

EVALUASI SISTEM INFORMASI AKTIVA TETAP PADA PT TMS

Imelda Suardi; Henny Hendarti

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

ABSTRACT

The purpose of this study is to evaluate and assess how well the information system of fixed assets implemented by PT TMS (including general control and application control) in minimizing the current risks through the implemented controls. The methodology used is literature study by collecting data from a variety of books related to the topic and field research, such as observation, interviews, and questionnaires. Results of the evaluation are risks that exist in the system presented in the form of matrix of risk and control which consist of problem findings, potential risks (impact and likelihood) and the reliability of existing control (design and effectiveness). The general control applied by the company is found quite well, but the application control still needs improvement.

Keywords: *evaluation, information systems, fixed assets, general control, application control*

ABSTRAK

Tujuan penelitian ini adalah mengevaluasi dan menilai seberapa baik sistem informasi aktiva tetap PT TMS (meliputi pengendalian umum dan pengendalian aplikasi) dalam meminimalisasi resiko yang ada melalui pengendalian yang diterapkan. Metodologi yang digunakan dalam penelitian adalah kepustakaan dengan mengumpulkan data-data dari berbagai buku yang terkait dengan topik penelitian dan penelitian lapangan, yaitu observasi, wawancara, dan kuesioner. Hasil evaluasi ini adalah berupa resiko-resiko yang ada pada sistem yang disajikan dalam bentuk matriks resiko dan pengendalian yang terdiri dari temuan masalah, potensi resiko (impact dan likelihood) dan keandalan pengendalian yang ada (design dan effectiveness). Pengendalian umum yang diterapkan oleh perusahaan sudah cukup baik, akan tetapi pengendalian aplikasi yang diterapkan masih kurang baik dan perlu dilakukan perbaikan.

Kata kunci: *evaluasi, sistem informasi, aktiva tetap, pengendalian umum, pengendalian aplikasi*

PENDAHULUAN

Aktiva tetap adalah aktiva berwujud yang diperoleh dalam bentuk siap pakai atau dengan dibangun lebih dahulu, yang digunakan dalam operasi perusahaan, tidak dimaksudkan untuk dijual dalam rangka kegiatan normal perusahaan dan mempunyai masa manfaat lebih dari satu tahun (Standar Akuntansi Keuangan, 2004). Aktiva tetap yang dapat dikelola dengan baik merupakan salah satu ‘ujung tombak’ dalam mencapai tujuan dan menjalankan bisnis perusahaan. Sebaliknya, aktiva tetap yang tidak dapat dikelola dengan baik akan menjadi hambatan sekaligus kerugian bagi perusahaan.

PT TMS bergerak di bidang produksi dan distribusi makanan ringan, seperti kacang, biskuit, permen, minuman ringan, dan lain sebagainya. Untuk itu, perusahaan yang memiliki aktiva tetap yang sangat kompleks ini tentunya sangat membutuhkan sebuah sistem informasi aktiva tetap yang andal dan terintegrasi untuk mengelolanya, sehingga dapat menunjang kinerja perusahaan dan menciptakan sebuah sinergi yang memungkinkan perusahaan tersebut mencapai tujuannya dan memiliki kelebihan yang jauh di atas perusahaan-perusahaan lainnya.

Menurut Weber (1999), audit sistem informasi adalah proses pengumpulan dan pengevaluasian bukti untuk menentukan apakah suatu sistem komputer dapat melindungi aset, memelihara keutuhan data, membuat pencapaian tujuan organisasi menjadi lebih efektif dan telah menggunakan sumber daya secara efisien. Weber (1999) juga mengungkapkan bahwa ada dua jenis pengendalian yang perlu diterapkan pada sistem informasi, yaitu pengendalian umum (pengendalian manajemen operasional dan pengendalian manajemen keamanan) dan pengendalian aplikasi (pengendalian masukan, pengendalian keluaran, dan pengendalian batasan).

