ISSN (Printed) : 2579-7271
ISSN (Online) : 2579-5406

Audit Sistem Informasi *Internal Control* Dengan Metode Audit *Through The Computer*

Megawati[1], Syaifullah[2], Nesdi E. Rozanda[3], Wendi Gusfan Hutapea[4]
Program Studi Sistem Informasi, Fakultas Sains dan Teknologi,
Universitas Islam Negeri Sultan Syarif Kasim Riau[1,2,3,4]
Jl. HR Soebrantas KM.15 Panam Pekanbaru - Riau
e-mail: megawati@uin-suska.ac.id[1]; syaifullah@uin-suska.ac.id[2];
nesdi.rozanda@uin-suska.ac.id[3]; gsfaan@gmail.com[4].

Abstrak

Sistem ALWIS sudah digunakan sejak tahun 2009, system ini adalah Enterprise resurce yang digunakan oleh perusahaan PT. Alamjaya Wirasentosa. Terdapat beberapa kendala pada sistem ALWIS tersebut, yaitu data kredit limit pelanggan hilang, data piutang tidak cocok dengan yang sebenarnya, dan selisih harga diskon barang. Tujuan dari penelitian ini adalah untuk mendapatkan nilai tingkat resiko, mendapatkan temuan negatif, serta memberikan rekomendasi penanganan resiko pada aplikasi ALWIS. Metode audit sistem informasi yang digunakan adalah metode audit through the computer, dan teknik pengumpulan bukti audit menggunakan metode blackbox, secara langsung berfokus pada operasi pemrosesan dalam sistem komputer. Hasil penelitian ini diperoleh 11 (sebelas) temuan berdasarkan dari pengujian pengendalian umum manajemen keamanan, pengendalian batasan, pengendalian masukan, pengendalian proses dan pengendalian keluaran. Berdasarkan penilaian diperoleh bahwa system ini berkategori resiko medium dengan hasil penilaian 16,4 pada rata-rata nilai temuan. Sehingga dapat disimpulkan bahwa pengendalian yang dilakukan perusahaan sudah cukup baik dalam menangani resiko yang ada.

Kata kunci: *ALWIS, audit through the computer, internal control*

Abstract

ALWIS system has been used since 2009, this system is an Enterprise resurce that is used by PT. Alamjaya Wirasentosa. There are several constraints on the ALWIS system, namely lost customer credit limit data, receivables data does not match the truth, and the difference in price of discounted goods. The purpose of this study is to get the value of the level of risk, get negative findings, and provide recommendations for risk management in the ALWIS application. The information system audit method used is the through the computer audit method, and the audit evidence collection technique uses the blackbox method, directly focusing on processing operations in the computer system. The results of this study were obtained 11 (eleven) findings based on general security management control testing, boundary control, input control, process control and output control. Based on the assessment, it was found that the system was categorized as medium risk with an assessment of 16,4 on the average value of the findings. So it can be concluded that the control by the company is good enough in dealing with existing risks.

Keywords*: ALWIS, audit through the computer, internal control*

1. Pendahuluan

Semakin pesatnya kemajuan teknologi, khususnya teknologi informasi dan komputer, PT. Alamjaya Wirasentosa ikut berperan dalam menggunakan teknologi berbasis komputerisasi untuk membantu jalannya proses bisnis. PT. Alamjaya Wirasentosa adalah salah satu perusahaan distribusi barang konsumen di Sumatera (Indonesia). Berdiri sejak 25 Agustus 1992, perusahaan ini berpusat di Medan yaitu di Tanjung Morawa. Sistem yang digunakan PT. Alamjaya Wirasentosa bernama Alamjayawirasentosa (AJWS). Sistem AJWS ini sudah dipakai sejak tahun 2009, dan sudah diperbarui ke versi baru dengan nama ALWIS. Sistem ALWIS merupakan sistem milik PT. Alamjaya Wirasentosa (*custom build*) yang dibangun oleh Bapak Herman Sentosa.

