces between them "*. Intinya, Audit sistem informasi didefinisikan sebagai proses audit yang terdiri dari *review* dan pengevaluasian seluruh aspek dari sistem pemrosesan informasi otomatis termasuk proses non-otomatis serta *interface* diantara keduanya.

Menurut Weber (1999, pp.11-13), tujuan dari audit sistem informasi adalah: Meningkatkan Perlindungan Terhadap Aset Perusahaan, Meningkatkan Integritas Data, Meningkatkan Efektifitas Sistem dan Meningkatkan Efisiensi Sistem.

Gondodiyoto dan Idris (2003, hh.155-158) berpendapat bahwa ada tiga metode audit sistem informasi antara lain:

1. *Audit Around the Computer*
   Untuk menerapkan metode ini, auditor pertama kali harus menelusuri dan menguji pengendalian masukan, kemudian menghitung hasil yang diperkirakan dari proses transaksi, lalu auditor membandingkan hasil sesungguhnya dengan hasil yang dihitung secara manual.
2. *Audit Through the Computer*
   Pada metode ini, auditor tidak hanya melakukan pengujian pada *input* dan *output* melainkan juga pemeriksaan secara langsung terhadap pemrosesan komputer melalui pemeriksaan logika dan akurasi program meliputi koding program, desain aplikasi, serta hal lain yang berkaitan dengan program aplikasinya.
3. *Audit With the Computer*
   Pada metode ini audit dilakukan dengan menggunakan komputer dan *software* untuk mengotomatisasi prosedur pelaksanaan audit. Metode ini sangat bermanfaat dalam pengujian substantif atas *file* dan *record* perusahaan. Salah satu *software* audit yang dapat digunakan adalah GAS (*Generalized Audit Software*) dan SAS (*Specialized Audit Software*).

Tahapan audit sistem informasi adalah sebagai berikut:

1. *Planning the Audit* (Perencanaan Audit).
2. *Tests of Control (*Pengujian Pengendalian).
3. *Tests of Transactions* (Pengujian Transaksi).
4. *Substantive Test* (Pengujian Substantif).
5. *Completion of the Audit* (Penyelesaian Audit).

Penulis menyimpulkan bahwa sistem pengendalian internal adalah sistem pengendalian dalam suatu organisasi yang dirancang untuk mencegah dan mendeteksi terhadap kesalahan yang akan terjadi serta mengendalikan dan melindungi seluruh aktivitas organisasi dari penyimpangan-penyimpangan lainnya yang dapat merugikan perusahaan.

Sistem pengendalian internal memiliki empat tujuan utama, yaitu untuk: Mengamankan aktiva organisasi, Memastikan akurasi dan keandalan dari catatan dan informasi akuntansi, Mempromosikan efisiensi operasi perusahaan, Mengukur kesesuaian dengan kebijakan dan prosedur yang telah ditetapkan manajemen.

Sistem pengendalian internal terdiri dari 5 (lima) komponen yang saling terintegrasi, yaitu: Lingkungan Pengendalian (*Control Environment*), Penaksiran Resiko (*Risk Assessment*), Aktivitas Pengendalian (*Control Activities*), Informasi dan Komunikasi (*Information and Communication*), Pengawasan (*Monitoring*).

Menurut Weber (1999, p.38) ada dua jenis sistem pengendalian internal, yaitu:

