BUKTI AUDIT DALAM LINGKUNGAN *ELECTRONIC* DATA *INTERCHANGE (EDI)*

Wisnu Wijayanto
Akademi Akuntansi YKPN
e-mail: wisnu2003@gmail.com

ABSTRAK

Perkembangan teknologi informasi membawa perubahan yang signifikan dalam pendekatan pengauditan. Bukti audit sebagai dasar pendukung pendapat auditor mengalami perubahan dari bukti yang berupa kertas menjadi bukti digital (EDI). Keamanan, keabsahan, kekuatan data sebagai bukti, dan keandalan pengendalian atas teknologi informasi menjadi pertimbangan auditor dalam mengevaluasi bukti-bukti audit. Pendekatan deskriptif kualitatif dilakukan untuk mengungkap problematika bukti audit dalam lingkungan sistem yang berbasis teknologi informasi dengan membandingkan antara paperbased audit dan paperless audit. Pengendalian atas teknologi informasi berpengaruh besar terhadap bukti kompeten yang mencukupi untuk mendukung pendapat auditor. Kompetensi auditor dibidang teknologi informasi menjadi faktor utama dalam menginterpretasikan bukti audit.

Keywords: *teknologi informasi, Electronic Data Interchnage, bukti audit, pengauditan.*

PENDAHULUAN

Integrasi ekonomi pada tahun 2020 yang diyakini oleh negara-negara di dunia akan membawa dampak dan perubahan yang sangat penting dalam transaksi antar negara, terutama transaksi komoditas yang antara lain meliputi otomotif, tekstil, *agro-based*, logistik, *wood-based*, dan lain-lain. Untuk memperlancar transaksi tersebut diperlukan *trade fasilitation* yang menyangkut kepabeanan, *transhipment*, pelabuhan, dan infrastruktur pendukung lain, karena integrasi ditujukan untuk menjadikan Asean sebagai *single market* dan *single production based*. Salah-satu wujudnya adalah dengan terbentuknya *Asean Single Window* (ASW). Masing-masing negara membentuk *National Single Windows* (NSW), suatu jaringan pertukaran dokumen bisnis yang bekerja berdasar *network* dan *Electronic Data Interchange* (EDI). NSW dibangun oleh pemerintah setempat untuk mengefisienkan birokrasi untuk tujuan bisnis. Dengan sistem ini, format, prosedur, dan dokumen dirancang dalam bentuk standar untuk tingkat ASEAN. Hal ini berdampak pada pemangkasan birokrasi pengurusan izin ekspor impor .

Beberapa perusahaan di Indonesia mulai mengembangkan EDI untuk aplikasi kepelabuhan. Aplikasi kepelabuhanan tersebut ditujukan untuk keperluan pertukaran dokumen elektronik antar mitra kerja dalam komunitas bidang pelabuhan, diantaranya: PT Pelabuhan Indonesia II, Perusahaan Pelayaran, Terminal Operator, Terminal Petikemas, Administrator Pelabuhan, Bea & Cukai, Karantina (Tumbuh-tumbuhan, Hewan & Kesehatan), serta Imigrasi. Sistem EDI Pabean adalah suatu sistem pertukaran dokumen secara elektronik yang dikembangkan bersama oleh Direktorat Jenderal Bea dan

Cukai (DJBC) dan PT EDI Indonesia. Pemanfaatan teknologi dalam sistem pelayanan pabean yang telah dijalankan adalah pelayanan jasa dokumen ekspor impor, yaitu jasa Pemberitahuan Impor Barang (PIB) dan Pemberitahuan Ekspor Barang (PEB). Implementasi ini meliputi Bea Cukai, importir, eksportir dan bank. Untuk mendukung implementasi EDI Pabean/ Pelabuhan di perbankan tersebut, dibuat Modul Bank berbasis Window. Dengan sistem EDI, administrasi pabean dapat memproses pemberitahuan pabean dalam sistem komputer para pengguna jasa pabean antara lain perusahaan pelayaran, importir, eksportir, dan Pengusaha Pengurusan Jasa Kepabeanan (PPJK), dan data-data di *transmit* secara elektronik. Sehingga data yang sama akan segera masuk ke sistem komputer Direktorat Jendaral Bea dan Cukai tanpa melalui proses *re-entry,* dimana dalam proses *re-entry* tersebut mungkin dapat terjadi *human error* seperti kesalahan pengetikan data, selain itu juga menambah waktu pengerjaan.

Penggunaan EDI dalam transaksi tanpa menggunakan dokumen berbahan kertas akan semakin luas. Perubahan sistem ini bukannya tanpa risiko, namun akan muncul risiko hukum, manajemen, teknologi, dan risiko komunikasi data. Dari sisi pengauditan, akan menambah risiko audit terutama risiko pengendalian, yang antara lain risiko keabsahan dokumen elektronik, keamanan data elektronik, keamanan komunikasi data, keamanan kontrak kerja dengan perusahaan provider EDI dan antar pihak pengguna, dan jaminan interkoneksi yang memadai antar pihak yang ada dalam sistem EDI.

