DAMPAK TEKNOLOGI INFORMASI TERHADAP AUDIT LAPORAN KEUANGAN

Islahuzzaman
Universitas Widyatama
islahst1@yahoo.co.id

ABSTRAK

Ketika perusahaan masih kecil, audit laporan keuangan dapat dilakukan secara manual. Sejalan dengan pertumbuhan jumlah perusahaan-perusahaan yang menggunakan fasilitas Teknologi Informasi (TI) dalam bisnisnya akan berpengaruh terhadap pelaksanaan audit. Satuan usaha (organisasi/perusahaan) disebut menggunakan sistem TI apabila dalam memproses data penyusunan laporan keuangan menggunakan komputer dari tipe dan jenis tertentu. Baik dioperasikan oleh perusahaan sendiri atau pihak lain. Kebutuhan terhadap auditing TI semakin perlu untuk dipenuhi agar tujuan auditing tetap dapat dicapai secara efektif dan efisien. Meskipun tujuan dasar auditing tetap tidak berubah, tapi proses audit mengalami perubahan yang signifikan baik dalam pengumpulan dan evaluasi bukti maupun pengendaliannya. Hal ini disebakan karena adanya perubahan dalam pemrosesan data akuntansi. Auditor harus pula memiliki pengetahuan pengolahan data elektronik memadai untuk menerapkan prosedur audit laporan keuangan. Makalah ini akan menjelaskan bagaimana dampak TI terhadap proses audit.

Kata Kunci: Teknologi informasi, audit laporan keuangan

1 PENDAHULUAN

Masalah TI dalam audit muncul ketika perusahaan yang akan diaudit menggunakan TI dalam proses transaksi mereka sampai kepada penyusunan laporan keuangan. Sebagian besar entitas, termasuk perusahaan keluarga berukuran kecil, mengandalkan TI untuk mencatat dan memroses transaksi bisnis. Akibat kemajuan TI yang luar biasa, perusahaan yang relatif kecilpun bahkan menggunakan komputer pribadi dengan perangkat lunak akuntansi komersial untuk menjalankan fungsi akuntansinya. Ketika perusahaan tumbuh dan semakin membutuhkan informasi, perusahaan itu biasanya meningkatkan sistem TI-nya. Fungsi akuntansi yang menggunakan jaringan TI yang rumit, Internet, dan fungsi TI terpusat sekarang sudah merupakan hal yang umum.

Namun demikian, pemasangan sistem komputer baru memiliki risiko baru. Kesalahan kecil komputer dapat menimbulkan permasalahan yang besar. Hal ini pernah dialami oleh Hershey's food ketika mulai menjalankan usahanya dengan sistem komputer baru seharga $112 juta pada bulan Juli 1999. Sistem baru itu diharapkan mengotomatisasi segalanya mulai dari pesanan permen hingga

penempatan pallet ke truk. Tetapi sistem itu malah mengacaukan sistem pemesanan serta distribusi, dan beberapa pelanggan tidak bisa mendapatkan permen selama musim Halloween yang penting.

Bagi perusahaan kecil, dampak dari masalah komputer ini bahkan bisa lebih parah. Texas Textbooks gulung tikar pada tahun 2001 setelah permasalahan komputer mempersulit para pelajar untuk menemukan buku yang mereka butuhkam. Kerugian penjualan dan ketidaksenangan pelanggan telah menciptakan suatu spiral penurunan yang tidak pernah bisa dipulihkan oleh perusahaan (Mahoney, 2001).

Guna menilai tingkat kesesuaian penyajian laporan keuangan, seorang auditor harus mengevaluasi *internal control* dan memperoleh bukti-bukti, yaitu segenap informasi yang bisa diperoleh untuk menentukan tingkat kesesuaian tersebut dalam laporan auditing, serta sumber-sumber lain yang dimungkinkan dan dibenarkan.

Salah satu jenis bukti tersebut adalah *file-file* data yang disimpan dalam media perekam data komputer, yang memerlukan komputer dan teknik-teknik khusus untuk membacanya. Secara fisik yang terlihat adalah bentuk dan jenis media penyimpannya (disket, *hardisk*, dan lainnya) yang sama. Pengujian terhadap bukti seperti itu, selain memerlukan komputer juga teknik-teknik pembacaan data, yang bergantung kepada desain aplikasi, bahasa pemograman dan sistem operasi yang sesuai. Seorang auditor, dalam hal tersebut, harus memilki pengetahuan mengenai konsep audit TI, mampu membaca dokumentasi aplikasi, dan bekerjasama dengan pengembang dan pemogram aplikasi tersebut.

Desain sebuah aplikasi disusun berdasarkan atas sasaran pengolahan data, konfigurasi peralatan komputer yang tersedia, kesediaan perangkat lunak, serta wawasan yang dimilki oleh penyusun sistem maupun pemrogramannya, selain sistem pengamanan (sekuriti) yang akan diterapkan. Salah satu saja dari unsus tersebut berbeda, maka dapat dipastikan akan berbeda pula desain aplikasi serta *file* penyimpanan datanya.