ALWIS dirancang dengan beberapa modul yaitu modul *Accounting Management*, *Inventory Management*, *Purchasing Management*, *Sales Management*, *Customer Relationship Management*, *Supply Chain Management*, *Warehouse Management*, *Quality Management*, *Logistic* dan Sistem Informasi Manajemen.

Terdapat masalah setelah AJWS di *upgrade* ke versi ALWIS terdapat selisih data piutang pelanggan, selisih harga program diskon barang pada sistem dengan berita acara program diskon barang dari *principle*, dan hilangnya data kredit limit pelanggan pada sistem. Dan ketika terjadi masalah maka perbaikan akan segera dilakukan dan terdapat kebijakan yang kurang tepat. Maka dalam penelitian ini penulis melakukan audit pada sebuah sistem informasi ALWIS untuk

ISSN (Printed) : 2579-7271
ISSN (Online) : 2579-5406

menemukan temuan *negatif* berdasarkan kelemahan-kelemahan sistem yang ada dan melakukan penilaian tingkat resiko pada sistem tersebut.

Untuk mengetahui resiko yang akan terjadi diperlukan adanya audit pengendalian *internal control*. Tujuan dilakukannya penelitian ini yaitu untuk melakukan audit *internal control* pada sistem ALWIS dalam menentukan nilai *level* resiko berdasarkan kelemahan yang ditemukan dan menemukan temuan-temuan *negatif* dari sistem ALWIS tersebut. Jika audit *internal control* tersebut berjalan dengan optimal maka kebutuhan pengoperasian perusahaan dapat terpenuhi.

Audit *Through The Computer* adalah salah satu metode audit sistem informasi dalam melakukan pengujian pada pengendalian aplikasi suatu sistem. Audit *Through The Computer* merupakan suatu pendekatan yang berorientasi pada komputer dengan melakukan pengujian sistem menggunakan metode *blackbox* dan secara langsung berfokus pada operasi pemrosesan dalam sistem komputer. Metode ini berasumsi bahwa apabila sistem pemrosesan mempunyai pengendalian yang memadai maka kesalahan dan penyalahgunaan tidak akan terlewat untuk di deteksi. Sebagai akibatnya keluaran dapat diterima. Tujuan dari Audit *Through The Computer* adalah untuk meneliti apakah aplikasi yang dioperasikan sesuai dengan kondisi yang sesungguhnya [1].

2. Metode Penelitian

Metode audit *Through The Computer* merupakan suatu pendekatan yang berorientasi pada komputer dan secara langsung berfokus pada operasi pemprosesan dalam sistem komputer. Metode ini berasumsi bahwa apabila sistem pemprosesan mempunyai pengendalian yang memadai maka kesalahan dan penyalahgunaan tidak akan terlewat untuk dideteksi. Sebagai akibatnya keluaran dapat diterima. Metode audit TI menggunakan audit *through the computer*. Ada lima pengendalian yang digunaan dalam pengujian audit TI, yaitu: (1) pengendalian manajemen keamanan; (2) pengendalian batasan; (3) pengendalian masukan; (4) pengendalian proses; dan (5) pengendalian keluaran.

a. Pengendalian Umum Manajemen Keamanan

Weber (1999) bahwa pengendalian manajemen keamanan bertanggung jawab atas keamanan aset sistem informasi. Ancaman yang utama terhadap keamanan asset sistem informasi [4], antara lain: Ancaman Kebakaran, Ancaman Banjir, Perubahan Tegangan Sumber *Energy*, Kerusakan Struktural, Polusi Ruangan TI, Penyusupan, Virus, dan *Hacking*.

b. Pengendalian Batasan

Pengendalian Batasan adalah menentukan hubungan atau relasi antara pemakai sistem dengan sistem itu sendiri. Pengendalian batasan ini didesain untuk mengenal identitas dan otentik tidaknya *user* sistem dan untuk menjaga agar sumberdaya sistem informasi digunakan oleh *user* dengan cara yang ditetapkan [1]. Kontrol terhadap subsistem *boundary* memiliki tiga tujuan, yaitu:

