MODUL PERKULIAHAN

EDP Audit

Operasi Sistem Informasi

(Information Systems Operations)

Abstract

Modul ini berisi tentang pembahasan Operasi sistem informasi meliputi kontrol internal pada fasilitas pengolahan data serta yang ditempatkan di lingkungan pengguna akhir, yang dirancang untuk membantu proses operasional organisasi agar berfungsi seefisien dan seefektif mungkin dalam batasan yang ditentukan oleh peraturan ekonomi, keuangan, politik, hukum, dan lingkungan

Kompetensi

Mahasiswa mampu pememahami dan mengenali tetantang Operasi sistem informasi meliputi kontrol internal pada fasilitas pengolahan data serta yang ditempatkan di lingkungan pengguna akhir.

Pengantar

Bab ini membahas mengenai bagaimana mengaudit operasi sistem informasi (SI) dari perspektif yang luas. Termasuk contoh berbagai kelemahan kontrol internal di dunia nyata dan inefisiensi yang terkait dengan operasi SI. Beberapa kontrol operasi komputer yang dibahas dalam bab ini berhubungan erat dengan kontrol keamanan fisik, yang dibahas secara lebih rinci dalam Bab 7.

Operasi sistem informasi meliputi kontrol internal pada fasilitas pengolahan data serta yang ditempatkan di lingkungan pengguna akhir, yang dirancang untuk membantu proses operasional organisasi agar berfungsi seefisien dan seefektif mungkin dalam batasan yang ditentukan oleh peraturan ekonomi, keuangan, politik, hukum, dan lingkungan. Karena semua operasi di seluruh organisasi saling terkait, auditor tidak harus melihat operasi SI sebagai fungsi yang benar-benar terpisah dari operasi lain dalam sebuah organisasi. Pada dasarnya merupakan bagian dari "sistem informasi" yang sama besar. Membentuk satu masukan yang komprehensif, pengolahan, dan mesin keluaran bekerja untuk mencapai tujuan strategis organisasi jangka panjang. Karena itu, ketika memeriksa operasi SI, auditor harus mempertimbangkan dampak keseluruhan dari inefisiensi dan prosedur yang tidak efektif pada kemampuan organisasi untuk mencapai tujuan jangka panjang.

Dengan berkembangnya sistem pengolahan data yang terdistribusi dalam beberapa tahun terakhir, operasi SI berbagai skala telah ada di hapir organisasi beberapa lokasi. Komputer dan perangkat keras peripheral yang terkait dapat berada terpusat, seperti di sebuah pusat data yang besar, serta di setiap lokasi fisik sebuah perusahaan, seperti dalam kasus jaringan area luas (WAN) yang mengizinkan semua proses dalam organisasi bertukar informasi secara eletronik. Dalam operasi SI ini, masing-masing area fungsional bertanggung jawab untuk melakukan proses dalam cara terkendali secara bertanggung jawab. Karena sebagaimana operasi SI tersebar luas, semua auditor harus terbiasa dengan pendekatan yang diperlukan untuk menilai kecukupannya. Untuk memberikan pendekatan tingkat tinggi, operasi SI dalam suatu organisasi terbagi menjadi dua komponen yang saling berkaitan yaitu operasi komputer dan operasi bisnis.

Operasi Komputer

Operasi komputer terdiri dari proses SI yang memastikan bahwa data masukan diproses dengan cara yang efisien dan efektif untuk mendukung tujuan strategis dan operasi bisnis dari suatu organisasi.

Audit operasi komputer harus mencakup penilaian kontrol internal yang memastikan bahwa:

- Pekerjaan produksi diselesaikan secara tepat waktu dan kapasitas produksi cukup untuk memenuhi kebutuhan pengolahan jarak pendek dan panjang.
- Media keluaran didistribusikan secara tepat waktu, akurat, dan aman.
- Prosedur cadangan dan pemulihan secara memadai melindungi data dan program terhadap kehilangan atau perusakan yang disengaja atau tidak disengaja.
- Prosedur perawatan secara memadai untuk melindungi perangkat keras komputer terhadap kerusakan.
- Perangkat keras komputer, perangkat lunak, dan data diasuransikan sebesar biaya penggantian.
- Prosedur pengelolaan masalah memastikan bahwa masalah sistem didokumentasikan dan diselesaikan secara tepat waktu dan efektif.

