MODUL PERKULIAHAN

EDP Audit

Aplikasi Organisasi Jasa Audit

(*Auditing Service Organization Applications*)

Abstract

Modul ini berisi Risiko lain dari aplikasi pemrograman secara internal adalah mungkin akan menjadi usang. Kadang-kadang perubahan teknologi, di lingkungan peraturan, atau dalam produk dan jasa yang ditawarkan oleh pesaing begitu signifikan atau tidak ada lagi biaya yang efektif untuk merawat aplikasi internal yang disesuaikan

Kompetensi

Mahasiswa mampu memahami tetang Risiko lain dari aplikasi pemrograman secara internal.

Pengantar

Banyak perusahaan menggunakan jasa organisasi eksternal dalam menyediakan aplikasi bisnis dan sumber pengolahan data yang di sisi lain akan terlalu mahal atau memakan waktu untuk mengembangkan dan memelihara secara internal. Organisasi-organisasi eksternal ini sering disebut sebagai organisasi jasa, biro jasa, atau prosesor pihak ketiga. Banyak organisasi jasa yang menyediakan berbagai aplikasi untuk hampir semua sektor industri dan pemerintah. Termasuk jasa untuk pengolahan penggajian, pelayanan pinjaman hipotek, pengamanan investasi, pengembangan dan pemeliharaan perangkat lunak, pengolahan transaksi automatic teller machine (ATM), pengolahan pemeriksaan, pembayaran tagihan elektronik, transfer bank, operasi kartu kredit, dan kepercayaan layanan.

Organisasi jasa menikmati skala ekonomi dengan mengembangkan dan memelihara aplikasi dan sistem komputer yang digunakan oleh ratusan atau ribuan perusahaan klien. Dengan pengolahan volume tinggi dari transaksi klien, biaya untuk memproses setiap transaksi melalui organisasi jasa sering secara signifikan lebih kecil daripada jika setiap klien mempekerjakan staf pemrograman dan pengembangan dan membeli atau menyewa perangkat keras komputer yang diperlukan untuk proses transaksi. Sebagai akibat dari kemajuan teknologi, perubahan dalam hukum dan peraturan, serta risiko bisnis lainnya, sebuah perusahaan mungkin menginvestasikan sumber keuangan yang signifikan dalam sebuah sistem komputer utama hanya untuk menemukan masalahnya dalam beberapa tahun. Demikian pula, sebuah perusahaan dapat mempekerjakan staf pemrograman untuk mengembangkan dan mempertahankan satu atau aplikasi lebih lainnya secara internal. Hanya setelah tahun penundaan proyek dan kelemahan dalam rancangan aplikasi perusahaan tidak menyadari bahwa itu akan menjadi lebih hemat biaya untuk mengadakan kontrak dengan organisasi jasa dalam memberikan aplikasi. Hal ini bukan untuk mengatakan bahwa perusahaan tidak harus mempertahankan pengembangan sistem dan staf pemeliharaan dan sistem komputer secara internal. Pada kenyataannya, organisasi-organisasi besar sangat berhasil menciptakan aplikasi mereka sendiri. Ada manfaat dan kelemahan pada kedua alternatif.

Aplikasi Organisasi Jasa Audit

Banyak perusahaan menggunakan jasa organisasi eksternal dalam menyediakan aplikasi bisnis dan sumber pengolahan data yang di sisi lain akan terlalu mahal atau memakan waktu untuk mengembangkan dan memelihara secara internal. Organisasi-organisasi eksternal ini sering disebut sebagai organisasi jasa, biro jasa, atau prosesor pihak ketiga. Banyak organisasi jasa yang menyediakan berbagai aplikasi untuk hampir semua sektor industri dan pemerintah. Termasuk jasa untuk pengolahan penggajian, pelayanan pinjaman hipotek, pengamanan investasi, pengembangan dan pemeliharaan perangkat lunak, pengolahan transaksi automatic teller machine (ATM), pengolahan pemeriksaan, pembayaran tagihan elektronik, transfer bank, operasi kartu kredit, dan kepercayaan layanan.

Organisasi jasa menikmati skala ekonomi dengan mengembangkan dan memelihara aplikasi dan sistem komputer yang digunakan oleh ratusan atau ribuan perusahaan klien. Dengan pengolahan volume tinggi dari transaksi klien, biaya untuk memproses setiap transaksi melalui organisasi jasa sering secara signifikan lebih kecil daripada jika setiap klien mempekerjakan staf pemrograman dan pengembangan dan membeli atau menyewa perangkat keras komputer yang diperlukan untuk proses transaksi. Sebagai akibat dari kemajuan teknologi, perubahan dalam hukum dan peraturan, serta risiko bisnis lainnya, sebuah perusahaan mungkin menginvestasikan sumber keuangan yang signifikan dalam sebuah sistem komputer utama hanya untuk menemukan masalahnya dalam beberapa tahun. Demikian pula, sebuah perusahaan dapat mempekerjakan staf pemrograman untuk mengembangkan dan mempertahankan satu atau aplikasi lebih lainnya secara internal. Hanya setelah tahun penundaan proyek dan kelemahan dalam rancangan aplikasi perusahaan tidak menyadari bahwa itu akan menjadi lebih hemat biaya untuk mengadakan kontrak dengan organisasi jasa dalam memberikan aplikasi. Hal ini bukan untuk mengatakan bahwa perusahaan tidak harus mempertahankan pengembangan sistem dan staf pemeliharaan dan sistem komputer secara internal. Pada kenyataannya, organisasi-organisasi besar sangat berhasil menciptakan aplikasi mereka sendiri. Ada manfaat dan kelemahan pada kedua alternatif.