Bukti-bukti tersebut merupakan jejak-jejak audit (*audit trails*) yang harus bisa ditelusuri sejak dari sumber asalnya, pengolahan serta penyimpanannya, atau merupakan pembuktian secara terbalik, dimulai dari audit atas akun-akun informasi akhir yang harus memperoleh dukungan dari sumber datanya, yang antara lain dibuktikan dengan bukti-bukti data yang terekam di dalam *file-file* penyimpan data

komputer tersebut. Makalah ini akan menjelaskan bagaimana TI mempengaruhi proses audit laporan keuangan.

2 PEMBAHASAN

Standar Profesional Akuntan Publik (SPAP) SA Seksi 335, Auditing dalam Lingkungan Pengolahan Data Elektronik tentang Keahlian dan kompetensi, menjelaskan:

Paragraf 03:

Bila melaksanakan audit dalam lingkungan pengolahan data elektronik, auditor harus memiliki pemahaman memadai mengenai perangkat keras, perangkat lunak dan sistem pengolahan komputer untuk merencanakan penugasan dan ia harus memahami bagaimana dampak pengolahan komputer untuk merencanakan penugasan dan ia harus memahami bagaimana dampak pengolahan data elektronik terhadap prosedur yang digunakan oleh auditor dalam memperoleh pemahaman dan melakukan prosedur audit, termasuk penggunaan teknik audit berbantuan komputer (*computer-assisted audit techniques*). (IAI, 2001). *Information technology refers to all forms of technology applied to processing, storing, and transmitting information in electronic form* (Lucas, 2000).

Sebelum membahas dampak TI terhadap proses audit mari kita telaah dampak pengendalian teknologi informasi terhadap proses audit dan jejak audit yang semakin berkurang sebagai konsekwensi dari adanya perubahan audit secara manual menjadi audit berbasis TI.

Dampak Pengendalian Teknologi Informasi terhadap Proses Audit

Sebelum menyimpulkan bahwa informasi yang dihasilkan komputer dapat diandalkan auditor harus memahami pengendalian dan proses audit berbasis-komputer tersebut. Penggunaan TI dapat menggantikan proses audit yang dapat terpengaruh oleh kesalahan manusia dengan proses audit yang berbasis komputer. Sebelum auditor mengaudit transaksi berbasis komputer, auditor terlebih dahulu menilai pengendalian atas sistem TI tersebut. Standar auditing menguraikan dua kategori pengendalian atas sistem TI: yaitu pengendalian umum dan pengendalian aplikasi.

Pengendalian Umum

Auditor bertanggung jawab untuk memahami pengendalian internal. Mereka harus mengetahui tentang pengendalian umum dan pengendalian aplikasi, tanpa memperhatikan apakah sistem TI klien kompleks atau sederhana. Pengetahuan tentang pengendalian umum akan meningkatkan kemampuan auditor dalam menilai dan mengandalkan pengendalian aplikasi yang efektif untuk mengurangi risiko pengendalian bagi tujuan audit terkait. Pengendalian umum mempunyai pengaruh pervasif terhadap keefektifan pengendalian aplikasi, sehingga auditor harus mengevaluasi terlebih dahulu pengendalian tersebut sebelum menyimpulkan apakah pengendalian aplikasi sudah efektif.

Pengendalian umum *(general controls)* diterapkan pada semua aspek fungsi TI, termasuk (a) administrasi TI; (b) pemisahan tugas TI; (c) pengembangan sistem, termasuk **pengujian percontohan *(pilot testing)***, yaitu sistem yang baru diimplementasikan pada satu bagian organisasi sementara lokasi lainnya masih terus mengandalkan sistem lama. Atau **pengujian paralel**, yaitu sistem lama dan baru beroperasi secara simultan dalam semua lokasi; (d) keamanan fisik dan *online* atas akses ke perangkat keras, perangkat lunak, dan data terkait; (e) *backup* dan perencanaan kontinjensi atas keadaan darurat yang tak terduga; serta (f) pengendalian perangkat keras. Auditor akan mengevaluasi pengendalian umum untuk perusahaan secara keseluruhan.

Apabila klien mempunyai aplikasi akuntansi yang diproses dalam lingkungan jaringan, auditor harus mempelajari konfigurasi jaringan, termasuk lokasi *server* komputer dan *workstation* yang saling terhubung satu sama lain, perangkat lunak jaringan yang digunakan untuk mengelola sistem, serta pengendalian atas akses dan perubahan program aplikasi serta *file* data yang ada pada *server*. Pengetahuan ini dapat berimplikasi bagi penilaian risiko pengendalian auditor ketika merencanakan audit laporan keuangan dan ketika menguji pengendalian dalam audit pengendalian internal atas pelaporan keuangan.

Jika klien menggunakan sistem manajemen *database,* maka auditor harus memahami perencanaan, organisasi, dan kebijakan serta prosedur klien untuk menentukan seberapa baik sistem itu dikelola. Pemahaman ini dapat mempengaruhi penilaian auditor atas risiko pengendalian dan pendapat auditor tentang keefektifan

pelaksanaan pengendalian internal atas pelaporan keuangan.

Pengendalian Aplikasi

Pengendalian aplikasi *(application controls)* berlaku bagi pemrosesan transaksi, seperti pengendalian atas pemrosesan penjualan atau penerimaan kas. Auditor harus mengevaluasi pengendalian aplikasi untuk setiap kelas transaksi atau akun di mana auditor berencana mengurangi risiko pengendalian yang ditetapkan. Pengendalian aplikasi hanya akan efektif jika pengendalian umum efektif.