Pengendalian umum adalah sistem pengendalian internal komputer yang berlaku umum meliputi seluruh kegiatan komputerisasi sebuah organisasi secara menyeluruh. Artinya ketentuan-ketentuan yang diatur dalam pengendalian internal tersebut, berlaku untuk seluruh kegiatan komputerisasi pada organisasi atau perusahaan tersebut. Sedangkan pengendalian aplikasi adalah sistem pengendalian intern (*internal control*) pada sistem informasi berbasis teknologi informasi yang berkaitan dengan pekerjaan atau kegiatan atau aplikasi tertentu (setiap aplikasi memiliki karakteristik dan kebutuhan pengendalian yang berbeda) (Gondodiyoto, 2007).

Sementara menurut *The Information System Control and Audit Association* (ISACA) yang dikutip dari Cangemi dan Singleton dalam bukunya *Managing the Audit Function* (2003, p65), sistem pengendalian internal adalah kebijakan-kebijakan, prosedur-prosedur, praktek-praktek, dan struktur organisasi yang dirancang untuk memberikan keyakinan yang memadai (*reasonable assurance*) agar tujuan bisnis dapat dicapai dan kejadian-kejadian yang tidak diinginkan dapat dicegah atau dideteksi dan dikoreksi.

Evaluasi sistem informasi aktiva tetap pada PT TMS dibatasi dari pembelian aktiva tetap berupa peralatan dan inventaris kantor secara kredit, pembayaran, perbaikan (reparasi), penyusutan (depresiasi) sampai dengan penghapusan (*disposal*) aktiva tetap tersebut. pengendalian internal yang dibahas adalah pengendalian umum (pengendalian manajemen keamanan dan pengendalian manajemen operasi) dan pengendalian aplikasi (pengendalian masukan, pengendalian keluaran, dan pengendalian batasan).

Tujuan dilakukan evaluasi sistem informasi aktiva tetap pada perusahaan adalah untuk mengetahui dan mengevaluasi apakah sistem informasi aktiva tetap yang ada sudah sesuai dengan *standard* dan *business process*, mengidentifikasi permasalahan atau kelemahan, resiko yang mungkin timbul, dan bahkan kelebihan yang terdapat pada sistem informasi aktiva tetap, mengevaluasi apakah

pengendalian-pengendalian yang diterapkan mampu meminimalisasi resiko yang ada, memastikan *output* yang dihasilkan sesuai dengan hasil *input* yang telah diproses sehingga *output* yang dihasilkan dapat dipercaya.

Sedangkan manfaat yang diperoleh selama evaluasi pada perusahaan adalah perusahaan dapat mengurangi dan memperbaiki permasalahan atau kelemahan yang ada serta dapat meningkatkan efektifitas dan efisiensi pada sistem yang dimiliki, mengelola aktiva tetap dengan lebih baik, serta mendapatkan gambaran sesungguhnya (praktek) mengenai dunia kerja, proses audit, sistem informasi dalam perusahaan dan sebagainya dari teori yang selama ini dipelajari.

METODE

Metodologi yang digunakan dalam evaluasi ini adalah persiapan evaluasi, pelaksanaan evaluasi yang terdiri dari penelitian kepustakaan dan penelitian lapangan (observasi, wawancara, dan kuesioner), serta penyelesaian evaluasi yang berupa Laporan Audit.

HASIL DAN PEMBAHASAN

Uraian Sistem Informasi Aktiva Tetap PT TMS

Proses pencatatan dan pengelolaan aktiva tetap dimulai dari pengajuan pembelian aktiva tetap oleh pemakai aktiva tetap dengan membuat Proposal Pengajuan Investasi Aktiva Tetap. Proposal tersebut diperiksa oleh Manajer Akuntansi dan Keuangan, yang kemudian disetujui oleh Manajer Pabrik. Bagian Pembelian melakukan pemilihan pemasok dan membuat PO berdasarkan proposal yang disetujui.

Setelah aktiva tetap yang disertai Surat Jalan, Faktur, dan Faktur Pajak dikirim oleh pemasok, Bagian Gudang akan memeriksa aktiva tetap yang diterima dan membuat Bukti Barang Masuk. Dengan mencocokkan PO dengan Faktur dari Pemasok, Bagian Akuntansi dan Keuangan membuat Bukti Kas Keluar yang disetujui oleh Manajer Pabrik untuk melakukan pembayaran.