Sementara organisasi jasa sering memproses transaksi dengan biaya yang lebih rendah dari pada ke klien mereka, mereka harus mencoba untuk menjaga aplikasi yang memenuhi seluruh kebutuhan kliennya. Beberapa klien mungkin memerlukan organisasi

jasa untuk mengembangkan modul yang disesuaikan dan memodifikasi ke aplikasi asli untuk memenuhi produk yang unik dan kebutuhan pelayananan. Organisasi jasa sebagian dapat mengimbangi kebutuhan ini dengan memasukkan tabel dan parameter ke dalam aplikasi mereka. Meja dan parameter ini kemudian dapat disesuaikan oleh masing-masing klien. Namun, akan selalu ada klien yang kebutuhannya tidak dapat diantisipasi ketika tabel dan parameter dirancang atau yang kebutuhannya begitu unik yang mengubah aplikasi utama dalam memenuhi kebutuhan tersebut yang dapat mempengaruhi klien lainnya. Dalam kasus ini, modul khusus harus dirancang dan terintegrasi dengan aplikasi utama di situs klien sementara aplikasi utama yang tersisa utuh. Dengan demikian, organisasi jasa harus terus-menerus memantau perubahan kebutuhan klien mereka dan memperbarui aplikasi mereka agar sesuai dengan kebutuhan orang-orang.

Jika sejumlah besar klien berkebutuhan khusus, organisasi jasa sering menjadi backlogged dan dengan demikian tidak mampu memenuhi kebutuhan semua kliennya pada waktu yang tepat. Mereka harus memprioritaskan permintaan klien mereka. Klien merupakan sumber pendapatan terbesar untuk organisasi jasa yang sering memberikan prioritas utama. Hal ini membuat klien kecil dirugikan dengan pesaing mereka yang mungkin akan memanfaatkan sebuah organisasi jasa yang berbeda atau yang mengembangkan dan memelihara aplikasi mereka sendiri. Kadang-kadang backlogs bisa berbulan-bulan atau bahkan bertahun-tahun. Dalam kasus terburuk, organisasi jasa mungkin harus menolak permintaan klien. Untungnya, kebanyakan perusahaan klien membentuk kelompok pengguna untuk membahas keberhasilan mereka dan kesulitan dengan aplikasi organisasi jasa. Jika beberapa perusahaan kecil meminta perubahan pemrograman yang sama, mereka mungkin dapat membentuk aliansi yang cukup kuat untuk meningkatkan permintaan mereka di depan klien yang besar. Ancaman klien meninggalkan dan mengambil bisnis mereka untuk persaingan organisasi jasa adalah cara yang efektif untuk mendapatkan permintaan pemrograman dilaksanakan. Seperti halnya dengan bisnis, organisasi jasa dapat bertahan hanya jika dikelola dengan cara yang mampu memenuhi persyaratan dari klien secara efisien dan cara efektif. Masalah tersebut bukan masalah utama organisasi jasa.

Banyak perusahaan mempertahankan staf pengembangan aplikasi internal dan personil servis. Perusahaan-perusahaan mampu membuat aplikasi yang disesuaikan sendiri tanpa bergantung pada organisasi jasa luar. Mereka tidak memiliki persaingan dengan perusahaan lain untuk melaksanakan permintaan pemrograman khusus. Manfaat ini sering memungkinkan perusahaan untuk menyesuaikan aplikasi mereka sesuai dengan kebutuhan

produk dan layanan mereka secara tepat waktu. Namun, hambatan yang sama yang dihadapi organisasi jasa dapat terjadi dalam perusahaan yang membuat program aplikasi mereka sendiri. Sebagai contoh, banyak perusahaan yang memiliki berbagai departemen, masing-masing memanfaatkan aplikasi yang berbeda untuk memproses informasi mereka. Ketika ada sistem baru atau perlu perubahan pemrograman pada sistem, masing-masing departemen mengajukan permintaan untuk daerah pengembangan atau pemeliharaan sistem informasi (SI) untuk tindakan. Area sistem informasi dihadapkan dengan sumber daya yang terbatas dan, seperti organisasi-jasa, harus memprioritaskan permintaan masing- masing departemen. Secara teori, permintaan yang paling menjanjikan manfaat keuangan organisasi yang diberikan prioritas. Seringkali, bagaimanapun, departemen yang terbesar keuangannya atau pengaruh politik terbesar mendapatkan permintaan mereka selesai lebih cepat dari departemen lain. Ketika sebuah perusahaan meramping secara signifikan, backlog dapat mencapai berbulan-bulan atau bertahun-tahun, seperti yang dibuktikan dalam kasus studi 5.1.

STUDI KASUS 5.1

Backlog Permintaan Pemrograman

Sebuah perusahaan perbankan besar telah mengkonsolidasikan pusat pengolahan data yang terletak di berbagai negara individu ke daerah pusat pengolahan data yang sedang diaudit. Sejak perusahaan juga menerapkan perampingan staf yang luas, sumber staf pengembangan dan pemeliharaan SI dikhususkan hampir secara eksklusif mengusahakan konsolidasi pengolahan data. Hanya dalam kasus di mana sistem menjadi tidak berfungsi atau diperlukan perubahan untuk mematuhi undang-undang pemerintah dan peraturan akan permintaan pemrograman yang dihormati secara tepat waktu. Semua permintaan lain masih diterima dan ditempatkan di antrian. Standar backlog untuk penyelesaian adalah dua tahun. Oleh karena itu, ketika audit sistem informasi yang dilakukan dan disampaikan rekomendasi perubahan pemrograman yang diperlukan, manajemen sering tidak dapat melaksanakan rekomendasi, sekalipun mereka setuju bahwa perubahan yang diperlukan harus dibuat sesegera mungkin. Manajemen puncak telah dipilih untuk menanggung risiko yang tidak meningkatkan kontrol atas sistem informasi mereka. Untungnya, kerugian yang signifikan tidak diketahui telah terjadi sebagai akibat dari dua tahun backlog untuk menyelesaikan sebagian permintaan perubahan pemrograman.

