PERAN TEKNOLOGI INFORMASI DALAM MENGANTISIPASI KECURANGAN AKUNTANSI
(Studi Kasus pada PT XYZ Tbk)

Amararenggana Dharmesti
Ali Djamhuri
Fakultas Ekonomi dan Bisnis
Universitas Brawijaya
Malang
Email: renggana.amara@gmail.com

ABSTRACT

The aim of this research is to find out the role of information technology of PT XYZ Tbk. in anticipating occurrences of accounting fraud by focusing on the adequacy of the application of IT Control with the COSO Internal Control Framework. The data used to support this research are primary data obtained from interviews and observations. This research is a descriptive qualitative research with the case study approach. The results of the study showed that information technology implemented by PT XYZ Tbk. is capable of anticipating occurrences of accounting fraud through both general control and application control. This also supports the reduction of accounting fraud experienced by PT XYZ. However, the information system is still unintegrated because the data backup procedure is manually conducted. This deficiency results in several risks and threats for the company in maintaining the principle of data security in risk management.

Keywords: Information Technology, Fraud in Accounting, Internal Control Systems.

ABSTRAK

Penelitian ini bertujuan untuk mengetahui peran teknologi informasi PT XYZ Tbk dalam mengantisipasi kecurangan akuntansi. Penelitian ini berfokus pada kecukupan penerapan teknologi informasi PT XYZ dengan *IT Control* yang telah dipopulerkan oleh COSO. Data yang digunakan untuk mendukung penelitian ini adalah data primer hasil wawancara dan observasi. Penelitian ini mengikuti desain penelitian studi kasus dengan pendekatan kualitatif deskriptif. Hasil penelitian menunjukkan bahwa teknologi informasi yang diimplementasikan oleh PT XYZ dapat mengantisipasi kecurangan akuntansi baik yang dilakukan melalui pengendalian umum (*general control*) maupun pengendalian aplikasi (*application control*). Hal tersebut telah mengurangi terjadinya *fraud* yang telah dialami oleh PT XYZ. Namun sebagai kelemahan yang masih ada, PT XYZ Tbk masih menggunakan sistem yang tidak terintegrasi dan penyimpanan data secara manual. Kekurangan ini menimbulkan beberapa risiko dan ancaman bagi perusahaan dalam mempertahankan prinsip keamanan data dalam manajemen risiko.

Kata Kunci: Teknologi Informasi, Kecurangan Akuntansi, Sistem Pengendalian Internal.

PENDAHULUAN

Dewasa ini di era yang semakin canggih dan serba otomatis, informasi merupakan hal yang tidak dapat terpisahkan dengan kehidupan organisasi dan bisnis. Informasi yang cepat, tepat waktu, akurat, dan relevan merupakan faktor penting dalam pengambilan keputusan yang tepat dan mendasar. Untuk itu, dibutuhkan Teknologi Informasi untuk menunjang segala kebutuhan organisasi-organisasi yang kerap menjadi semakin kompetitif dalam membenahi teknologi sebagai fondasi pekerjaan mereka. Perkembangan teknologi informasi akan mampu memberikan dampak yang signifikan bagi organisasi di berbagai aspek, namun salah satu aspek yang akan diangkat dalam penelitian ini adalah bahwa teknologi informasi dengan serangkaian sistem yang telah terintegrasi ini dapat membantu pengendalian internal untuk mengurangi kemungkinan terjadinya bentuk fraud dalam suatu organisasi.

Pengendalian internal berbasis Teknologi Informasi (IT) sudah diperkenalkan dan diterapkan oleh banyak organisasi di seluruh dunia, terutama organisasi-organisasi yang *well-integrated*. Tidak diragukan lagi bahwa perkembangan teknologi informasi memiliki peran yang sangat siginifikan dalam memudahkan dan mengembangkan pengendalian internal menjadi serangkaian pengendalian yang ketat, aman, dan terpercaya. Teknologi informasi yang terus berkembang akan mampu memberikan kontribusi terhadap keefektifan pengendalian internal dalam mempersempit celah-celah terjadinya fraud.

Association of Certified Fraud Examiner (ACFE) mendefinsikan fraud sebagai pemanfaatan suatu pekerjaan/jabatan untuk kekayaan seseorang melalui penyalahgunaan yang dilakukan secara sengaja atau penyalahgunaan atas sumberdaya atau aset organisasi. Hasil dari survey yang dilakukan oleh Pickett (2003) dengan melibatkan 10.000 organisasi di lebih dari 15 industri menyatakan beberapa poin yang dapat membuka mata para pelaku bisnis bahwa 82% fraud dilakukan oleh karyawan dimana sepertiganya dilakukan oleh manager, 40% partisipan yang mengira organisasi mereka rentan atas fraud menunjukan bahwa organisasi mereka memiliki kekurangan kebijakan yang spesifik, dan organisasi yang tidak melakukan review atas kerentanan fraud teridentifikasi bahwa mereka telah menderita fraud selama 12 bulan sebelumnya. (Pickett, 2003: 425)

K. H. Spencer Pickett (2003: 425) menegaskan bahwa fraud muncul ketika "*things go wrong*" dan fraud berkaitan erat dengan sistem pengendalian internal perusahaan yang tidak berjalan dengan baik. Survey tersebut melaporkan bahwa fraud memiliki kecenderungan terbesar untuk dilakukan oleh manajemen, sehingga manajemen menjadi putus asa ketika akan investigasi dan dituntut untuk mengatasi fraud. Untuk itu, perusahaan menyerahkan pekerjaannya kepada unit yang lebih independen, yaitu audit internal untuk menyelidiki kasus fraud. Dengan ini dapat disimpulkan bahwa akar utama dalam mengantisipasi terjadinya kecurangan akuntansi atau fraud adalah memperbaiki sistem pengendalian internal. Tuanakotta (2007:272) juga menyatakan hal yang sama bahwa pencegahan fraud harus dimulai dengan pembenahan sistem pengendalian internal dalam perusahaan.