Setelah dilakukan pembayaran, aktiva tetap akan diakuisisi atau diakui melalui pencatatan aktiva tetap ke dalam sistem aplikasi ACCPAC (Sistem Informasi Aktiva Tetap).

Setiap bulan, penyusutan aktiva tetap akan dilakukan secara otomatis oleh ACCPAC. Metode yang digunakan untuk proses penyusutan adalah Metode Garis Lurus (*straight-line method*) dan disusutkan sesuai dengan masa manfaatnya.

Jika terjadi kerusakan pada aktiva tetap, pemakai akan memberitahukan kepada Bagian GA yang akan menghubungi pemasok. Setelah selesai diperbaiki, pemasok akan memberikan Faktur. Bukti Kas Keluar pun akan dibuat oleh Bagian Akuntansi dan Keuangan untuk melakukan pembayaran atas transaksi reparasi ini. Penghapusan aktiva tetap pada perusahaan ini hanya ditujukan untuk aktiva tetap yang dipindahkan ke cabang lain.

Setiap bulan, Bagian Pembelian akan membuat laporan pembelian dan penerimaan barang, sedangkan Laporan Aktiva Tetap dan Laporan Keuangan dibuat oleh Manajer Akuntansi dan Keuangan.

Hasil Evaluasi pada Pengendalian Umum

Di bawah ini adalah beberapa temuan pada audit *security management controls*:

- Temuan 1 : Tidak dilakukan *scan virus* secara rutin.
Resiko : Selain dapat menghambat proses kerja komputer perusahaan, data penting perusahaan pun dapat terkena *virus*, rusak, dan bahkan hilang. Jika hal ini tidak segera diatasi, maka dapat merusak data dan *software* serta mengganggu kegiatan operasional perusahaan. Kerugian finansial karena penggantian perangkat terus-menerus juga dapat disebabkan oleh hal ini.
Rekomendasi : *Scanning virus* secara otomatis di seluruh komputer setiap hari secara rutin pada saat komputer dinyalakan. Selain itu, juga pada saat membuka atau *mengcopy file* dari media eksternal seperti *flashdisk*.
- Temuan 2 : Tidak terdapat alarm kebakaran.
Resiko : Kesulitan dan hambatan untuk memberitahukan kepada seluruh karyawan dan sekitarnya akan terjadinya kebakaran, sehingga tindakan penyelamatan terhadap aset ataupun karyawan menjadi lama dan kebakaran tidak dapat segera ditangani. Hal ini dapat menyebabkan kerugian yang cukup besar dan berpengaruh bagi kegiatan bisnis maupun keuangan perusahaan.
Rekomendasi : Meletakkan alarm kebakaran tempat yang strategis atau memberikan larangan merokok di area kantor karena dapat meminimalkan kerusakan dan kerugian akibat kebakaran. Serta memastikan alat pemadam kebakaran pada perusahaan berfungsi dengan baik.
- Temuan 3 : Karyawan tidak diberikan larangan membawa makanan di dekat peralatan komputer.
Resiko : Makanan ataupun minuman yang tumpah dapat mengakibatkan ruangan menjadi kotor dan mendatangkan serangga ataupun tikus yang dapat merusak kabel-kabel, *disk drive*, *harddisk*, dll. Resiko lainnya adalah kinerja karyawan menjadi kurang efektif dan efisien karena kurangnya konsentrasi dan disiplin.
Rekomendasi : Memberikan larangan kepada karyawan untuk tidak membawa makanan dan minuman ke dalam ruang atau peralatan komputer. Perusahaan juga perlu mensosialisasikan prosedur kebersihan kepada seluruh karyawan.
- Temuan 4 : Tidak terdapat prosedur kebersihan aset sistem informasi.
Resiko : Karyawan tidak memiliki *awareness* terhadap resiko keamanan aset sistem informasi dan akibat yang ditimbulkan dari kecerobohan ini. Hal ini juga dapat mengakibatkan kerusakan pada aset seperti debu, kebakaran, dll.
Rekomendasi : Lakukan prosedur kebersihan aset sistem informasi dengan baik agar aset perusahaan dapat beroperasi dengan baik. Agar prosedur kebersihan dilakukan dengan baik oleh seluruh karyawan, perusahaan dapat menempelkan poster-poster atau kartu-kartu yang menarik mengenai kebersihan, hal-hal yang perlu dan tidak boleh dilakukan, di tempat-tempat yang sering dilalui.
- Temuan 5 : Tidak terdapat pemisahan antara ruang komputer dengan tempat penyimpanan dokumen pada bagian akuntansi.
Resiko : Dapat terjadi kehilangan data akibat pencurian oleh pihak yang tidak berwenang dan terjadi manipulasi terhadap data, serta pengarsipan maupun *input* data yang kurang efektif.
Rekomendasi : Dilakukan pemisahan antara ruang komputer dengan tempat penyimpanan dokumen pada bagian akuntansi.