Risiko lain dari aplikasi pemrograman secara internal adalah mungkin akan menjadi usang. Kadang-kadang perubahan teknologi, di lingkungan peraturan, atau dalam produk dan jasa yang ditawarkan oleh pesaing begitu signifikan atau tidak ada lagi biaya yang efektif untuk merawat aplikasi internal yang disesuaikan. Karena aplikasi internal mereka dan prosedur operasional yang terkait begitu unik, perusahaan mungkin menemukan bahwa kontrak dengan organisasi jasa dan merevisi prosedur operasional yang ternyata sangat mahal, dampak perubahan untuk produk dan layanan pelanggan, dan membuat stres staf operasional. Untuk alasan ini, manajemen masing-masing perusahaan harus melakukan analisis rinci untuk menentukan apakah kebutuhan produk dan layanan yang terbaik harus dipenuhi oleh kontraktor dengan organisasi jasa atau mempekerjakan staf khusus untuk mengembangkan dan memelihara aplikasi secara internal. Bagian berikutnya dari bab ini memberikan latar belakang mengenai laporan yang disiapkan oleh auditor eksternal yang independen (juga dikenal sebagai auditor jasa) pada kecukupan kontrol kebijakan SI dan prosedur di tempat di organisasi jasa.

LAPORAN AUDITOR JASA

Kebanyakan organisasi jasa utama mengontrak sebuah perusahaan audit independen untuk mengungkapkan pendapat mengenai kecukupan kebijakan dan prosedur dalam organisasi jasa yang dapat mempengaruhi lingkungan pengendalian internal organisasi klien. Dalam beberapa kasus, auditor independen mungkin dikontrak untuk melakukan pengujian tambahan dalam menentukan apakah kebijakan dan prosedur beroperasi secara efektif di dalam organisasi jasa. Laporan auditor jasa memberikan beberapa jaminan kepada klien yang memadai mengenai pengendalian ada dalam organisasi jasa untuk memastikan keandalan, integritas, dan kerahasiaan informasi pelanggan klien. Standar audit profesional yang berkaitan dengan penerbitan laporan auditor jasa di sebagian besar negara maju serupa tetapi tidak berarti identik. Beberapa standar memberikan jaminan yang lain daripada yang lain. Oleh karena itu, ketika memeriksa laporan auditor jasa, pembaca harus sadar di mana negara organisasi jasa berkedudukan. Paragraf berikut memeriksa status saat ini dari standar profesional audit yang berkaitan dengan berbagai jenis laporan auditor jasa yang dikeluarkan di Amerika Serikat, Kanada, Britania Raya dan Australia.

Amerika Serikat

Di Amerika Serikat, organisasi jasa dapat mempekerjakan auditor eksternal yang independen untuk mengungkapkan salah satu dari dua jenis pendapat pada kebijakan dan prosedur di organisasi jasa yang mungkin relevan dengan struktur pengendalian internal organisasi yang memanfaatkan jasa. Pelaporan dan persyaratan untuk pengujian auditor eksternal melakukan keterlibatan tersebut seperti yang ditentukan Pernyataan Standar Audit 70 (SAS 70), yang dikeluarkan oleh Badan Standar Audit dari American Institute of Certified Public Accountant (AICPA). SAS 70 mengatakan "Organisasi Jasa" dan untuk laporan auditor jasa efektif setelah tanggal 31 Maret 1993. (Catatan: SAS 70 diamandemen, efektif Desember 1999, dari "Laporan pengolahan transaksi oleh organisasi jasa" oleh SAS 88 berjudul "Organisasi layanan dan konsistensi pada laporan."). Jenis laporan pertama mengungkapkan, antara lain, pendapat auditor mengenai apakah kebijakan dan prosedur yang relevan ditempatkan dalam operasi organisasi jasa "pada tanggal tertentu."[1] Jenis laporan tidak mengungkapkan pendapat untuk efektivitas operasi dari kebijakan dan prosedur tersebut. Tipe laporan kedua menyatakan pendapat auditor mengenai apakah kebijakan dan prosedur yang relevan ditempatkan di organisasi jasa dan apakah kebijakan dan prosedur tersebut beroperasi secara efektif. Untuk merumuskan pendapat di antara kedua jenis laporan, auditor perlu melakukan berbagai tes untuk mengkonfirmasikan bahwa kebijakan dan prosedur dalam organisasi jasa berfungsi dengan benar. SAS 70 meneruskan dengan menyatakan bahwa "untuk menjadi berguna untuk pengguna auditor, laporan biasanya harus mencakup periode pelaporan minimal enam bulan."[2] SAS 70 menggantikan SAS 44, yang berjudul "tujuan khusus laporan pada akuntansi kontrol internal di organisasi jasa "dan diperlukan untuk tujuan khusus laporan pada kontrol akuntansi internal setelah tanggal 31 Desember 1982. Perbedaan utama antara SAS 70 dan SAS 44 adalah bahwa SAS 70 menentukan minimum periode pelaporan enam bulan. Di bawah SAS 44, jangka waktu yang diperlukan tidak ditentukan. Sebaliknya, periode pengujian yang diperlukan telah diserahkan kepada penilaian auditor. Laporan SAS 44 biasanya ditutupi jangka waktu sekitar dua sampai empat bulan, kecuali dalam kasus di mana kontrol kelemahan-kelemahan penting teridentifikasi.

Kanada

Di Kanada yang setara dari SAS 70 adalah Pasal 5900 dari Handbook of Audit yang diterbitkan oleh Canadian Institute of Chartered Accountants (CICA). Pasa 5900 berjudul "Pendapat tentang prosedur pengendalian di organisasi jasa" dan ini efektif untuk keterlibatan yang periodenya pada atau setelah 1 Juli 1987. Seperti SAS 70, Pasal 5900

merincikan dua jenis pendapat yang mungkin diungkapkan oleh auditor eksternal. Salah satunya terkait dengan "desain dan keberadaan prosedur pengendalian di organisasi jasa" sedangkan yang kedua terkaitan dengan "desain, operasi yang efektif, dan kontinuitas prosedur kontrol di organisasi jasa." Jenis pertama dari pendapat ini menuntut auditor hanya untuk membuktikan desain dan keberadaan prosedur pengendalian " pada satu titik waktu."[3] Tidak ada pendapat yang dinyatakan mengenai efektivitas operasional dari prosedur kontrol. Pendapat jenis kedua mesyaratkan auditor untuk melakukan tes dan memperoleh pernyataan manajemen mengenai operasi yang efektif dari prosedur pengendalian "sepanjang waktu yang ditentukan."[4] Tidak seperti SAS 70, Pasal 5900 tidak merekomendasikan secara khusus periode pengujian waktu enam bulan. Jangka waktu yang diperlukan untuk memperoleh keyakinan mengenai apakah prosedur pengendalian beroperasi secara efektif telah diserahkan kepada penilaian profesional dari auditor eksternal. Namun, pengujian periode enam bulan dapat disimpulkan dari contoh Laporan Auditor Jasa di Pasal 5900, yang menyatakan bahwa auditor "melakukan tes efektivitas prosedur pengendalian tersebut untuk periode 1 Januari 19X1 sampai 30 Juni, 19X1."[5]