1) Memastikan pemakai komputer adalah orang yang memiliki hak atau wewenang.
2) Memastikan identitas yang diberikan oleh pemakai adalah benar.
3) Membatasi tindakan pemakai untuk menggunakan komputer ketika melakukan tindakan otorisasi.

c. Pengendalian Masukan

Pengendalian masukan dirancang dengan tujuan untuk mendapat keyakinan bahwa data transaksi *input* adalah *valid*, lengkap, serta bebas dari kesalahan dan penyalahgunaan. Pengendalian ini merupakan pengendalian aplikasi yang penting karena *input* yang salah akan menyebabkan *output* juga keliru [1]. Kriteria standar atas pengendalian masukan, yaitu:

1) Terdapat kontrol terhadap dokumen sumber yang akan di*input* (*source document controls*).
2) Terdapat otoritas bagi pihak yang melakukan *delete* atau *update* data (*validation controls*).
3) Terdapat pesan *error* apabila terdapat kesalahan dalam peng*input*an data (*input error correction*).

d. Pengendalian Proses

Pengendalian proses ialah pengendalian intern untuk mendeteksi jangan sampai data menjadi *error* karna adanya kesalahan proses. Tujuan pengendalian pengolahan adalah untuk

ISSN (Printed) : 2579-7271
ISSN (Online) : 2579-5406

mencegah agar tidak terjadi kesalahan-kesalahan selama proses pengolahan data [1]. Kriteria standar atas pengendalian proses, yaitu:

1) Sistem harus mampu mencegah atau mendeteksi kehilangan data dan data yang tidak *valid* selama proses dilakukan (*error detection and correction*).
2) Kesalahan yang dilakukan selama pemrosesan harus dapat segera diperbaiki.
3) Setiap proses yang dilakukan harus terekam ke dalam *database*.

e. Pengendalian Keluaran

Pengendalian keluaran merupakan pengendalian yang dilakukan untuk menjaga *output* sistem agar akurat, lengkap dan digunakan sebagaimana mestinya [1]. Pengendalian keluaran ini didesain agar *output*/informasi disajikan secara akurat, lengkap, mutakhir, dan di distribusikan kepada orang-orang yang berhak secara cepat waktu dan tepat waktu. Kriteria standar atas pengendalian keluaran [1], yaitu:

1) Hasil *output* yang akurat, langkap, *up to date*, dan didistribusikan kepada pihak yang berhak serta tepat waktu.
2) Terdapat prosedur permintaan laporan rutin atau permintaan laporan baru.
3) Terdapat kontrol terhadap penghancuran laporan yang tidak dibutuhkan.

3. Analisis dan Hasil

Dalam pelaksanaan audit sistem informasi pengendalian aplikasi dalam pengumpulan bahan bukti audit dengan menetukan apakah sistem komputerisasi dapat memelihara kebenaran dan integritas data dalam pencapaian tujuan perusahaan secara efektif dan efisien. Untuk memperoleh hasil temuan audit dapat dilakukan dengan cara wawancara langsung kepada KAK dan *admin sales* dengan cara wawancara dan pengamatan (observasi) langsung di lapangan. Adapun tahapan-tahapan proses audit adalah sebagai berikut:

1) Perencanaan audit

Pada tahapan ini ditetapkan persiapan audit, ruang lingkup, tujuan pelaksanaan audit, dan pelaksanaan audit terhadap sistem ALWIS.

a) **Persiapan audit**; Penetapan materi audit dan literatur yang berhubungan dengan audit TI.
b) **Ruang lingkup audit**; Ruang lingkup audit *internal control* hanya sebatas pengendalian umum manajemen keamanan dan pada pengendalian aplikasi hanya sebatas pengendalian batasan, masukan, proses, dan keluaran.
c) **Tujuan pelaksanaan audit**; Adapun tujuannya ialah untuk menemukan temuan *negatif* pada sistem ALWIS, dan untuk melakukan penilaian *level* resiko pada temuan yang ditemukan pada sistem ALWIS.
d) **Metode audit**; Pelaksanaan audit *internal control* ini menggunakan metode audit *through the computer*.
e) **Persiapan penelitian lapangan**; Adapun persiapan yang dilakukan untuk melakukan audit *internal control* dengan melakukan pengujian berdasarkan instrumen pada masing-masing pengendalian, wawancara, dan observasi.

