Jurnal Ilmiah Rekayasa dan Manajemen Sistem Informasi, Vol. 7, No. 1, Februari 2021, Hal. 89-95
e-ISSN 2502-8995 p-ISSN 2460-8181

AUDIT SISTEM PORTAL DENGAN PENDEKATAN BERBASIS RISIKO PADA CV. GIFANKI INDAH MANDIRI PEKANBARU

[1]Megawati, [2]Syaifullah, [3]Heggi Sugiawan

[1,2,3]Program Studi Sistem Informasi Fakultas Sains dan Teknologi UIN Suska Riau
[1,2,3]Jl. HR Soebrantas, KM. 18.5, No. 155, Simpang Baru, Pekanbaru, Indonesia, 28293
Email: [1] megawati@uin-suska.ac.id, [2]syaifullah@uin-suska.ac.id, [3]Heggisugiawan@gmail.com

ABSTRAK

Penggunaan teknologi dan sistem informasi memjadi keharusan dalam menjalankan bisnis. CV INDAH MANDIRI PEKANBARU adalah perusahaan pengurusan PPJK surat menyurat impot eksport barang di Sumatera (Indonesia). Aplikasi yang digunakan perusahaan bernama PORTAL. Aplikasi didapatkan dari pihak bea cukai ketika membuka perusahaan pengurusan PPJK. Terdapat beberapa kendala pada aplikasi PORTAL, yaitu terjadi kesalahan dalam penginputan banyak data, dan ditemukan beberapa data yang tidak valid akibat belum terintegrasinya sistem dengan pihak Bea-cukai. Tujuan dari penelitian ini adalah untuk melakukan audit kelemahan dan mengidentifikasi temuan positif dan negatif serta memberikan saran rekomendasi perbaikan. Metode audit sistem informasi yang digunakan dalam penelitian ini adalah metode *audit through the computer*, dan teknik penentuan level resiko menggunakan *NIST 800-30.* Dari pengujian pengendalian pada PORTAL menggunakan metode audit *through the computer* terdapat 11 (sebelas) temuan negatif, yaitu (1) Karyawan tidak melakukan scan berskala, (2)perusahaan tidak memiliki prosedur *hacking*, (3)tidak ada larangan membawa makanan atau minuman pada ruangan kerja, (4)tidak ada batasan kegagalan dalam menginput *username* dan *pasword*, (5)tidak ada batasan ukuran (panjang maksimal) ketika login, (6)fitur aplikasi masih manual, (7) tidak ada peringatan dari aplikasi apabila pengguna melupakan mengisi salah satu tabel data, (8) tidak ada konfirmasi data ketika menginput data, (9)tidak terdapat pesan *error* jika terdapat kesalahan dalam penginputan, (10)pihak perusahaan harus menunggu konfirmasi dari pihak bea cukai apakah surat kita diterima atau tidak, (11)laporan yang dihasilkan sesring mengalami keterlambatan.

Kata kunci: *PORTAL, throught the computer, audit sistem informasi, NIST 800-30*

Abstract

The use of technology and information systems is imperative in running a business. CV INDAH MANDIRI PEKANBARU is a PPJK management company for the import and export of goods in Sumatra (Indonesia). The application used by the company is called PORTAL. Applications are obtained from customs when opening a PPJK management company. There are several problems with the PORTAL application, namely an error occurred in inputting a lot of data, and some invalid data was found due to the system's not being integrated with Customs. The purpose of this study is to audit weaknesses and identify positive and negative findings and provide recommendations for improvement. The information system audit method used in this study is the through the computer audit method, and the risk level determination technique uses NIST 800-30. From the control test at PORTAL using the audit through the computer method, there were 11 (eleven) negative findings, namely (1) Employees did not perform scaled scans, (2) the company did not have hacking procedures, (3) there was no prohibition on bringing food or drinks into the room work, (4) there is no failure limit in inputting username and password, (5) there is no size limit (maximum length) when logging in, (6) the application features are still manual, (7) there is no warning from the application if the user forgets to fill in one one data table, (8) there is no data confirmation when inputting data, (9) there is no error message if there is an error in the input, (10) the company must wait for confirmation from the customs whether our letter was received or not, (11) reports generated frequently experience delays