Dalam perpektif pengauditan, selama ini pendapat auditor didasarkan pada bukti-bukti audit yang berupa kertas (*paper based)* baik berupa dokumen-dokumen maupun *print-out* komputer. Akibat perkembangan teknologi informasi maka dokumen-dokumen pendukung berupa kertas (*paper base*d) akan semakin ditinggalkan, dan transaksi-transaksi dalam aktivitas bisnis akan menuju transaksi tanpa kertas *(paperless based)*. Bagi auditor keabsahan dokumen menjadi faktor penting dalam memperoleh kesimpulan terhadap keandalan data, dan dari sisi perundangan keabsahan dokumen elektronik belum sepenuhnya dapat diterima oleh para penegak hukum. Artikel ini dibuat untuk mendeskripsikan dampak transaksi elektronik terhadap tuntutan kebutuhan bukti audit.

TINJAUAN TEORITIS

Pengertian EDI

EDI menggunakan komunikasi antar komputer dengan tujuan meningkatkan efektivitas dan mengurangi pekerjaan yang sifatnya klerikal. Bodnar (1999) mendefinisikan EDI sebagai pergerakan dokumen bisnis dalam format terstruktur antar mitra bisnis dari suatu organisasi. Romney (2003) mendefinisikan EDI sebagai berikut. "*Electronic Data Interchange (EDI) is a standard protocol for electronically transfering information between organization and across bisnis processes."* Secara formal, EDI didefinisikan oleh *International Data Exchange Association (IDEA*) sebagai "transfer data terstruktur dengan format standard yang telah disepakati, yang dilakukan dari satu sistem komputer ke sistem komputer lain dengan menggunakan media elektronik".

Tujuan utama dari pemakaian teknologi EDI, sebenarnya adalah agar teknologi ini dapat membantu para pelaku bisnis mengkomunikasikan dokumennya dengan pihak lain secara cepat, akurat dan efisien, serta untuk mengurangi pemakaian kertas dan biaya-biaya lain yang timbul pada metode konvensional.

Dokumen Standar EDI

Di dalam suatu transaksi bisnis yang menggunakan EDI akan terjadi pertukaran dokumen elektronik - dari satu aplikasi komputer kepada aplikasi komputer yang lain - dengan suatu format yang terstruktur. Dokumen elektronik diatur dalam dua format yaitu dengan standard *American National Standards Institute (ANSI)-XI2*, yang banyak digunakan di wilayah Amerika, dan standard berdasarkan *UNEDIFACT (United Nations Electronic Document Interchange for Administration, Commerce and Transport*). Dalam lingkungan Direktorat Jendral Bea dan Cukai, dokumen-dokumen PIB yang dipertukarkan melalui jaringan EDI merupakan dokumen dalam format *United Nation Electronic Data Interchange for Administration, Commerce, and Transport* (UNEDIFACT) yaitu:

1. *Customs Conveyance Report Message* (CUSREP) merupakan dokumen elektronik mengenai rencana kedatangan sarana pengangkut yang diajukan oleh Perusahaan Pelayaran kepada Bea dan Cukai.
2. *Customs Cargo Report Message* (CUSCAR) adalah dokumen elektronik mengenai kargo yang dimuat dalam sarana pengangkut (manifest) yang dilaporkan oleh Perusahaan Pelayaran kepada Bea dan Cukai.
3. *Customs Declaration Message* (CUSDEC) adalah dokumen elektronik mengenai barang yang akan dilepas dari pengawasan pabean, seperti PIB yang diajukan importer atau kuasanya kepada Bea dan Cukai.
4. *Customs Response Message* (CUSRES) adalah dokumen yang merupakan tanggapan dari Bea dan Cukai atas diterimanya CUSREP, CUSCAR, dan CUSDEC. Tanggapan ini dapat berupa pemberian nomor registrasi, penetapan jalur pemeriksaan, atau persetujuan pengeluaran barang.

Disamping dokumen tersebut di atas, dalam kaitannya dengan EDI di bidang kepabeanan terdapat juga beberapa dokumen standar yang akan dipertukarkan yaitu dokumen yang berkaitan dengan pemenuhan pembayaran bea masuk dan PDRI. Mengingat sistem pembayaran bea masuk dapat dilakukan melalui Bank Devisa Persepsi, maka transaksi elektronik ini melibatkan perbankan. EDI dalam sistem pembayaran dikenal dengan *Electronic Fund Transfer* (EFT), yang meliputi:

1. *Payment Order* (PAYROD) adalah dokumen elektronik yang berisi perintah dari pengguna jasa kepabeanan (importer) kepada bank untuk membayar bea masuk dan PDRI ke Kas Negara
2. *Debit Advice* (DEBADV) merupakan dokumen elektronik yang berisi informasi dari bank kepada importer yang menyatakan bahwa rekening *importer* telah didebet sebesar uang yang tertera dalam *payment order* untuk pembayaran bea masuk dan PDRI.
3. *Credit Advice* (CREADV) adalah dokumen elektronik yang berisi informasi dari bank kepada Kantor Perbendaharaan dan Kas Negara serta Bea dan Cukai yang menyatakan bahwa pada rekening kas Negara telah dikreditkan sejumlah uang untuk pembayaran bea masuk dan PDRI atas barang yang diimpor oleh importer.