2) Persiapan penelitian lapangan

Dalam melakukan penelitian, auditor memerlukan beberapa persiapan untuk melakukan audit *internal control* pemeriksaan, wawancara pada KAK dan admin sales dan melakukan pengamatan langsung di lapangan (obervasi).

a) Instrumen pengendalian manajemen keamanan.
Pertanyaan mengenai *internal control* terhadap manajemen keamanan baik fisik maupun sistem (*security management controls*) yang dimaksudkan untuk menjamin agar sistem informasi tetap aman. Aset sumber daya informasi mencakup fisik (perangkat mesin dan fasilitas penunjangnya) serta aset tak berwujud (non-fisik) yaitu data/informasi dan sistem aplikasi komputer.

b) Instrumen pengendalian batasan.
Pertanyaan mengenai pengendalian batasan dimaksud untuk identitas *user* valid dalam memproses sistem dan menjaga agar sumber daya sistem informasi digunakan oleh *user* dengan cara yang ditetapkan.

c) Instrumen pengendalian masukan.
Pertanyaan dirancang dengan tujuan mendapat keyakinan bahwa data transaksi *input* bernilai *valid*, lengkap, serta bebas dari kesalahan dan penyalahgunaan.

ISSN (Printed) : 2579-7271
ISSN (Online) : 2579-5406

d) Instrumen pengendalian proses.
Pertanyaan dirancang untuk mendeteksi jangan sampai data menjadi *error* karna adanya kesalahan saat pemrosesan data.

e) Instrumen pengendalian keluaran.
Pertanyaan dirancang untuk menjaga *output* sistem agar akurat, lengkap, dan didistribusikan kepada pihak yang memilki kewenangan.

3) Wawancara

Melakukan wawancara lisan dengan KAK dan *admin sales* sistem tersebut untuk mendapatkan informasi tentang prosedur sisitem ALWIS dan melakukan wawancara sesuai dengan instrumen yang tersusun sebelumnya untuk mendapatkan hasil temuan audit agar dapat memberikan nilai tingkatan resiko setiap temuan.

4) Observasi

Audit ini dilakukan melalui pengamatan secara langsung kepada sistem ALWIS untuk mengetahui gambaran umum tentang proses-proses yang terdapat pada sistem tersebut dan melakukan pengoperasian langsung pada sistem ALWIS.

3.1. Tahap Pengujian Audit *Internal Control*

Langkah kedua dalam audit ini adalah tahap pengujian pengendalian. Pengujian pengendalian bertujuan untuk mengetahui apakah pengendalian yang ada telah dilakukan sesuai dengan prosedur yang telah ditetapkan dengan melakukan pemeriksaan, wawancara, dan observasi. Terdapat tiga tahap yang terdapat dalam tahap pengujian pengendalian, yaitu:

1) Melaksanakan pengujian pengendalian berupa pengumpulan bukti audit berdasarkan program audit yang telah dibuat dengan sejumlah instrumen (wawancara dan kuesioner).
2) Melakukan evaluasi terhadap bukti audit, berupa menganalisis bukti audit untuk mencari temuan-temuan yang terdapat pada ALWIS.
3) Menentukan penilaian resiko, menggunakan *Level* Penilaian Resiko *National Institute of Standard and Technology* (NIST) melalui publikasi khusus 800-30 tentang *Risk Management Guide for Information Technology System*. *Level* penilaian resiko merupakan suatu cara untuk menganalisa seberapa besar pengaruh kemungkinan terjadinya ancaman (*Threat Likelihood*) terhadap dampak yang ditimbulkan (*Impact*) [3]. Definisi *likelihood level* dapat dilihat pada Tabel 1 dan definisi *magnitude of impact* dapat dilihat pada Tabel 2.