Keywords*: PORTAL, throught the computer, audit system informasi, NIST 800-30.*

A. PENDAHULUAN

Perkembangan teknologi informasi saat ini sudah menjadi kebutuhan yang sangat penting bagi hampir semua organisasi perusahaan baik pemerintahan maupun swasta sebagai penunjang dalam meningkatkan efektifitas dan efisiensi proses kinerja untuk mencapai hal tersebut diperlukan suatu

pengelolaan TI yang baik dan benar, sehingga keberadaan TI dirasakan termanfaatkan oleh organisasi [1]. Penerapan teknologi informasi pada suatu perusahaan dipandang sebagai salah satu solusi yang nantinya akan dapat meningkatkan tingkat kompetensi sebuah perusahaan. Pengguna teknologi informasi pada suatu perusahaan tentunya juga akan membawa banyak keuntungan bagi itu sendiri [2].

Cv.Gifanki indah mandiri pekanbaru didirikan pada tahun 2018. Perusahaan ini berfokus pada eksportir, importer, dan PPJK. PPJK mengurus barang impor yang wajib membayar pajak bea masuk sehingga padanya dikenakan jaminan. PPJK telah bertanggung jawab untuk melunasi pajak bea masuk berdasarkan kuasa dari perusahaan atau perorangan selaku importer. Perusahaan ini menggunakan suatu sistem dalam menjalankan bisnis tersebut. Sistem ini dinamakan sistem portal.Tetapi meskipun telah menerapkan teknologi dalam menjalankan bisnis masih terdapat kesalahan pada sistem yaitu ketidaksesuaian data yang dinput dengan hasil data output, yang menyebabkan banyak data yang tidak valid atau tidak lengkap dan sering terjadinya kehilangan data.

Data tidak valid dikarenakan tidak adanya pemberitahuan dari sistem kepada pengguna apabila dalam pengiputan terjadi kesalahan, atau kerusakan pada modul sistem. Sedangkan kehilangan data dikarenakan adanya virus diflasfisk ketika pengguna mengambil ataupun menginput data.Permasalahan ini memperlambat dalam proses kinerja pada cv gifanki indah mandiri. Untuk meningkatkan kepuasan konsumen, juga untuk terus memperbaiki efektifitas dalam mengimplementasikan pengendalian internal. Cv gifanki secara terus menerus memperbaiki dan meningkatkan sistem yang diterapkan agar aksebilitas dapat ditingkatkan, memberikan jaminan keamanan dan keandalan sistem, serta memberikan layanan berbasis TI. Untuk mengetahui kesalahan yang terjadi perlu adanya suatu audit pengendalian control. Jika pengendalian control telah berjalan dengan optimal maka kebutuhan pengoperasian perusahaan dapat terpenuhi.

Audit merupakan suatu proses terpadu mengenai pengumpulan, penilaian dan pengujian atas aktifitas suatu kegiatan. Audit Sistem Informasi merupakan proses terpadu kegiatan yaitu melakukan pengumpulan, penilaian dan pengujian atas aktifitas kegiatan di lingkungan Sistem Informasi [3]. Metode Throught the komputer bertujuan untuk dapat memberikan evaluasi terhadap kinerja sistem, dan dapat memberikan masukan untuk meningkatkan pengelolaan yang lebih baik. Metode ini memberikan keuntungan bagi perusahaan, dimana pengujian sistem aplikasi memiliki peningkatan secara efektif dalam ruang lingkup dan kemampuan pengujian menjadi lebih luas

B. LANDASAN TEORI

B.1 **Audit Sistem Informasi**

Proses pengumpulan dan pengevaluasian bukti untuk menentukan apakah sistem informasi dapat melindungi aset, teknologi informasi yang ada telah memelihara integritas data sehingga keduanya dapat diarahkan kepada pencapaian tujuan bisnis secara efektif dengan menggunakan sumber daya secara efisien (Wardani dan Puspitasari, 2014).