1. Pengendalian Manajemen (*Management Controls)*
   Pengendalian Manajemen terdiri dari tujuh sub sistem, yaitu Pengendalian *Top* Manajemen, Pengendalian Manajemen Sistem Informasi, Pengendalian Manajemen Pengembangan Sistem, Pengendalian Manajemen Sumber Data, Pengendalian Manajemen Jaminan Kualitas, Pengendalian Manajemen Keamanan, Pengendalian Manajemen Operasi.
   Dalam ruang lingkup audit Sistem Informasi Persediaan PT. Eratel Media Distrindo, Pengendalian Manajemen ditekankan pada:
   a. *Security Management Controls* yang secara garis besar bertanggung jawab dalam menjamin aset sistem informasi tetap aman. Adapun ancaman utama terhadap keamanan aset sistem informasi adalah kebakaran, banjir, kerusakan struktural, polusi, perubahan tegangan sumber energi, penyusup, virus, *hacking.* Apabila ancaman keamanan tidak terhindarkan lagi maka diperlukan pengendalian akhir (*control of last resort*) guna meminimalisasi kerugian dan memastikan operasi perusahaan tetap berjalan meliputi:
      1) Rencana Pemulihan Bencana
         – Rencana Darurat (*Emergency Plan*).
         – Rencana *Backup* (*Backup Plan*).
         – Rencana Pemulihan (*Recovery Plan*).
         – Rencana Pengujian (*Test Plan*).
      2) Asuransi
   b. *Operations Management Controls* yang secara garis besar bertanggung jawab pada fungsi-fungsi sebagai berikut: Pengoperasian Komputer (*Computer Operations*), Pengoperasian Jaringan (*Network Operations*), Persiapan dan Pengentrian Data (*Preparation and Data Entry*), Pengendalian Produksi (*Production Controls*), Perpustakaan (*File Library*), Dokumentasi dan Perpustakaan Program (*Documentation and Program Library*), *Help Desk*/*Technical Support*, Perencanaan Kapasitas dan Pengawasan Kinerja (*Capacity Planning and Performance Monitoring*), dan *Management of Outsourced Operations.*
2. Pengendalian Aplikasi (*Application Controls*)
   Menurut Gondodiyoto dan Henny (2006, h.328), Pengendalian Aplikasi (*Application Controls*) adalah Sistem pengendalian *intern* pada sistem informasi berbasis teknologi informasi yang berkaitan dengan pekerjaan/kegiatan/aplikasi tertentu (setiap aplikasi memiliki karakteristik dan kebutuhan pengendalian yang berbeda). Pengendalian aplikasi terdiri dari 6 (enam) pengendalian, yaitu:
   1) Pengendalian Batasan (*Boundary Controls*)
      Tiga tujuan pengendalian subsistem *boundary* adalah sebagai berikut:
      - Untuk menetapkan identitas dan kewenangan *user* dari sistem komputer.
      - Untuk menetapkan identitas dan kewenangan dari sumber daya yang digunakan *user*.
      - Membatasi tindakan-tindakan yang dilakukan oleh *user* yang menggunakan sumber daya komputer terhadap tindakan-tindakan yang tidak terotorisasi.
   2) Pengendalian Input (*Input Controls*)
      Tiga alasan pentingnya *Input Controls*, yaitu:
      - Pada sistem informasi kontrol yang besar jumlahnya adalah pada subsistem *input*, sehingga auditor harus memberikan perhatian yang lebih kepada keandalan *input* kontrol yang ada.
      - Kegiatan subsistem *input* melibatkan jumlah kegiatan yang besar dan rutin dan merupakan kegiatan yang monoton sehingga dapat menyebabkan terjadinya kesalahan.
      - Subsistem *input* seringkali merupakan target dari *fraud*, banyak kegiatan yang tidak seharusnya dilakukan seperti penambahan, dan penghapusan.
   3) Pengendalian *Output* (*Output Controls*)
      Gondodiyoto dan Henny (2006, h.363) berpendapat bahwa "Pengendalian *output* merupakan pengendalian yang dilakukan untuk menjaga *output* sistem agar akurat, lengkap, dan digunakan sebagaimana mestinya." Berdasarkan sifatnya, metode pengendalian *output controls* terdiri dari tiga jenis : *Preventive Objective*, *Detection Objective*, *Corrective Objective.*
   4) Pengendalian Proses (*Process Controls*)
   5) Pengendalian Komunikasi (*Communication Controls*)
   6) Pengendalian Basis Data (*Database Controls*)

3. ANALISIS SISTEM YANG BERJALAN

Prosedur barang masuk diawali oleh perusahaan dengan membuat nomor anggota dan pin anggota, setelah nomor anggota dan pin anggota selesai dibuat, bagian gudang mengirimkan nomor anggota dan pin tersebut ke percetakan (yang sudah menjalin kerja sama dengan Perusahaan) dan membuat *Surat Permintaan Pencetakan Barang* melalui *email* kepada percetakan untuk mencetak