Pembuatan Jadwal Pekerjaan dan Pemantauan

Penjadwalan pekerjaan otomatis dan inisiasi perangkat lunak secara signifikan dapat meningkatkan efisiensi operasional dengan memulai secara otomatis program produksi penjadwalan berikutnya segera pada saat penyelesaian program sebelumnya. Setiap pekerjaan harus diberi nomor prioritas (misalnya, satu sampai sembilan, dengan satu yang memiliki prioritas tertinggi), yang memungkinkan perangkat lunak penjadwalan pekerjaan memulai program dengan prioritas tertinggi. Sementara operator komputer masih perlu memantau antrian program dalam kegagalan program abnormal dan kadang-kadang mungkin perlu mengubah urutan inisiasi program, perangkat lunak semacam ini dapat mengurangi kebutuhan operator komputer secara signifikan untuk memulai setiap program secara manual, sehingga membebaskan mereka untuk melakukan tugas-tugas lain. Software penjadwalan pekerjaan otomatis juga mengurangi risiko operator komputer dapat

menjalankan program tidak berdasarkan urutan atau lupa menjalankan salah satunya sama sekali. Ketika program dijalankan tidak berurutan atau tidak berjalan sama sekali, keluaran data berikutnya mungkin tidak benar karena tergantung pada data terbaru dari program yang telah selesai sebelumnya.

Untuk memantau efektivitas perangkat lunak penjadwalan pekerjaan otomatis, manajemen wilayah operasi komputer harus menerima laporan harian produksi yang dihasilkan sistem yang menunjukkan mulai dan berkahirnya setiap pekerjaan, sebaiknya dibandingkan dengan jadwal produksi yang direncanakan, dan pekerjaan apa pun yang abnormal dihentikan. Informasi ini memberikan manajemen alat untuk menilai secara mandiri apakah pekerjaan diselesaikan secara tepat waktu dan sesuai dengan jadwal yang sudah disetujui. Masalah mungkin mengidentifikasi kebutuhan untuk mengubah urutan di mana pekerjaan dijadwalkan agar secara lebih efisien dalam memanfaatkan kemampuan pengolahan sistem. Manajemen juga dapat melihat apakah sejumlah besar pekerjaan berakhir dengan normal. Kegiatan tersebut dapat mengindikasikan masalah pemrograman sistem atau kebutuhan untuk memperluas kapasitas produksi atas perangkat keras sistem.

Kontrol pemantauan lain yang harus ada yaitu memeriksa jumlah penyimpanan disk yang tersedia dan pemanfaatan kapasitas sistem dinamis secara berkala. Memeriksa jumlah ruang penyimpanan disk yang tersedia mirip dengan memeriksa jumlah ruang disk yang tersedia pada hard drive komputer pribadi. Pemanfaatan kapasitas sistem dinamis lebih sulit ditentukan. Kontrol pemantauan ini melibatkan pelacakan persentase kapasitas pengolahan total sistem yang digunakan selama periode waktu tertentu , misalnya satu hari, satu minggu, satu bulan, atau satu tahun. Lebih baik sistem mencatat informasi ini secara otomatis dan menghasilkan laporan manajemen untuk periode yang diinginkan. Informasi ini dapat membantu manajemen dalam menjadwalkan pemeliharaan sistem, merencanakan jadwal produksi, dan mengidentifikasi ketika sistem mencapai tingkat pemanfaatan kapasitas yang membutuhkan upgrade sistem untuk mengakomodasi volume yang lebih tinggi dari pengolahan data. Beberapa sistem yang lebih canggih diprogram dalam halaman atau email administrator sistem jika kapasitas pengolahan telah ditentukan sebelumnya atau ambang batas penyimpanan data terlampaui.

Studi kasus 9.1 menggambarkan beberapa kelemahan kontrol internal yang berkaitan dengan penjadwalan pekerjaan dan pemantauan di daerah operasi komputer dari satu organisasi. Studi kasus 9.1 merupakan potret 10 jam dari jenis laporan yang dapat

digunakan manajemen untuk memantau penyimpanan data dan kapasitas pengolahan dinamis dari unit jaringan pengolahan pusat tertentu (CPU). Perhatikan bahwa kapasitas CPU mulai meningkat secara dramatis setelah pukul 08:00, ketika para pekerja mulai mengakses ke jaringan dan melakukan berbagai fungsi. Puncak pemrosesan CPU terjadi antara pukul 10:00 dan siang hari, ketika produktivitas kerja berada pada puncaknya. Siang hari ada celah yang diharapkan ketika pekerja pergi makan siang, dengan peningkatan lain ketika pekerja kembali dari makan siang. Setelah pukul 14:00 pemrosesan CPU menurun secara signifikan karena pekerja mulai menyelesaikan harinya.