Inggris (Britania Raya)

Pada bulan September 1994, Fakultas Teknologi Informasi (FIT) dari Institut Chartered Accountants di Inggris dan Wales (ICAEW) mengeluarkan Technical Release FIT 1/94, yang setara dengan SAS 70, "laporan pada pengolahan transaksi oleh organisasi jasa." FIT 1/94 dimaksudkan hanya untuk menerapkan hal-hal yang berkaitan dengan organisasi jasa yang memberikan jasa pemrosesan data, meskipun beberapa prinsip-prinsip yang juga mungkin relevan dengan jenis-jenis jasa yang disediakan oleh organisasi jasa. FIT 1/94 sangat mirip dengan SAS 70 dan Pasal 5900 Kanada. Auditor dapat mengeluarkan pendapat mereka tentang kebijakan dan prosedur organisasi jasa saja atau pada kebijakan dan prosedur serta tes kepatuhan terhadap kebijakan dan prosedur. Tujuan pengendalian untuk organisasi jasa ditentukan dalam laporan, termasuk sumber daya mereka. Untuk pendapat dengan tes kepatuhan, FIT 1/94 menetapkan bahwa "agar efektif untuk auditor pengguna, laporan biasanya akan perlu menutupi minimum pelaporan periode enam bulan."[6]
Dokumen panduan mirip dengan FIT 1/94 yang dirilis oleh Kelompok Pelaporan Keuangan Dan Audit (FRAG) dari ICAEW pada Mei 1994. Technical Release FRAG 21/94, berjudul "laporan pada kontrol internal atas penjaga investasi dibuat tersedia untuk pihak ketiga," lebih kecil dalam lingkup daripada FIT 1/94. Fokus utama pada kegiatan kustodian yang berhubungan dengan bisnis investasi. Kegiatan usaha lainnya tidak ditangani. Laporan di

bawah FRAG 21/94 termasuk pendapat auditor apakah "kontrol kebijakan dan prosedur yang sesuai dirancang untuk mencapai tujuan kontrol tertentu" dan bahwa "yang berhubungan dengan tujuan pengendalian dicapai selama periode tersebut."[7] Tidak seperti FIT 1/94, FRAG 21/94 tidak memerlukan jangka waktu minimum laporan. Juga, kecukupan tujuan kontrol tidak dinilai oleh auditor. Apendiks III dari FRAG 21/94 termasuk contoh ilustratif laporan manajemen, yang meliputi bagian kontrol kebijakan dan prosedur yang ditetapkan untuk memastikan bahwa tujuan pengendalian tercapai. Antara kontrol kebijakan dan prosedur, termasuk Bagian FRAG 21/94 di tujuan "keamanan dan integritas sistem komputer".[8] Bagian ini terbagi 11 daerah kontrol:

1. Daerah masuk pengolahan data yang tidak sah
2. Pembatasan akses ke sistem operasi, perangkat lunak utilitas, aplikasi, perangkat lunak komunikasi dan data
3. Pencatatan dan deteksi atas upaya akses sistem yang tidak sah
4. Keakuratan data entry dan integritas dari informasi yang disalurkan melalui jaringan
5. Rekonsiliasi data output
6. Definisi dan deskripsi dari semua laporan
7. Prosedur tertulis untuk memastikan keakuratan, kelengkapan, dan otorisasi dari semua transaksi
8. Jejak audit yang akurat
9. Dokumentasi yang memadai dari semua sistem pengolahan data
10. Pengarsipan yang memadai dan penyimpanan catatan dan program
11. Pelaksanaan atas prosedur kontingensi yang memadai

Daerah kontrol ini cukup komprehensif dan dapat diterapkan untuk banyak jenis kontrol lingkungan SI. Oleh karena itu, mereka dapat difungsikan sebagai referensi yang berguna untuk auditor eksternal.

Australia

Australia tidak memiliki standar audit yang berlaku untuk auditor jasa seperti penulisan buku ini. Australian Accounting Research Foundation (AARF) mengakui ketiadaan standar tersebut sebagai kekurangan dan dalam proses penyusunan Pernyataan Pedoman Audit (AGS) pada entitas outsourcing.[9] Manajer proyek AARF yang bertanggung jawab atas AGS baru pada entitas outsourcing melaporkan bahwa hal ini berfokus pada tiga konsep:

1. Berlaku untuk perjanjian outsourcing, termasuk namun tidak terbatas pada perjanjian entitas jasa (berlaku, organisasi jasa)
2. Mendorong "efektivitas" pelaporan kontrol daripada pelaporan "desain-saja"
3. Mendorong pelaporan "periode waktu" daripada pelaporan "waktu tertentu"

Butir 1 lebih komprehensif daripada SAS 70, Pasal 5900 atau FIT 1/94. Butir 2 dan 3 konsisten dengan kedua jenis laporan SAS 70, yang mengungkapkan pendapat auditor mengenai apakah kebijakan dan prosedur relevan pada tempat di organisasi jasa dan apakah kebijakan dan prosedur bahkan beroperasi secara efektif. Manajer Proyek AGS Australia juga menyatakan bahwa AGS baru didasarkan pada sebagian besar pada AARF dokumen komentar undangan (IC) berjudul "laporan kontrol internal," yang disusun oleh Badan Standar Audit dari AARF pada bulan April 1996. Beberapa highlights yang relevan dengan dokumen IC termasuk:

- Melaporkan pengendalian internal yang dianggap sebagai jenis tertentu dari audit kinerja dan harus dibaca dalam hubungannya dengan AUS 806, "Audit Kinerja", dan AUS 808, "Perencanaan dan Audit Kinerja," untuk mendapatkan pemahaman yang lebih komprehensif. AUS 806 dan AUS 808 memberikan prinsip-prinsip umum, praktik, dan panduan yang relevan terhadap laporan auditor dalam kontrol internal.
- Laporan pengendalian internal adalah keterlibatan yang terpisah dari laporan keuangan audit. Meskipun mungkin dilakukan dalam hubungannya dengan satu sama lain, masing-masing membutuhkan sebuah laporan terpisah.
- IC mengadopsi definisi umum pengendalian internal, yang meliputi:
    1. Efektivitas, efisiensi dan ekonomisasi operasi
    2. Kehandalan manajemen dan pelaporan keuangan
    3. Sesuai dengan hukum yang berlaku dan peraturan serta kebijakan internal

  Definisi pengendalian internal ini konsisten dengan kerangka kerja dari Committee of Sponsoring Organizations (COSO) di Amerika Serikat, Criteria of Control Board (CoCo) di Kanada, dan Cadbury Committee di Britania Raya. Kerangka pengendalian internal ini dibahas lebih rinci pada Bab 10.
- Dokumen IC didasarkan pada alasan bahwa setiap evaluasi efektivitas pengendalian internal tidak terpisahkan dari pertimbangan tujuan yang mengarahkan pengendalian internal dan risiko yang mengancam pencapaian tujuan tersebut. Kriteria yang memperhitungkan tujuan dan risiko tersebut harus diidentifikasi secara jelas sebelum pendapat yang bermakna tentang efektivitas dinyatakan. Tanpa

kriteria tersebut, laporan auditor akan terbuka untuk interpretasi yang berbeda secara luas dan subjektif dari masing-masing pengguna.

- Pengujian dari efektivitas operasi harus dilakukan selama periode waktu yang cukup untuk menentukan bahwa pengendalian internal beroperasi secara efektif. Periode waktu di mana auditor akan melakukan pengujian efektivitas operasi merupakan masalah penilaian.

Berdasarkan informasi tersebut, hal ini wajar untuk mengharapkan Pernyataan Panduan Audit pada Entitas Outsourcing AARF akan memberikan banyak pedoman atau lebih untuk auditor eksternal yang menyiapkan laporan mengenai lingkungan pengendalian internal organisasi jasa di Australia seperti halnya SAS 70, Pasal 5900, dan FIT 1/94. Sebagai bagian dari AGS, juga akan cukup diharapkan kontrol internal atas sistem informasi dalam organisasi jasa akan diatasi secara memadai.

Di bulan Januari 1997, pengurus standar audit AARF mengeluarkan AGS 1026 berjudul "dana pensuin—laporan auditor atas pengelolaan aset." AGS 1026 ini sangat mirip dengan dokumen FRAG 21/94 di Britania Raya yang memberikan beberapa pedoman tentang kontrol SI, meskipun hanya untuk jenis entitas tertentu. AGS 1026 ditujukan terutama untuk auditor dana pensiun dan terbatas pada penjelasan dan aplikasi standar yang ada dengan keadaan di mana auditor dana pensiun mungkin perlu memperoleh bukti- bukti audit yang diperlukan mengenai pengelolaan aset eksternal melalui laporan yang dikeluarkan oleh auditor dari manajer eksternal. Panduan ini dimaksudkan untuk memberikan indikasi yang jelas mengenai kebutuhan pengawas dan auditor dana pensiun serta berusaha untuk mencapai konsistensi yang lebih besar dalam permohonannya akan laporan oleh auditor dari manager eksternal.[11]

Laporan AGS 1026 mencakup pendapat auditor pada apakah manajer dana pensiun eksternal menegakkan pengendalian internal yang efektif untuk aset di bawah manajemen pada periode akhir tanggal, berdasarkan pada kriteria yang ditetapkan dalam laporan manajemen tentang pengendalian internal, yang dilampirkan pada laporan audit. AGS 1026 tidak menentukan minimum periode pelaporan secara khusus, dan kecukupan atas kriteria kontrol manajemen yang tidak diperlukan untuk dinilai oleh auditor. Seperti FRAG 21/94, Apendiks 3 dari AGS 1026 termasuk contoh ilustratif laporan manajemen atas kontrol internal, yang meliputi bagian pada kontrol kebijakan dan prosedur yang ditetapkan untuk memastikan bahwa tujuan pengendalian tercapai. Antara kontrol kebijakan dan prosedur, AGS 1026 termasuk pada bagian tujuan yang berjudul "Keamanan dan Integritas Sistem

Komputer."[12]. Bagian ini berisi 10 daerah kontrol, yang sebagian besar ditetapkan dalam FRAG 21/94:

1. Daerah masuk pengolahan data yang tidak sah
2. Pembatasan akses ke sistem operasi, perangkat lunak utilitas, aplikasi, perangkat lunak komunikasi dan data
3. Pencatatan dan deteksi atas upaya akses sistem yang tidak sah
4. Keakuratan data entry dan integritas dari informasi yang disalurkan melalui jaringan
5. Prosedur tertulis untuk memastikan keakuratan, kelengkapan, dan otorisasi dari semua transaksi
6. Jejak audit yang akurat
7. Dokumentasi yang memadai dari semua sistem pengolahan data
8. Pengarsipan yang memadai dan penyimpanan catatan dan program
9. Prosesf formal untuk menguji program baru sebelum dikeluarkan
10. Pelaksanaan prosedur kontingensi yang memadai

Butir 9 merupakan daerah kontrol yang tidak termasuk dalam FRAG 21/94. Proses formal untuk menguji program baru sebelum dikeluarkan merupakan daerah kontrol yang layak disebutkan secara spesifik. Daerah kontrol ini dapat diterapkan tidak hanya dalam konteks dana pension tetapi untuk semua kontrol lingkungan SI. Perbedaan lain antara AGS 1026 dan FRAG 21/94 bahwa AGS mengecualikan dua daerah kontrol yang berkaitan dengan rekonsiliasi data output dan definisi serta deskripsi dari semua laporan (daerah kontrol 5 dan 6 di bawah FRAG 21/94). Tampaknya bahwa butir-butir tersebut dikeluarkan karena lebih operasional dalam sifatnya daripada berkaitan secara khusus dengan keamanan dan integritas sistem informasi komputer. Oleh karena itu, pengecualian tersebut tidak boleh dianggap kerugikan yang signifikan dari pedoman AGS 1026.