Komponen Sistem EDI

Dalam struktur EDI terdapat tiga atau empat komponen utama yaitu: pertama aplikasi bisnis dan alat penghubung (*interface*), kedua proses penterjemahan (*translation*), ketiga alat penghubung komunikasi *(interface communication)*, dan VAN (*Vale Added Network).*
Dalam sistem EDI kepabeanan di lingkungan Direktorat Jendral Bea dan Cukai, terdapat lima komponen

utama yang diperlukan untuk menjalankan sistem pertukaran dokumen secara elektronik, yaitu:

1. Aplikasi *In-House* pengguna sistem EDI, yang terdiri dari:
    a. Aplikasi *in-house* Bea dan Cukai, yaitu aplikasi sistem pelayanan pabean yang dikenal dengan sebutan *Customs Fast Release System* (CFRS) yang merupakan aplikasi utama yang akan mengolah data yang terkait dengan kegiatan impor barang.
    b. Aplikasi i*n-house* pengguna jasa kepabeanan, yaitu aplikasi yang dipergunakan oleh pengguna jasa kepabeanan untuk menyiapkan data yang diperlukan oleh bea dan cukai. Disamping itu aplikasi ini juga berfungsi untuk merekam dan mengolah data yang diterima dari Bea dan Cukai yang berkaitan dengan proses impor.
2. Aplikasi *interface* pengguna sistem EDI Kepabeanan, yang terdiri dari:
    a. *Translator*, yang berfungsi untuk menterjemahkan informasi dari apliksi *in-house* yang akan dikirimkan kepada mitra bisnis menjadi data dokumen standar EDI, atau sebaliknya yaitu menterjemahkan dokumen standar EDI yang diterima dari mitra bisnis menjadi informasi yang dimengerti oleh aplikasi *in-house*.
    b. Pengendali Komunikasi Data, yang berfungsi untuk mengendalikan pengiriman maupun penerimaan dokumen kepada atau dari mitra bisnis.
    c. Aplikasi Mapper, yang berfungsi untuk mendukung translator membaca data dalam format *in-house* dan menerjemahkan menjadi standar EDI, atau sebaliknya.
    d. Aplikasi Integrasi Sistem, yang dipergunakan untuk memasukkan data yang akan dikirim dari sistem *in-house* ke translator, atau sebaliknya.
3. Jaringan EDI (*EDI Network*), sebagai sarana pertukaran dokumen secara elektronik dengan mitra bisnis.
4. Sistem Komputer dan Komunikasi Data, merupakan proses pengolah data untuk membantu pengguna dalam melakukan pengiriman dan penerimaan data (modem).
5. Fasilitas Telekomunikasi, merupakan sarana dasar yang menghubungkan para mitra bisnis yang terlibat dalam pertukaran dokumen secara elektronik. Data PIB yang diinput melalui PIB-EDI disimpan dalam suatu format *in-house database*, kemudian data dibentuk ke dalam format EDI dengan menggunakan translator EDI.

Translator EDI yang digunakan untuk pengoperasian PIB-EDI adalah *Intercept-Plus (I-Plus)*. *Intercept-Plus* adalah suatu perangkat lunak EDI yang memiliki fungsi sebagai:

1. *Translator* EDI
2. Mengubah data dalam bentuk *in-house* format ke dalam bentuk UNEDIFACT
3. Modul Komunikasi
4. Melakukan koneksi dengan jaringan EDI untuk mengirim atau menerima dokumen

EDI DAN IMPLIKASINYA PADA AUDIT

Teknologi Informasi dan Audit

Pada dasarnya tidak terdapat perbedaan konsep audit untuk sistem komputerisasi yang kompleks dan sistem manual. Perbedaannya hanya terletak pada metode penangangan yang dipandang sesuai dengan sistem informasi akuntansi yang ada, terutama dalam rangka mendapatkan pemahaman internal control untuk keperluan perencanaan audit yang mencakup penentuan sifat, saat dan luas pengujian yang akan dilakukan.

Statement on Auditing Standar (AICPA) dan Standar Profesional Akuntan Publik (IAI) telah mengatur masalah ini. Beberapa elemen dalam standar audit tersebut mengatur tata cara audit dalam lingkungan system informasi berbasis komputer. Prinsip dasar tugas auditor dalam melaksanakan audit laporan keuangan adalah: 1). Melaksanakan uji kepatuhan terhadap prosedur yang berlaku, baik prosedur manual maupun prosedur berbasis komputer 2). Melaksanakan uji substantif atau pengujian terhadap output proses akuntansi dan 3). Mengolah dan menyimpulkan hasil pengujian. Jenis dan luas pengujian tidak tergantung pada ukuran perusahaan atau ukuran volume transaksi, melainkan ditentukan oleh kompleksitas lingkungan TI yang ada, seperti intensitas sistem *on-line* yang digunakan, tipe dan signifikansi transaksi keuangan, sifat dokumen/*database*, serta program yang digunakan.