Pengendalian aplikasi dirancang untuk setiap aplikasi perangkat lunak dan dimaksudkan untuk membantu perusahaan memenuhi enam tujuan audit yang terkait dengan transaksi. Walaupun beberapa pengendalian aplikasi mempengaruhi satu atau hanya beberapa tujuan audit yang terkait dengan transaksi, kebanyakan pengendalian mencegah atau mendeteksi beberapa jenis salah saji. Pengendalian aplikasi lainnya bersangkutan dengan tujuan saldo akun serta penyajian dan pengungkapan.

Pengendalian aplikasi terdiri dari tiga kategori; *input*, pemrosesan, dan *output*. Walaupun tujuan setiap kategori sama, prosedur untuk memenuhi setiap tujuan itu sangat berbeda. Mari kita telaah masing-masingnya secara lebih terinci.

Pengendalian Input. Pengendalian input dirancang untuk memastikan bahwa informasi yang dimasukkan ke dalam komputer sudah diotorisasi, akurat, dan lengkap. Pengendalian input sangat penting karena sebagian besar kesalahan dalam sistem TI diakibatkan oleh kesalahan memasukkan data, sehingga kesalahan input akan menimbulkan kesalahan output tanpa dipengaruhi oleh mutu pemrosesan informasi. Misalnya antara lain: Otorisasi manajemen atas transaksi, penyiapan dokumen sumber input yang memadai, personil yang kompeten, pengujian validasi atas keakuratan input yang dilakukan komputer, seperti validasi nomor pelanggan terhadap *file* induk pelanggan, dan pengendalian input berbasis-*online* atas aplikasi *e-commerce* di mana pihak eksternal, seperti pelanggan dan pemasok, melaksanakan penginputan transaksi dengan benar.

Untuk sistem TI yang mengelompokkan semua transaksi yang serupa ke

dalam *batch,* penggunaan total *batch* keuangan, total *hash,* dan total perhitungan *record* akan membantu meningkatkan keakuratan serta kelengkapan input.

Pengendalian Pemrosesan. Pengendalian pemrosesan *(processing controls)* mencegah dan mendeteksi kesalahan ketika data transaksi diproses. Pengendalian pemrosesan aplikasi khusus sering diprogram ke dalam perangkat lunak untuk mencegah, mendeteksi, dan mengoreksi kesalahan pemrosesan. Contoh Apakah label internal pada pita *file* induk penggajian sesuai dengan label yang ditunjukkan dalam perangkat lunak aplikasi? Apakah *file* transaksi input penggajian telah disortir per departemen sebelum pemrosesan? Apakah jumlah pembayaran bersih ditambah perhitungan pungutan yang ditahan sama dengan pembayaran kotor untuk keseluruhan penggajian? Apakah pembayaran gaji kotor karyawan melebihi 60 jam atau Rp500.000,00 untuk seminggu? Apakah nomor, nama karyawan, jumlah jam biasa, jumlah jam lembur, nomor departe dan sebagainya, dimasukkan untuk setiap karyawan?

Pengendalian *Output.* Pengendalian *output* berfokus pada mendeteksi kesalahan setelah pemrosesan diselesaikan, bukan pada mencegah kesalahan. Pengendalian *output* yang paling penting adalah review kelayakan data oleh seseorang memahami *output* itu. Para pemakai sering kali dapat mengidentifikasi kesalahan karena mereka mengetahui jumlah yang dianggap benar. Beberapa pengendalian yang biasanya digunakan untuk mendeteksi kesalahan *output* mencakup:

- Merekonsiliasi *output* yang dihasilkan komputer dengan total pengendalian manual.
- Membandingkan jumlah unit yang diproses dengan jumlah unit yang diserahkan untuk pemrosesan.
- Membandingkan sampel *output* transaksi dengan dokumen sumber *input*.
- Memverifikasi tanggal dan waktu pemrosesan untuk mengidentifikasi setiap pemrosesan yang tidak sesuai urutan.

Untuk *output* komputer yang sensitif, seperti cek penggajian, pengendalian dapat ditingkatkan dengan mengharuskan karyawan memperlihatkan identifikasi karyawan sebelum menerima ceknya. Selain itu, akses ke *output* sensitif yang disimpan dalam *file* elektronik atau dikirimkan melalui jaringan, termasuk Internet,

sering kali juga dibatasi dengan kata sandi, ID pemakai, dan teknik enkripsi.

Enam kategori pengendalian umum tersebut di atas mempengaruhi semua fungsi TI. Biasanya auditor mengevaluasi pengendalian umum pada awal audit karena dampaknya terhadap pengendalian aplikasi.

Jejak audit semakin berkurang

Salah saji mungkin tidak terdeteksi dengan meningkatnya penggunaan TI akibat hilangnya jejak audit yang nyata, termasuk berkurangnya keterlibatan manusia. Selain itu, komputer juga menggantikan jenis otorisasi tradisional dalam sistem TI.