Jumlah fluktuasi kapasitas penyimpanan data umumnya hampir rata daripada fluktuasi pengolahan CPU. Kapasitas memuncak pada pukul 10:00, sepertinya sebagai puncak produktivitas pekerja diperlukan penghematan sementara pada beberapa file data baru. Dari pukul 16:00 pemanfaatan kapasitas total penyimpanan data jatuh kembali turun hampir ke tingkat awalnya pada pukul 6:00, karena pengguna jaringan menyelesaikan kelebihan dan file data yang tidak perlu sebelum akhir hari kerjanya. Sayangnya, banyak sistem yang tidak memberikan kemampuan untuk memantau pemanfaatan kapasitas sistem dinamis.

STUDI KASUS 9.1

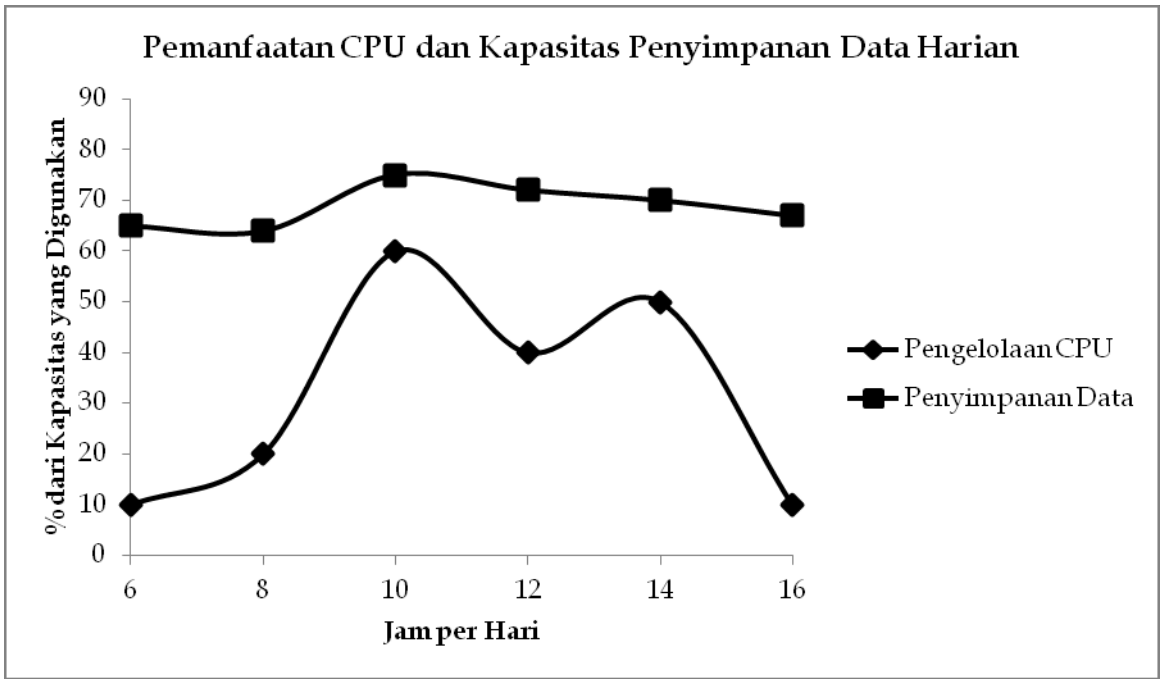
Kurangnya Perangkat Lunak Penjadwalan Pekerjaan Otomatis dan Kontrol Pemantauan Pemanfaatan Kapasitas

Selama audit departemen operasi komputer dari sebuah organisasi, terlihat bahwa program dijalankan secara manual oleh operator komputer. Setelah menyelesaikan pekerjaan, sistem akan tetap menganggur sampai operator komputer memasukkan nama pekerjaan berikutnya. Fakta bahwa pekerjaan yang dijalankan tidak otomatis membuat risiko operator tidak dapat memulai pekerjaan berdasarkan urutan atau bisa lupa untuk memulai pekerjaan sama sekali. Juga, jika operator sibuk dengan masalah lain, dia mungkin tidak menyadari ketika pekerjaan normal berakhir. Situasi ini dapat menyebabkan penundaan serius dalam jadwal produksi jika menjalankan pekerjaan besar yang membutuhkan waktu berjam-jam berakhir dan operator tidak menyadari hal itu untuk waktu yang lama. Akibatnya, ada peluang yang signifikan untuk meningkatkan efisiensi dan efektivitas penjadwalan pekerjaan dan inisiasi.

Aplikasi perangkat lunak sistem dilisensi dari penjual, dan penjual dikabarkan menawarkan modul yang akan memungkinkan penjadwalan pekerjaan diotomatisasi dan menginisiasi aplikasi yang sudah ada. Oleh karena itu, direkomendasikan agar manajemen departemen operasi komputer menghubungi penjual untuk menentukan apakah hal tersebut akan menghemat biaya dalam memperoleh penjadwalan pekerjaan dan inisiasi software otomatis.

