AUDIT LINGKUNGAN DAN PENGENDALIAN TEKNOLOGI INFORMASI PADA PT. XYZ

Matheus Supriyanto Rumetna
Fakultas Ilmu Komputer, Program Studi Sistem Informasi
Universitas Victory Sorong
Email: matheus.rumetna@gmail.com

ABSTRAK

Perkembangan Teknologi Informasi (TI) saat ini sangat berdampak pada berbagai aspek kehidupan, tanpa kecuali pada proses bisnis yang dilakukan oleh perusahaan. PT. XYZ merupakan salah satu perusahaan yang mengandalkan TI dalam operasional kerja, maka perlu dilakukan proses audit yang dikerjakan oleh auditor. Tujuannya adalah untuk memastikan apakah semua pengendalian (*Environmental Controls, Physical Controls, Logical Controls, IS Controls*) sesuai dengan ketentuan atau prosedur yang ada, baik dalam hal keamanan gedung kantor sampai kepada aplikasi yang digunakan. Metode yang digunakan, antara lain *interview, survey, review* (kebijakan/prosedur), *perform tests of key controls* dan *audit techniques* (*audit software & test data*). Hasil yang diperoleh berupa informasi (temuan dan rekomendasi) yang dapat membantu PT. XYZ dalam kelancaran operasional sehari-hari, sehingga nantinya sistem yang ada menjadi maksimal, lebih efektif dan efisien dalam pengoperasiannya.

Kata kunci: *information system* audit program*; information system audit programme; risk assessment*; pengukuran kerja.

ABSTRACT

The development of Information Technology (IT) is currently very impact on various aspects of life, without exception on the business processes undertaken by the company. PT. XYZ is one of the companies that rely on IT in operational work, it is necessary to do an audit process undertaken by the auditor. The goal is to ascertain whether all controls (Control Controls, Physical Controls, Logical Controls, IS Controls) are in accordance with existing provisions or procedures, both in the case of office building security to the applications used. Methods used include interview, survey, review (policy/procedure), perform tests of key controls and audit techniques (audit software & test data). The results obtained in the form of information (findings and recommendations) that can help PT. XYZ in the smooth operation of everyday, so that later the existing system to be maximal, more effective and efficient in its operation.

Keywords: *information system audit program; information system audit programme; risk assessment work measurement.*

1. PENDAHULUAN

Perkembangan Teknologi Informasi (TI) saat ini sangat berdampak pada berbagai aspek kehidupan, tanpa kecuali pada proses bisnis yang dilakukan oleh perusahaan. Perusahaan atau organisasi cenderung memanfaatkan teknologi untuk meningkatkan efisiensi yang bertujuan mendongkrak pendapatan dan memperbaiki kinerja (1)(2)(3)(4). Pemanfaatan teknologi sudah menjadi hal yang sangat penting dalam proses bisnis. Fenomena tersebut mempengaruhi perilaku dan kebutuhan semua pihak yang berhubungan dengan perusahaan baik secara langsung maupun tidak langsung, termasuk auditor baik auditor internal maupun auditor eksternal (5)(6).

PT. XYZ adalah perusahaan yang bergerak di bidang jasa penyedia informasi lowongan kerja. Perusahaan ini didirikan pada tanggal 27 Maret 2006. Terdapat beberapa departemen dalam perusahaan ini, diantaranya Departemen *Finance*, Departemen *Marketing*, Departemen *Corpcare* dan Departemen *Sales*. Setiap Departemen terintegrasi dengan mengandalkan sistem informasi serta jaringan internet untuk menunjang serta memudahkan dalam melaksanakan pekerjaan, sehingga operasional perusahaan menjadi lebih efektif dan efisien, namun karena terintegrasi maka perlu dilakukan proses audit yang dikerjakan oleh auditor.

Ruang lingkup digunakan untuk mengetahui serta membatasi area kerja auditor dalam melakukan audit. Ruang lingkup disini mencakup lingkungan sekitar bangunan kantor PT. XYZ, setiap ruang kantor PT. XYZ, koneksi jaringan dan keamanannya, serta aplikasi JBOS yang digunakan oleh PT. XYZ.

Tujuan audit adalah untuk memastikan apakah semua pengendalian (*Environmental Controls, Physical Controls, Logical Controls, IS Controls*) sesuai dengan ketentuan atau prosedur yang ada, baik dalam hal keamanan gedung kantor sampai kepada aplikasi yang digunakan. Agar dapat membantu PT. XYZ dalam kelancaran operasional sehari-hari, sehingga nantinya sistem yang ada menjadi maksimal, lebih efektif dan efisien dalam pengoperasiannya (7)(8).

2. METODOLOGI PENELITIAN

Beberapa metode yang auditor gunakan, antara lain *Interview* (pihak terkait), *Survey* (bagian terkait), *Review* (kebijakan/prosedur), *Perform tests of key controls* dan *Audit techniques* (*Audit Software & Test Data*). Berikut penjelasan dari tiap metode yang digunakan (9)(10) :

a. *Interview*
   Merupakan salah satu metode yang digunakan oleh auditor untuk melakukan *interview* (wawancara) secara langsung dengan bagian *sales* dari PT. XYZ, serta mantan *manager sales*.
b. *Survey*
   Merupakan salah satu metode yang digunakan oleh auditor untuk melakukan peninjauan secara langsung dengan bagian *sales* serta dengan cara melihat aplikasi JBOS yang digunakan oleh PT. XYZ.
c. *Review*
   Merupakan salah satu metode yang digunakan oleh auditor untuk mengerahui kebijakan serta prosedur yang ada dengan cara membaca prosedur yang terdapat pada aplikasi JBOS serta dengan bertanya langsung mengenai prosedur yang ada kepada mantan *manager sales*.
d. *Perform tests of key controls*
   Merupakan salah satu metode yang digunakan oleh auditor untuk melakukan pengujian performa untuk pengendalian keamanan dari segi *Environmental Controls, Physical Controls, Logical Controls, IS Controls*. Untuk hasil performanya dapat dilihat pada Tabel 3.
e. *Audit techniques*
   Terdapat beberapa teknik audit yang dapat digunakan dalam melakukan audit, namun disini auditor menggunakan 2 teknik, yaitu *Audit Software* & *Test Data.*
   1) *Audit Software* digunakan untuk membantu dalam melakukan tugas khusus.
   2) *Test Data* digunakan untuk pengujian data dengan menggunakan data *dummy* yang dibuat oleh auditor.