Visibilitas jejak audit. Karena sebagian besar informasi dimasukkan secara langsung ke dalam komputer, penggunaan TI sering kali mengurangi atau bahkan meniadakan dokumen dan catatan sumber yang memungkinkan organisasi untuk menelusuri informasi akuntansi. Dokumen dan catatan tersebut disebut jejak audit. Karena hilangnya jejak audit, pengendalian lainnya harus dimasukkan untuk menggantikan kemampuan tradisional dalam membandingkan informasi *output* dengan data salinan yang tercetak.

Keterlibatan manusia yang berkurang. Dalam sistem TI, karyawan yang terlibat dengan pemrosesan awal transaksi tidak pernah melihat hasil akhirnya. Karena itu, mereka kurang mampu mengidentifikasi salah saji pemrosesan. Walaupun mereka melihat *output* akhir, sering kali sulit untuk mengenali salah saji karena hasilnya sering sangat ringkas. Selain itu, karyawan juga cenderung memperhatikan *output* yang dihasilkan melalui penggunaan teknologi sebagai "benar" karena dihasilkan oleh komputer.

Tidak adanya otorisasi tradisional. Sistem TI yang sangat canggih sering memprakarsai jenis transaksi tertentu secara otomatis, seperti penghitungan bunga atas rekening tabungan di bank dan pemesanan persediaan apabila tingkat pesanan yang ditentukan sebelumnya telah dicapai. Karena itu, otorisasi yang tepat bergantung pada prosedur perangkat lunak dan keakuratan *file* induk yang digunakan untuk membuat keputusan otorisasi.

Karena pengendalian umum mempengaruhi tujuan audit dalam beberapa siklus, maka jika pengendalian umumnya tidak efektif, kemampuan auditor dalam menggunakan pengendalian aplikasi untuk mengurangi risiko pengendalian pada

semua siklus akan berkurang. Sebaliknya, jika pengendalian umum efektif, kemampuan auditor dalam menggunakan pengendalian aplikasi pada semua siklus akan meningkat. Sebagai contoh, untuk mencegah pembayaran kepada karyawan fiktif, auditor dapat membandingkan nomor identifikasi karyawan yang telah diinput dalam komputer dengan *file* induk karyawan. Hal ini dapat mengurangi risiko pengendalian untuk tujuan keterjadian pada transaksi penggajian. Auditor juga dapat mengidentifikasi pengendalian manual dan terotomatisasi pada waktu yang sama atau secara terpisah, tetapi tidak boleh mengidentifikasi defisiensi atau menilai risiko pengendalian sampai kedua jenis pengendalian itu telah diidentifikasi.

Setelah mengidentifikasi pengendalian aplikasi khusus yang dapat digunakan untuk mengurangi risiko pengendalian, auditor lalu mengurangi pengujian substantif. Karena pengendalian aplikasi yang terotomatisasi bersifat sistematis, hal itu akan memungkinkan auditor mengurangi ukuran sampel yang digunakan untuk menguji pengendalian tersebut baik dalam audit laporan keuangan maupun audit pengendalian internal atas pelaporan keuangan.

Dampak TI terhadap Proses Audit Laporan Keuangan

Banyak organisasi yang merancang dan menggunakan perangkat lunak akuntansi untuk memroses transaksi bisnis sedemikian rupa, sehingga dokumen sumber dapat dilacak kembali dalam format yang dapat dibaca serta dapat ditelusuri dengan mudah melalui sistem akuntansi ke *output*. Sistem seperti itu tetap menggunakan banyak dokumen sumber tradisional seperti pesanan pembelian pelanggan, catatan pengiriman dan penerimaan, serta faktur penjualan dan vendor. Perangkat lunak tersebut juga menghasilkan jurnal dan buku besar tercetak yang memungkinkan auditor menelusuri transaksi melalui catatan akuntansi. Pengendalian internal dalam sistem tersebut sering kali melibatkan personil klien yang membandingkan catatan yang dihasilkan-komputer dengan dokumen sumber.

Dalam situasi ini, penggunaan TI tidak terlalu berdampak terhadap jejak audit. Biasanya, auditor memahami pengendalian internal dan melakukan pengujian pengendalian, pengujian substantif atas transaksi, serta prosedur verifikasi saldo akun dengan cara yang sama seperti dalam sistem akuntansi manual. Auditor juga masih bertanggung jawab untuk memahami pengendalian umum dan aplikasi karena pengetahuan semacam ini sangat bermanfaat dalam mengidentifikasi yang dapat

mempengaruhi laporan keuangan. Namun, biasanya auditor melaksanakan pengujian atas pengendalian yang terotomatisasi. Pendekatan auditing ini sering disebut auditing di sekitar komputer *(auditing around the computer)* auditor tidak menggunakan pengendalian yang terotomatisasi untuk mengurangi penilaian risiko pengendalian. Sebagai gantinya, auditor menggunakan pengendalian manual untuk mendukung pengurangan penilaian risiko pengendalian.

Auditor perusahaan yang lebih kecil sering kali mengaudit di sekitar komputer apabila pengendalian umum kurang efektif ketimbang dalam lingkungan TI lebih kompleks. Perusahaan yang lebih kecil sering kali tidak memiliki personil kompeten di bidang TI, atau mengandalkan keterlibatan konsultan TI secara periodik untuk membantu memasang dan memelihara perangkat keras serta perangkat lunak. Tanggung jawab atas fungsi TI sering dilimpahkan ke departemen pemakai, seperti departemen akuntansi, di mana biasanya terdapat perangkat keras. Auditing sekitar komputer dianggap efektif karena sistem ini sering kali menghasilkan jejak audit yang mencukupi guna memungkinkan auditor membandingkan dokumen sumber, seperti faktur vendor dan penjualan, dengan *output*, dan mungkin pengendalian manual atas proses input dan *output yang* berjalan efektif mencegah serta mendeteksi salah saji laporan keuangan yang material.