Penelitian ini terinspirasi oleh penelitian terdahulu dengan judul "Dampak Teknologi Informasi dalam Pengendalian Internal untuk Mengantisipasi Kecederungan Kecurangan Akuntansi" yang dilakukan oleh Korompis (2014). Ketertarikan peneliti muncul pada bagian pencegahan terjadinya kecurangan akuntansi (fraud) dengan sistem pengendalian internal berorientasi pada kecanggihan teknologi informasi. Penelitian tersebut tidak secara khusus menekankan aplikasi penggunaan teknologi informasi dalam menunjang pengendalian internal namun hanya menjelaskan pengaruh teknologi informasi secara umum terhadap fraud. Oleh karena itu, perbedaan yang akan ditekankan oleh peneliti adalah pengaplikasian teknologi informasi berupa software maupun hardware secara spesifik di dalam sistem pengendalian internal dalam kaitannya untuk mencegah tindakan fraud.

Walaupun operasi bisnis perusahaan sudah terkomputerisasi, risiko *fraud* tidak serta merta berkurang, namun juga akan menambah risiko terjadinya *fraud* yang disebabkan oleh program aplikasi itu sendiri. Risiko fraud yang disebabkan oleh IT dapat berupa kesalahan proses dari program, akses yang tidak sah, pencurian data, kerusakan data, dan hilangnya jejak audit (Bodnar dan Hopwood, 2013). Risiko ini mendorong perusahaan agar perlu mengadakan adanya kontrol yang terpogram pada sistem tekonologi informasi. Untuk mengatasi risiko-risiko yang berkaitan dengan teknologi informasi, perusahaan menerapkan pengendalian yang diperkenalkan oleh *Committee of Sponsoring Organization* (COSO), yaitu berupa pengendalian umum dan pengendalian aplikasi (Arens, 2012:374). Dengan meneliti kedua pengendalian tersebut, maka dapat diketahui bagaimana teknologi informasi

berkontribusi terhadap kecurangan akuntansi (fraud) sekaligus sebagai sarana mengevaluasi pengendalian internal yang bertujuan untuk menciptakan efektivitas dan efisiensi operasi bisnis dan keandalan informasi. Melalui penelitian ini, peneliti ingin membuktikan sekaligus mengamati apakah teknologi informasi yang terus berkembang setiap harinya dapat memfasilitasi pengendalian internal untuk menutup berbagai celah terjadinya tindakan fraud pada PT XYZ.

TINJAUAN PUSTAKA

Teknologi Informasi

Istilah teknologi informasi terdiri dari dua kata, yaitu kata teknologi dan kata informasi. Kata teknologi berasal dari istilah "techne" yang berarti suatu cara dan "logos" yang berarti suatu ilmu atau pengetahuan, sehingga dengan itu teknologi dapat diartikan sebagai pengetahuan akan suatu cara. Menurut Martin (1999), teknologi informasi tidak hanya terbatas pada teknologi komputer yang berkaitan dengan proses, alat bantu, dan pengolahan informasi, melainkan juga terdapat teknologi komunikasi yang tersedia untuk menyebarluaskan informasi tersebut dari perangkat satu ke perangkat lainnya dengan kecepatan tinggi.

Pada umumnya, untuk dapat memanfaatkan penggunaan teknologi informasi dibutuhkan setidaknya tiga komponen, yaitu perangkat keras (*hardware*), perangkat lunak (*software*), dan pengguna (*brainware*). Ketiga komponen tersebut merupakan unsur-unsur pendukung yang mampu membangun penggunaan komputer yang bersinergis membentuk teknologi informasi. Komputer diibaratkan manusia, *hardware* merupakan tubuh, sedangkan *software* merupakan otak. Namun, hardware dan software tersebut tidak akan sepenuhnya berguna tanpa adanya manusia yang mengoperasikannya tersebut, sehingga fungsi dan kinerja ketiga komponen inilah yang tidak bisa terpisahkan.

Pengendalian Internal

Sistem pengendalian internal (*internal control system*) bukan lagi hanya merupakan pedoman akuntansi, namun juga merupakan alat yang sangat diperlukan untuk meminimalisir risiko-risiko bahkan juga ancaman-ancaman terhadap sistem akuntansi, data, dan aset (Cangemi dan Singleton, 2003:65).

Committee of Sponsoring Organization of the Treadway Commission (COSO) mendeskripsikan kerangka pengendalian internal yang sekarang ini telah diterima di Amerika Serikat dan dijadikan sebagai *best practice* oleh seluruh dunia. Komponen-komponen sistem pengendalian internal oleh COSO adalah sebagai berikut: (1) *Control Environment* (Lingkungan Pengendalian); (2) Penilaian Risiko (*Risk Assessment*); (3) Aktivitas Pengendalian (*Control Activities*); (4) Pemantauan (*Monitoring*); dan (5) Informasi dan Komunikasi (*Information and Communication*)

Dari kelima komponen pengendalian internal tersebut, yang akan dijadikan peneliti sebagai dasar analisis adalah komponen aktivitas pengendalian. Hall (2010: 20) menjelaskan bahwa aktivitas pengendalian merupakan kebijakan dan prosedur yang dirancang oleh suatu organisasi dalam menghadapi risiko-risiko yang teridentifikasi. Maka dari itu, peneliti menggunakan komponen aktivitas pengendalian sebagai dasar analisis untuk dapat mengetahui tindakan perusahaan dalam mengantisipasi adanya keterjadian *fraud.* Namun, terdapat dua aktivitas pengendalian, yaitu pengendalian teknologi informasi (*IT Control*) dan pengendalian fisik (*physical control*). Dalam penelitian ini, peneliti menggunakan *IT Control* sebagai dasar analisis yang lebih mendalam untuk dapat mengetahui peran teknologi informasi dalam mengantisipasi adanya keterjadian *fraud*.