3. HASIL DAN PEMBAHASAN

3.1 Identifying Computer System

Identifikasi sistem komputer dilakukan oleh auditor dengan maksud agar auditor lebih mengetahui secara jelas jumlah komputer, spesifikasi komputer, *database management system* (DBMS) sampai *application description* dari tiap komputer (lihat Tabel 1) bahkan dapat melakukan penilaian resiko (lihat Tabel 2) .

Tabel 1. ***Inventory of computing system***

No	*Computer Software Application*	*DBMS*	*Hardware Spesification*	*Primary Operating System*	*Jumlah (Unit)*	*Department / Process Owner*	*Application description*
FINANCE							
1.	JBOS	MySQL	Notebook : Lenovo Thinkpad X220 Processor : Intel Core i5 2.7GHz RAM : 4GB DDR3 HDD : 320GB Layar : 12.5”	*Windows* 8	1	*Manager Finance*	Digunakan untuk : - *Decision Support System*. - Menggantikan tugas staff ketika staff yang bersangkutan tidak hadir.

No	*Computer Software Application*	*DBMS*	*Hardware Spesification*	*Primary Operating System*	*Jumlah (Unit)*	*Department / Process Owner*	*Application description*
2.	JBOS	MySQL	PC : Intel Core i3-4160 3.0GHz RAM 2GB DDR3 HDD 500GB Monitor : HP 15.6”	*Windows* 7	10	*Staff Finance*	Digunakan untuk : - Pengecekan rekening perusahaan berkaitan dengan pembayaran dari klien. - Penguncian akun klien apabila tidak melakukan pembayaran sesuai dengan ketentuan.
HR							
3.	JBOS	MySQL	Notebook : Lenovo Thinkpad X220 Processor : Intel Core i5 2.7GHz RAM : 4GB DDR3 HDD : 320GB Layar : 12.5”	Windows 8	1	HR (*Manager*)	Digunakan untuk : - *Decision Support System*.
MARKETING							
4.	JBOS	MySQL	Notebook : Lenovo Thinkpad X220 Processor : Intel Core i5 2.7GHz RAM : 4GB DDR3 HDD : 320GB Layar : 12.5”	*Windows* 8	1	*Marketing* (Manager)	Digunakan untuk : - *Decision Support System*. - Menggantikan tugas staff ketika staff yang bersangkutan tidak hadir.
5.	JBOS	MySQL	PC : Intel Core i3-4160 3.0GHz RAM : 2GB DDR3 HDD : 500GB Monitor : HP 15.6”	*Windows* 7	11	*Marketing* (*Staff*)	Digunakan untuk : - Pengurusan yang berkaitan dengan branding. - Pembuatan *email* blast (sebaran/*broadcast*) berkaitan dengan informasi lowongan pekerjaan ke

No	*Computer Software Application*	*DBMS*	*Hardware Spesification*	*Primary Operating System*	*Jumlah (Unit)*	*Department / Process Owner*	*Application description*
							kandidat (pelamar) atau perusahaan (klien) lain.
COPCARE							
6.	JBOS	MySQL	Notebook : Lenovo Thinkpad X220 Processor : Intel Core i5 2.7GHz RAM : 4GB DDR3 HDD : 320GB Layar : 12.5”	*Windows* 8	1	*Corpcare* (*Manager*)	Digunakan untuk : - *Decision Support System*. - Menggantikan tugas staff ketika staff yang bersangkutan tidak hadir.
7.	JBOS	MySQL	Notebook : Lenovo Thinkpad X220 Processor : Intel Core i5 2.7GHz RAM : 4GB DDR3 HDD : 320GB Layar : 12.5”	*Windows* 8	1	*Staff Training Corpcare*	Digunakan untuk : - *Decision Support System*.
8.	JBOS	MySQL	PC : Intel Core i3-4160 3.0GHz RAM : 2GB DDR3 HDD : 500GB Monitor : HP 15.6”	*Windows* 7	20	*Corpcare* (*Staff*)	Digunakan untuk memasang iklan lowongan kerja.
SALES							
9.	JBOS	MySQL	Notebook : Lenovo Thinkpad X220 Processor : Intel Core i5 2.7GHz RAM : 4GB DDR3 HDD : 320GB Layar : 12.5”	*Windows* 8	1	*Head of Sales*	Digunakan untuk : - *Decision Support System*. - Menggantikan tugas staff ketika staff yang bersangkutan tidak hadir.
10.	JBOS	MySQL	Notebook : Lenovo Thinkpad X220 Processor : Intel Core i5 2.7GHz RAM : 4GB DDR3 HDD : 320GB	*Windows* 8	1	*Field Sales* (*Manager*)	Digunakan untuk : - *Decision Support System*.