B.2 Audit Trought The Computer

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

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

2)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 (Hendarti, Husni, dan Tandra, 2010).

3)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 (Hendarti dkk., 2010).

4)Pengendalian proses

Pengendalian proses ialah pengendalian intern untuk mendeteksi jangan sampai data menjadi error karna adanya kesalahan proses. Tujuan pengendalian pengolahan adalah untuk mencegah agar tidak terjadi kesalahan-kesalahan selama proses pengolahan data (Megawati, Rozanda, dan Hutapea, n.d.).

5)Pengendalian keluaran

Pengendalian keluaran merupakan pengendalian yang dilakukan untuk menjaga output sistem agar akurat, lengkap dan digunakan sebagaimana mestinya . 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 (Megawati dkk., n.d.).

B.3 NIST 800-30

NIST 800-30 adalah dokumen standar yang dikembangkan onle National insitute of standars and Technology yang mana merupakan kelanjutan dari tanggung jawab hukum dibawah undang-undang computer security act tahun 1987 dan the information technology management reform act tahun 1996. NIST 800-30 terdapat dua tahap penting yaitu likehood dan impact likehood Untuk mendapatkan peringkat kemungkin keseluruha yang menunjukkan kemungkinan bahwa potensi kerentanan dapat dilaksanakan dalam konstruksi lingkungan. Kemungkinan potensi kerentanan dapat dilakukan oleh sumber ancaman tertentu dapat digambarkan sebagai tinggi, sedang, atau rendah. gambar 2.1 di bawah menjelaskan tiga tingkat kemungkinan ini.

Risk Description	Likehood Description
High	Sumber ancaman dianggap sangat mungkin terjadi dan kontrol untuk mencegah vurnerability 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

Gambar 1. *Level Likehood*

Impact menentukan dampak merugikan yang dihasilkan dari pelaksanaan ancaman kerentanan yang berhasil. Beberapa dampak nyata dapat diukur secara kuantitatif dalam pendapatan yang hilang, biaya perbaikan sistem, atau tingkat upaya yang diperlukan untuk memperbaiki masalah yang disebabkan oleh tindakan ancaman yang berhasil. Dampak lainnya (misalnya, hilangnya kepercayaan publik, hilangnya kredibilitas, kerusakan kepentingan organisasi) tidak dapat diukur dalam unit tertentu tetapi dapat dikualifikasikan atau dijelaskan dalam istilah dampak tinggi, sedang, dan rendah dapat dilihat gambar 2.2

Risk Level	Risk Description
High	Jika sebuah temuan dievaluasi sebagai High Risk makan penting untuk mempertimbangkan tindakan perbaikan
Medium	Jika 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

Gambar 2. *Level Impact*

C. METODE PENELITIAN

C.1 Tahap Perencanaan

Tahap perencanaan adalah tahapan yang harus direncanakan saat akan melakukan penelitian, guna untuk menentukan topik yang akan diangkat dalam penelitian. Dimulai dengan penentuan topik, identifikasi masalah, membuat perencanaan penelitian dan studi pustaka. Pada tahap ini dilakukan penetapan permasalahan yang akan diteliti sehingga ditemukan dengan topik audit sistem informasi internal control pada cv.gifanki indah mandiri pekanbaru..

C.2 Sumber Data

Sumber data penelitian yaitu dari responden, yakni orang yang menjawab pertanyaan penelitian, yaitu tertulis dan lisan. Sumber data terbagi menjadi dua yaitu data primer serta data sekunder. Data primer merupakan observasi dan hasil wawancara, sementara data sekunder merupakan hasil lembar kerja audit dan penelitian terdahulu.

C.3 Metode Analisis Data

Data yang dikumpulkan oleh penulis dengan menggunakan metode pengumpulan data. Metode pengumpulan data yang akan digunakan penulis merupakan metode analisis kualitatif. Analisis Kualitatif yaitu analisis yang dilakukan dengan cara mendeskripsikan jawaban narasumber.