Banyak organisasi yang memiliki lingkungan TI yang tidak rumit sering sangat bergantung pada mikrokomputer untuk melakukan fungsi-fungsi sistem akuntansi. Penggunaan mikrokomputer dapat menimbulkan pertimbangan audit yang unik yaitu ketergantungan yang terbatas pada pengendalian yang terotomatisasi, akses ke *file* induk, dan risiko virus komputer.

- ***Ketergantungan yang terbatas pada pengendalian yang terotomatisasi.*** Dalam lingkungan TI yang kurang canggih, pengendalian yang terotomatisasi sering kali dapat diandalkan. Sebagai contoh, program perangkat lunak komputer dapat diload pada *hard drive* komputer dengan format yang tidak memungkinkan diubah oleh personil klien, yang membuat risiko perubahan yang tidak diotorisasi dalam perangkat lunak menjadi rendah. Sebelum mengandalkan pengendalian yang terpasang dalam perangkat lunak, auditor harus yakin bahwa vendor perangkat lunak itu mempunyai reputasi mutu yang baik.
- ***Akses ke file induk.*** Apabila klien menggunakan mikrokomputer, auditor harus memperhatikan akses ke *file* induk oleh orang-orang yang tidak berwewenang.

Pemisahan tugas yang tepat di antara personil yang memiliki akses pada induk dan yang bertanggung jawab atas pemrosesan merupakan hal yang penting. Review oleh pemilik-manajer yang teratur atas *output* transaksi dapat meningkatkan pengendalian internal.

- ***Risiko virus komputer.*** Virus komputer dapat menyebabkan hilangnya data program. Virus-virus tertentu bahkan dapat merusak *file* elektronik atau menyebabkan *shut down* jaringan komputer secara keseluruhan. Perangkat lunak anti virus yang diupdate secara teratur untuk menangkal infeksi virus akan meningkatkan pengendalian.

Sebuah perusahaan publik yang menggunakan mikrokomputer dalam proses pelaporan keuangan dapat mempengaruhi audit pengendalian internal atas pelaporan keuangan. Jika auditor menyimpulkan bahwa pengendalian umum tidak efektif, pengujian auditor atas pengendalian aplikasi yang terotomatisasi mungkin perlu ditingkatkan. Auditor juga harus mempertimbangkan implikasi dari tidak adanya pengendalian umum yang efektif terhadap pendapat mengenai efektivitas pelaksanaan pengendalian internal atas pelaporan keuangan.

Jika organisasi memperluas penggunaan TI, pengendalian internal sering kali disisipkan dalam aplikasi yang hanya tersedia secara elektronik. Apabila dokumen sumber tradisional seperti faktur, pesanan pembelian, catatan penagihan, dan catatan akuntansi seperti jurnal penjualan, daftar persediaan, dan catatan tambahan piutang usaha hanya tersedia dalam format elektronik, auditor harus mengubah pendekatan auditingnya. Pendekatan ini sering disebut auditing melalui komputer *(auditing through the computer)*. Tabel 1 mengilustrasikan beberapa perbedaan antara auditing di sekitar komputer dan auditing melalui komputer.

Tabel 1: Contoh-contoh Auditing Di Sekitar Komputer dan Melalul Komputer

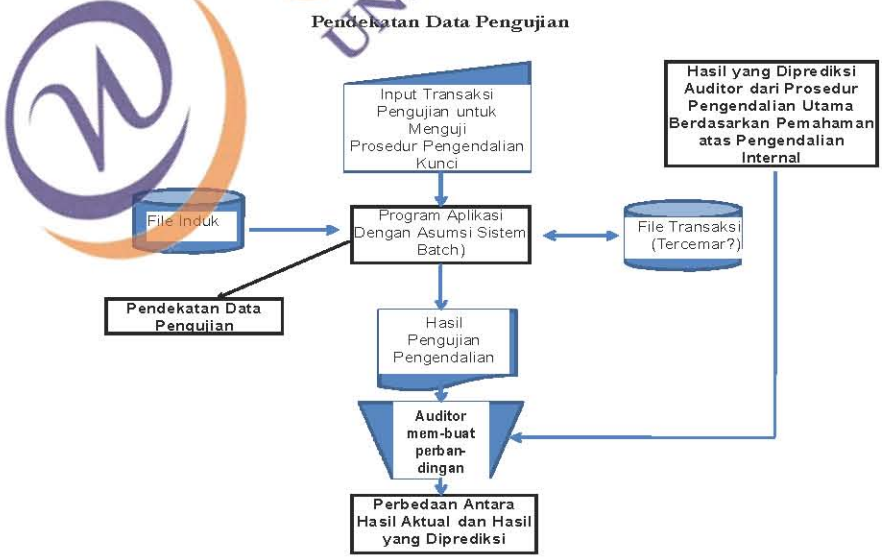
Pengendalian Internal	Pendekatan Auditing Di Sekitar Komputer	Pendekatan Auditing Melalui Komputer
Kredit disetujui untuk penjualan kredit.	Memilih sampel transaksi penjualan dari jurnal penjualan dan memperoleh pesanan penjualan pelanggan yang berkaitan untuk menentukan apakah sudah diparaf oleh manajer kredit, yang menunjukkan persetujuan atas penjualan kredit itu.	Memperoleh salinan program aplikasi penjualan klien dan *file* induk batas kredit yang berkaitan, serta memroses sampel data pengujian transaksi penjualan untuk menentukan apakah perangkat lunak aplikasi tersebut telah menolak dengan benar pengujian transaksi penjualan yang melebihi jumlah batas kredit pelanggan dan menerima semua transaksi lainnya.
Penggajian hanya diproses	Memilih sampel pengeluaran penggajian dari jurnal penggajian	Membuat *file* data pengujian dari nomor ID karyawan yang sah dan tidak sah serta