No	*Computer Software Application*	*DBMS*	*Hardware Spesification*	*Primary Operating System*	*Jumlah (Unit)*	*Department / Process Owner*	*Application description*
			Layar : 12.5”				
11.	JBOS	MySQL	Notebook : Lenovo Thinkpad X220 Processor : Intel Core i5 2.7GHz RAM : 4GB DDR3 HDD : 320GB Layar : 12.5”	*Windows* 8	1	*Telesales* (*Manager*)	Digunakan untuk : - *Decision Support System*.
12.	JBOS	MySQL	Notebook : Lenovo Thinkpad X220 Processor : Intel Core i5 2.7GHz RAM : 4GB DDR3 HDD : 320GB Layar : 12.5”	*Windows* 8	1	*Assisten Manager Branch* (*Sales*)	Digunakan untuk : - *Decision Support System*.
13.	JBOS	MySQL	Notebook : Lenovo Thinkpad X220 Processor : Intel Core i5 2.7GHz RAM : 4GB DDR3 HDD : 320GB Layar : 12.5”	*Windows* 8	1	*Assisten Manager Retention Team* (*Sales*)	Digunakan untuk : - *Decision Support System*.
14.	JBOS	MySQL	Notebook : Lenovo Thinkpad X220 Processor : Intel Core i5 2.7GHz RAM : 4GB DDR3 HDD : 320GB Layar : 12.5”	*Windows* 8	1	*Manager Telemarketing* (*Sales*)	Digunakan untuk : - *Decision Support System*.
15.	JBOS	MySQL	PC : Intel Core i3-4160 3.0GHz RAM : 2GB DDR3 HDD : 500GB Monitor : HP 15.6”	*Windows* 7	65	*Sales* (*Staff*)	Digunakan untuk : - Penjualan. - *Maintanance* klien (*after sales service*).
COUNTRY MANAGER							
16	JBOS	MySQL	Notebook : Lenovo Thinkpad	*Windows* 8	1	*Country Manager*	Digunakan untuk : - *Decision*

No	*Computer Software Application*	*DBMS*	*Hardware Spesification*	*Primary Operating System*	*Jumlah (Unit)*	*Department / Process Owner*	*Application description*
			X220 Processor : Intel Core i5 2.7GHz RAM : 4GB DDR3 HDD : 320GB Layar : 12.5”				- *Support System*.
BUSINESS ANALYST							
17.	JBOS	MySQL	Notebook : Lenovo Thinkpad X220 Processor : Intel Core i5 2.7GHz RAM : 4GB DDR3 HDD : 320GB Layar : 12.5”	*Windows* 8	1	*Business Analyst*	Digunakan untuk : - *Decision Support System*.
QUALITY ASSURANCE							
18.	JBOS	MySQL	Notebook : Lenovo Thinkpad X220 Processor : Intel Core i5 2.7GHz RAM : 4GB DDR3 HDD : 320GB Layar : 12.5”	*Windows* 8	1	*Quality Assurance*	Digunakan untuk : - *Decision Support System*.
OTHERS							
19.			Printer Canon + Fotocopy		3		
20.			Printer Canon + cetak foto		3		
21.			Printer Epson		1		

Setelah mengetahui secara jelas jumlah komputer spesifikasi komputer, DBMS dan *application description* dari tiap komputer, selanjutnya auditor melakukan *risk assessment* agar dapat mengetahui resiko dan dapat memberikan cara mengatasi resiko tersebut. Hal ini dapat di lihat pada Tabel 2.

Tabel 2. ***Risk assessment***

No	*Risk description*	*Probability of occurrence*	*Impact of occurrence*	*Overall risk ranking*	*Control descriptions*
1.	Kerusakan, perubahan, penyisipan, penipuan yang dilakukan oleh pengguna yang tidak sah baik *internal* maupun *external*	2	4	8	Menggunakan *login* akun dengan id dan *password*. Memasang keamanan pada jaringan *server* untuk menanggulangi masalah *hacker*.
2.	Hilang dan atau rusaknya data karena bencana (misalnya: virus, kebakaran, banjir, gempa	3	4	12	Data telah tersimpan pada *server* pusat dan *server* cadangan. Melakukan *backup* data

No	*Risk description*	*Probability of occurrence*	*Impact of occurrence*	*Overall risk ranking*	*Control descriptions*
	bumi, gunung berapi, terorisme, dll)				secara berkala. Memasang anti virus yang handal.
3.	Data tidak dapat diakses karena listrik padam, koneksi internet terputus, ataupun *server down*	4	5	20	Menggunakan UPS pada setiap PC dan juga menyediakan generator sebagai pembangkit tenaga listrik cadangan. Ketika *server down* maka dilakukan *backup* data ke *server* lain.
4.	Pencurian perangkat keras komputer, peripheral, laptop, dll	1	3	3	Menggunakan CCTV pada setiap ruangan. Menggunakan id untuk masuk ke ruangan.
5.	*Human error*	2	2	4	Memberikan pengarahan atau prosedur untuk penggunaan sistem kepada setiap user yang terlibat dalam sistem.
6.	Kegagalan untuk mematuhi hukum dan peraturan yang berkaitan dengan privasi	1	2	2	Menghimbau kepada *user* agar mematuhi aturan yang berlaku.
7.	Pembajakan perangkat lunak atau pelanggaran hak cipta	2	4	8	Memberikan hak cipta pada sistem.
8.	Biaya pemeliharaan yang berlebihan dan biaya *upgrade*	1	2	2	Melakukan pemeliharaan dan *upgrade* sesuai dengan kebutuhan sistem yang menjadi prioritas.

Bobot penilaian*:*
1 : Tidak beresiko
2 : Sedikit beresiko
3 : cukup beresiko
4 : beresiko
5 : sangat beresiko

3.2 Information System Audit Program

Program audit sistem informasi dimaksudkan untuk memastikan apakah semua pengendalian (*Environmental Controls, Physical Controls, Logical Controls, IS Controls*) sesuai dengan ketentuan atau prosedur yang ada, baik dalam hal keamanan gedung kantor sampai kepada aplikasi yang digunakan. Secara rinci dapat dilihat pada Tabel 3.