C.4 Metode Pengumpulan Data

Pengumpulan data mencangkup pencarian izin, pelaksanaan audit dengan lembar kerja audit, mengembangkan caracara untuk merekam informasi, baik secara digital maupun kertas, menyimpan data, dan mengantisipasi persoalan etika yang mungkin muncul.

D. HASIL DAN PEMBAHASAN

D.1 RACI Chart

RACI Chart merupakan matrik dari seluruh aktivitas dan wewenang yang digunakan untuk membantu organisasi dalam pengambilan keputusan. Berikut i-ni adalah penjelasan tentang RACI Chart (ISACA, 2012): R (Responsible): O- rang yang melakukan tugas atau pekerjaan. A (accountable): Orang pertama yang bertanggung jawab secara menyeluruh pada suatu tugas atau pekerjaan dan memiliki wewenang untuk memtuskan suatu permasalahan dan orang yang berhak menyetujui atau menolak eksekusi dari sebuah aktivitas (penanggung jawab dan pengambil keputusan). C (consulted): orang yang memberikan masukan, pendapat atau kontribusi, memberikan umpan (penasehat). I (Informed): Orang yang perlu mengetahui tindakan dan hasil keputusan yang diambil, orang yang bertanggung jawab atas tugas.(Ahmad bhaihaky,2018) Berdasarkan keterangan dari RACI Chart diatas maka ditetapkan jumlah kusioner yang akan disebarkan berjumlah 3 respon- den. Adapunrincian kusioner adalah Directur,admin IT,dan pajak.Berikut meru- pakan diagram RACI Chart yang dapat dilihat pada Tabel 1

Tabel 1. RACI Chart

No	Tugas dan Peran	Directur	Admin TI	Pajak
1	Mengembangkan,mengelola mengoperasikan,serta memelihara sistem portal,dan database pada cv gifanki pekanbaru	RACI	RCI	RCI
2	Mengelola,mengoperasikan,dan mengevaluasikan kegiatan operasi IT	RACI	RACI	RACI
3	Memutuskan dan menyetujui bertanggung jawab atas kerja seluruh pegawai cv gifanki	RAC	RCI	I
4	Memberikan solusi bisnis pada cv gifanki	RCI	RAI	RI

D.2 Penilaian Resiko

Teknik perhitungan dalam Level penilaian resiko menggunakan fungsi perkalian antara Threat Likelihood dengan Impact. Caranya yaitu:

i. Tentukan kemungkinan terjadinya ancaman (Threat Likelihood) berdasarkan nilai yang ada, apakah High, Medium, atau Low
ii. Tentukan dampak yang mungkin terjadi (Impact) berdasarkan nilai yang ada, apakah High (), Medium, atau Low.
iii. Setelah itu masukan rumus kalikan antara Threat Likelihood dengan Impact.

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

b. Pengujian Tingkat Resiko

No	Temuan Negatif	Likehood (L)	Impact (I)	Nilai (L x I)	Level Beresiko	Keterangan
1.	Karyawan tidak melakukan scan anti virus secara berskala pada laptop	0.5	50	25	M	Pengendalian manajeman keamanan sistem portal
2.	Perusahaan tidak mempunyai prosedur hacking	1.0	100	100	H	
No	Temuan Negatif	Likehood (L)	Impact (I)	Nilai (L x I)	Level Beresiko	Keterangan
3.	Tidak ada peraturan tentang pelarangan membawa makanan dan minuman dekat peralatan komputer	0.1	10	1	L	
HASIL(Jumlah nilai : Jumlah pertanyaan) 126:3=42 (M)						
4.	Tidak ada batasan kegagalan dalam menginput username dan pasword	0.5	50	25	M	Pengendalian Batasan
5.	Tidak ada batasan ukuran (panjang maksimal) ketika login	0.1	10	1	L	
HASIL(Jumlah nilai:Jumlah pertanyaan)26:2=13 (M)						
6.	Fitur aplikasi masih manual, contohnya ketika membuat tanggal laporan pengguna harus mengetik manual	0.5	50	25	M	Pengendalian Masukan