Juga tidak ada laporan atau kontrol lain yang memungkinkan departemen operasi komputer memantau pemanfaatan kapasitas sistem secara dinamis selama periode tertentu. Dalam kasus ini, manajemen melaporkan bahwa penjual, yang juga pengecer hardware berlisensi untuk komputer yang digunakan oleh organisasi, bisa memasok laporan pemanfaatan kapasitas sistem yang dinamis, menunjukkan poin yang tinggi dan rendah dari output komputasi selama periode yang diinginkan. Sayangnya, manajemen melaporkan bahwa penjual hanya dapat menyediakan laporan tersebut berdasarkan permintaan individual, bukan secara berkala. Selain itu, manajemen di departemen operasi komputer tidak mempertimbangkan kelemahan laporan tersebut menjadi perhatian yang signifikan. Mereka merasa bahwa mereka sangat menyadari kinerja sistem dan tahu kapan akan perlu mengupgradenya. Meskipun kita tahu bahwa manajemen tidak setuju dengan rekomendasi kami, kami masih merekomendasikan agar manajemen mempertimbangkan bekerja sama dengan penjual untuk menghasilkan laporan periodik yang menunjukkan pemanfaatan kapasitas sistem dari waktu ke waktu. Dengan cara ini, kami mendokumentasikan fakta bahwa kami telah mengidentifikasi masalah ini dan memberikan rekomendasi yang layak untuk manajemen, bahkan jika mereka memilih untuk tidak menerapkan perubahan.

Tampilan SK 9.1 Pemanfaatan CPU dan Kapasitas Penyimpanan Data Harian



Sebuah alternatif yang sederhana kadang-kadang efektif dalam memantau kinerja sistem atas dasar pengecualian untuk memeriksa jumlah dan jenis panggilan ke divisi bantuan sistem. Jika sistem lambat merespon atau jika itu benar-benar tertutup karena kelebihan kapasitas atau masalah lain, pengguna pasti memanggil divisi bantuan untuk menanyakan kapan sistem akan hidup dan berjalan lagi atau untuk sekedar mengeluh. Jika panggilan ini secara akurat mencatat waktu dan klasifikasi jenis masalah, grafik perwakilan ketika kinerja sistem mengalami penurunan dapat dibuat. Namun, grafik tersebut tidak mengidentifikasikan periode penggunaan kapasitas sistem yang rendah. Informasi tersebut membantu manajer SI mengetahui ketika aktivitas sistem tertentu (misalnya, program *batch*) dilakukan untuk memanfaatkan kapasitas sistem secara lebih optimal.

Distribusi Media Keluaran

Banyak pekerjaan produksi menghasilkan pembuatan file keluaran elektronik. File keluaran ini disimpan dalam antrian sementara yang kadang-kadang disebut sebagai *spool*, merupakan singkatan dari "operasi online peripheral serentak". File keluaran di *spool* dapat dicetak, disalin ke direktori lain, atau keduanya, tergantung pada kebutuhan pemilik data. Kegiatan ini dilakukan oleh daerah distribusi keluaran pada waktu yang tepat sehingga pemilik data dapat memanfaatkan informasi tersebut secara efektif. File keluaran juga harus

dibersihkan dari *spool* secara teratur, biasanya dalam satu atau dua hari, untuk mengosongkan ruang penyimpanan disk.

Media keluaran fisik (cetakan kertas, *microfiche*, dan *microfilm*) harus dikontrol secara ketat untuk memastikan personil yang tidak sah tidak dapat melihat atau mendapatkan informasi penting. Demikian pula, akses logis untuk file *spool* harus diberikan hanya untuk kebutuhan staf operasi komputer dan administrator keamanan sistem. Ini merupakan kontrol yang penting karena pengguna yang tidak sah dengan akses ke *spool* bisa dengan cepat melihat, menyalin, dan mungkin mengubah berbagai file data yang berisi informasi penting.

Studi kasus 9.2 menggambarkan bagaimana informasi penting yang membahayakan, banyak yang mengagetkan dari departemen audit internal.

STUDI KASUS 9.2

File *Spool* yang Tidak Terlindungi

Departemen audit internal dari lembaga keuangan besar yang memiliki banyak cabang melakukan audit cabang mendadak yang dimulai pada hari Senin. Laporan kegiatan keuangan tertentu dibuat oleh departemen audit internal selama pertengahan minggu sebelumnya agar hasil cetakan tersebut tersedia pada hari Jumat sebelum auditnya dimulai.