Tabel 3. ***Information system audit programme***

Section	*Procedures*	*Objectives*	*Auditor/ Date*	*Result of tests*
A	***Environmental Controls***			
	1. Memastikan apakah atasan memberikan pengarahan atau prosedur untuk penggunaan sistem kepada setiap *user* yang terlibat dalam sistem. Melakukan evaluasi, apakah *user* telah mengikuti arahan atau prosedur yang berlaku dalam penggunaan sistem.	Agar setiap *user* mengerathui dan mengerti prosedur yang ada dalam sistem.	Matheus , 26/10/16	Sudah sesuai

Section	*Procedures*	*Objectives*	*Auditor/ Date*	*Result of tests*
	2. Meninjau apakah sistem telah dipasang hak cipta.	Agar sistem tidak dianggap sebagi sistem yang ilegal.	Matheus ,21/10/16	Sudah sesuai
	3. Melakukan peninjauan setiap dokumen pelaporan *error* dan memastikan bahwa setiap pelaporan mendapatkan penanganan yang baik.	Agar sistem berjalan dengan baik dan dokumen tersebut digunakan sebagai acuan untuk memperbaiki sistem.	Matheus , 26/10/16	Sudah sesuai
	4. Mendokumentasikan tindakan apa yang telah diambil untuk mengendalikan lingkungan akses pada area-area seperti pusat data dan setiap ruangan.	Agar semua area-area tercover dan terbatas hak aksesnya, sehingga apabila terjadi *trouble* mudah untuk pengendaliannya.	Matheus , 26/10/16	Sudah sesuai
	5. Memastikan bahwa divisi IT adalah kelompok pendukung dalam organisasi. Menentukan apakah ada komite pengawas efektif IT atau komite yang setara dalam organisasi.	Agar dapat mengawasi dan melakukan *maintenance* sistem serta menjadi bagian pendukung dari sebuah organisasi yang sudah komputerisasi.	Matheus , 26/10/16	Sudah sesuai
B	***Physical Controls***			
	1. Menentukan apakah pengendalian lingkungan komputer berikut telah terpasang: a. Peralatan pemadaman api (misalnya, sistem *sprinkler* dan alat pemadam lainnya) b. *Uninterruptible power supply* (UPS) c. *Emergency Power System* (EPS) (misalnya, generator) d. Pengontrol suhu dan kelembaban pengendali (memastikan cadangan AC tersedia)	Agar semua aset baik fisik maupun non fisik terlindungi dengan baik, dan apabila terjadi masalah sudah ada sistem untuk pengendaliannya.	Matheus , 26/10/16	Untuk poin a, c dan d sudah sesuai. Tetapi untuk poin b belum sesuai
	2. Memastikan bahwa seluruh akses ke setiap ruang departemen terbatas pada masing-masing managemen dan staff agar semua hak ases ke sistem berjalan dengan semestinya.	Agar hak akses yang telah ditentukan berjalan dengan baik serta apabila terjadi *trouble* lebih cepat dalam mencari letak permasalahan tersebut.	Matheus , 26/10/16	Sudah sesuai
	3. Meninjau apakah pemeliharaan rutin dilakukan pada peralatan sistem untuk memastikan kinerja peralatan beroperasi sesuai harapan.	Agar sistem dan juga seluruh peralatan yang ada bekerja dengan baik, serta terhindar dari kerusakan besar yang mengganggu kelancaran operasional organisasi.	Matheus , 26/10/16	Sudah sesuai
	4. Meninjau apakah gedung dan fasilitas sesungguhnya aman dari bahaya bencana dan mendapatkan dokumen tentang pengantisipasian apabila terjadi bencana.	Agar gedung serta fasilitas yang ada terhindar dari bencana serta semua *user* yang ada dapat mengetahui tindakan yang dilakukan apabila terjadi bencana.	Matheus , 26/10/16	Sudah sesuai
	5. Mengidentifikasikan pengendalian *hardware* yang dibangun ke dalam peralatan komputer oleh produsen, mengecek peralatan *hardware* apakah sudah sesuai kebutuhan	Agar peralatan komputer yang digunakan benar-benar sesuai kebutuhan dan juga spesifikasi yang dituntut dalam menunjang	Matheus , 26/10/16	Sudah sesuai