Tabel 1: Contoh-contoh Auditing Di Sekitar Komputer dan Melalul Komputer		
Pengendalian Internal	Pendekatan Auditing Di Sekitar Komputer	Pendekatan Auditing Melalui Komputer
untuk orang-orang yang saat ini dipekerjakan.	dan memverifikasinya dengan mereview *file* bagian SDM bahwa yang dibayar saat ini memang dipekerjakan.	memroses *file* itu dengan menggunakan salinan program aplikasi penggajian klien yang terkendali untuk menentukan bahwa semua nomor ID karyawan yang tidak sah ditolak dan semua nomor karyawan yang sah diterima.
Total kolom untuk jurnal pengeluaran kas disubtotal secara otomatis oleh komputer.	Memperoleh print*out* jurnal pengeluaran kas dan secara manual menjumlahkan setiap kolom untuk memverifikasi keakuratan total kolom yang tercetak.	Memperoleh salinan elektronik transaksi jurnal pengeluaran kas dan menggunakan perangkat lunak audit yang digeneralisasi untuk memverifikasi keakuratan total kolom.

Sumber: Randal, *et all* (2008)

Auditor menggunakan tiga kategori pendekatan pengujian ketika mengaudit melalui komputer: pendekatan data pengujian, simulasi paralel, dan pendekatan modul audit tertanam.

Pendekatan Data Pengujian. Dalam pendekatan data pengujian *(test data approach)*, auditor memroses data pengujiannya sendiri dengan menggunakan sistem komputer klien dan program aplikasi untuk menentukan apakah pengendalian yang terotomatisasi memroses dengan tepat data pengujian itu. Auditor merancang data pengujian dengan menyertakan transaksi yang harus diterima atau ditolak oleh sistem klien. Setelah data pengujian diproses pada sistem klien, auditor membandingkan *output* aktual dengan *output* yang diharapkan untuk menilai keefektifan pengendalian program aplikasi yang terotomatisasi tersebut. Gambar 1 mengilustrasikan penggunaan pendekatan data pengujian.



Gambar 1: Pendekatan data Pengujian (Randal, *et all,* 2008)

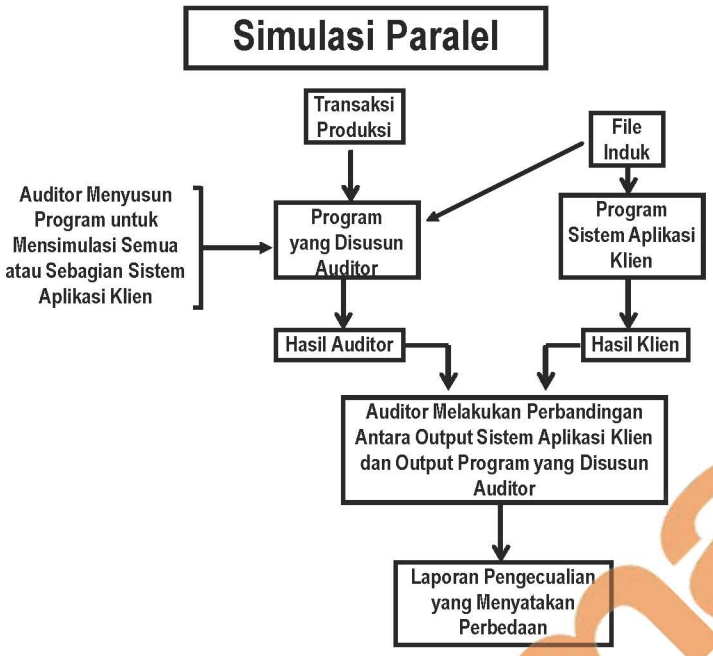
Apabila menggunakan pendekatan data pengujian, auditor mempunyai tiga

pertimbangan utama:

1. ***Data pengujian harus mencakup semua kondisi yang relevan yang ingin diuji auditor.*** Auditor harus merancang data pengujian untuk menguji semua pengendalian kunci berbasis-komputer dan memasukkan data yang realistik yang mungkin akan menjadi bagian dari pemrosesan normal klien, termasuk transaksi sah dan tidak sah. Sebagai contoh, asumsikan aplikasi penggajian klien berisi pengecekan batas yang tidak mengizinkan transaksi penggajian yang melebihi 80 jam per minggu. Untuk menguji pengendalian ini, auditor dapat menyusun transaksi penggajian dalam urutan 79, 80, dan 81 jam bagi masing-masing minggu yang dijadikan sampel dan memrosesnya melalui sistem klien dengan cara yang ditunjukkan pada Gambar 1. Jika pengendalian atas pengecekan batas berjalan efektif, sistem klien harus menolak transaksi sebesar 81 jam, dan daftar kesalahan klien harus melaporkan kesalahan transaksi 81-jam itu.
2. ***Program aplikasi yang diuji oleh data pengujian auditor harus sama dengan yang digunakan klien selama tahun berjalan.*** Salah satu pendekatan adalah menjalankan data pengujian atas dasar kejutan, mungkin secara acak selama tahun berjalan, walaupun agak mahal dan menghabiskan waktu. Metode lainnya adalah mengandalkan pengendalian umum klien pada fungsi pengembangan sistem dan pustakawan guna memastikan bahwa program yang diuji sama dengan yang digunakan dalam pemrosesan normal.
3. ***Data pengujian harus dieliminasi dari catatan klien.*** Jika auditor memroses data pengujian sedangkan klien memroses transaksinya sendiri, auditor harus menghilangkan data pengujian dalam *file* induk klien setelah pengujian itu selesai. Auditor dapat melakukan hal ini dengan mengembangkan dan memroses data yang membalik pengaruh data pengujian itu.

Karena kompleksitas dari banyak program perangkat lunak aplikasi klien, auditor yang menggunakan pendekatan data pengujian dapat minta bantuan kepada spesialis audit komputer. Banyak kantor akuntan publik yang lebih besar mempunyai staf yang ditugaskan untuk membantu menguji pengendalian aplikasi klien.

Simulasi Paralel. Auditor sering kali menggunakan perangkat lunak yang dikendalikan auditor untuk melaksanakan operasi yang sama dengan yang dilaksanakan oleh perangkat lunak klien, dengan menggunakan *file* data yang juga sama. Tujuannya adalah untuk menentukan keefektifan pengendalian yang terotomatisasi dan untuk mendapatkan bukti tentang saldo akun elektronik. Pendekatan pengujian ini disebut pengujian simulasi paralel *(parallel simulation testing,* Gambar 2.).



Gambar 2. Simulasi Paralel (Randal, *et all*, 2008)

Dengan simulasi ini auditor dapat menguji pengendalian atau saldo akhir, membandingkan *output* dari perangkat lunak auditor dengan *output* dari perangkat lunak klien untuk menguji keefektifan perangkat lunak klien, dan untuk menentukan apakah saldo klien sudah benar.

Biasanya auditor melakukan pengujian simulasi paralel dengan menggunakan perangkat **perangkat lunak audit tergeneralisasi *(generalized audit software - GAS)***, yaitu program yang dirancang secara khusus untuk tujuan auditing (Cushing, *et all*,1994). Perangkat lunak audit yang tersedia secara komersial seperti ACL atau IDEA, dapat dengan mudah dioperasikan pada komputer *desktop* atau *laptop* auditor. Auditor akan memperoleh salinan *database* atau *file* induk klien dalam format yang terbaca mesin, dan menggunakan perangkat lunak audit tergeneralisasi untuk melaksanakan berbagai pengujian atas data elektronik klien. Selain GAS, beberapa auditor juga menggunakan perangkat lunak *spreadsheet* untuk melaksanakan pengujian simulasi paralel yang sederhana. Sementara yang lain mengembangkan perangkat lunak auditnya sendiri.

Perangkat lunak audit tergeneralisasi memiliki tiga keunggulan: relatif mudah melatih staf audit untuk menggunakannya, meskipun mereka hanya mempunyai pelatihan yang minim di bidang TI yang berkaitan dengan audit, perangkat lunak

tersebut dapat diterapkan pada berbagai klien dengan penyesuaian yang minimal, dan mampu melaksanakan pengujian audit jauh lebih cepat dan lebih terinci ketimbang menggunakan prosedur manual yang tradisional.

Tabel 2 menyajikan beberapa penggunaan umum dari perangkat lunak audit tergeneralisasi. Dua diantaranya sebagai contoh:

1. *Perangkat lunak tergeneralisasi digunakan untuk menguji pengendalian yang terotomatisasi.* Auditor akan memperoleh salinan *file* induk batas kredit pelanggan milik klien serta *file* pesanan pelanggan, dan kemudian menginstruksikan komputer auditor untuk membuat daftar transaksi yang melebihi batas kredit pelanggan yang diotorisasi. Auditor kemudian membandingkan output audit dengan daftar pesanan pelanggan yang ditolak karena melewati batas kredit yang diotorisasi.
2. *Perangkat lunak audit tergeneralisasi digunakan untuk memverifikasi saldo akun klien.* Auditor dapat menggunakan perangkat lunak itu untuk menjumlahkan *file* induk piutang usaha pelanggan guna menentukan apakah totalnya sesuai dengan saldo buku besar.