Tabel 1. L*ikelihood Level*

Likelihood Level	Likelihood Definition
High	Sumber ancaman dianggap sangat mungkin terjadi dan kontrol untuk mencegah vulnerability terjadi dianggap tidak efektif.
Medium	Sumber ancaman mungkin terjadi, tetapi kontrol ditetapkan di tempat-tempat yang dapat mengganggu keberhasilan pencegahan vulnerability.
Low	Sumber ancaman kecil kemungkinan terjadi atau kontrol ditetapkan untuk mencegah atau setidaknya menghalau vulnerability.

Tabel 2. Definisi *magnitude of impact*

Risk Level	Risk Description and Necessary Actions
High	Jika sebuah temuan dievaluasi sebagai High Risk, maka penting untuk mempertimbangkan tindakan perbaikan.
Medium	Jika sebuah temuan ditentukan sebagai Medium Risk, tindakan perbaikan diperlukan dan sebuah rencana harus diterapkan.
Low	Jika sebuah temuan ditentukan sebagai Low Risk, dipertimbangkan apakah diperlukan tindakan perbaikan atau memutuskan untuk menerima resiko.

Besarnya nilai *Threat Likelihood* dinyatakan dengan: *High* (H) diberi nilai 1,0; *Medium* (M) diberi nilai 0,5; dan *Low* (L) diberi nilai 0,1. Sedangkan besarnya nilai *Impact* dinyatakan dengan: *High* (H) yang diberi nilai 100; *Medium* (M) diberi nilai 50; dan *Low* (L) yang diberi nilai 10. Teknik perhitungan dalam *Level* penilaian resiko menggunakan fungsi perkalian antara *Threat Likelihood* dengan *Impact*, caranya yaitu:

1) Tentukan kemungkinan terjadinya ancaman (*Threat Likelihood*) berdasarkan nilai yang ada, apakah *High*, *Medium*, atau *Low*.
2) Tentukan dampak yang mungkin terjadi (*Impact*) berdasarkan nilai yang ada, apakah *High*, *Medium*, atau *Low*.

ISSN (Printed) : 2579-7271
ISSN (Online) : 2579-5406

3) Setelah itu kalikan antara *Threat Likelihood* dengan *Impact*.
4) Hasil perkalian tersebut dijumlahkan dan dibagi dengan jumlah pertanyaan.
5) Hasil pembagian tersebut dinilai dengan menggunakan *Risk Scale* apakah termasuk kategori *High*, *Medium*, atau *Low* dapat dilihat pada Tabel 3.
6) Ancaman yang dijadikan resiko dan diberikan rekomendasi hanya kategori *Medium* dan *High*.

Tabel 3. *Risk Scale*

Risk Scale	Low	Medium	High
	1 – 10	>10 - 50	>50-100

Adapun spesifikasi sistem yang diaudit diantaranya: (1) Spesifikasi pada *server* (*Processor pentium dual core, Harddisk* 500 GB, Ram 2 GB. (2) Spesifikasi pada *client*: (*Processor pentium dual core,* Ram 2 GB).

3.2. Hasil Audit

Hasil audit yang didapat merupakan temuan-temuan *negatif* dari program audit yang dilaksanakan. Temuan-temuan *negatif* tersebut dapat dilihat pada Tabel 9. Berdasarkan program audit sistem informasi yang telah dilaksanakan penulis, secara keseluruhan terdapat 11 temuan yang terdapat pada ALWIS.