Section	*Procedures*	*Objectives*	*Auditor/ Date*	*Result of tests*
	sistem atau belum.	sistem itu benar-benar tidak dimanipulasi oleh produsen.		
C	***Logical Controls***			
	1. Mengidentifikasi seluruh aplikasi yang menyediakan mekanisme keamanan. Serta memastikan apakah kemampuan berikut telah dilaksanakan: a. *User* id yang unik ditetapkan kepada semua pengguna. b. Terminal secara otomatis akan *log off* setelah 30 menit tidak aktif. c. Pengguna diharuskan untuk mengubah *password* setidaknya setiap 90 hari. d. *Password* lama tidak dapat digunakan kembali. e. Sandi yang benar akan disembunyikan pada sistem.	Tujuan dari poin : a. Agar *user* id tidak sama antar *user*. b. Agar *user* lain tidak dapat mengakses sistem menggunakan *user* id yang bukan miliknya. c. Agar terhindar dari pembobolan *password*. d. Agar terhindar dari pembobolan *password* karena sudah pernah terekam dalam sistem. e. Agar terhindar dari *user* nakal yang ingin melihat sandi *user* lainnya.	Matheus ,21/10/16	Sudah sesuai
	2. Memastikan otorisasi yang tepat diperoleh sebelum memberikan akses pengguna ke sumber daya sistem. Mengevaluasi prosedur yang ditetapkan untuk menghapus *user* id atau *password* dari sistem ketika seorang karyawan pergi.	Agar membatasi hak akses dan pemberian hak aksespun dilakukan oleh otoritas yang tepat. Semua karyawan yang sudah keluar tidak dapat mengakses sistem.	Matheus , 26/10/16	Sudah sesuai
	3. Mengecek apakah ada proses perubahan program aplikasi. Meninjau prosedur apabila terjadi perubahan untuk memastikan fungsi-fungsi penting berikut dilakukan: a. Tidak ada perubahan harus dilakukan untuk program dan file hingga otorisasi diberikan secara tertulis. b. Hanya programmer komputer yang dapat melakukan perubahan. c. Mendokumentasikan permintaan perubahan program. d. Persetujuan pengguna atas permintaan perubahan.	Tujuan poin : a. Agar semua proses perubahan terdokumentasi dan pihak otorisasi mengetahui. b. Agar perubahan sistem tertangani dengan baik dan dilakukan oleh orang yang tepat. c. Agar semua perubahan terdokumentasi dan juga lebih gampang bagi divisi IT untuk melakukan perubahan. d. Agar semua perubahan yang terjadi diketahui oleh pengguna.	Matheus , 26/10/16	Sudah sesuai
	4. Memastikan bahwa semua *user* telah memperoleh pemahaman tentang proses pengembangan sistem dan perubahan program.	Agar setiap *user* mengetahui setiap perubahan sistem dan mudah dalam menggunakan sistem.	Matheus , 26/10/16	Sudah sesuai
	5. Memastikan bahwa jaringan yang digunakan telah terpasang sistem keamanan (ter-enkripsi) yang baik agar dapat melindungi data (dari pihak yang tidak bertanggung	Agar jaringan yang digunakan tidak mudah diretas/dibobol, sehingga data menjadi aman.	Matheus , 21/10/16	Sudah sesuai

Section	*Procedures*	*Objectives*	*Auditor/ Date*	*Result of tests*
	jawab) saat melakukan transaksi.			
D	***IS Controls***			
	1. Meninjau dan mengevaluasi apakah operasional sistem informasi telah berjalan dengan baik dan sesuai dengan standar yang ada.	Agar proses operasional sistem berjalan dengan baik.	Matheus, 26/10/16	Sudah sesuai
	2. Memastikan bahwa jurnal transaksi *online* didukung untuk memberikan pemulihan atas transaksi kalau memperbarui *database*, sesuai dengan prosedur yang ada.	Agar terhindar dari *duplicate* data saat terjadi permbaharuan *database*.	Matheus, 26/10/16	Sudah sesuai
	3. Melakukan pengecekan terhadap dokumen prosedur untuk memastikan bahwa salinan *backup* sistem, program dan file (data) akan dipindah ke lokasi penyimpanan yang aman secara terjadwal. Mempertimbangkan apakah inventarisasi salinan *backup* diambil secara berkala.	Agar *backup* sistem sesuai dengan prosedur dan data dalam sistem tersimpan ditempat yang aman.	Matheus, 26/10/16	Sudah sesuai
	4. Menentukan apakah divisi IT telah mengembangkan rencana untuk pemulihan sumber daya teknologi informasi. Menentukan apakah rencana tersebut mencakup pemulihan teknologi informasi di sebuah *hot-site*. Jika demikian, diperoleh kontrak antara klien dan penyedia *hot-site*.	Agar penanganan pemulihan sistem terjadi secara cepat dan juga kontak yang ada digunakan sebagai acuan dalam batasan penggunaan layangan *hot-side*.	Matheus, 26/10/16	Sudah sesuai
	5. Melakukan peninjauan dokumentasi penanganan terhadap kesalahan *software* yang mungkin terjadi dalam sistem operasi.	Agar setiap kesalaha terdokumentasi menjadi acuan apabila terjadi kesalahan yang sama sudah ada cara penanganannya.	Matheus, 26/10/16	Sudah sesuai
	6. Memeriksa dokumen terkait masalah penggunaan *bandwidth* serta penanganannya, apabila sewaktu-waktu jaringan mengalami masalah dalam pengaksesannya.	Agar *bandwidth* penggunaan menjadi maksimal.	Matheus, 26/10/16	Sudah sesuai
	7. Memastikan bahwa sistem telah terpasang *dashboard* yang dapat memantau kinerja sistem dalam hal: a. Monitoring CPU b. Monitoring RAM c. Monitoring data *storage* d. Monitoring *bandwidth* e. Monitoring klien f. Monitoring kandidat g. Monitoring pemasangan iklan h. Monitoring transaksi	Agar memudahkan operasional organisasi, mudah dalam pengambilan keputusan karena dengan menggunakan dashboard membuat pengontrolan menjadi lebih mudah.	Matheus, 26/10/16	Untuk poin a, b, c dan d sudah sesuai. Tetapi untuk poin e, f, g dan h belum sesuai

3.3 Access Control Matrix

Matriks akses kontrol digunakan oleh auditor sebagai acuan untuk mengetaui *level user* dan hak akses tiap *user* pada aplikasi JOBS. Lebih rinci matriks ini dapat dilihat pada Tabel 4.