Implikasi EDI Terhadap Pelaksanaan Audit

Sistem EDI mengakibatkan kebutuhan pengendalian atas sistem komputer menjadi lebih besar, dan hal ini jelas berimplikasi besar terhadap proses pelaksanaan audit. Di dalam suatu lingkungan non-EDI, pengauditan lebih banyak dilaksanakan dengan pendekatan *around the computer*. Dalam lingkungan EDI, auditor tidak bisa melakukan audit "*around the computer*" sebab arus catatan/kertas/bukti transaksi yang masuk ke dalam dan ke luar dari komputer dilaksanakan secara elektronik.
Dalam lingkungan sistem EDI auditor dapat menggunakan komputer untuk mengidentifikasi dan mengambil data atau mengembangkan program rutin untuk mengidentifikasi transaksi yang tidak lazim atau yang salah. Auditor juga dimungkinkan untuk mendapatkan salinan data yang asli dari klien untuk selanjutnya diproses sendiri dan kemudian dibandingkan dengan hasil pemrosesan menurut klien.

Kecepatan auditor memperoleh data transaksi akan berpengaruh atas proses audit. Dengan sistem EDI, waktu yang diperlukan untuk suatu pengujian siklus transaksi akan berkurang dan akan berdampak pada saldo komponen-komponen dalam laporan keuangan. Transaksi utang piutang menjadi sangat cepat (*real time)*, begitu muncul utang dengan otomatis akan dilakukan pembayaran dengan mengurangi saldo rekening bank melalui *e-banking* yang *on line* dengan sistem EDI. Dampaknya, saldo utang/piutang menjadi sangat kecil sehingga prosedur audit tradisional seperti konfirmasi mungkin tidak perlu dilakukan karena saldo piutang dan hutang menjadi sangat kecil dan tidak material.

Dengan semakin luasnya implementasi EDI, muncul tuntutan bagi auditor untuk meningkatkan ketrampilan mereka dalam bidang teknologi informasi. Auditor harus mengenal baik berbagai aspek operasi bisnis berbasis TI, mulai dari aspek pengendalian, aspek hukum, aspek operasi bisnis, aspek keaslian data, aspek *data encryption*, dan aspek EDI serta pemrosesan data berbasis TI secara umum.

Sifat Bukti Audit

Dalam standar auditing, standar pekerjaan lapangan ketiga mengharuskan auditor untuk mengumpulkan bukti kompeten dalam jumlah yang cukup untuk mendukung pendapat yang diberikan. Empat faktor yang menentukan apakah suatu bukti dapat untuk mendukung kesimpulan adalah:

1. **Relevansi**, bukti audit harus berkaitan atau relevan terhadap tujuan audit
2. **Kompetensi,** bukti dianggap kompeten akan membantu auditor meyakinkan bahwa laporan keuangan disajikan dengan wajar. Lima karakteristik bukti yang kompeten adalah sebagai berikut.
   a. Suber bukti, bukti dari pihak luar perusahaan akan lebih andal daripada bukti dari dalam

perusahaan.

b. Efektifitas struktur pengendalian intern, jika struktur pengendalian intern perusahaan klien sangat efektif, bukti yang diperoleh akan lebih dapat diandalkan.
c. Tingkat pemahaman auditor atas bukti, bukti yang diperoleh langsung oleh auditor, misalnya hasil pemeriksaan fisik oleh auditor, hasil pengamatan, hasil perhitungan, dan hasil inspeksi akan lebih kompeten daripada bukti tidak langsung.
d. Kualifikasi orang yang menyediakan informasi, penyedia informasi harus memiliki kompetensi yang cukup agar bukti audit dapat dikatakan andal.
e. Tingkat obyektifitas, bukti yang obyektif akan lebih andal daripada bukti yang masih memerlukan pertimbangan apakah bukti tersebut benar atau tidak. Misalnya jawaban konfirmasi bank, jawaban konfirmasi kantor pengacara.

3. **Kecukupan bukti**, menyangkut jumlah bahan bukti yang diperoleh akan mentukan kecukupan bukti. Jumlah diukur dengan besar sample yang dipilih auditor. Pada perusahaan yang pengolahan datanya terkomputerisasi, auditor dapat menggunakan software audit untuk mengambil seluruh data yang ada, dan kemudian melakukan pengujian atas data keseluruhan dalam waktu singkat. Jadi sample data jumlahnya sama dengan populasi data (seluruh data diuji).
4. **Ketepatan waktu**, berkaitan dengan kapan bahan bukti dikumpulkan berkaitan dengan periode yang di audit. Pada perusahaan yang pengolahan informasi keuangannya telah terkomputerisasi, biasanya tanggal file tercantum dalam direktori/folder/ file bersangkutan, sehingga dapat secara mudah auditor meng copy file yang diperlukan sesuai periode yang diaudit.