	tidak ada fitur otomatis					
	Tidak ada					
7.	peringatan dari aplikasi apabila pengguna melupakan mengisi salah satu tabel data	0.5	50	25	M	
HASIL(Jumlah nilai:Jumlah pertanyaan)50:2=25 (M)						
No	Temuan Negatif	Likehood (L)	Impact (I)	Nilai (L x I)	Level Beresiko	Keterangan
8.	Tidak ada peringatan dari aplikasi apabila ada data kurang ketika penginputan	0.5	50	25	M	Pengendalian Proses
9.	Tidak ada konfirmasi data ketika proses penginputan data yang diinput langsung terkirim kesistem bea cukai	0.5	50	25	M	
10.	Apabila terjadi kesalahan dalam penginputan tidak bisa diperbaiki dengan cepat karna pengguna aplikasi harus menunggu konfirmasi dari bea cukai,pihak bea cukailah yg memeriksa data apakah data tersebut sudah benar atau belum	0.5	50	25	M	
HASIL(Jumlah nilai:Jumlah pertanyaan)75:3=25 (M)						
11.	Laporan yang dihasilkan sering mengalami keterlambatan	0.5	50	25	M	Pengendalian Keluar
HASIL(Jumlah nilai:Jumlah pertanyaan)25:1=25 (M)						

KESIMPULAN

Setelah dilakukan pengujian pengendalian pada PORTAL menggunakan metode audit through the computer terdapat 11 temuan negatif, yaitu Karyawan tidak melakukan scan secara berskala,perusahaan tidak memiliki prosedur hacking,tidak ada larangan membawa makanan atau minuman saat dekat peralatan komputer,tidak ada batasan kegagalan dalam menginput username dan pasword, tidak ada batasan ukuran (panjang maksimal) ketika login,fitur aplikasi masih manual, tidak ada peringatan dari aplikasi apabila pengguna melupakan mengisi salah satu tabel data, tidak ada konfirmasi data ketika menginput data, tidak terdapat pesan error jika terdapat kesalahan dalam penginputan, pihak perusahaan harus menunggu konfirmasi dari pihak bea cukai apakah surat kita diterima atau tidak, laporan yang dihasilkan sering mengalami keterlambatan. Hasil dari tingkat resiko berdasarkan NIST 800-30 yang dilakukan pada cv gifanki menunjukan tingkat resiko yang berada posisi medium yang disimpulkan bahwa pengendalian pada cv gifanki cukup baik. Berdasarkan temuan negatif yang diperoleh rekomendasi manajamen yang diberikan berupa membuat suatu kebijakan untuk menjaga aset dan mengurangi dampak resiko yang

akan terjadi di kemudian hari. Juga perlu adanya pembaharuan baru mengenai keamanan akses dan panambahan fitur program pada aplikasi portal

REFERENSI

[1] Hakim, A., Saragih, H., dan Suharto, A. (2014). Evaluasi tata kelola teknologi informasi dengan framwork cobit. 5 di kementerian esdm. Jurnal Sistem Informasi, 10(2), 108–117.

[2] Wardani, S., dan Puspitasari, M. (2014). Audit tata kelola teknologi informasi mengunakan framework cobit dengan model maturity level (studi kasus fakultas abc). Jurnal Teknologi, 7(1), 38–46.

[3] Stoneburner, G., Goguen, A., dan Feringa, A. (2002). Risk management guide for information technology systems. Nist special publication, 800(30), 800–30.

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

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

[6] Hendarti, H., Husni, H. S., dan Tandra, T. W. (2010). Evaluasi pengendalian sistem informasi persediaan pada cv. xyz. Dalam Seminar nasional aplikasi teknologi informasi (snati)..

[7] Megawati, S., Rozanda, N. E., dan Hutapea, W. G. (n.d.).(2019).Audit sistem informasi internal control dengan metode audit through the computer.