Kecurangan Akuntansi (Fraud)

Chartered Institute of Public Finance and Accountancy (CIPFA) membagi fraud dalam tiga kategori, yaitu: (1) Fraud yang diketahui dan tercatat di muka umum; (2) Fraud yang diketahui, namun hanya di dalam organisasi tersebut dan tidak akan dipublikasikan ke masayarakat umum; (3) Fraud yang belum dapat diketahui

Arens, dkk (2012:373) menyatakan bahwa walaupun teknologi informasi memberikan keuntungan dalam kontrol proses bisnis perusahaan, namun perusahaan akan tetap terlibat dengan berbagai risiko yang berasal dari hardware dan software itu sendiri. Risiko-risiko penggunaanTI tersebut adalah sebagai berikut: (1) Ketergantungan pada kemampuan *software* dan *hardware*; (2) Akses yang tidak sah; (3) Kehilangan data; (4) Visibilitas jejak audit; (5) Rendahnya otorisasi secara tradisional; (6) Kurangnya pemisahan tugas; (7) Keahlian personel TI.

Hubungan antara Teknologi Informasi, Sistem Pengendalian Internal, dan Kecurangan Akuntansi

Pickett (2003:167) melaporkan bahwa sistem pengendalian internal yang tidak efektif

merupakan salah satu penyebab terjadinya kecurangan akuntansi/fraud.. Manurung dan Apriani (2012: 10) juga menambahkan bahwa pengendalian internal yang baik akan mempersulit pihak yang akan melakukan fraud.

Zanaria (2017: 92) mengungkapkan bahwa daya saing global yang semakin berkembang ini mempengaruhi tingkat kebutuhan perusahaan dalam mengamankan aset-aset mereka, sehingga memerlukan serangkaian teknologi informasi yang dapat menunjang keamanan aset perusahaan dari oknum-oknum yang akan melakukan fraud. Teknologi informasi yang terintegrasi dapat meningkatkan kinerja perusahaan sekaligus mampu mempersempit peluang terjadinya fraud. Wilkinson dan Cerullo (1997) menjelaskan bahwa peran teknologi informasi dengan penggunaan komputer dapat memenuhi kebutuhan informasi dalam kegiatan bisnis dengan cepat, tepat waktu, relevan, dan akurat.

METODE PENELITIAN

Penelitian ini merupakan penelitian kualitatif deskriptif dengan pendekatan studi kasus. Penelitian ini dilakukan pada PT XYZ Tbk yang bergerak di bidang manufaktur dengan produk penjualan terbesarnya berupa chips, fiber, dan benang filamen. Teknik pengumpulan data yang digunakan oleh peneliti antara lain: wawancara, dokumentasi, studi kepustakaan dan observasi.

Berdasarkan pernyataan yang telah dijelaskan di bab 2, peneliti menggunakan komponen *IT Control* yang terdiri dari pengendalian umum dan pengendalian aplikasi sebagai dasar analisis. Penelitian ini dilakukan dengan cara membandingkan kriteria-kriteria pemenuhan *IT Control* sebagai *best practice* dengan aplikasinya pada PT XYZ

HASIL DAN PEMBAHASAN

Analisis Hasil Pengamatan

Setiap sistem pasti memiliki kekurangannya masing-masing. Kelemahan sistem yang dioperasikan oleh XYZ adalah tidak terintegrasinya antara *MM System* dan *WDM System* ke CODA. Hal ini merupakan kelemahan atas implementasi sistem dan pengendalian internal yang ingin diwujudkan oleh XYZ. Sistem yang tidak terintegrasi dapat menghambat arus informasi dalam sebuah organisasi. Hal tersebut dinyatakan dalam bentuk keterbatasan perusahaan dalam mengkomunikasikan atau membagikan suatu informasi yang dihasilkan dari departemen tertentu ke sistem lain secara rutin. Beda halnya dengan sistem yang terintegrasi secara otomatis. Integrasi sistem secara otomatis dalam perusahaan dapat menghasilkan kondisi *less paper, less time, less cash, less complexity*, dan mencegah adanya duplikasi. Upload sistem yang dilakukan oleh *Material Management System* (MM System) dan *Warehouse Dispatch Management System* (WDMS) ke *CODA Financial System* akan mengurangi risiko pengendalian internal yang buruk dibanding sistem-sistem tersebut tidak dikomunikasikan sama sekali atau *stand alone*. CODA, WDMS, MM System, dan HRMS adalah sistem aplikasi yang dibangun berdasarkan *Taylor Made* atau sistem yang dibangun sendiri-sendiri atau terpisah, sehingga ada kemungkinan bahwa sistem–sistem tersebut perlu di-*update* dan di-*maintain* secara periodik agar tidak terdapat risiko-risiko yang mungkin diciptakan sendiri oleh sistem. Risiko yang mungkin timbul adalah duplikasi dan ketidakkonsitenan.

Risiko lain yang mungkin terjadi adalah database dari sistem tidak terhubung ke CODA secara konsisten atau setiap hari. Apabila user tidak upload database ke CODA satu hari saja, maka pengakuan hutang dan kewajiban lainnya untuk memroses pembayaran yang harus dilakukan oleh XYZ tidak *real time* atau telat melakukan pengakuan hutang. Telat dilakukannya upload ke CODA bisa dikarenakan *user* lalai dalam me-*maintain* pengiriman database setiap hari. Akibatnya adalah XYZ telat melakukan pengakuan hutang maupun piutang, sehingga XYZ dapat merugikan pihak ketiga. Hal tersebut tidak hanya merugikan pihak ketiga, tetapi juga mampu mengganggu relasi XYZ dengan pihak ketiga. Selain itu, telatnya melakukan pengakuan hutang juga tidak sesuai dengan prinsip akuntansi karena hutang harus diakui ketika surat tagihan telah diterima atau barang atau jasa telah diterima atau dinikmati.