Seperti FRAG 21/94, daerah-daerah kontrol AGS 1026 cukup komprehensif dan dapat berfungsi sebagai referensi yang berguna dan dapat diterapkan oleh auditor serta pihak yang berkepentingan untuk hampir semua jenis kontrol lingkungan SI.

Auditor internal dan pihak penting lainnya yang memanfaatkan SAS 70, Pasal 5900, FIT 1/94, dan laporan serupa harus waspada terhadap kenyataan bahwa jika auditor eksternal menyatakan tidak wajar atau pendapat tidak memenuhi syarat sebagai efektivitas operasi dari kebijakan dan prosedur yang relevan dalam organisasi jasa, mungkin ada kebijakan dan prosedur yang relevan dimana auditor eksternal tidak dipekerjakan untuk mengungkapkan pendapat. Pada kenyataannya, SAS 70 menyatakan, "manajemen dari

organisasi jasa menentukan apakah semua atau aplikasi terpilih dan tujuan kontrol akan ditutupi oleh pengujian efektivitas operasi."[13] Inilah sebabnya hal ini penting untuk memeriksa laporan dengan hati-hati agar memahami daerah yang diuji dan untuk menentukan apakah sebuah organisasi harus mendapatkan keyakinan tambahan dari organisasi jasa mengenai keberadaan dan kebijakan dan prosedur efektivitas operasi yang tidak diuji dalam laporan asli auditor jasa. Studi kasus 5.2 membahas situasi di mana risiko signifikan mempengaruhi lingkungan kontrol klien yang ada dengan aplikasi organisasi jasa, tapi risiko tersebut tidak disebutkan sebagai kontrol pertimbangan untuk organisasi klien. Pembaca harus menyadari masalah yang disajikan dalam studi kasus adalah langka. Sebagian besar laporan auditor jasa berkualitas tinggi dan sangat berguna dalam mengevaluasi pengendalian internal organisasi klien serta memahami lingkungan kontrol di organisasi jasa. Selain masalah yang dijelaskan dalam studi kasus 5.2, jeda laporan auditor jasa yang dimaksud sangat baik.

STUDI KASUS 5.2

Risiko Signifikan Dengan Aplikasi Organisasi Jasa

Audit internal dilakukan atas kontrol keamanan logis dari sebuah aplikasi yang berlisensi dari organisasi jasa dan diinstal pada perangkat keras komputer di organisasi klien. Organisasi jasa memberikan pemeliharaan dan dukungan untuk perangkat lunak dan juga data yang diolah kepada organisasi klien yang lebih kecil. Setiap dua tahun sekali, organisasi jasa menyewa auditor independen untuk menyiapkan laporan SAS 70 pada kebijakan dan prosedur yang relevan yang ditempatkan dalam operasi dan efektivitas operasi dari kebijakan dan prosedur tersebut. Salah satu langkah audit adalah menguji laporan SAS 70 pada organisasi jasa. Menurut pendapat auditor jasa, kebijakan dan prosedur yang beroperasi dengan efektivitas yang cukup untuk memberikan kewajaran, namun tidak mutlak, keyakinan bahwa tujuan pengendalian yang ditentukan dalam laporan tersebut dicapai selama periode enam bulan pengujian. Dengan kata lain, tidak ada masalah signifikan yang dapat mempengaruhi organisasi klien yang teridentifikasi dalam laporan auditor jasa.

Pengujian rinci atas kontrol keamanan logis dari aplikasi yang ditempatkan di organisasi klien kemudian dilakukan. Selama rangkaian pengujian, tercatat bahwa kekurangan kontrol utama yang ada dalam desain aplikasi mempengaruhi setiap klien yang menggunakan aplikasi organisasi jasa. (Pada saat itu ada sekitar 600 organisasi klien.) Kelemahannya adalah file password di setiap lokasi klien tidak dienkripsi. Alhasil,

pengguna dengan kemampuan akses sistem administrasi di setiap lokasi klien bisa melihat password semua pengguna dalam organisasinya. Kejadian ini bisa dilakukan secara rutin dalam aplikasi perangkat lunak. Administrator sistem keamanan bahkan tidak perlu mencari file password pada tingkat sistem operasi. Selain itu, karena dukungan teknisi di organisasi jasa memerlukan kemampuan sistem administrasi ketika mereka memasang melalui modem ke organisasi klien, mereka juga bisa melihat password dari semua pengguna jika mereka mau. Karena klien dari organisasi jasa semuanya lembaga keuangan, kelemahan kontrol dianggap menjadi masalah besar.

Salah satu contoh dari risiko yang terkait dengan kelemahan ini adalah teller di organisasi klien bergantung pada password untuk memastikan bahwa hanya transaksi mereka yang diposting di bawah nomor unik identifikasi teller. Salah satu tujuan dari kontrol password untuk memberikan jejak audit jika ada transaksi yang memerlukan penyelidikan, termasuk situasi di mana penipuan transaksi mungkin terposting . Namun, siapa pun dengan kemampuan akses sistem administrasi atau teknisi organisasi jasa yang dipanggil untuk organisasi klien bisa mencari password teller dan kemudian melakukan transaksi yang tidak sah menggunakan nomor identifikasi teller, dengan demikian menghapuskan kepemilikan tunggal atas transaksi yang diposting pada sistem. Juga, jika teller menyadari bahwa orang lain bisa mencari passwordnya, kasir bisa melakukan transaksi yang tidak sah dan kemudian mengklaim bahwa administrator sistem keamanan atau teknisi organisasi jasa telah melihat passwordnya dan melakukan transaksi. Dalam pengadilan, kasir bisa membuktikan bahwa ada beberapa orang yang memiliki kemampuan untuk melihat password dan dengan demikian menciptakan sebuah "keraguan yang beralasan", apakah teller telah melakukan transaksi .