Berikutnya, temuan pada audit *operations management controls* adalah sebagai berikut:

- Temuan 1 : Tidak terdapat pelatihan khusus untuk karyawan baru dalam menggunakan ACCPAC.
Resiko : Karyawan dapat mengalami kesulitan dalam menggunakan ACCPAC dan akan mengganggu kegiatan operasional perusahaan.
Rekomendasi : Berikan pelatihan secara khusus dan panduan kepada karyawan terutama karyawan baru yang akan menggunakan aplikasi tentang penggunaan ACCPAC.
- Temuan 2 : Tidak terdapat fasilitas menu *help* pada ACCPAC.
Resiko : Dengan tidak adanya menu *help*, ada kemungkinan terjadinya *human error*, karyawan tidak dapat mengetahui letak kesalahan yang dilakukan dan tidak dapat dengan segera memperbaikinya. Apabila terlalu lama dibiarkan, kesalahan mungkin tidak diperbaiki, sehingga laporan yang dihasilkan tidak benar.
Rekomendasi : Menyediakan menu *help* pada ACCPAC karena dapat memberikan informasi kepada karyawan apa yang harus dilakukan ketika melakukan *entry* data ke komputer dan mempermudah manajer dalam melakukan pemeriksaan.
- Temuan 3 : Terdapat beberapa menu pada ACCPAC yang tidak digunakan dalam transaksi maupun proses bisnis perusahaan.
Resiko : Menu-menu tersebut dapat membingungkan bagi karyawan yang baru menggunakan ACCPAC dan menghambat kinerja karyawan serta dapat menimbulkan kesalahan dalam *input* data.
Rekomendasi : Sebaiknya menu-menu pada ACCPAC dapat digunakan dan mendukung dalam proses bisnis perusahaan. Dan yang terpenting adalah karyawan diberikan buku panduan ataupun penjelasan lisan yang terperinci tentang ACCPAC.

Berikutnya, temuan pada audit *input control* sebagai berikut:

- Temuan 1 : Tidak terdapat *error message* pada saat terjadi kesalahan dalam *input* data.
Resiko : Jika terjadi kesalahan dalam *input* data, waktu yang dibutuhkan untuk menemukan letak kesalahan lebih lama dibandingkan dengan adanya *error message*.
Rekomendasi : Pada ACCPAC ditambahkan fungsi *error message*, sehingga karyawan dapat segera memperbaiki jika terjadi kesalahan dalam *penginputan*. Selain itu, verifikasi *independent* juga dapat dilakukan untuk mengatasi hal ini.
- Temuan 2 : Tidak terdapat *pre-printed-number* pada Bukti Bank Keluar.
Resiko : Pengeluaran tidak dapat dikendalikan dengan baik, memungkinkan penggunaan kas untuk hal pribadi atau kurang penting. Dalam jangka panjang, hal ini dapat mempengaruhi efektifitas dan efisiensi penggunaan kas dan membawa dampak negatif bagi keuangan perusahaan.
Rekomendasi : Bukti Bank Keluar sebaiknya memiliki *pre-printed-number* dan dilakukan otorisasi serta pemisahan tugas dan fungsi. Selain untuk mencegah resiko-resiko, hal ini juga dapat memudahkan proses audit dan mendeteksi kesalahan maupun penyalahgunaan dana lebih cepat.
- Temuan 3 : Tidak terdapat *warning message* apabila terjadi pemasukan data yang ganda.
Resiko : Dapat terjadi redundansi data, yang juga memungkinkan kesalahan pembuatan laporan dan evaluasi laporan yang salah.
Rekomendasi : Perusahaan memiliki mekanisme untuk mencegah *input* transaksi yang lebih dari satu (pemeriksaan data). Hal ini juga sebagai upaya untuk menghindari terjadinya manipulasi data yang ilegal.