Aktivitas Pengendalian

Berikut ini merupakan uraian pelaksanaan pengendalian umum (*general control*) di XYZ:

1. *Administration of IT Function*

Dukungan dewan direksi dan jajaran senior management memberikan dampak yang besar terhadap terbentuknya IT Department. Perusahaan yang mempunyai kompleksitas yang tinggi akan membangun IT Department untuk mengawasi kebutuhan teknologi perusahaan, sedangkan untuk perusahaan yang lebih kecil, perusahaan hanya membutuhkan IT Manager atau konsultan untuk menangani masalah IT (Arens, 2012). PT XYZ Tbk membuktikan teori ini dengan adanya

dukungan maksimal dari BOD atas penunjukkan pimpinan IT dan pembetukkan organisasi IT itu sendiri. Dengan ini, XYZ membuktikan bahwa teknologi informasi merupakan prioritas yang tinggi bagi perusahaan sebagai pengendalian yang utama.

2. *Segregation of IT Duties*

Pemisahan tugas pada departemen Teknologi Informasi masih harus menjadi titik yang penting dalam membangun sistem pengendalian internal yang baik. Dikatakan penting karena tanggung jawab dan wewenang sudah terpisah yaitu dengan menghadirkan bagian *Desktop Development*, *Web Development*, *Maintenance Production*, *Maintenance Non-Production*, *Network and Device Maintenance*, *Server and Policy Maintenance*, dan *IT Documentation*. Masing-masing fungsi tersebut sudah menjalankan tanggung jawab sesuai dengan bagiannya dan sudah memenuhi kebutuhan operasional perusahaan. Namun, masing-masing fungsi kurang mendefinisikan tanggung jawab secara spesifik dan spesialisasi dari masing-masing fungsi. Fungsi tersebut yaitu level yang berada di paling bawah atau level *supervisor*. Pada praktiknya, Departmen TI selalu mengadakan *briefing* singkat untuk membahas mengenai pekerjaan yang akan dilakukan setiap harinya. Auditor Internal mengakui bahwa struktur organisasi TI dan pendelegasian wewenang TI memang harus banyak diperbaiki dan dikembangkan. Maka dari itu, walaupun masing-masing fungsi sudah menjalankan tugas dan tanggung jawabnya, namun XYZ harus perlu menjelaskan *job description* sesuai dengan struktur organisasinya agar karyawan dapat menyadari apa yang menjadi kewajiban karyawan dalam bekerja.

3. *System Development*

Pengembangan sistem yang dipaparkan oleh Arens (2012:377) mencakup dua hal penting, yaitu pembelian software atau pengembangan sendiri (*in-house development*) dan menguji semua perangkat lunak yang memadai. Pengujian tersebut dilakukan agar perangkat lunak yang baru dapat berjalan sesuai dengan hardware dan software yang sudah ada serta menguji apakah perngkat lunak yang baru dapat menangani jumlah transaksi yang banyak. Hal ini tercerminkan pada implementasi yang dilakukan oleh Departemen IT di XYZ dengan adanya pembelian software (*CODA Financial System*) kepada pihak ketiga. Usaha XYZ untuk memenuhi kebutuhan perusahaan melalui sistem tersebut tidak berhenti sampai situ, XYZ juga melakukan *in-house development* terhadap sistem CODA. Sistem tersebut dapat dikembangkan oleh XYZ karena adanya *source code* yang dimiliki oleh perusahaan, sehingga XYZ mampu memodifikasi sistem sesuai dengan kebutuhan perusahaan. Sebelum sistem tersebut dieksekusi, perusahaan ingin mendapatkan keyakinan apakah sistem tersebut sudah sesuai dengan rencana pengadaannya. Maka dari itu, perusahaan melakukan pengujian apakah sistem yang sudah dirancang dapat berjalan sesuai dengan *IT Blueprint*. Pengujian tersebut dilakukan melalui beberapa tahap sebagai berikut:

a. Pengujian yang dilakukan untuk mengetahui apakah sistem yang dirancang sudah sejalan dengan sistem lain yang sudah berjalan.
b. Pengujian yang dilakukan untuk mengetahui apakah sistem yang baru dibangun dapat terintegrasi dengan sistem-sistem lainnya atau yang sudah ada.
c. Pengujian yang dilakukan untuk mengetahui apakah sistem baru tersebut memiliki proses yang cepat dan apakah pengiriman data antara satu sistem ke sistem lain cepat.
d. Pengujian yang dilakukan untuk mengetahui apakah sistem yang dirancang dapat mengangkut jumlah transaksi yang banyak.
e. Pengujian yang dilakukan oleh *user* untuk mengetahui apakah sistem yang dirancang sudah sesuai dengan kebutuhannya, kemudian mendapatkan evaluasi dari *user* apabila sistem masih belum sesuai serta mendapatkan persetujuan apabila sistem sudah sesuai.
f. Pengujian yang dilakukan oleh seluruh karyawan untuk memastikan bahwa sistem sudah siap beroperasi untuk mendukung kegiatan operasional setiap harinya.