Dianjurkan kepada manajemen yang sesuai dalam organisasi klien permohonan harus disampaikan ke organisasi jasa untuk memodifikasi aplikasi sehingga password file terenkripsi. Setelah tiga tahun, manajemen klien masih belum mengambil tindakan. Kelemahan ini dibahas dengan auditor lain di beberapa organisasi klien, bahkan hanya satu yang menyadari kelemahan kontrol. Sayangnya, organisasi klien lain juga tampaknya tidak cukup peduli dengan kelemahan kontrol yang sangat menyarankan kepada organisasi jasa bahwa file password akan dienkripsi.

Para manajer audit internal organisasi jasa ditanya apakah dia menyadari kelemahan dan mengapa hal itu tidak disebutkan dalam laporan auditor jasa. Dia menyatakan bahwa dia tidak menyadari masalah ini dan harus mengkonfirmasikannya dengan teknisi. Setelah berdiskusi dengan teknisi, manajer audit internal menyatakan bahwa modul sistem otorisasi

baru telah ada selama lebih dari satu tahun dan bahwa modul baru ini memiliki file password terenkripsi. Dia menyatakan bahwa modul pada organisasi klien yang diperiksa adalah versi lama. Organisasi jasa tidak mengingkari kenyataan bahwa enkripsi file password adalah salah satu perangkat tambahan dari modul sistem otorisasi baru. Meskipun dianjurkan untuk manajemen organisasi klien agar modul baru diadopsi, mereka tidak melihat alasan yan cukup kuat untuk mengadopsi modul baru. Karena organisasi jasa tidak membutuhkan kliennya untuk bermigrasi ke sistem otorisasi baru, banyak organisasi klien yang masih terkena risiko bahwa pengguna dengan kemampuan sistem administrasi bisa melihat password pengguna lain dan melakukan fungsi yang tidak sah.

Dan seperti mengapa kelemahan file password tidak disebutkan dalam laporan auditor jasa terbaru, manajer audit internal organisasi jasa menyatakan bahwa auditor eksternal telah menguji modul sistem otorisasi baru saja. Dia tidak bisa menjelaskan mengapa laporan auditor jasa sebelum penciptaan modul sistem otorisasi baru tidak mengidentifikasi fakta bahwa file password pengguna tidak terenkripsi. Dia kemudian berkata bahwa manajer audit eksternal bertugas menyiapkan laporan auditor jasa yang memiliki rincian lebih detail tentang penyusunan laporan auditor jasa. Sebagai masalah catatan, manajer audit internal di organisasi jasa sebelumnya menjadi auditor di perusahaan audit eksternal yang menyiapkan laporan auditor jasa.

Manajer di perusahaan audit eksternal ditanya apakah dia sadar bahwa administrator sistem keamanan bisa melihat password pengguna di bawah modul sistem otorisasi lama. Dia menyatakan bahwa organisasi jasa tidak mengidentifikasi kelemahan auditor jasa dan pengujian auditor jasa tidak mengidentifikasi kelemahan. Dia setuju bahwa itu adalah masalah pengendalian internal yang signifikan dan memahami kenyataan bahwa kelemahan kontrol ini telah diidentifikasi sehingga mereka bisa mengujinya selama pemeriksaan berikutnya atas aplikasi organisasi jasa. Pengujian akan diterapkan ke modul sistem otorisasi yang baru dan setiap modul yang lama masih digunakan di organisasi klien . Tergantung pada hasil pengujian mereka, mereka mungkin mengidentifikasi kelemahan kontrol dalam laporan auditor jasa berikutnya. Manager auditor jasa menyatakan bahwa ia berharap ia mengetahui kelemahan sebelum penyelesaian pengujian laporan auditor jasa yang terbaru, karena yang berikutnya tidak akan disiapkan untuk dua tahun lagi.

Baik manajer audit internal di organisasi jasa maupun manajer di perusahaan auditor jasa menyatakan bahwa kami adalah organisasi klien pertama yang menyebutkan kelemahan kontrol untuk mereka. Hal ini sangat mengguncang pikiran bahwa lebih dari 600 organisasi klien, yang semuanya adalah lembaga keuangan, hanya satu yang menyadari

kelemahan kontrol dan menemukan itu cukup signifikan untuk didiskusikan dengan organisasi jasa dan auditor jasa. Masalah ini tampaknya belum dibahas di setiap konferensi kelompok pengguna tahunan dimana organisasi klien dan organisasi jasa membahas peningkatan aplikasi yang diinginkan.

Kesalahan desain lain dari aplikasi organisasi jasa adalah kemampuan akses ditentukan oleh tingkat keamanan hirarkis. Seorang pengguna dengan tingkat keamanan 8, misalnya, bisa melakukan semua fungsi akses yang dipetakan ke tingkat keamanan 8 serta semua yang dipetakan ke salah satu tingkat yang lebih rendah (0 sampai 7). Dengan ratusan fungsi, banyak yang diperlukan untuk digunakan dalam beberapa departemen, hampir mustahil untuk menentukan tingkat keamanan kepada pengguna di daerah tertentu tanpa memberikan mereka kemampuan akses tambahan yang tidak diperlukan untuk tugas normal mereka. Sebuah alternatif telah menetapkan tingkat keamanan terendah untuk semua pengguna dan kemudian, secara individual, khususnya menetapkan setiap fungsi akses tambahan yang diperlukan bagi mereka untuk melakukan tugas normal mereka. Dengan ratusan pengguna, alternatif ini secara operasional tidak praktis untuk daerah yang melaksanakan tugas administrasi sistem pada organisasi klien yang saya periksa.