- Temuan 4 : Tidak ada kombinasi warna dalam aplikasi ACCPAC apabila *user* melakukan kesalahan dalam *penginputan*.
- Resiko : Dapat terjadi kesalahan dalam *entry* data karena tidak ada perbedaan warna pada tampilan dan dapat menghambat pekerjaan karyawan.
- Rekomendasi : Menggunakan kombinasi warna yang membuat proses *entry* data dapat dilakukan dengan cepat, tepat dan tidak membuat operator cepat lelah (menggunakan warna – warna yang *soft*).
- Temuan 5 : Tampilan menu *input* kurang efektif dalam proses *penginputan* karena ada kolom-kolom yang tidak terpakai.
- Resiko : Menghambat proses *input* data, menimbulkan kesalahan dalam *penginputan* dari dokumen sumber.
- Rekomendasi : Perusahaan menggunakan sistem yang memiliki menu *input* cukup efektif untuk mempermudah dan mempercepat proses *penginputan*. Untuk sistem yang sudah berjalan, untuk setiap karyawan yang belum dapat menggunakan ACCPAC dengan baik, sebaiknya diberikan pelatihan dan pendalaman khusus terhadap ACCPAC. Kesalahan-kesalahan seperti ini meskipun bersifat tidak material, akan tetapi dapat menghambat proses bisnis perusahaan jika dibiarkan terlalu lama terjadi.
- Temuan 6 : Tidak terdapat menu peringatan jika data belum *dibackup* pada aplikasi ACCPAC
- Resiko : Karyawan dapat lupa melakukan *backup* data sehingga informasi tidak *up to date*. Jika terjadi bencana, maka dapat terjadi kehilangan data – data penting perusahaan
- Rekomendasi : Karyawan sebaiknya melakukan *backup* data setiap hari dan disediakan menu peringatan untuk mengingatkan *user*. Hal lain yang bisa dilakukan adalah dengan membuat peringatan-peringatan tertulis untuk melakukan *backup* data, seperti membuat *screensaver* pada komputer yang bertuliskan untuk *backup* data, membuat catatan pengingat pada setiap komputer, dan sebagainya.
- Temuan 7 : Kode PO dan BBM pada dokumen sumber tidak sama dengan layar *input*.
- Resiko : Dapat mengalami kesulitan dan hambatan jika dilakukan pemeriksaan data antara dokumen sumber dan layar *input*. Hal ini juga berakibat kesalahan dalam membuat laporan. Selain itu, karyawan dapat melakukan kesalahan dan mengalami kesulitan dalam *input* data.
- Rekomendasi : Perusahaan menggunakan kode PO dan BBM yang sama pada dokumen sumber dan pada layar *input*.