Bukti Audit

Masalah bukti transaksi adalah penting dalam lingkungan EDI. Auditor merasa nyaman dengan jejak audit pada *paper-based* dimana auditor dapat memperoleh bukti-bukti tertulis pada kertas. Untuk mencapai manfaat penuh dari sistem EDI, maka catatan berupa kertas dihapuskan. Auditor perlu memahami sistem EDI secara mendalam dalam rangka menentukan jenis, ketersediaan dan lokasi bukti. Jika tingkat kepercayaan tidak bisa disandarkan pada pengendalian intern, maka diperlukan format/ teknik yang baru yang dapat memberikan suatu pembuktian (evidential matter) seperti Teknik Audit Berbantuan Komputer (CAATs). CAATs bisa menyediakan beberapa format bukti secara efisien.

Keamanan Data

Faktor keamanan data pada transaksi elektronik merupakan pokok kekhawatiran utama para pelaku bisnis karena. Salah satu cara untuk mengamankan data adalah dengan *Symetric Cryptograph*y dimana digunakan kunci yang dipakai bersama oleh pengirim data dan penerima data. Kriptografi juga memenuhi kebutuhan umum suatu transaksi dalam hal:

1. Kerahasiaan (*confidentiality*) data.
2. Keutuhan (*integrity*) data.
3. Jaminan keabsahan (*authenticity*) data dan keotentikan data dengan fasilitas tanda tangan digital (*digital signature*).
4. Transaksi dapat dijadikan barang bukti yang tidak bisa disangkal (*non-repudiation*) dengan memanfaatkan tanda tangan digital dan sertifikat digital.

Faktor keamanan data transaksi menjadi perhatian utama dalam pengujian pengendalian oleh

para auditor. Pengamanan data dilakukan untuk melindungi data dari resiko penyingkapan/akses-akses yang tidak sah (tidak di otorisasi), pengubahan atau penghilangan data, pengamanan dilakukan seperti halnya perlindungan perangkat lunak dan perangkat keras.

Otorisasi dan Keaslian Transaksi

Auditor dalam melakukan pengauditan berdasar pada transaksi-transaksi yang telah dijamin keabsahannya dan keasliannya. Otorisasi dan keabsahan suatu transaksi merupakan hal yang krusial dalam suatu transaksi, oleh karenanya pengendalian secara otomatis di dalam suatu otorisasi elektronik, dan pengendalian atas akses phisik maupun akses logik pada suatu sistem EDI, mutlak diperlukan. Pemberian otorisasi harus dikenali secara unik oleh sistem dan dapat dibuktikan keasliannya oleh sistem. Salah satu metode yang digunakan adalah dengan menggunakan kode pengesahan pesan (*Message Authentication Codes atau MAC*). MAC adalah suatu kode yang dapat memverifikasi bahwa data tidak diubah.

Kebutuhan akan pengendalian yang kuat terhadap akses merupakan hal yang tidak mudah, karena ada peningkatan risiko yang disebabkan penggunaan jaringan publik dan menerima transaksi-transaksi dari luar dalam penggunaan EDI. Sekali link komunikasi diterapkan dengan menggunakan jaringan EDI dengan partner bisnis, maka partner bisnis akan menerima data-data dari luar melalui suatu lingkungan teknologi informasi. Risiko yang akan muncul adalah ancaman akses-akses data yang tidak di otorisasi atas data dan program melalui fasilitas jaringan komunikasi, software, dan interface aplikasi.

Pengendalian atas "transaksi yang tidak dapat disangkal keberadaannya" (*Non-repudiation*)" merupakan gambaran penting dalam membantu meningkatkan keamanan otorisasi dalam suatu pesan tertentu sehingga tidak terjadi penolakan terhadap suatu transaksi di kemudian hari. Suatu bukti dengan predikat "Tidak dapat disangkal keberadaannya" dapat meyakinkan mitra dagang bahwa sumber pesan dan pesannya dapat diterima dan sah secara kontraktual.

Suatu kunci kriptografi yang digunakan secara umum dalam program (*publik key*), akan mengacak pesan/transaksi yang masuk, dilain pihak penerima pesan/transaksi harus mempunyai kunci encryption (*private-key*) nya untuk menguraikan kembali pesan/transaksi tersebut. Hal ini merupakan satu teknik yang sekarang ini digunakan untuk pengirim transaksi yang "Tidak dapat disangkal keberadaannya". Berfungsinya program akan meyakinkan para penerima data transaksi yang bersifat "Tidak dapat disangkal keberadaannya". Oleh sebab itu penting bagi mitra dagang dilingkungan EDI dalam membuat persetujuan untuk memasukkan unsur-unsur yang diperlukan untuk membuktikan keaslian suatu transaksi.