Pengujian - pengujian tersebut dilakukan dengan tujuan untuk menemukan kesalahan atau kegagalan yang terjadi pada perangkat lunak. Pengujian ini akan diberhentikan ketika sistem tersebut sudah tidak memiliki kegagalan dan sudah memenuhi kebutuhan perusahaan. Pengujian tersebut didokumentasi oleh XYZ dan disimpan oleh *Application Software Developer* dan *User* dengan tujuan bahwa sistem yang diotorisasi lah yang digunakan dan ditaati kebijakan dan prosedurnya oleh stakeholder. Dengan adanya pengujian ini lah, XYZ membuktikan bahwa jalannya suatu sistem menentukan kesuksesan operasional bisnis XYZ di zaman milenial ini dan

dengan memprioritaskan IT sebagai backbone perusahaan.

4. *Physical and Online Security*

Pengendalian ini diterapkan oleh XYZ dengan menggunakan ID Card bagi seluruh karyawan sebagai akses masuk dan keluar kantor, dan *fingerprint* sebagai rekaman kehadiran karyawan setiap hari. Terutama untuk IT Department, karyawan IT memiliki ID Card khusus untuk keluar masuk ruangan IT dan ruangan server. Ruangan IT Department juga diawasi dengan CCTV agar memudahkan bagian keamanan mengawasi akses ruangan tersebut. Pengendalian akses online pun juga diaplikasikan oleh XYZ dengan memberi *ID/Username* dan *password* kepada masing-masing karyawan untuk mengakses jaringan internet (WiFi), software (*CODA Financial System*) dan hardware (komputer yang disediakan oleh kantor). Serangkaian pengendalian yang diterapkan oleh XYZ sudah cukup baik dalam melindungi data dan informasi dari seseorang yang tidak memiliki hak untuk mengakses sistem komputer tersebut. Praktik ini sudah sesuai dengan yang diungkapkan oleh Arens (2012:377) bahwa sistem dan data-data yang ada di dalam sistem perlu diamankan baik secara fisik maupun online.

5. *Back up and Contingency Planning*

Kemungkinan terjadinya bencana alam maupun buatan berpotensi dalam menghambat proses operasional bisnis perusahaan (Arens, 2012:377). Oleh sebab itu, perusahaan perlu membuat adanya rencana kemungkinan (*contingency plan*) untuk meminimalisir kehilangan data dan menjaga agar perusahaan tetap beroperasi. Bencana-bencana yang mungkin terjadi diminamilisir XYZ dengan cara menjaga data-data dan software perusahaan yang di back-up dan dikirim ke Kantor Pusat (*Head Office*). Hal ini merupakan tindakan yang cukup baik bagi XYZ dalam merespon langsung ketika insiden terjadi dalam rangka mengantisipasi, mendeteksi, dan mengurangi akibat bencana terhadap aset perusahaan. Namun, prosedur *back up* data masih ditangani secara manual. *Back up* manual ini terlihat dari pengiriman *database* yang menggunakan kurir menuju Kantor Pusat. Hal tersebut berakibat bahwa data *back up* tidak dilakukan dengan konsisten atau tiap hari karena kelalaian manusia. Dengan demikian, ketidakkonsistenan pada prosedur *back up* dapat mengakibatkan banyak data yang terlewat untuk disimpan.

6. *Hardware Controls*

Pengendalian umum yang terakhir adalah pengendalian atas perangkat keras. Hal penting yang ditekankan oleh Arens (2012:378) pada pengendalian ini adalah pengendalian atas perangkat keras sudah terpasang di dalam komputer (*built in*) oleh pabrik pembuatnya dan bagaimana perusahaan menangani kegagalan yang terdeteksi oleh perangkat keras itu sendiri. Ada beberapa pengendalian atas perangkat keras yang diterapkan oleh XYZ sebagai berikut:

a. Mempersiapkan detail list atas seluruh hardware mengenai umur, spesifikasi, jumlah, distribusi, *schedule maintenance* yang telah dan akan dilakukan.
b. Melakukan *maintenance* dan *service* yang dilakukan oleh bagian *IT Maintenance Analyst* setiap periodik.
c. Mengunci komputer dengan dengan sistem *sign in* terlebih dahulu agar dapat mengakses komputer.
d. Memasang detektor asap dan api serta tabung pemadam kebakaran.
e. Menghindari komputer dan perangkat keras lainnya dari barang-barang yang mudah terbakar.
f. Meyakinkan bahwa alat-alat input/output berfungsi sebagaimana mestinya. Contohnya memastikan apakah printer berfungsi mencetak sesuai dengan input yang diperintahkan.
g. Mengecek apakah data yang telah disimpan ke luar telah terekam dan terbaca dengan benar.
h. Memastikan ruangan server tidak *overheat* sehingga ruangan server harus difasilitasi AC dengan suhu dingin yang sangat rendah agar server dapat bekerja secara maksimal.
i. Memastikan listrik pada server tidak boleh mati sehingga harus difasilitasi dengan UPS dan *generator-set.*

Terhadap pengendalian yang memadai tersebut, XYZ menunjukkan bahwa perangkat keras sudah dilengkapi dengan keamanan yang mampu menjaga stabilitas sistem, keandalan informasi, dan memaksimalkan kerja software dan hardware itu sendiri. Selain itu, peneliti juga menggunakan pengendalian aplikasi (*application control*) sebagai alat untuk menganalisis kecukupan pengendalian pada sistem keuangan dan akuntansi XYZ (*CODA Financial System*). Berikut merupakan uraian pelaksanaan pengendalian aplikasi di XYZ:

Pengendalian Masukan (*Input Control*)