Berikutnya, temuan pada audit *boundary control* sebagai berikut:

- Temuan 1 : Panjang *password* yang digunakan tidak dibatasi oleh ACCPAC.
- Resiko : Setiap *user* dapat memiliki panjang *password* yang berbeda – beda dan *password* yang digunakan dapat mudah ditebak.
- Rekomendasi : Batasi panjang *password* sebanyak 6 karakter dan dilakukan *invisible password*.
- Temuan 2 : Tidak terdapat prosedur bantuan jika *user* lupa *passwordnya* dalam aplikasi ACCPAC.
- Resiko : Hal ini dapat memperlambat karyawan dalam mengakses ACCPAC. Selain itu, ada kemungkinan karyawan juga tidak dapat menggunakan ACCPAC dan harus menghubungi bagian IT di kantor pusat
- Rekomendasi : Pada ACCPAC disediakan menu *help* dan diberikan fasilitas pertanyaan keamanan pada sistem jika karyawan lupa akan *passwordnya*. Alternatif lain adalah dengan membuat prosedur penggantian *password* yang mudah dimengerti oleh *user*.
- Temuan 3 : Tidak terdapat pembatasan umur *password* beserta fasilitas *automatically warning* yang mengingatkan *user* untuk mengganti *passwordnya* secara berkala.

- Resiko : *Password* dapat diketahui oleh pihak lain dan dapat terjadi penyalahgunaan wewenang yaitu mengakses, membuka dan meng*copy* tanpa wewenang
- Rekomendasi : Dibuat pembatasan umur *password* (kadaluarsa *password*). Tidak boleh memberitahukan *password* kepada orang lain dan selalu mengganti *password* secara rutin. Sebaiknya diberikan kebijakan dalam penjadwalan untuk melakukan perubahan *password* yang dilakukan tiga bulan satu kali dengan menentukan tanggal perubahan. Jadi perubahan *password* dilakukan secara serentak oleh setiap karyawan. Misalnya, dari tanggal 23 sampai dengan tanggal 30 Desember adalah jangka waktu untuk merubah *password*. Karyawan yang terlambat harus menerima konsekuensinya, yaitu *user* tidak dapat menggunakan ACCPAC.
- Temuan 4 : Tidak dibatasi kesalahan dalam penginputan *login* akses pada ACCPAC
- Resiko : Memberikan peluang tidak terbatas kepada pihak yang tidak berwenang untuk dapat mengakses ACCPAC.
- Rekomendasi : Melakukan enkripsi dan *invisible password*, dengan menentukan batasan kesalahan dalam menginput *password* sebanyak 3 kali dan jika melewati batas tersebut maka ACCPAC akan tertutup secara otomatis.
- Temuan 5 : Tidak terdapat batas waktu (*time limit*) dalam penggunaan aplikasi ACCPAC jika *user* lupa atau tidak *log off*.
- Resiko : Pihak yang tidak berwenang (*unauthorized user*) dapat mencuri dan memodifikasi aset perusahaan pada saat komputer baru ditinggalkan beberapa saat.
- Rekomendasi : Pada ACCPAC diberikan batas waktu sehingga jika *user* lupa *log off* dan melakukan kontrol akses sehingga ACCPAC secara otomatis akan tertutup sehingga *user* harus memasukkan *user ID* dan *password* kembali. Sebagai tambahan, setiap komputer juga dapat diberikan *screensaver* (dengan jangka waktu yang tidak terlalu lama) dan *password*, sehingga kemungkinan komputer digunakan oleh orang yang tidak berkepentingan dapat diminimalisasi.
- Temuan 6 : ACCPAC tidak memiliki *audit trail*.
- Resiko : Jika ACCPAC tidak memiliki *audit trail*, proses audit dapat terhambat karena auditor akan mengalami kesulitan saat mengevaluasi sistem untuk mengetahui aktivitas *user* mulai dari *login*, proses selama penggunaan aplikasi, hingga *log off*.
- Rekomendasi : Sebaiknya dibuat *audit trail* pada ACCPAC.