Member Kit. Setelah *Member Kit* selesai, percetakan mengirimkan *Member Kit* tersebut dengan disertai *Faktur* serta *Surat Jalan (SJ)* masing-masing 3 rangkap. *Faktur* dan *Surat Jalan* asli diserahkan ke *Bagian Gudang*, *faktur* rangkap 2, 3 dan *Surat Jalan* rangkap 2, 3 untuk bagian percetakan. Setelah menerima dan melakukan pengecekan barang, *Bagian Gudang* menandatangani *Faktur* serta *Surat Jalan* tersebut. Berdasarkan *Faktur* dan *Surat Jalan* tersebut, *Bagian Gudang* membuat *Bukti Penerimaan Barang (BPB)* sebanyak 3 rangkap. *BPB* rangkap 1 untuk *Percetakan*, rangkap 2 diarsip oleh *Bagian Gudang*, *BPB* rangkap 3 diserahkan kepada *Bagian Akuntansi*. Setelah dokumen *BPB* diotorisasi, *Bagian Gudang* mengisi *Kartu Stock Manual* untuk barang masuk serta membuat *Laporan Barang Masuk* untuk diserahkan ke *Direktur*.

Proses pengeluaran barang gudang dimulai ketika *Bagian Penjualan* menyerahkan *Form Order* (FO) yang berisi pesanan customer yang ingin membeli *member kit* ke *bagian Gudang*. Selanjutnya *Bagian Gudang* akan melakukan validasi o*rder* yaitu mengecek *stock* barang yang tersedia. Jika barang tersedia, *Bagian Gudang* menyiapkan barang serta mengkonfirmasikan ke *Bagian Penjualan*. Kemudian *Bagian Penjualan* membuat *Faktur* dan mengkonfirmasikan nomor *Faktur* ke *Bagian Gudang* untuk dibuatkan *Surat Jalan (SJ)* sebanyak 3 rangkap. *SJ* rangkap 1, 3 diserahkan ke *Bagian Penjualan* dan *SJ* rangkap 2 diarsip oleh *Bagian Gudang*. Kemudian *Bagian Gudang* menyerahkan barang beserta *Surat Jalan* tersebut ke *Bagian Penjualan*. Selanjutnya *Bagian Gudang* mengisi *Kartu Stock Manual* barang keluar. *Laporan Persediaan* diserahkan kepada *Direktur Utama* setiap akhir bulan.

Dokumen-dokumen yang digunakan pada sistem informasi persediaan Perusahaan i ni adalah:

1. Surat Permintaan Pencetakan Barang
   Dokumen berupa surat yang berisi jenis dan jumlah barang yang dipesan oleh perusahaan untuk dicetak oleh bagian Percetakan. Dokumen surat ini dikirim melalui email ke bagian Percetakan.
2. Bukti Penerimaan Barang (BPB)
   Suatu dokumen yang dikeluarkan oleh Bagian Gudang sebagai bukti bahwa barang yang dibeli perusahaan telah diterima oleh Gudang sebagaimana yang tercantum pada BPB (mencakup kondisi, kuantitas, dan jenisnya). Dokumen BPB ini juga merupakan dokumen sumber yang dijadikan dasar peng*input*an data barang masuk pada sistem informasi persediaan.
3. Kartu *Stock* Manual
   Dokumen yang digunakan oleh Bagian Gudang untuk mencatat setiap perubahan data *stock* (barang keluar dan barang masuk) yang terjadi secara manual.
4. Form Order (FO)
   Merupakan dokumen yang dikeluarkan oleh Bagian Penjualan sebagai permintaan barang keluar kepada Bagian Gudang. Dokumen ini juga digunakan sebagai dasar pembuatan Surat Jalan dan proses peng*update*an data *stock* pada kartu *stock* manual.
5. Surat Jalan
   Dokumen yang dibuat oleh Bagian Gudang berdasarkan FO yang dikeluarkan oleh Bagian Penjualan sebagai tanda keluarnya barang gudang sekaligus sebagai dokumen sumber peng*update*an data barang keluar pada kartu *stock* manual.

Laporan yang dihasilkan dari sistem informasi persedian Perusahaan ini adalah:

1. Laporan Barang Masuk
   Laporan ini merupakan laporan yang berisi seluruh item barang yang masuk ke dalam gudang.
2 Laporan Persediaan
   Laporan ini berisi barang yang masuk dan barang yang keluar yang dibuat setiap bulan untuk diserahkan kepada Direktur.