PT XYZ Tbk memiliki pengendalian masukan yang sudah cukup dalam arti perusahaan yakin bahwa data masukan sebagai transaksi sehari-hari merupakan data yang valid, lengkap, dan bebas dari kesalahan atau penyalahgunaan. Pengendalian tersebut diuraikan oleh XYZ sebagai berikut:

a. **Terdapat kontrol terhadap dokumen sumber yang akan diinput**, yaitu dokumen sumber memiliki nomor urut (*pre-numbered*) yang ter-*generate* oleh sistem secara otomatis. Selain itu, hal ini didukung juga bahwa dokumen yang telah di-input selalu dibubuhkan dengan tanda cek. Dengan mengaplikasikan nomor urut dan tanda centang pada dokumen sumber, hal ini dapat mencegah *user* untuk dapat menginput dokumen yang sama, sehingga tidak bisa terjadi *double-post* di dalam sistem. Dengan adanya dokumen sumber juga dapat menjadi bahan pengecekkan apakah data inputan sama dengan dokumen sumbernya.
b. **Terdapat kontrol berupa *batch processing data entry***, seperti *numeric and alphabetic check*. Perusahaan memastikan bahwa *field* yang *value*-nya adalah angka hanya dapat diisi dengan angka (begitu juga dengan alfabet). Apabila tidak sesuai dengan jenis field yang telah ditentukan, maka akan muncul pesan error. Kemudian terdapat *size check,* yaitu perusahaan membuat batasan kapabilitas suatu inputan sehingga tidak ada inputan yang melebihi batas kapabilitas penyimpanannya. Apabila melebihi batas kapabilitas yang ditentukan, maka tidak akan bisa tersimpan inputannya.
c. **Terdapat control berupa *online data entry control***, yaitu berupa *completeness check*. Perusahaan memastikan bahwa data inputan dapat disimpan apabila semua field sudah terisi sesuai yang ditetapkan oleh perusahaan. Kemudian terdapat *validity check*. Contohnya, perusahaan hendak membeli suatu barang dengan membuat *Purchase Requisition* (PR) seharga lima ratus juta rupiah. Sistem akan langsung membaca kepada pihak mana PR tersebut harus di*approve* atau diotorisasi melalui sistem. Selanjutnya, terdapat *reasonableness test*. Hal ini ditunjukkan perusahaan ketika perusahaan hendak akan mengeluarkan barang jadi atas adanya penjualan. Hasil timbangan atas barang yang dikeluarkan akan *linkage* dengan sistem WDMS. Sistem WDMS pun juga akan mencocokkan dengan PO dari pelanggan. Apabila hasil timbangan sesuai dengan PO, maka surat jalan baru akan bisa terbit.
d. **Terdapat otorisasi atas dokumen sumber**. Hal ini ditandai dengan adanya otorisasi berbentuk tanda tangan pihak yang berkaitan pada dokumen sumber sebelum di-*input* ke dalam sistem. Otorisasi pada dokumen sumber menjadi hal yang sangat penting karena dengan adanya otorisasi tersebut, *user* yakin bahwa data tersebut valid dan sah. Terlebih lagi, otorisasi pengeluaran aset sudah terancang melalui sistem. Oleh karena itu, pengendalian ini dapat mencegah adanya tindakan memalsukan pernyataan (*fraudulent statement*).
e. **Terdapat pesan error apabila terdapat kesalahan input data,** yaitu dengan adanya konfirmasi berbentuk kotak dialog apabila ada data input yang tidak sesuai dengan default sistem. Hal ini ditandai dengan adanya kolom debit dan kredit hanya bisa diisikan dengan angka, serta konfirmasi apabila user belum menyimpan data inputan. Dengan adanya pesan error ini, perusahaan dapat yakin bahwa data masukan merupakan data yang lengkap.
f. **Terdapat kontrol atas kesalahan input data,** atau prosedur *cancellation***,** yaitu fungsi *delete* pada sistem CODA tidak dapat digunakan oleh *user*. Apabila terjadi kesalahan input data yang dilakukan oleh *user,* maka data tersebut tidak bisa dihapus. Hal ini merupakan salah satu kontrol bagi XYZ untuk menghindari adanya praktik kecurangan akuntansi yang dilakukan oleh *user* dengan membuat pernyataan palsu. Apabila memang terjadi kesalahan, auditor dapat mengetahui kesalahan tersebut dari *transaction log,* dan mampu menyelidiki kesalahan dari detil-detil biaya, rekonsiliasi akhir periode, serta membuat jurnal memorial. Penyesuaian tersebut harus diotorisasi oleh manajer terkait. Kontrol tersebut mampu mencegah adanya penyalahgunaan data masukan.

Pengendalian Proses (*Process Control*)

PT XYZ Tbk sudah cukup memiliki pengendalian proses yang baik yang bertujuan untuk mencegah sekaligus mendeteksi adanya kesalahan-kesalahan pada saat data diproses.

Berikut uraian pengendalian pengendalian proses pada XYZ:

a. **Terdapat rekaman atas setiap proses ke dalam database.** Kontrol ini dirancang XYZ dengan menggunakan *transaction log*. Dengan adanya *transaction log*, perusahaan dapat melihat aktivitas *user*, nama-nama *user*, halaman yang diakses oleh *user*, dan segala sesuatu yang dilakukan oleh user di dalam sistem tersebut dapat terekam ke dalam *transaction log* tersebut. Dalam sistem CODA, user tidak bisa secara sengaja menghilangkan data atau menghapus data yang telah dilakukan *post to book* karena sistem tidak mengijinkan user menggunakan fitur tersebut. Dengan adanya pengendalian tersebut, data masukan dapat diproses dengan benar.
b. **Terdapat perbaikan atas kesalahan yang dilakukan selama pemrosesan.** XYZ memiliki bagian IT Accounting yang bertugas dalam menangani sistem CODA. Bagian ini-lah yang melakukan pengawasan terhadap jalannya proses sistem CODA sehari-harinya dan menjadi *troubleshooting* bagi user atas adanya pertanyaan atau masalah mengenai CODA. IT Accounting membantu mendeteksi kesalahan pada sistem, sehingga kesalahan pada pemrosesan dapat diperbaiki dengan tanggap.
c. **Terdapat kontrol berupa *batch control totals*. PT XYZ** menerapkan kontrol ini di bagian siklus pembelian. Ketika perusahaan menerima barang atas pembeliannya, perusahaan menerima *delivery notes* dari vendor. Kemudian, pihak gudang harus membuat GRN melalui sistem MM berdasarkan *delivery notes* yang telah diterima. Sistem akan membaca setiap perhitungan rincian biaya barang yang diterima. Jumlah nilai pembelian barang akan dideteksi oleh sistem tanpa memperlihatkan perhitungannya, namun sistem akan meminta perhitungan dari user. Apabila perhitungan *user* belum sesuai dengan perhitungan sistem, maka sistem akan menampilkan pesan error dan data inputan tidak akan bisa disimpan sampai perhitngan terseut sesuai. Hal ini dirancang agar tidak terdapat kesalahan perhitungan barang yang diterima oleh pihak lain dan pengeluaran kas yang tidak sesungguhnya.