Tabel 4. ***Access control matrix***

Menu Aplikasi (Fungsi Menu)	***Level User***							
	Sales		***Finance***		***Marketing***		***Corpcare***	
	Staff	***Manager***	***Staff***	***Manager***	***Staff***	***Manager***	***Staff***	***Manager***
Menu *Home*	R	R	R	R	R	R	R	R
Menu *Order* (untuk aktivasi paket apa yang diambil oleh *client*/*company*)	CRUD	CRUD						
Menu Company 360 (*company* detail nama alamat no.telp)	CRUD	CRUD	CRUD	CRUD			CRUD	CRUD
Menu *History* Pembelian	R	R						
Menu *History* Pembayaran	R	R						
Menu *Link* ke *Siva Company*	R	R						
Menu *Action Remarks* (untuk memberikan informasi terbaru dari *company*)	CRUD	CRUD						
Menu *Report*	R	R						
Menu *Transaction*			CRU	CRU				
Menu *Payment*			CRU	CRU				
Menu *Tax*			CRU	CRU				
Menu *Mass Email* (untuk *email blast*)					CRUD	CRUD		
Menu Statistik					CRUD	CRUD		
Menu *Setting* (untuk *setting* waktu)							CRUD	CRUD

Catatan*:*
C : create
R : read
U : update
D : delete

3.4 Computer Assisted Audit Techniques (CAATs)

Audit *Software* digunakan oleh auditor untuk membantu dalam melakukan tugas khusus. Disini auditor memberikan contoh sebagai berikut :

Auditor menggunakan *Microsoft Office Excel* untuk mencari *fraud* "dugaan penggelapan uang penjualan *package* oleh *sales* dengan motif menghubungi klien (*company*) melalui *email* pribadi dan meminta untuk membayar tagihan ke rekening pribadi *sales* berdasarkan *invoice*."

Files dan *Fields* yang digunakan untuk pengujian dapat dilihat pada Tabel 5.

Tabel 5. *Files* & *fields tested*

Files	*Fields*	*Fields Tested*
Transaksi	1) No. Invoice	1) No. Invoice
	2) Company Name	2) Company Name
	3) Package	3) Package
	4) Nama Sales	4) Nama Sales
	5) Activation Date	5) Total
	6) Amount	
	7) Pajak (10%)	
	8) Total	
Company	1) Kode Company	1) Company Name
	2) Company Name	2) No. Telepon
	3) Alamat	3) Email
	4) Kota	
	5) No. Telepon	
	6) Email	
	7) Website	
Package	1) Kode Package	1) Package
	2) Package	
Sales	1) Kode Sales	1) Nama Sales
	2) Nama Sales	2) No.Telpon
	3) Alamat	*3)* Email
	4) No.Telp	
	5) Email	

Fungsi yang digunakan dalam pengujian adalah sebagai berikut :

a. *SORT* digunakan untuk mengurutkan *Company Name* secara *Ascending*.
b. *FIND* digunakan untuk mencari *Company Name* yang belum melakukan pembayaran tagihan berdasarkan *invoice* yang ada.
c. *FIND* juga digunakan untuk mencari nama *Sales* yang menangani transaksi terhadap klien yang belum melakukan pembayaran tagihan.

Berdasarkan uraian dugaan di atas, maka dilakukan pencarian *fraud* dengan cara berikut :

a. Pihak *accounting* mengecek *invoice* yang belum dibayarkan (*open invoice*) oleh pihak klien (*company*) melalui *file* transaksi. (IDJKINV/16100005)
b. Setelah menemukan *open invoice* tersebut, *Accounting* menghubungi *Sales* yang menangani transaksi pada saat itu. (Skil; 083949384)
c. Jika *Sales* tidak dapat dihubungi, maka *Accounting* akan mengecek siapa klien (*Company*) yang terdaftar dalam *invoice* tersebut melalui *file* transaksi. Selanjutnya, *Accounting* akan mencari No.Telp klien yang ditemukan melalui *file Company*. (PT. OPQ; 0848633)
d. *Accounting* melakukan konfirmasi pembayaran kepada PT. OPQ agar segera melunasi tagihan. Namun, pihak PT. OPQ mengatakan bahwa mereka telah melakukan pembayaran terhadap tagihan tersebut dengan transfer ke rekening *Sales* yang bersangkutan yaitu Skil.
e. *Accounting* meminta bukti transaksi kepada pihak PT. OPQ dan mereka mengirimkan bukti transaksi via bank dan juga via *email*.
f. *Accounting* menemukan nama *Sales* (Skil) pada bukti *transfer* uang ke rekening Skil yang seharusnya dikirim kepada pihak PT. XYZ.
g. Hasilnya, *Accounting* melaporkan kejadian ini ke *Manager Sales* dan atas tindakannya, maka Skil diberikan sanksi karena terbukti melakukan penggelapan uang penjualan *package* terhadap PT. OPQ.

3.5 Working Paper of Test Data

Test Data digunakan untuk pengujian data dengan menggunakan data *dummy* yang dibuat oleh auditor. Berikut contoh *test data* yang ditampilkan dalam Tabel 6.

Tabel 6. ***Test data***

Field Name	*Dummy Data*	*Tested Control (Option)*	*Estimated Result*	*Occurred Result*	*Conclusion/Finding*
No. *Invoice*	IN20161019001	✓ *Validity check* ✓ *Sequence check*	Sistem menerima	Sistem menerima	
	20161019001122 1	✓ *Size check* ✓ *Check digit*	Sistem menolak (maksimal 13 digit)	Sistem menolak	No. *Invoice* yang dimasukkan tidak sesuai dengan jumlah digit yang dibatasi/ditentukan dalam sistem
Company Name	Dibiarkan kosong	✓ *Completeness check* ✓ *Blank check*	Sistem menolak (*company name* tidak boleh kosong)	Sistem menolak	*Company Name* tidak boleh dibiarkan kosong karena menyangkut dengan pengolahan data company
	PT. Cendrawasih	✓ *Validity check*	Sistem menerima	Sistem menerima	
	PT. X	✓ *Reasonableness check*	Sistem menolak (*company name* tidak terdaftar)	Sistem menolak	*Company Name* tidak sesuai dengan yang terekam dalam sistem
	PT. 56633	✓ *Parity check*	Sistem menolak (*company name* tidak terdaftar)	Sistem menolak	*Company Name* tidak sesuai dengan yang terekam dalam sistem
Package	1 year 30 jobs	✓ *Validity check* ✓ *Parity check*	Sistem menerima	Sistem menerima	
	1 month 50 jobs	✓ *Reasonableness check* ✓ *Existence check*	Sistem menolak (*package* tidak ada)	Sistem menolak	*Package* tidak sesuai dengan yang ada pada sistem
Activation Date	13/10/16	✓ *Date check* ✓ *Validity check* ✓ *Logical relationship*	Sistem menerima	Sistem menerima	
	32 okt 2016	✓ *Reasonableness check*	Sistem menolak (tanggal 32)	Sistem menolak	Tanggal yang dimasukkan ke sistem harus sesuai dengan rentan waktu yang sebenarnya (1-31)
	13/10/16 - 13/10/17	✓ *Range check* ✓ *Limit check*	Sistem menolak (tidak sesuai format)	Sistem menolak	Tanggal yang dimasukkan tidak sesuai dengan format yang ada dalam sistem