Seorang pengguna di pusat data yang memiliki kemampuan akses sistem memungkinkan dia untuk melihat *spool* yang berisi program-program produksi yang baru saja diselesaikan, termasuk dari departemen audit internal. Dari pengalamannya, pengguna tersebut tahu bahwa laporan standar tertentu dimulai setiap minggu oleh departemen audit internal sebelum melakukan audit cabang mendadak. Karena pengguna memiliki teman seorang auditor internal cabang, dia berpikir akan memamerkan pengetahuannya dengan mencari laporan audit internal di *spool* untuk mengetahui cabang yang diaudit minggu berikutnya. Kemudian, pada Senin pagi, sebelum auditor tiba untuk melakukan audit mendadak, wanita tersebut memanggil cabang dan meninggalkan pesan untuk auditor cabang. Ini jelas menghapus setiap unsur dadakan dari audit. Auditor menerima pesannya segera setelah audit dimulai, banyak yang cemas dari auditor yang bertanggung jawab.

Pengguna di pusat data ditegur atas tindakannya, dan kontrol diberlakukan di tempat dimana file keluaran audit internal pindah ke direktori terbatas secara otomatis setelah selesainya program untuk mencegah kejadian yang serupa.

Prosedur Cadangan dan Pemulihan

Seperti yang dibahas dalam Bab 7, setiap organisasi harus memiliki rencana pemulihan bisnis. Sebagai bagian dari rencana, harus ada prosedur yang memadai untuk melindungi data dan program terhadap kehilangan atau perusakan yang disengaja atau tidak disengaja. Kontrol utama untuk memberikan perlindungan ini adalah melakukan pencadangan secara berkala (harian, mingguan, bulanan) atas perangkat lunak sistem, program aplikasi, dan data serta penyimpanan dan rotasi media cadangan seperti pita perekam suara, disk, dan compact disk (CD) ke luar lokasi situs yang aman. Pencadangan harian biasanya hanya diperlukan untuk data karena program aplikasi dan perangkat lunak sistem tidak berubah secara signifikan. Pencadangan penuh dari seluruh sistem, yaitu perangkat lunak sistem, program aplikasi, dan data, harus dilakukan secara mingguan atau bulanan, tergantung pada jumlah dan jenis perubahan yang telah dibuatnya. Pencadangan sistem penuh juga harus dilakukan pada penyelesaian upgrade besar atau perubahan signifikan terhadap parameter operasional dan keamanan sistem. Selain itu, manajemen harus menegaskan agar pengujian dilakukan untuk memastikan bahwa sistem operasi sebenarnya bisa pulih sepenuhnya dengan menggunakan media cadangan. Ini merupakan salah satu pengujian yang sering diabaikan. Lihat Bab 7 untuk informasi tambahan dan contoh-contoh topik dari cadangan periodik dan program pemulihan bisnis.

Prosedur Pemeliharaan

Semua perangkat keras komputer harus dilayani sesuai dengan rekomendasi pabrik sebagaimana ditentukan dalam kontrak dengan penjual perangkat keras. Prosedur pemeliharaan harus cukup melindungi perangkat keras komputer terhadap kegagalan selama masa manfaat yang diharapkan dari peralatan. Dalam kebanyakan kasus, pemeliharaan yang tepat juga merupakan persyaratan agar garansi produsen atas kinerja peralatan tetap berlaku. Untuk alasan ini, penting agar setiap organisasi memiliki catatan akurat dari semua pemliharaan yang dilakukan. Tergantung pada jenis peralatan yang

dimanfaatkan dalam sebuah organisasi, teknisi penjual atau pemborong mungkin perlu melakukan jasa pemeliharaan yang diperlukan. Jika demikian, biaya dan ketersediaan prosedur pemeliharaan yang rutin dan tidak rutin harus didokumentasikan dalam kontrak dengan penjual atau pemborong. Sebelum mengizinkan jasa pemeliharaan dilakukan oleh teknisi gedung, manajemen harus meninjau persyaratan kontrak untuk memastikan setiap garansi akan berlaku jika teknisi yang bukan dari penjual melakukan pemeliharaan. Kontrak tersebut memungkinkan teknisi yang bukan dari penjual melakukan pemeliharaan, tetapi meminta mereka yang bersertifikat ahli dalam teknologi pemeliharaan agar garansi tetap berlaku.

Asuaransi

Sebagaimana yang dibahas dalam Bab 7, setiap organisasi harus membeli asuransi dalam jumlah memadai yang menanggung semua hardware dan software komputer sebesar biaya penggantian, biaya untuk pemulihan data yang hilang, dan mungkin nilai pendapatan yang hilang yang merupakan akibat langsung dari kegagalan perangkat keras atau perangkat lunak komputer. Polis asuransi mungkin memerlukan prosedur pemeliharaan rutin yang ditentukan oleh produsen komputer yang dilakukan dalam rangka agar pertanggungan tetap berlaku. Polis tersebut juga dapat menetapkan pembuatan dan penyimpan perangkat lunak dan data cadangan harian, mingguan, dan bulanan di lokasi luar situs yang aman. Hal yang dapat dikurangkan harus ditentukan pada tingkat yang memberikan keseimbangan wajar antara premi tahunan dan nilai pertanggungan secara keseluruhan. Lihat Bab 7 untuk informasi tambahan dan contoh-contoh atas pertanggungan asuransi.