Pengendalian Keluaran (*Output Control*)

PT XYZ Tbk memiliki pengendalian keluaran yang cukup baik yang dapat digambarkan berikut ini:

a. **Terdapat kontrol atas laporan (hasil ouput) yang akurat, lengkap, dan *up-to-date*.** Pengendalian ini dilakukan dengan cara melakukan *manual review* atas laporan yang dihasilkan dari sistem. Pemeriksaan ini meliputi melakukan rekonsiliasi piutang dan kas pada bank, mencocokkan jumlah persediaan dengan stock opname bulanan, mengecek aging schedule hutang, melakukan *cross-check* penjualan dengan WDMS (kuantitas pada surat jalan), dan sebagainya. Setelah dilakukan *manual review*, laporan tersebut akan dicek lagi oleh manajer akuntansi dan direktur keuangan. Setelah laporan tersebut dicetak, perusahaan akan melakukan cek atas akurasi dari saldo-saldo tersebut. Arens (2012:379) menyatakan bahwa pengendalian output yang paling penting adalah review atas kewajaran laporan oleh seseorang yang memiliki pengetahuan atas laporan tersebut. Dengan adanya *triple-check* ini, perusahaan dapat meyakini bahwa laporan adalah akurat, lengkap, dan sah, sehingga output dari sistem CODA sudah cukup baik.
b. **Terdapat kontrol atas penghancuran laporan (*record retention*).** Penghancuran laporan di XYZ akan dilakukan apabila laporan serta bukti-bukti transaksi sudah melebihi dari 10 tahun. Hal ini dikarenakan adanya pemeriksaan laporan keuangan yang dilakukan oleh bagian pajak. Apabila laporan sudah tidak memiliki kepentingan lagi untuk pemeriksaan, maka semua laporan akan dimusnahkan untuk menghindari adanya risiko fraud. Risiko tersebut yaitu penyalahgunaan bukti-bukti transaksi yang mungkin bisa dapat digunakan lagi.
c. **Terdapat pengamanan atas ouput.** Seluruh laporan atau dokumen berupa bukti transaksi yang masih berbentuk *soft copy* masih harus diamankan menggunakna *password*. Terutama laporan yang masih disimpan di USB, *Hardisk*, dan lainnya. Hal tersebut ditujukan untuk mengamankan laporan dari bentuk penyalahgunaan oleh orang yang tidak memiliki kepentingan.

KESIMPULAN DAN SARAN

Kesimpulan

1. Berdasarkan hasil penelitian yang dilaksanakan di PT XYZ Tbk, peneliti menyimpulkan bahwa

teknologi informasi yang diterapkan oleh XYZ dapat mengantisipasi kecurangan akuntansi. Hal ini terbukti dengan adanya pengendalian umum (*general control*) yang dijalankan oleh XYZ. Pengendalian tersebut berupa dukungan maksimal dari BOD terhadap pengelolaan fungsi IT, pengembangan sistem, pengamanan akses online dan fisik, pengendalian terhadap perangkat keras, dan *back up* data. Selain pengendalian umum, pengendalian aplikasi (*application control*) pun juga turut mengantisipasi kecurangan akuntansi dengan sangat baik. Bentuk dari pengendalian aplikasi adalah pengendalian input, proses, dan output. Hal ini tergambarkan oleh adanya kontrol terhadap dokumen sumber yang diinput, rekaman setiap aktivitas yang dilakukan tiap user (*transaction log*), otorisasi sistem, pesan error atas kesalahan input data, dan prosedur rekonsiliasi.

2. Peneliti masih menemukan beberapa kekurangan pada pengendalian umum XYZ. Kekurangan tersebut adalah bahwa departemen IT tidak mendeskripsikan tugas dan tanggung jawab masing-masing fungsi IT secara spesifik. Hal ini dapat mengurangi efektivitas kinerja operasional harian karena karyawan tidak dapat menyadari apa yang menjadi kewajiban dirinya dalam bekerja. Selain itu, prosedur *back up* data masih menggunakan metode yang sangat tradisional. Hal tersebut ditunjukkan dari pengiriman data *back up* yang menggunakan jasa kurir. Apabila prosedur *back up* data dilakukan secara manual, maka pengiriman data XYZ tidak dapat dilakukan dengan konsisten. Di samping kekurangan yang ada, pengendalian umum dan aplikasi yang dilaksanakan oleh XYZ memberikan keyakinan kepada perusahaan bahwa semua transaksi telah diinput dan diotorisasi dengan benar, serta diproses dengan baik dan tepat waktu.
3. XYZ menggunakan sistem informasi dalam mengendalikan proses bisnis. Setiap proses bisnis dikendalikan oleh sistem informasi yang memiliki bahasa pemograman yang berbeda-beda. Artinya, sistem informasi yang digunakan oleh XYZ tidak saling berhubungan satu sama lain (tidak terintegrasi). Walaupun sistem-sistem tersebut tidak bisa terintegrasi, XYZ dapat menghubungkan sistem secara manual dengan cara *upload*. Menghubungkan sistem informasi secara manual memang merupakan solusi yang lebih baik dibanding sistem tersebut tidak dihubungkan sama sekali. Namun, *upload* dapat menimbulkan risiko baru, yaitu duplikasi dan ketidakkonsistenan. Terhadap risiko duplikasi tersebut, XYZ sudah memberikan kontrol berupa pemeriksaan internal terhadap proses bisnis yang memiliki risiko yang signifikan. Sedangkan, XYZ belum memiliki kontrol terhadap risiko atas ketidakkonsistenan *upload*.