Spesifikasi *Hardware:* *Processor: Intel Pentium 4 (3.06 Ghz), Motherboard: Asus, Memory: 256 Mb, Hardisk: 40 Gb, Keyboard dan Mouse, Monitor: 14", Printer* (2 buah), *Fax* (1 buah).
Spesifikasi *Software:* *Software* aplikas*i* yang digunakan adalah *Erasoft Sales Invoicing* 7.0 *SQL Edition, Operating System Microsoft windows Xp Professional, Software Anti Virus* yang digunakan adalah *Norton Anti Virus* 2006.

4. AUDIT SISTEM INFORMASI PERSEDIAAN PERUSAHAAN

Proses audit ini terdiri dari beberapa tahap, yaitu: perencanaan dan program audit, instrumen pengumpulan bukti audit yang digunakan untuk setiap pengendalian, matriks penilaian resiko dan rekomendasi pengendalian berdasarkan standar yang ditetapkan serta menyajikan laporan audit.

Auditor membatasi ruang lingkup auditnya sebagai berikut:

1. Audit yang dilakukan terhadap sistem informasi persediaan (*member kit*) yang dimulai dari proses barang masuk, proses pengeluaran barang serta proses peng*update*an data jumlah *stock* pada sistem informasi persediaan.
2. Pengendalian yang merupakan pembahasan penulis yang meliputi:
   - Pengendalian Manajemen (*Management Control*): Pengendalian Manajemen Keamanan (*Security Management Controls*) dan Pengendalian Manajemen Operasi (*Operations Management Controls*).
   - Pengendalian aplikasi (*Aplication control*): Pengendalian *Boundary, Input, dan Output.*
3. Metode audit yang digunakan dalam melakukan audit adalah dengan pendekatan *Audit Arround the Computer*.
4. Menyajikan laporan.

Tujuan audit sistem informasi persediaan adalah sebagai berikut:

- Mengetahui pengendalian yang diterapkan oleh perusahaan dalam sistem informasi persediaannya.
- Mengidentifikasi kelemahan–kelemahan dari pengendalian yang diterapkan oleh perusahaan dalam sistem persediaannya.
- Melakukan audit terhadap pengendalian sistem informasi persediaan yang sedang berjalan.
- Melakukan penilaian terhadap resiko berdasarkan kelemahan-kelemahan yang ditemukan pada pengendalian sistem informasi persediaannya.
- Membuat rekomendasi perbaikan berdasarkan kelemahan–kelemahan dan resiko yang ditemukan dari proses audit tersebut.

Instrumen pengumpulan bukti audit yang digunakan: studi pustaka, wawancara, kuesioner, observasi, *testing* aplikasi.

Temuan-temuan negatif audit terhadap Pengendalian Manajemen (M*anagement Controls*) dan Pengendalian Aplikasi (A*pplication Controls*) adalah:

Temuan Pada Pengendalian Manajemen (*Management Controls*)

a. Temuan pada *Security Management Controls*
   - Tidak pernah dilakukan *backup* data secara rutin.
   - Tidak pernah dilakukan *scan virus* secara rutin pada saat membuka atau meng*copy file*.
   - Setiap komputer tidak dilengkapi dengan UPS *(Uninteruptable Power Supply)* yang mampu menstabilkan dan mengatasi gangguan sumber energi listrik.
   - Perusahaan tidak memiliki *genset* sebagai tindakan antisipatif jika listrik padam.
   - Perusahaan tidak dilengkapi dengan peralatan kebakaran (tabung pemadam kebakaran) maupun *alarm* kebakaran otomatis di setiap ruangan.
   - Pemisahan tugas bagi karyawan untuk setiap bagian belum berjalan dengan baik.
   - Tidak ada larangan untuk membawa media penyimpanan seperti disket keluar kantor.
   - *Backup* data hanya ditempatkan di ruangan IT (tidak diletakkan ditempat lain).
   - Tamu yang datang ke perusahaan tidak diwajibkan untuk melapor ke *security*.
   - Karyawan diperbolehkan membawa makanan dan minuman ke ruangan tempat mereka bekerja di mana terdapat beberapa komputer.