***Backup and Recovery* Data**

Perhatian auditor juga mengarah kepada sistem backup dan recovery data-data transaksi untuk menilai kehandalan struktur pengendalian intern yang ada. Dengan sistem EDI, suatu organisasi sangat bergantung pada jaringan sistem komputernya dan sistem jaringan dari partner bisnisnya serta sistem jaringan dari pihak ketiga. Perlu ditetapkan prioritas tindakan jika terjadi kegagalan sistem, rencana pemulihan harus mengidentifikasi program aplikasi mana saja yang diperlukan agar organisasi tetap dapat berjalan, dan juga hardware dan software yang dibutuhkan untuk mendukungnya, serta urutan dan penetapan waktu bagi aktivitas pemulihan.

Backup file data and program, prosedur-prosedur untuk berjaga-jaga dari ketidakpastian yang mungkin terjadi, meminimalkan *downtime*, dan perencana kelangsungan bisnis kedepan dari semua mitra bisnis, semuanya dilakukan dengan menetapkan prioritas tindakan ketika terjadi kegagalan sistem yang berpengaruh terhadap semua siklus bisnis para mitra yang terkait dengan siklus bisnisnya sendiri.

Jejak Audit (*Audit Trail*)

EDI biasanya digunakan untuk menggantikan sistem pencatatan dengan menggunakan kertas sebagai media pencatatan (*paperbased system*), hal ini akan mengakibatkan hilangnya jejak audit yang tercetak pada kertas bukti audit sehingga akan menimbulkan kesukaran dalam melakukan verifikasi secara manual. Namun demikian hal ini tidak berarti hilangnya atau melemahnya suatu sistem pengendalian. Isu kunci dalam audit di lingkungan EDI adalah apakah transaksi, file elektronik atau catatan berupa kertas, dapat bersertifikat atau sah sebagai suatu arsip yang terjaga ke-otentikannya dari transaksi yang terjadi. Oleh karena itu, sistem pengendalian arsip elektronik harus dapat memastikan bahwa data tidak bisa diubah, hal ini merupakan bagian yang kritis dalam audit. Misalnya, menyimpan pesan transaksi EDI dalam bentuk tidak bisa di ubah (*read only).*

Jejak audit adalah hal penting untuk membuat seseorang harus bertanggungjawab atas tindakannya. Dalam banyak sistem EDI jejak audit yang lengkap mungkin ada untuk hanya suatu jangka waktu pendek di dalam komputer dalam format yang dapat dibaca. Jika tidak dikendalikan dengan baik, tidak cukupnya catatan/arsip bisa mengancam kemampuan audit pada sistem EDI.

Bukti Audit Dari Sisi Hukum

Di Indonesia sampai saat ini sistem pembuktian hukum privat masih mengunakan ketentuan yang diatur di dalam KUHPer, HIR (untuk Jawa Madura) dan RBg (untuk luar Jawa Madura). Dalam hukum pembuktian ini, alat-alat bukti dalam perkara perdata terdiri dari: bukti tulisan, bukti saksi-saksi, persangkaan-persangkaan, pengakuan dan bukti sumpah (ps.1866 KUHPer atau 164 HIR). Sementara itu, dengan pesatnya Tekonologi Informasi melalui internet telah mengubah berbagai aspek kehidupan, diantaranya mengubah kegiatan perdagangan yang semula dilakukan dengan cara kontak fisik, saat ini dilakukan secara elektronik dalam bentuk *Electronic Commerce* atau *E-Commerce* atau dalam Bursa Efek dikenal dengan *online trading.* Keadaan tersebut belum mendapat pengaturan dalam sistem hukum pembuktian, karena sampai saat ini hukum pembuktiannya masih menggunakan ketentuan hukum yang lama (KUHPer,HIR, dan RBg). Namun demikian, keberadaan Undang-undang No.8 Tahun 1997 tentang Dokumen Perusahaan (UU Dokumen Perusahaan) telah mulai menjangkau ke arah pembuktian data elektronik.

UU Dokumen Perusahaan memang tidak mengatur masalah pembuktian, namun UU ini telah memberi kemungkinan kepada dokumen perusahaan mendapat kedudukan sebagai alat bukti tertulis otentik untuk diamankan melalui penyimpanan dalam mikro film. Selanjutnya, terhadap dokumen yang disimpan dalam bentuk elektronik *(paperless)* ini dapat dijadikan sebagai alat bukti yang sah. Di samping itu dalam ps.3 UU Dokumen Perusahaan telah memberi peluang luas terhadap pemahaman atas alat bukti, yaitu: “dokumen keuangan terdiri dari catatan, bukti pembukuan, dan data pendukung administrasi keuangan, yang merupakan bukti tentang adanya hak dan kewajiban serta kegiatan usaha perusahaan”. Selanjutnya, ps.4 UU tersebut menyatakan: “dokumen lainnya terdiri dari data atau setiap tulisan yang berisi keterangan yang mempunyai nilai guna bagi perusahaan meskipun tidak

terkait langsung dengan dokumen perusahaan".
Dari perspektif hukum, digital *signature* adalah sebuah pengaman pada data digital yang dibuat dengan kunci tanda tangan pribadi (*private siganture key*), yang penggunaannya tergantung pada kunci publik (*public key*) yang menjadi pasangannya. Eksistensi digital *signature* ini ditandai oleh keluarnya sebuah sertifikat kunci tanda tangan (*signature key certificate*) dari suatu badan pembuat sertifikat (*certifier*). Dalam sertifikat ini ditentukan nama pemilik kunci tanda tangan dan karakter dari data yang sudah ditandatangani, untuk kekuatan pembuktian (German Draft Digital signature Law, 1996).