Pengelolaan Masalah

Jumlah dan jenis masalah sistem yang timbul harus dicatat dengan hati-hati untuk membantu memastikan bahwa masalah sistem didokumentasikan dan diselesaikan secara tepat waktu dan efektif. Beberapa organisasi menegakkan departemen divisi bantuan pusat yang menjawab berbagai pertanyaan melalui telepon pengguna, termasuk yang berhubungan dengan masalah sistem. Organisasi lain mungkin memerlukan pemilik proses masing-masing sistem untuk menjawab dan menyelesaikan masalah sistemnya. Dalam salah satu kasus, semua masalah sistem harus dicatat, sebaiknya dalam format elektronik

yang memfasilitasi peninjauan manajemen dan dapat diberikan kepada penjual sistem untuk penggunaan dalam pemecahan masalah dari penyebab masalah. Jenis informasi yang harus dicatat termasuk tanggal dan waktu masalah tersebut dilaporkan, deskripsi masalah, nama, judul, departemen, alamat email, dan nomor telepon dari orang yang melaporkan masalah, dan langkah-langkah tindakan yang diambil oleh orang yang menjawab laporan tersebut. Tindakan yang mungkin yaitu menyelesaikan masalah melalui telepon, merujuk masalah ke teknisi, atau memperluas masalah kepada manajer. Prosedur tindak lanjut harus ada dimana orang yang ditunjuk di daerah penyelesaian masalah atau divisi bantuan melacak setiap langkah tindakan yang diambil setelah laporan awal dan menuangkannya dalam catatan sampai masalah diselesaikan. Bahkan masalah kecil sistem harus dicatat dalam pencatatan karena tingginya insiden atas masalah kecil bisa menjadi pemicu masalah yang lebih serius. Jika masalah tertentu tidak dapat diselesaikan, alasannya harus dicatat dalam pencatatan.

Secara periodik, (misalnya, mingguan), laporan pengelolaan masalah sistem harus disiapkan. Laporan harus mengklasifikasikan masalah untuk jenis dan tingkat keparahan untuk memungkinkan manajemen menentukan frekuensi dan urgensi dari masalah-masalah yang terjadi selama periode laporan. Masalah yang belum terselesaikan harus digarisbawahi, terutama yang belum dikoreksi dalam jangka waktu yang lama. Laporan tersebut harus ditinjau ulang oleh manajemen di daerah yang terkena. Kecenderungan masalah yang signifikan dan masalah lain terkait kinerja sistem harus dikomunikasikan kepada penjual, teknisi, dan pihak lain yang terkait.

OPERASI BISNIS

Operasi bisnis terdiri dari semua fungsi lain dalam organisasi selain yang berada di daerah operasi komputer. Daerah operasi bisnis biasanya memberikan data masukan ke daerah operasi komputer dan memanfaatkan hasil yang dikeluarkan dalam proses sehari-harinya. Audit operasional bisnis harus mencakup penilaian atas kecukupan kontrol internal yang berkaitan dengan semua aspek penting dari proses tertentu menurut pertimbangan. Jelas, jumlah dan jenis kontrol internal dalam operasi bisnis sangat bervariasi tergantung pada jenis usaha atau proses yang diaudit. Dalam lingkungan operasi di hampir

setiap organisasi, ada banyak kontrol SI pengguna akhir. Kontrol ini harus berfungsi bersama-sama dengan kontrol operasi komputer tradisional terpusat untuk melindungi organisasi secara memadai terhadap akses sistem yang tidak sah dan untuk membantu memastikan bahwa operasi bisnis dilakukan dengan cara yang efisien dan efektif. Dengan kata lain, kontrol internal dalam daerah operasi komputer terpusat mengimbangi hal-hal di unit operasi bisnis, dan sebaliknya. Juga tidak dapat berfungsi secara efektif tanpa yang lain. Seperti yang disebutkan di awal bab ini, operasi komputer dan operasi bisnis bersama-sama mencakup operasi SI dalam organisasi. Memang benar bahwa lingkungan kontrol internal organisasi hanya sekuat komponen yang paling lemah.