b. Temuan Pada *Operations Management Controls*
   - Mesin absensi yang digunakan untuk mencatat kehadiran dan waktu kerja tidak pernah diperiksa secara periodik.
   - Perusahaan tidak menyediakan karyawan untuk mengelola penyimpanan data (*libarian*).
   - Tidak terdapat bagian yang bertugas sebagai *Help Desk* di perusahaan.
   - Tidak dilakukan pemeriksaan secara periodik terhadap peralatan pendukung (*server*, lampu, kabel, dan sebagainya)
   - Proses m*aintenance* terhadap *hardware* dan *software* tidak dilakukan secara berkala/rutin, hanya dilakukan ketika terjadi *troubleshooting*.
   - Perusahaan tidak memiliki *standard*/kriteria khusus dalam merekrut karyawan baru.
   - Jaringan yang digunakan perusahaan tidak diperiksa secara periodik selama tidak terjadi masalah pada jaringan tersebut.
   - Jumlah *Staff IT* hanya terdiri dari 2 orang yaitu: Sistem *Analyst* dan *Programmer* perusahaan mengalami kesulitan jika sistem mengalami masalah.

Temuan Pada Pengendalian Aplikasi (*Application Controls*)

a. Temuan Pada *Boundary Controls*
   - Tidak dilakukan perubahan *password* secara berkala.
   - Sistem tidak memiliki batasan waktu dan tidak secara otomatis melakukan *log-off* sendiri ketika *user* tidak menggunakan sistem meskipun masih berada di dalam sistem maupun bila *user* lupa melakukan *log- off*.
   - Sistem tidak memiliki fasilitas menu *help* ketika *user* lupa akan *password*nya.

b. Temuan Pada *Input Controls*
   - Tidak terdapat pemisahan tugas antara pihak yang melakukan *input* data dengan yang mengeluarkan *output* laporannya
   - Tidak terdapat peringatan otomatis pada sistem jika data belum di *backup* maka prosesnya tidak bisa dilanjutkan.
   - Tampilan menu *input* tidak mempermudah proses peng*input*an sehingga proses peng*input*an data menjadi lambat.
   - Tidak terdapat petugas yang melakukan pengawasan terhadap keakuratan *input* data dengan data pada dokumen sumber.
   - Prosedur penghancuran dokumen sumber dilakukan diatas 5 tahun.
   - Sistem tidak memiliki menu *input* yang *user friendly* sehingga sulit dimengerti oleh *user* dan proses peng*input*annya lambat.

c. Temuan Pada *Output Controls*
   - Tidak terdapat otorisasi dari pihak yang berwenang dalam pencetakan laporan.
   - Tidak terdapat pengklasifikasian laporan (rahasia, umum, dsb).
   - Printer digunakan secara bersama untuk melaksanakan kegiatan perusahaan.
   - Tidak terdapat pembatasan halaman pada laporan yang dihasilkan.
   - Pada Laporan Barang Masuk hanya terdapat kolom kode barang dan tidak terdapat kolom no BPB.

Setelah melaksanakan proses audit sistem informasi persediaan pada perusahaan yang meliputi Pengendalian Keamanan (*Management Controls*) dan Pengendalian Aplikasi (*Aplication Controls*) serta berdasarkan bukti-bukti yang diperoleh, maka dapat dirumuskan kesimpulannya sebagai berikut:

- Perusahaan tidak memiliki S*ecurity Management Controls* yang memadai baik secara *physic* maupun *logic* sehingga ditemukannya beberapa resiko-resiko yang memerlukan perbaikan *control* untuk menghindari tingkat resiko yang lebih besar.
- Perusahaan memiliki *Operation Management Controls* yang sudah cukup baik namun masih perlu dilakukan pengawasan dan pemeriksaan terhadap *asset* dan fasilitas perusahaan secara periodik.
- Perusahaan belum memiliki *Boundary Controls* yang memadai karena tidak terdapat sistem *log-off* otomatis.
- Perusahaan belum memiliki *Input Controls* dan *Output Controls* yang memadai karena disain input dan outputnya tidak *user friendly* sehingga belum dapat menjaga integritas data.