Beberapa masalah yang mungkin timbul dari sistem digital *signature* ini terkait dengan sistem hukum yang sudah ada. Pada banyak negara, disyaratkan bahwa suatu transaksi harus disertai dengan bukti tertulis, dengan pertimbangan kepastian hukum. Permasalahannya, bagaimana sebuah dokumen elektronik yang ditandatangani dengan sebuah digital *signature* dapat dikategorikan sebagai bukti tertulis? Di lnggris, bukti tertulis haruslah berupa tulisan *(typing),* ketikan *(printing),* litografi *(lithography),* fotografi, atau bukti-bukti yang mempergunakan cara-cara lain, yang dapat memperlihatkan atau mengolah kata kata dalam bentuk kasat mata. Definisi dari bukti tertulis itu sendiri sudah diperluas hingga mencakup juga "telex, telegram, atau cara-cara lain dalam telekomunikasi yang menyediakan rekaman dan perjanjian" (*UNCITRAL Model Law on Internatinal Commercial Arbitration, art.7 (2)).*

Sebenarnya, dari fakta-fakta tersebut dapat ditarik kesimpulan bahwa dokumen elektronik yang ditandatangani dengan sebuah digital *signature* dapat dikategorikan sebagai bukti tertulis. Tetapi, terdapat suatu prinsip hukum yang menyebabkan sulitnya pengembangan penggunaan dokumen elektronik atau digital *signature*, yakni adanya syarat bahwa dokumen tersebut harus dapat di lihat, dikirim dan disimpan dalam bentuk kertas.

Masalah lain yang dapat timbul berkaitan dengan dokumen elektronik dan digital *signature* adalah masalah cara untuk menentukan dokumen yang asli dan dokumen salinan. Berkaitan dengan hal ini sudah menjadi prinsip hukum umum bahwa:

a. dokumen asli harus dalam bentuk perjanjian tertulis yang ditandatangani oleh para pihak yang melaksanakan perjanjian;
b. dokumen asli hanya ada satu dalam setiap perjanjian; dan
c. semua reproduksi dari perjanjian tersebut merupakan salinan.

Pengujian Terhadap Pengendalian

Pengujian pengendalian dilakukan dengan mengidentifikasi aktivitas control (*policy dan procedure)* yang ada untuk mencegah dan mendeteksi salah saji material dalam laporan keuangan. Dua aktivitas utama yang diuji adalah pengendalian pemrosesan informasi yaitu *general control* dan *application control*. *General control* terkait dengan semua aktivitas komputer mencakup *system development*, *access security*, *program change*, *data center*, *network*, dan *maintenance*. *Aplication control* berhubungan dengan *specific task* yang dijalankan suatu sistem aplikasi, termasuk prosedur cek dengan TI misalnya *edit check* saat input data..

Pengujian pengendalian bertujuan untuk mengumpulkan bukti tentang seberapa efektif dan konsisten suatu prosedur pengendalian berjalan. Pengujian ini dilakukan dengan wawancara, inspeksi dokumen terkait atau inspeksi file elektronik terkait, observasi penerapan pengendalian dan pemrosesan ulang transaksi. Dalam merancang pengujian *automated control (computerised control dan application control*), auditor harus mempertimbangkan kebutuhan untuk mendapatkan bukti pendukung atas

efektifitas pengendalian operasi secara langsung maupun tak langsung terkait dengan asersi atas laporan keuangan. Teknik yang digunakan untuk pengujian tentu saja berbeda dengan teknik pengujian manual.

Telekomunikasi

Saluran komunikasi yang dapat digunakan untuk berkomunikasi adalah standard telephone lines, coaxial cable, fiber optics, microwave systems, communications satellites, cellular radio and telephone. Sedangkan konfigurasi jaringan yang dapat dipakai untuk berkomunikasi adalah Wide Area Network (WAN), Local Area Network (LAN), dan Client/Server Configurations (Romney, 2000).
Pengendalian terhadap transmisi data perlu ditekankan untuk mengurangi risiko kegagalan transmisi data, perusahaan harus memantau jaringan untuk mendeteksi titik lemah, memelihara cadangan komponen, dan merancang jaringan sedemikian rupa sehingga kapasitas yang tersedia cukup untuk menangani periode padat pemrosesan data. Perusahaan juga harus menetapkan jalur komunikasi ganda antar komponen dalam jaringan, sehingga sistem tetap dapat berfungsi meskipun salah satu jalurnya tidak berfungsi. Selain itu, dengan pemeliharaan preventif, perusahaan dapat meningkatkan kapasitas saluran telekomunikasi yang digunakan saat ini menjadi lebih cepat dan lebih efisien, memiliki lebih sedikit problem, dan lebih sedikit kemungkinan gagal.
Kesalahan transmisi data dapat diminimumkan dengan menggunakan *data encription* (melindungi data yang ditransmisi agar tidak dimonitor pihak lain), *routing verification* (memastikan data yang ditransmisi tidak salah alamat), *parity checking* (mendeteksi kesalahan karena hilangnya bit selama proses transmisi data), dan *message acknowledgement procedures* (konfirmasi dari penerima bahwa data telah diterima untuk dicocokkan).