Saran

1. Bagi Perusahaan
   a. Mengingat teknologi informasi yang digunakan dalam proses penyimpanan data *back up* masih menggunakan cara yang manual, peneliti menganjurkan agar perusahaan dapat menggunakan layanan penyimpanan *cloud* atau *cloud storage*. Mengingat penyimpanan *cloud* memerlukan biaya yang sangat tinggi, maka peneliti menganjurkan agar perusahaan dapat merancang suatu metode. Metode yang dimaksud adalah metode yang dapat memperingatkan user bahwa terdapat data-data yang terlewat untuk dilakukan *back up*.
   b. Dikarenakan sistem informasi yang digunakan oleh XYZ masih berjalan manual dan sudah beroperasi sejak berdirinya perusahaan, maka peneliti menganjurkan agar perusahaan dapat menggunakan sistem yang terintegrasi. Keuntungan dari sistem yang terintegrasi ini adalah perusahaan dapat meningkatkan arus informasi yang diperlukan oleh departemen atau sistem lain. Selain itu, perusahaan dapat terhindar dari kehilangan dan pencurian data.
   c. Seiring dengan perkembangan teknologi, kecurangan akuntansi (*fraud*) juga dapat dilakukan dengan cara yang canggih. Peneliti menganjurkan untuk perusahaan agar terus mengevaluasi dan memperbaharui sistem dan teknologi informasi sesuai dengan perkembangan teknologi sekarang. Hal ini ditujukan untuk menghindari kemungkinan terjadi *fraud* oleh user yang sudah terbiasa dengan penerapan teknologi informasi dan yang sudah mengetahui kelemahan sistem.
   d. Perusahaan harus mempertegas adanya tanggung jawab dan wewenang organisasi TI dan harus didokumentasikan secara spesifik tiap analis atau supervisor TI.
2. Bagi Peneliti Selanjutnya

Peneliti selanjutnya dapat melakukan penelitian sejenis dengan memperbaiki keterbatasan masalah pada penelitian in. Peneliti selanjutnya dapat melakukan penelitian serupa dengan melampirkan dokumentasi berupa gambar. Hal tersebut ditujukan agar peneliti mampu mendapatkan hasil yang lebih sempurna dan komprehensif.

Keterbatasan Penelitian

Penelitian ini telah diusahakan dan dilaksanakan sesuai dengan prosedur ilmiah, namun demikian masih memiliki keterbatasan. Keterbatasan tersebut adalah bahwa responden tidak berkenan dalam memberikan informasi berupa gambar sebagai dokumentasi di dalam skripsi peneliti, sehingga peneliti tidak dapat memberikan informasi yang jelas kepada pembaca.

DAFTAR PUSTAKA

Arens A.A., Elder, R. J., & Besley, M. (2012). *Auditing and Assurance Services: An Integrrated Approach* (edisi 14). England: Pearson Education Inc.

Bodnar, G. H. & Hopwood, W. S. (2013). *Accounting Information Systems (*edisi 11). New Jersey: Pearson Education Inc.

Cangemi, M.P., & Singleton, T. (2003). *Managing the Audit Function: A Corporate Audit Department Procedures Guide* (edisi 3). Canada: John Wiley & Sons, Inc.

Hall, James A. (2011). *Information Technology Auditing and Assurance* (edisi 3). South Western: Cengage Learning.

Korompis, C.W.M. (2014). Dampak Teknologi Informasi dalam Pengendalian Internal untuk Mengantisipasi Kecenderungan Kecurangan Akuntansi. *Jurnal Riset Akuntansi Going Concern*, 9(4), 27-33.

Manurung, E.T & Apriani, F. (2012). Evaluasi Pengendalian pada Siklus Penggajian dan Kepegawaian untuk Menentukan Risiko Fraud (Studi Kasus pada PT World Yamatex Spinning Mills). *Bina Ekonomi Majalah Ilmiah Fakultas Ekonomi Unpar*. 16(2), 9-27.

Martin, E. (1999). *Managing Information Technology What Managers Need to Know*. New Jersey: Pearson Education International.

Moeller, Robert R. (2008). *Sarbanes - Oxley Internal Controls: Effective Auditing with AS5, CobiT, and ITIL*. New Jersey: John Wiley & Sons Inc.

Pickett, K. H. Spencer. (2003). *The Internal Auditing Handbook* (edisi 2). England: John Wiley & Sons, Inc

Tuanakotta, Theodorus M. (2010). *Akuntansi Forensik dan Audit Investigatis* (edisi 2). Penerbit Salemba Empat: Jakarta

Wilkinson, J.W. & Cerullo, M. J. (1997). *Accounting Information System* (A. Maulana, Penerjemah) (edisi 3). Binarupa Aksara:Jakarta

Zanaria, Yulita. (2017). Pengaruh Aplikasi Teknologi, Accounting Reporting Terhadap Pencegahan Fraud serta Implikasinya Terhadap Reaksi Investor. https://media.neliti.com/media/publications/89942-ID-pengaruh-aplikasi-teknologi-accounting-r.pdf. *Akuisisi*. 13(1), 91-100.