Berdasarkan simpulan di atas maka dapat dirumuskan beberapa saran agar sistem informasi persediaan pada Perusahaan dapat berjalan dengan baik, yaitu sebagai berikut:

- Mengadakan perbaikan-perbaikan pada *Security Management Controls* secara *physic* maupun *logic* khususnya *backup* data yang dilakukan secara rutin serta menyediakan sistem dan alat untuk mengantisipasi ancamana kebakaran dan padamnya listrik.
- Meningkatkan *Operation Management Controls* yaitu dengan melakukan pengawasan dan pemeriksaan secara periodik terhadap *asset* dan fasilitas perusahaan.
- Melakukan perbaikan pada *Boundary Controls* yang meliputi adanya sistem yang melakukan *log-off* secara otomatis ketika user tidak menggunakan sistem/lupa melakukan *log-off.*
- Melakukan perbaikan pada *Input Controls* dan *Output Controls* yaitu dengan membuat disain input dan output yang *user friendly* untuk menjaga integritas data.

PUSTAKA

Arens, A. A and Loebecke, J.K. yang diterjemahkan oleh Jusuf, A.A, (1997). *Auditing Pendekatan Terpadu,* buku 1 (Edisi Indonesia). Salemba Empat, Jakarta.

Arens, A. A and Loebecke, J.K. yang diterjemahkan oleh Jusuf, A.A, (1999). *Auditing Pendekatan Terpadu,* buku 2 (Edisi Indonesia). Salemba Empat, Jakarta.

Cangemi, P. Michael and Singleton, Tommie. (2003). *Managing The Audit Function*, *third edition*. John Willey & Sons.

George H. Bodnar and William S. Hopwood. (2001). *Accounting Information System*. Prentice Hall, New Jersey.

Bodnar, George H, dan Hopwood, William S. (2000). *Sistem Informasi Akuntansi*, Buku satu, Edisi Indonesia. Diterjemahkan oleh Amir Abadi Jusuf dan Rudi Tambunan. Salemba Empat, Jakarta.

Gondodiyoto, Sanyoto (2003). *Audit Sistem Informasi Pendekatan Konsep*. PT. Media Global Edukasi (McGraw-Hill Education), Jakarta.

Gondodiyoto dan Henny (2006). *Audit Sistem Informasi*, (edisi pertama). Mitra Wacana Media, Jakarta.

Hall, J.A. (2001). *Sistem Informasi Akuntansi,* (Edisi ketiga). Terjemahan Jusuf,A.A. Salemba Empat, Jakarta.

http://proquest.umi.com

Mcleod, Raymond, Schell, George. (2001). *Management Information Systems*, 8th edition; Prentice-Hall.

Mcleod, Raymond Jr. Yang diterjemahkan oleh Teguh, H. (2001). *Sistem Informasi Manajemen,* Jilid 1, Edisi Bahasa Indonesia. PT. Prenhallindo, Jakarta.

Mulyadi, Puradiredja, Kanaka. (1998). *Auditing,* buku dua 5th Edition. Salemba Empat, Jakarta.

Mulyadi. (2001). *Sistem Akuntansi*. Edisi ke-3. Salemba Empat, Jakarta.

Mulyadi. (2002). *Auditing.* Edisi ke-6. Salemba Empat, Jakarta.

O'brien, James. A. (2003). *Introduction to Information (Essentials For The E-Business Enterprise), eleventh edition*. The McGraw Hill Companies, Inc. United Status of America.

Peltier, Thomas. R (2001). *Information Security Risk Analysis*. John Willey & Sons. Auerbach, United States of America.

Pickett, K.H. Spencer. (2005). *The Essential Handbook of Internal Auditing.* John Willey & Sons.

Skousen, K.Fred. (2001). *Akuntansi Keuangan Menengah.* Edisi ke-1. Salemba Empat, Jakarta.

Turban, Efraim, Reiner, R. Kelly, Jr., Potter, E. Richard. (2003). Introduction to Information Technology, 2nd edition; John Wiley and Sons, Inc.

Weber, Ron. (1999). *Information Systems Control and Audit.* Prentice Hall.

www.library.gunadarma.ac.id

www.library.usu.ac.id

www.librijournal.org