Field Name	*Dummy Data*	*Tested Control (Option)*	*Estimated Result*	*Occurred Result*	*Conclusion/Finding*
Amount	Rp. 70.000,-	✓ *Currency check* ✓ *Numeric check*	Sistem menerima	Sistem menerima	
	Tujuh Puluh Ribu Rupiah	✓ *Validity check*	Sistem menolak (bukan numerik)	Sistem menolak	Harus sesuai dengan format yang ditentukan sistem

3.6 Temuan dan Rekomendasi

Selama melakukan audit, auditor mendapati beberapa temuan yang harus ditindak lanjuti. Untuk itu auditor memberikan rekomendasi mengenai temuan tersebut agar segera diperbaiki. Temuan serta rekomendasi tersebut dapat dilihat pada Tabel 7.

Tabel 7. Temuan dan rekomendasi

Temuan	*Rekomendasi*
a. Setiap pelaporan *error* langsung diinformasikan kepada pihak IT dan penanganannya langsung secara regional (Malaysia) serta dibuatkan dokumentasinya. b. Terdapat seorang tenaga IT untuk menanggunlangi *trouble*, namun secara garis besar setiap *trouble* secara keseluruhan diawasi langsung oleh divisi IT yang terdapat pada regional (Malaysia).	Sebaiknya pada tiap departemen ditambah tenaga IT jangan hanya satu orang, karena apabila sewaktu-waktu terjadi *trouble* pada jaringan tiap departemen maka tenaga IT tersebut tidak terlalu repot dalam melakukan perbaikan serta semakin cepat dalam penanggulangannya. Mengingat aplikasi JBOS ini menggunakan jaringan yang rentang juga terdahap *trouble.*
Uninterruptible power supply (UPS) belum terpasang pada setiap PC.	Mengingat bahwa semua operasional perusahaan saat ini sudah *computerized*, maka sangat penting untuk memiliki UPS yang terpasang pada setiap PC karena apabila sewaktu-waktu terjadi pemadaman listrik UPS tersebut berfungsi untuk membantu PC tetap menyala dan dapat menyimpan semua pekerjaan yang sedang dikerjakan sambil menunggu aktifnya pembangkit listrik *emergency*.
Sistem *maintenance* terjadi 2 kali dalam setahun, *maintenance* dilakukan agar semua hal yang menunjang sistem dapat berjalan dengan baik dan semua proses didokumentasikan.	Sebaiknya sistem *maintenance* dilakukan dalam 3 bulan mengingat banyaknya aktivitas yang terjadi di dalam sistem tersebut dan juga *maintenance* yang dilakukan lebih baik terurut sesuai dengan kebutuhan.
Setiap hak akses diberikan berdasarkan otorisasi langsung dari atasan melalui sistem. Untuk proses penghapusan *user* id serta *email* ketika karyawan keluar (*resign*) akan dievaluasi dan secara langsung terjadi pada sistem.	Dalam hal pemberian hak akses, penghapusan *user* id dan *email* sebaiknya dilakukan evaluasi dan pelaksanaannya dalam waktu kurang dari 24 jam, agar semua *user* yang akan terekam di sistem dan yang akan dihapus oleh sistem dapat di akses dengan cepat.
Proses pengecekan apabila terjadi perubahan aplikasi : a. Semua perubahan harus mendapatkan otorisasi langsung dari atasan, semua *file* serta program di awasi oleh atasan. b. Divisi IT yang berada di Malaysia (regional) yang mendapatkan akses penuh untuk melakukan perubahan pada sistem. c. Setiap perubahan yang terjadi dicatat dan dibuatkan dokumentasi sebagai pelaporan	Dalam hal perubahan sistem atau aplikasi sebaiknya dilakukan dengan cepat dan disosialisasikan dengan cepat, mengingat banyaknya *user* yang terhubung dalam aplikasi ini dan juga divisi IT harus bergerak cepat dalam hal melakukan perubahan sistem serta *maintenance*. Paling tidak apabila terjadi perubahan pada sistem, sistem sudah dipasang *notification* agar tiap *user* yang terhubung dengan sistem dapat mengetahui hal tersebut.