Temuan pada audit *output control* yaitu:

- Temuan 1 : Tidak terdapat pembatasan berapa kali Laporan Keuangan, Laporan Pembelian dan Penerimaan Barang dan Laporan Aktiva tetap dapat dicetak pada ACCPAC.
- Resiko : Laporan dapat dimodifikasi oleh pihak yang tidak berwenang. Pencetakan laporan yang berulang-ulang dan tidak sesuai kebutuhan juga dapat menimbulkan resiko laporan kehilangan kerahasiaannya.
- Rekomendasi : Diberikan batasan dalam pencetakan laporan jika ditemukan kesalahan dalam pembuatan laporan dilakukan pengawasan terhadap proses pencetakan laporan. Selain itu, juga memberikan otorisasi dalam pencetakan laporan serta pemisahan tugas dan fungsi.
- Temuan 2 : Kode PO dan BBM pada layar *input* tidak sama dengan kode pada format Laporan Pembelian dan Penerimaan Barang.
- Resiko : Membingungkan karyawan yang melakukan *input* data, sehingga memungkinkan terjadinya kesalahan dalam pembuatan laporan.
- Rekomendasi : Kode PO dan BBM pada layar *input* seharusnya tidak dibedakan dengan format Laporan Pembelian dan Penerimaan Barang.

- Temuan 3 : Pada semua laporan tidak terdapat keterangan pihak yang berwenang menerimanya dan otorisasi pihak yang membuat laporan. Selain itu, pada Laporan Keuangan dan Laporan Pembelian dan Penerimaan Barang tidak tercantum *control page*, *control copy*, judul, tanggal, periode dan nomor urut.
- Resiko : Dapat terjadi penyalahgunaan laporan dan pemberian laporan yang salah
- Rekomendasi : Pada Laporan Keuangan dan Laporan Pembelian dan Penerimaan Barang harus tercantum *control page*, *control copy*, judul, tanggal, periode, nomor urut, keterangan pihak yang berwenang menerimanya dan otorisasi pihak yang membuat laporan.
- Temuan 4 : Tidak dilakukan *control* terhadap jumlah kertas yang digunakan secara berkala.
- Resiko : Inefektif dan inefisiensi dalam penggunaan kertas dan dapat mengakibatkan kerugian finansial pada perusahaan.
- Rekomendasi : Dilakukan perhitungan atau memperkirakan berapa penggunaan kertas setiap bulannya.

PENUTUP

Simpulan

Pengendalian Keamanan dan Pengendalian Operasi yang diterapkan perusahaan cukup baik dan tidak memiliki dampak negatif yang sangat berpengaruh terhadap sistem informasi perusahaan, serta tidak mengganggu aktivitas operasional perusahaan secara keseluruhan. Sedangkan Pengendalian *Input*, *Output*, dan *Boundary* yang diterapkan perusahaan masih kurang baik karena pengkodean pada dokumen sumber, layar *input* dengan laporan tidak sama, masih terdapat beberapa kelemahan dalam penggunaan *password*. Jadi, pengendalian yang ada masih perlu ditingkatkan lagi untuk mencapai tujuan perusahaan.

Saran

Perusahaan perlu memperhatikan pengendalian internal yang diterapkan untuk meminimalisasi resiko-resiko yang mungkin terjadi. Untuk Pengendalian Keamanan sebaiknya perusahaan melakukan *scanning virus* secara rutin dan lebih memperhatikan kebersihan pada aset. Pada pengendalian operasi, perusahaan perlu memberikan pelatihan dan panduan secara khusus untuk karyawan baru dalam penggunaan ACCPAC. Pada Pengendalian *Input*, perusahaan perlu memperhatikan kesesuaian antara dokumen sumber dengan layar *input*. Pada pengendalian batasan, perusahaan perlu lebih memperhatikan ketentuan dalam penggunaan *password*. Untuk Pengendalian *Output*, perusahaan perlu memberikan batasan dalam pencetakan laporan, memperbaiki format laporan, semua laporan sebaiknya dicetak melalui ACCPAC.

DAFTAR PUSTAKA

- Cangemi, P. Michael and Singleton, Tommie. (2003). *Managing The Audit Function* (3rd edition). New Jersey: John Willey & Sons.
- Gondodiyoto, S. (2007). *Audit Sistem Informasi + Pendekatan CobIT* (edisi revisi). Jakarta: Mitra Wacana Media.
- Weber, Ron. (1999). *Information Systems Control and Audit*. New Jersey: Prentice Hall.