Tabel 2: **Penggunaan Perangkat Lunak Audit Tergeneralisasi**

Penggunaan	Uraian	Contoh
Memverifikasi perkalian dan footing	Memverifikasi keakuratan perhitungan klien dengan menghitung informasi secara independen.	Memfoot neraca saldo piutang usaha.
Memeriksa catatan tentang mutu, kelengkapan, konsistensi, dan kebenaran.	Memindai semua catatan dengan menggunakan kriteria tertentu.	Mereview *file* penggalian untuk karyawan yang berhenti.
Membandingkan data pada *file* terpisah.	Menentukan bahwa informasi dalam dua *file* data atau lebih telah sesuai	Membandingkan perubahan saldo piutang usaha di antara dua tanggal dengan menggunakan penjualan dan penerimaan kas pada *file* transaksi.
Mengikhtisarkan atau mengurutkan kembali data dan melaksanakan analisis.	Mengubah atau mengagregatkan data.	Mengurutkan kembali item persediaan sesuai lokasi untuk memudahkan observasi fisik
Memilih sampel audit.	Memilih sampel dari data yang dapat dibaca mesin.	Secara acak memilih piutang usaha untuk konfirmasi.
Mencetak permintaan konfirmasi.	Mencetak data dari item sampel yang dipilih untuk mengujian konfirmasi.	Mencetak nama pelanggan, aramat, dan informasi tentang akun dari *file* induk.
Membandingkan data yang diperoleh melalui prosedur audit lain dengan catatan	Membandingkan data yang dapat dibaca mesin dengan bukti audit yang dikumpulkan secara manual,	Membandingkan respons konfirmasi dengan *file* induk akun piutang usaha.

perusahaan.	yang diubah ke format yang dapat dibaca mesin.	

Sumber: Randal, *et all* (2008)

Pendekatan Modul Audit Tertanam. Ketika menggunakan pendekatan modul audit tertanam *(embedded audit modul approach),* auditor menyisipkan modul audit dalam sistem aplikasi klien untuk mengidentifikasi jenis transaksi tertentu. Sebagai contoh, auditor mungkin ingin menggunakan modul audit tertanam guna mengidentifikasi semua pembelian yang melebihi Rp25.000.000 untuk ditindaklanjuti dengan pemeriksaan yang lebih terinci bagi tujuan keterjadian dan keakuratan yang berkaitan dengan transaksi. Dalam beberapa kasus, auditor akan menyalin transaksi yang diidentifikasi pada *file* data terpisah, dan kemudian memroses transaksi itu dengan menggunakan simulasi paralel untuk menduplikasi fungsi yang dijalankan oleh sistem klien. Lalu auditor membandingkan *output* klien dengan *output* auditor. Perbedaannya dicetak pada laporan pengecualian untuk ditindaklanjuti oleh auditor.

Pendekatan modul audit tertanam memungkinkan auditor untuk terus meng-audit transaksi dengan mengidentifikasi transaksi aktual yang diproses oleh klien yang dibandingkan dengan data pengujian dan pendekatan simulasi paralel.

Walaupun dapat menggunakan satu atau setiap kombinasi dari pendekatan pengujian, biasanya auditor menggunakan:

- Data pengujian untuk melaksanakan pengujian pengendalian dan pengujian substantif atas transaksi.
- Simulasi paralel untuk pengujian substantif, seperti menghitung ulang jumlah transaksi dan menjumlahkan *file* induk catatan tambahan saldo akun.
- Modul audit tertanam untuk mengidentifikasi transaksi tidak biasa bagi pengujian substantif.

3 KESIMPULAN

Penggunaan teknologi informasi dapat meningkatkan pengendalian internal. Meskipun demikian penggunaan sistem akuntansi berbasis-TI juga menghadirkan risiko baru yang biasanya tidak berkaitan dengan sistem manual tradisional. Auditor memperoleh kemampuan yang besar dan efektif dalam melaksanakan auditnya. Auditor harus memiliki pengetahuan dan pemahaman yang cukup tentang TI

khususnya audit TI dan pengendalian umum serta aplikasi klien agar dapat merencanakan audit secara efektif. Pengetahuan tentang pengendalian umum akan memberikan dasar bagi auditor untuk mengandalkan pengendalian aplikasi yang terotomatisasi, dan dapat mengurangi luas pengujian atas pengendalian kunci yang terotomatisasi dalam audit laporan keuangan dan pengendalian internal. Beberapa pengujian pengendalian auditor dapat dilakukan oleh komputer, yang sering kali sebagai cara untuk mencapai audit yang lebih efektif dan efisien.

4 DAFTAR PUSTAKA

Cushing. Berry E, Marshall B, Romney., 1994. Accounting Information Systems. Sixth Edition., Addison-Wesley Publishing Company.

IAI, 2001**. Standar Profesional Akunatn Publik (SPAP).**

Lucas, Jr., Henry C. (2000)., *Information Technology for Management*. Seventh Edition., Mc Graw-Hill-Irwin.

Mahoney Jerry, Texas Textbooks Closes Doors in Austin Texas, In Wake Yearlong Demise` *Knight-Ridder Tribune* Business News: Austin *American* Statesman (6 April 2001)).

Randal J. Elder., Mark S. Beasley., Arens Alvin A., 2008. *Auditing and Assurance Servise: An Integrated Approach*. 12th. Edition. Pearson International Edition, Pearson Education, Inc., Upper Saddle River, New Jersey, Prentice Hall.