Tabel 9. Hasil Temuan Audit

Jenis Pengendalian	Temuan
Manajemen Keamanan	-Perusahaan tidak memiliki *alarm* kebakaran otomatis di sekitar ruangan TI, tetapi terdapat tabung pemadam kebakaran.
	-Karyawan boleh membawa makanan dan minuman ke ruangan TI pada saat jam istirahat.
Pengendalian Batasan	-Tidak ada batasan peng*input*an *login* akses. Aplikasi akan tetap menampilkan pesan yang berisi kesalahan pada saat *login*.
	-Aplikasi tidak dapat memberikan respon dengan menutup secara otomatis jika terjadi kegagalan *login*.
	-Tidak ada kebijakan yang mengatur umur *password*.
	-Tidak ada kebijakan yang mengatur kriteria *password*.
Pengendalian Masukan	-Terdapat *manual book* sistem namun masih versi yang lama.
Pengendalian Proses	-Terdapat pada pengisian diskon barang tidak terpogram langsung pada sistem (*manual*).
	-Penyusunan laporan keuangan masih *manual* menggunakan Ms. Excel.
Pengendalian Keluaran	-Tidak ada penggunaan *password* pada laporan keuangan yang masih *softcopy*.
	-Penyimpanan dokumen di ruangan admin dan diruangan Ka Depo tertata dengan rapi. Tetapi ada penumpukan dokumen dan tidak tertata dengan baik di gudang.

4. Kesimpulan

Berdasarkan hasil penilaian resiko yang telah dilakukan terhadap pengendalian manajemen keamanan, pengendalian batasan, pengendalian masukan, pengendalian proses dan pengendalian keluaran pada sistem ALWIS, maka dapat disimpulkan pada Tabel 10 bahwa pengendalian pada ALWIS memiliki kategori resiko *medium*. Pengendalian yang dilakukan perusahaan sudah cukup baik dalam artian jika sewaktu ada permasalahan pada sistem, perusahaan dapat mengatasinya. Kesimpulan dari audit TI ini: (1) Perusahaan tidak memiliki *alarm* kebakaran otomatis di sekitar ruangan TI, Karyawan diperbolekan membawa makanan dan minuman ke ruang TI pada jam istirahat; (2) tidak ada batasan peng*input*an *login* akses jika terjadi kesalahan pada peng*input*an *password* atau *username*; (3) ALWIS tidak dapat menutup secara otomatis jika terjadi kegagalan saat *login* akses; (4) tidak ada kebijakan yang mengatur kriteria dan jangka umur *password* (*automatically expired password*); (5) *manual book* sistem tidak diperbaharui; (6) pengisian diskon program barang masih *manual*; (7) penyusunan laporan keuangan masih menggunakan Ms. Excel; (8) laporan keuangan yang masih *softcopy* tidak menggunakan proteksi *password*; (9) terdapat penumpukan dokumen yang tidak terpakai di gudang barang.

Tabel 10. Kesimpulan Audit

Jenis Pengendalian	Nilai	Bobot
Pengendalian Manajemen Keamanan	13	M
Pengendalian Batasan	14	M

ISSN (Printed) : 2579-7271
ISSN (Online) : 2579-5406

Pengendalian Masukan	25	M
Pengendalian Proses	15	M
Pengendalian Keluaran	15	M
Nilai Akhir	82 : 5 = 16.4	M

Daftar Pustaka

[1] Gondodiyoto, S. (2007). Audit sistem informasi+ pendekatan cobit. *Edisi Revisi*, *Penerbit: Mitra Wacana Media, Jakarta*.

[2] Mustaqbal, M. S., Firdaus, R. F., dan Rahmadi, H. (2016). Pengujian aplikasi menggunakan black box testing boundary value analysis (studi kasus: Aplikasi prediksi kelulusan smnptn). *Jurnal Ilmiah Teknologi Informasi Terapan, 1*(3).

[3] Stoneburner, G., Goguen, A. Y., dan Feringa, A. (2002). Sp 800-30. Risk management guide for information technology systems.

[4] Weber, R. (1999). Information systems control and audit prentice-hall. *Inc., Upper Saddle River,* NJ.