KESIMPULAN

Berbisnis dengan berbasis EDI, harus mempertimbangkan resiko yang akan muncul yaitu adanya kelemahan-kelemahan pengendalian terhadap transaksi-transaksi dengan mitra dagang atau jaringan komunikasi dari pihak ketiga, didalam perjanjian kerjasama penggunaan EDI. Mitra dagang dan jaringan komunikasi perdagangan, harus tunduk dan mengikuti aturan audit pengendalian intern yang ada dari masing-masing mitra, dan hal itu secara teknis harus dipastikan oleh pihak independen yang secara teknis memiliki kompetensi dalam bidang tersebut, dengan tujuan untuk memastikan bahwa pengendalian yang cukup telah dilakukan.

Bagi auditor hal tersebut diperlukan untuk memperoleh kepercayaan atas hasil audit pihak ketiga. Klausul-klausul penting yang harus dicantumkan dalam perjanjian perdagangan antara lain: hak untuk mengaudit atau menerima laporan audit dari pihak ketiga, keharusan untuk memberitahu adanya kegagalan secara cepat, dan kelemahan yang signifikan lainnya di dalam sistem yang harus dicantumkan dengan jelas serta dinyatakan di dalam perjanjian perdagangan tersebut.

Perjanjian bisnis dalam lingkungan EDI, dengan masing-masing mitra dagang dan perjanjian penggunaan jaringan dengan pihak ketiga, merupakan mekanisme kunci yang digunakan untuk mengelola resiko. Perjanjian tersebut harus mencatumkan berbagai masalah teknis dan operasional yang berkaitan dengan jaringan. Perjanjian tersebut harus ditelaah oleh penasehat hukum perusahaan, dan pada batas minimum, berkenaan dengan penetapan aturan main, tanggung-jawab, terminologi, standard, kepemilikan data, hak mengaudit, dan pertimbangan aspek-aspek hukum lain pada saat

transaksi dikirimkan keluar negeri atau keluar wilayah hukum tertentu.

EDI adalah suatu teknologi baru yang didalam penerapannya akan mengubah cara melakukan bisnis. Bagi para auditor, implementasi EDI memerlukan kehati-hatian dalam melakukan evaluasi atau re-evaluasi, dalam melakukan penyesuaian-penyesuaian, dan dalam pendekatan audit. EDI memperkenalkan isu dan resiko yang berbeda tetapi menyediakan tantangan baru dan kegairahan baru baik untuk organisasi perusahaan dan maupun auditor nya.

Auditor dimasa yang akan datang lebih berorientasi pada strategi audit yang mengutamakan pengendalian (*lower level of control risk too low*), pemahaman risiko bisnis klien yang lebih komprehensif, dan prosedur analitis (*analytical Procedures*), menjadi pendekatan utama para auditor. Selain kemampuan di bidang teknologi informasi, auditor di tuntut memahami aspek hukum yang berhubungan dengan informasi terkait dengan keabsahan suatu bukti.

Dalam aspek pengendalian, auditor harus lebih memperhatikan aspek teknis dalam perjanjian penggunaan EDI antar dua pihak terkait, apakah aspek-apek teknis yang terkandung dalam perjanjian tersebut telah dilaksanakan klien.

DAFTAR PUSTAKA

Ashead, John (2004). *Principal EDI and Paperless Auditing.* Informatics and Consulting Office of the Auditor General. Ottawa Ontario. Canada.

Arens, Alvin A (1980). *Auditing An Integrated Approach.* Prentice Hall,Inc.. Englewood Cliffs. New Jersey.

Glenn L. Helms, and Jane Mancino (1999). "Electronic Auditor". A&M University, Corpus Christi, Texas. www.tetranet.net.

Ikatan Akuntan Indonesia (1994). "Standar Profesional Akuntan Publik". Sekolah Tinggi Ilmu Ekonomi YKPN. Yogyakarta.

Leng, Pwee (2003). "Evaluasi *Pilot Project Electronic Data Interchange (*EDI) di Bidang Kepabeanan". Studi Kasus pada Kantor Pelayanan Bea dan Cukai (KPBC) Tanjung Perak. Surabaya.

Ikatan Akuntan Indonesia (1999). "Standar Akuntansi Keuangan". Salemba Empat, Jakarta.

Jusup, Al.Haryono (2001). *Auditing (pengauditan).* Sekolah Tinggi Ilmu ekonomi YKPN. Yogyakarta.

Romney, Marshall. Steinbart, John Paul (2003). *Accounting Information Systems*. Nineth Edition. Prentice Hall.