Temuan	*Rekomendasi*
kepada atasan juga sebagai acuan untuk proses *maintenance.* d. Setiap permintaan perubahan akan dikaji terlebih dahulu dan diberikan informasi kepada pengguna	
Sistem merekam semua transaksi yang terjadi, apabila terjadi pembaharuan pada *database*, maka pembaharuan akan mengikuti transaksi yang terjadi sesuai dengan prosedur pembaharuan transaksi yang berlaku.	Khusus mengenai *database* yang berkaitan dengan transaksi harus memiliki informasi penanganan yang berkelanjutan mengingat dalam sebuah sistem, jurnal transaksi merupakan hal yang paling sensitif karena berkaitan dengan keuangan.
Semua sistem telah terkontrol oleh divisi IT regional (Malaysia) dengan baik. Proses pemulihan, penanganan *trouble*, *maintenance* serta *backup* sumber daya teknologi telah direncanakan dan dilakukan dengan baik. Penanganan penyedia layanan internet pun dilakukan dengan baik. Mencakup *server side* serta *client side.*	Khusus untuk *backup client side*, harus dilakukan pendekatan yang lebih mendalam. Mengingat terkadang *client* tidak terlalu mengerti tentang sistem dan hanya mau agar sistem beroperasi dengan cepat tanpa mengetahui kendala yang terjadi dibelakang sistem.
Untuk penanganan *bandwidth* serta penggunaannya secara langsung direkam dan didokumentasi langsung pada pusat (*server*) dan diteruskan ke regional (Malaysia).	Masalah *bandwidth* berkaitan dengan pihak ketiga (*outsource*) sebagai jasa penyedia layanan internet (ISP). Sebaiknya menggunakan 2 ISP atau lebih dalam pengoperasionalan sistem, karena apabila sewaktu-waktu terjadi *bandwidth down* dan membuat pekerjaan menjadi terhambat masih ada layanan internet lain yang siap mem*backup*.
JBOS memantau kinerja : a. Monitoring CPU telah terpasang pada setiap PC b. Monitoring RAM telah terpasang pada setiap PC c. Monitoring data *storage* telah terpasang pada setiap PC d. Monitoring *bandwidth* hanya terpasang pada *server* e. Monitoring klien belum terpasang pada sistem f. Monitoring kandidat belum terpasang pada sistem g. Monitoring pemasangan belum terpasang pada sistem iklan h. Monitoring transaksi belum terpasang pada sistem	Untuk masalah *dashboard* sebaiknya dipasang atau dibuat oleh divisi IT agar setiap departemen lebih mudah dalam mengontrol setiap pekerjaan. Karena dengan adanya *dashboard* setiap *user* dapat mengontrol pekerjaannya darimana saja dan kapan saja melalui *smartphone*.

4. KESIMPULAN

Pengendalian (*Environmental Controls* dan *Logical Controls)* pada PT. XYZ telah sesuai dengan ketentuan atau prosedur yang ada, baik dalam hal keamanan gedung kantor sampai kepada aplikasi yang digunakan. Namun yang perlu diperhatikan adalah pada *physical controls* dan *IS controls* karena terdapat beberapa temuan yang belum sesuai dengan ketentuan atau prosedur.

Berdasarkan temuan yang paling besar resikonya adalah *Uninterruptible power supply* (UPS) yang belum terpasang pada setiap PC, karena apabila sewaktu-waktu terjadi pemadaman listrik UPS tersebut berfungsi untuk membantu PC tetap menyala dan dapat menyimpan semua pekerjaan yang sedang dikerjakan sambil menunggu aktifnya pembangkit listrik *emergency*.

Masalah *bandwidth* berkaitan dengan pihak ketiga (*outsource*) sebagai jasa penyedia layanan internet (ISP). Sebaiknya menggunakan 2 ISP atau lebih dalam pengoperasionalan sistem, karena apabila

sewaktu-waktu terjadi *down bandwidth* dan membuat pekerjaan menjadi terhambat masih ada layanan internet lain yang siap mem*backup*.

Monitoring klien, monitoring kandidat, monitoring pemasangan iklan, monitoring transaksi adalah hal penting, untuk itu sebaiknya dipasang atau dibuat *dashboard* oleh divisi IT agar setiap departemen lebih mudah dalam mengontrol setiap pekerjaan. Karena dengan adanya *dashboard* setiap *user* dapat mengontrol pekerjaannya darimana saja dan kapan saja melalui *smartphone*.

DAFTAR PUSTAKA

[1] Arza FI. Proses Audit pada Era Teknologi Informasi serta Implikasi terhadap Pembelajaran Auditing di Perguruan Tinggi. Akunt Manaj. 2007;2(2):23–31.
[2] Chen Y, Zhang H, Tang Z. The Interaction of The Sound and Color Stimuli in The Auditory and Visual Cortexes. Int J Comput Sci Netw Secur [Internet]. 2011;11(7):81–3. Available from: http://paper.ijcsns.org/07_book/201107/20110713.pdf
[3] Chimmanee S, Veeraprasit T, Srisa-an C. A Performance Evaluation of Vulnerability Detection : NetClarity Audito , Nessus , and Retina. Int J Comput Sci Netw Secur. 2014;14(3):34–41.
[4] Maria E, Haryani E. Audit Model Development of Academic Information System : Case Study on Academic Information System of Satya Wacana. J Art, Sci Commer. 2011;II(April 2011):12–24.
[5] Nugroho M. Audit Lingkungan TI: Perspektif Dan Dampak Pada Proses Auditing Secara Komprehensif. Pendidik Akunt Indones. 2011;IX(1):24–42.
[6] Omosh HAM, Bani-Ahmad A, Kh. E-DAE-R. The Effect of Applying the Information Technology Audit Standard# 21 on the Risk Related To ERP System in the Jordanian Companies. Glob J Manag Bus Res [Internet]. 2014;14(1):1–9. Available from: http://www.journalofbusiness.org/index.php/GJMBR/article/view/1212
[7] Raggad BG, Collar EJ. The Simple Information Security Audit Process : SISAP. Int J Comput Sci Netw Secur Comput Sci Sci. 2006;6(6):189–98.
[8] Setiawan H, Mustofa K. Metode Audit Tata Kelola Teknologi Informasi di Instansi Pemerintah Indonesia. IPTEK-KOM. 2013;15(1):1–15.
[9] Utomo AP. Dampak Pemanfaatan Teknologi Informasi terhadap Proses Auditing dan Pengendalian Internal. J Teknol Inf Din. 2006;XI(2):66–74.
[10] Yulianti DT, Patria MC. Audit Sistem Informasi Sumber Daya Manusia Pada PT X Menggunakan Cobit Framework 4.1. Sist Inf. 2011;6(1):15–33.