Kontrol sistem informasi yang ada di lingkungan operasi bisnis dapat terkait dengan masing-masing tiga dasar kategori pengolahan data elektronik: masukan, proses, dan keluaran (hasil). Tetapi ada kontrol lain yang berdampak pada sistem informasi yang sangat penting dalam fungsi efektif dari operasi bisnis. Beberapa contoh dari kontrol operasi bisnis yang mungkin ditemui akan disajikan berikutnya.

Mengedit dan Memeriksa Kewajaran

Untuk membantu mencegah data yang tidak valid dimasukkan dalam sistem, banyak sistem yang diprogram dengan mengedit otomatis dan pemeriksaan kewajaran. Misalnya, pemeriksaan mengedit dapat mencegah huruf dimasukkan ke dalam bidang yang seharusnya hanya memiliki nomor, atau sebaliknya. Pemeriksaan mengedit juga dapat mencegah kode yang tidak valid masuk ke bidang tertentu dan dapat mencegah masuknya tanggal atau jumlah luar dari rentang yang tidak ditentukan. Beberapa sistem memerlukan orang entri data kedua untuk mengunci kembali beberapa atau semua data yang dikunci masuk oleh orang entri data pertama dan akan menerima data hanya jika keduanya menyususun data yang persis sama.

Atau, pemeriksaan mengedit dapat dideteksi dalam sifatnya. Dengan kata lain, kontrol mengedit dapat secara manual maupun setelah fakta. Sebagai contoh, sistem dapat menghasilkan laporan entri data yang harus dibandingkan dengan dokumen masukan asli untuk mengidentifikasi kesalahan, atau sistem dapat menerima dan berusaha memproses semua data yang semula dimasukkan dan menghasilkan laporan pengecualian di mana data yang dikuci masuk tidak memenuhi standar atau penyaringan yang ditentukan. Penerima

laporan pengecualian kemudian harus memasukkan koreksi yang diperlukan pada data awal. Kontrol deteksi SI biasanya kurang efisien dan efektif dibandingkan dengan kontrol pencegahan karena membutuhkan tindakan tambahan dan dengan demikian memperlambat proses keseluruhan.

Pemeriksaan Integritas/Kelengkapan

Ketika volume besar data elektronik diimpor dari atau diekspor ke sistem lain , integritas data dan kontrol kelengkapan dapat memberikan keyakinan yang memadai bahwa penerima telah menerima semua data utuh , tanpa perubahan atau informasi yang hilang . Total kontrol adalah bentuk paling umum dari integritas / kelengkapan cek. Pengirim menyediakan penerima dengan total kontrol, seperti jumlah total catatan dalam file data dan jumlah total dolar dari catatan . Ketika penerima memproses data, jumlah total jumlah dan dolar barang yang diterima dapat dibandingkan dengan yang diberikan oleh pengirim untuk menentukan apakah ada bisa hilang atau diubah catatan . Namun, total kontrol mungkin tidak mengidentifikasi kasus di mana catatan telah diubah dalam bidang selain jumlahnya. Misalnya, nomor rekening tujuan atau nama pelanggan dapat berubah dengan yang account yang tidak sah . Dalam hal ini , jumlah total jumlah dan dolar catatan asli tidak akan berubah dan dengan demikian tidak akan diidentifikasi oleh total kontrol dasar.

Total Hash

Total hash adalah bentuk umum dari kontrol integritas/kelengkapan yang dapat mengurangi risiko perubahan catatan. Total hash hanyalah sebuah angka yang dihitung berdasarkan bidang kunci yang tidak memiliki perhitungan numerik dengan normal yang dilakukan di atasnya. Sebagai contoh, total rumus hash sederhana dapat menambahkan nomor akun atau nomor faktur dari setiap catatan dalam file data. Sebuah perubahan bahkan pada salah satu nomor akun atau faktur akan menyebabkan total hash berubah. Ketika penerima mengulang pengolahan data yang diterima, total tidak akan sama dengan total hash yang diberikan oleh pengirim, sehingga mewaspadai penerima memungkinkan merubah yang tidak sah atau tidak disengaja berebut data selama proses transmisi. Total hash yang lebih kompleks yang menggunakan algoritma aritmatika untuk menghitung variasi dan kombinasi dari beberapa bidang dapat dirancang. Hasilnya bahkan dapat

dienkripsi sebelum dikirim atau diangkut. Tujuan dasarnya adalah sama dengan total hash yang sederhana.

Pemisahan Tugas

Ketika memeriksa operasi bisnis atau proses tradisional SI terpusat seperti operasi komputer, pengembangan sistem, dan kontrol perubahan program, salah satu tujuan kontrol internal yang paling penting adalah pemisahan tugas. Tugas harus dipisahkan dengan benar untuk secara memadai melindungi organisasi dari akses yang tidak sah atas informasi, hilangnya aset fisik atau keuangan, dan segudang potensi risiko lainnya. Pemisahan tugas karenanya dapat berada di daerah entri data, daerah pengolahan data, dan di daerah operasi bisnis di mana hasil pengolahan dimanfaatkan. Pemisahan tugas dapat dilakukan lebih efektif melalui penyebaran yang tepat dan administrasi kemampuan akses sistem. (Lihat Bab 8 untuk pembahasan lengkap atas kontrol akses sistem.) Pelaksanaan dari kontrol prosedural yang kuat sama pentingnya tetapi lebih sulit dilakukan karena kemungkinan tingginya kesalahan atau gangguan manusia. Seperti yang akan terlihat dalam beberapa contoh selanjutnya dalam bab ini, pemisahan tugas di mana operasi bisnis sering goyah.

Kontrol Efisiensi/Efektivitas

Dalam setiap operasi bisnis, selalu hampir ada kesempatan untuk meningkatkan efisiensi dan efektivitas dengan mengotomatisasi prosedur manual. Manajemen mungkin sering mengabaikan kesempatan yang nyata karena mereka disibukkan dengan pemenuhan tenggat waktu yang sedang berlangsung dan berurusan dengan masalah operasional sehari-hari. Ironisnya, jika manajemen mengotomatisasi beberapa prosesnya yang paling sulit dan yang memakan waktu, mereka akan meningkatkan kemampuannya untuk memenuhi tenggat waktu dan mengurangi keparahan atas kesulitan operasional yang menyebabkannya menjadi yang paling berduka.

Penyeimbangan dan Pemantauan Database Internal

Laporan manajemen dan informasi lainnya yang berasal dari database yang dihasilkan secara internal hanya dapat diandalkan seperti data dari mana mereka berasal. Banyak organisasi membuat database ekstrak untuk digunakan dalam mempersiapkan berbagai jenis laporan khusus. Database ekstrak, pada dasarnya merupakan salinan database produksi asli, yang memungkinkan beberapa daerah pengguna akhir

mempersiapkan laporan khusus dan melakukan berbagai analisis basis data dan operasi lainnya tanpa mempengaruhi operasi produksi. Sehingga database ekstrak membuat lebih banyak informasi yang tersedia dari pengguna dalam sebuah organisasi yang melalui analisisnya, dapat membantu organisasi lebih efektif dalam mencapai tujuannya. Keamanan atas informasi yang nyata harus ketat untuk memastikan bahwa informasi tersebut tidak membahayakan. Tambahan, mungkin perhatian yang lebih penting adalah bahwa program ekstrak tersebut membuat database yang akurat. Jika tidak, informasi dan analisis hasil yang diperoleh dari database ekstrak mungkin tidak lengkap atau tidak berarti, kemungkinan akibat salah saji material informasi atau keputusan strategis yang buruk.

Dukungan yang Tidak Memadai dari Aplikasi Pengguna Akhir

Program aplikasi komputer khusus sedang dikembangkan pada tingkat yang mengkhawatirkan di daerah pengguna akhir. Banyak dari aplikasi ini dibuat oleh individu yang memiliki jumlah keterbatasan pelatihan teknis. Akibatnya, dokumentasi mengenai logika dan desain aplikasi biasanya terbatas atau tidak ada. Kemudian, ketika pengembang berpindah atau berhenti, begitu pula semua pengetahuannya tentang bagaimana mendukung aplikasi. Beberapa aplikasi pengguna akhir relatif sederhana dan dapat dengan mudah dipulihkan dan bahkan ditingkatkan ketika pengembang pergi. Juga ada banyak aplikasi yang sangat kompleks di mana organisasi pengguna akhir menjadi sangat bergantung. Jika pengembang dipindahkan atau dihentikan dan masalah muncul, manajemen bisa terlihat panik mencoba menghubungi pengembang sebelumnya. Dampak yang dihasilkan pada operasi bisnis bisa dihindari manajemen yang meminta pengembang meluangkan waktunya untuk mendokumentasikan aplikasi dari awal sehingga orang lain dengan pengetahuan yang cukup tentang bahasa atau perangkat lunak pengembangan dapat mendukung aplikasi.

Studi kasus 9.3 sampai 9.7 menggambarkan beberapa banyak jenis kelemahan kontrol internal SI dan inefisiensi yang mungkin terjadi dalam operasi bisnis di suatu organisasi. Bagi auditor, penting mencari jenis peluang untuk menunjukkan nilai mereka kepada manajemen sebagai konsultan bisnis yang dapat memberikan kontribusi terhadap pencapaian tujuan strategis.

Daftar Pustaka

1. See the discussion and examples on backup system security administrators in Chapter7 for some examples of why their activities need to be limited.
2. Pete Loshin, "IP: The Next Generation," *Information Security* (October 1998): 21.