Untuk memperumit masalah, manajemen pengolahan data di organisasi klien memilih untuk tidak memisahkan tugas administrasi keamanan, operasi komputer, dan analisis perangkat lunak sistem. (Organisasi klien tidak memiliki programer dalam apapun.) Organisasi klien memetakan semua fungsi yang diperlukan untuk melakukan tugas-tugas yang berbeda untuk tingkat keamanan tertinggi hirarki. Setiap pengguna di departemen pengolahan data diberikan tingkat keamanan ini. Oleh karena itu, semua pengguna di departemen pengolahan data memiliki kemampuan untuk menjalankan pekerjaan, instalasi dan pengujian perangkat lunak, menambah dan menghapus pengguna, mengubah kemampuan akses pengguna dan parameter sistem keamanan, dan melakukan segudang fungsi lainnya. Selain itu, seluruh departemen pengolahan data memiliki kemampuan untuk mendapatkan password dari setiap pengguna yang mereka inginkan dan kemudian melakukan transaksi yang tidak sah. Kami menyajikan masalah ini kepada manajemen pengolahan data dan merekomendasikan agar tugas tersebut dipisahkan. Manajemen memilih untuk tidak melaksanakan rekomendasi tersebut dengan dalih bahwa semua pengguna di departemen pengolahan data bisa dipercaya.

Sekali lagi, laporan auditor jasa tidak mengidentifikasi tabel tingkat keamanan hirarkis sebagai pertimbangan kontrol klien atau kelemahan kontrol. Setidaknya dengan modul sistem otorisasi yang baru, tabel tingkat keamanan hirarkis dihapuskan. Sebaliknya,

kelompok independen dari pengguna dapat ditentukan, masing-masing dengan mengatur sendiri fungsi akses yang dipetakannya. Karena kelompok yang non hirarkis, akses ke satu kelompok tidak memberikan akses ke setiap fungsi akses dari setiap kelompok pengguna lainnya. Sayangnya, organisasi klien yang tidak mengadopsi sistem modul otorisasi baru akan beresiko signifikan lebih besar dari akses yang tidak sah daripada mereka yang mengadopsi modul baru. Organisasi jasa tidak memerlukan klien untuk bermigrasi ke modul baru, kemungkinan besar karena potensi ketidaknyamanan kepada organisasi klien. Ketidaknyamanan ini, ditambah dengan masalah layanan lainnya, dapat menyebabkan organisasi klien untuk mencari organisasi jasa baru.

Karena situasi seperti yang dibahas dalam studi kasus 5.2, auditor jasa selalu menyertakan pernyataan bahwa pengujian mereka tidak memberikan jaminan mutlak atas semua masalah pengendalian internal yang signifikan yang mempengaruhi organisasi klien akan diidentifikasi. Pernyataan disclaimer tersebut dapat meringankan auditor jasa dari beberapa atau semua kewajiban tuntutan hukum terhadap mereka karena kerugian yang terjadi sebagai akibat dari kelemahan pengendalian yang tidak teridentifikasi dalam laporan mereka.

PENGGUNAAN LAPORAN AUDITOR JASA UNTUK AUDIT INTERNAL

Setelah sebuah organisasi telah menetapkan bahwa akan mengontrak organisasi jasa, salah satu langkah pertama tim pengembangan proyek di organisasi klien harus lakukan pemeriksaan salinan laporan auditor jasa yang baru dari setiap penawaran organisasi jasa. Pemeriksaan ini harus dilakukan sebelum ada kontrak apapun yang masuk dengan organisasi jasa. Kelemahan kontrol yang signifikan dalam laporan auditor jasa memberi isyarat bahwa organisasi jasa tidak dapat memberikan organisasi klien dengan tingkat perlindungan layanan dan informasi yang memadai. Jika organisasi jasa tidak memiliki laporan auditor jasa yang disiapkan, organisasi klien harus secara serius mempertimbangkan penurunan organisasi jasa dari pertimbangan. Kurangnya laporan auditor jasa juga mungkin menandakan bahwa kontrol internal di organisasi jasa secara signifikan bisa membahayakan operasi klien. Lingkungan pengendalian internal dapat berubah sewaktu-waktu di organisasi jasa, seperti dengan setiap organisasi. Oleh karena itu, bahkan setelah organisasi jasa dikontrak dan jasanya telah digunakan, pemilik proses dan auditor internal di organisasi klien harus memeriksa laporan auditor jasa yang disiapkan.

Meskipun standar audit profesional tidak memerlukan persiapan laporan auditor jasa untuk semua jasa organisasi, organisasi jasa paling terkemuka memiliki satu yang disiapkan setiap tahunnya atau setidaknya diadakan setiap dua tahun sekali. Untuk membantu membiayai sebagian biaya menyewa auditor jasa dalam mempersiapkan laporan, beberapa organisasi jasa membebankan organisasi klien biaya untuk setiap salinan dari laporan auditor jasa. Departemen audit internal harus mendapatkan salinan laporan auditor jasa untuk setiap pemanfaatan organisasi jasa oleh organisasi klien secara tahunan atau setiap kali laporan disiapkan.

Laporan auditor jasa dapat cukup panjang (sampai dengan 100 halaman atau lebih) dan terdiri dari beberapa bagian. Meskipun standar profesional tidak menentukan bagaimana laporan auditor jasa diatur, umumnya termasuk dalam empat bagian informasi:

1. Laporan auditor independen
2. Penjelasan tentang kebijakan dan prosedur yang relevan (yang disediakan oleh manajemen organisasi klien)
    a. Keterangan umum operasi, termasuk struktur organisasi
    b. Deskripsi elemen lingkungan pengendalian
    c. Deskripsi aliran transaksi, termasuk diagram alur
    d. Ikhtisar aplikasi
    e. Prosedur perubahan program
    f. Informasi kepatuhan peraturan (jika ada)
3. Tujuan pengendalian sebagaimana ditentukan oleh manajemen organisasi klien dan hasil pengujian auditor jasa atas efektivitas operasi pada tujuan pengendalian
4. Pertimbangan pengendalian klien

LAPORAN AUDITOR INDEPENDEN

Laporan auditor independen mencakup pernyataan pendapat mengenai kebijakan dan prosedur yang memadai dan, jika dikontrak oleh organisasi jasa, pendapat apakah kebijakan dan prosedur yang beroperasi cukup efektif selama periode tertentu. Auditor internal di organisasi klien harus memeriksa pendapat dengan teliti. Jika pendapat "wajar" karena satu atau lebih kelemahan kontrol yang signifikan di organisasi jasa, auditor internal harus menentukan apakah kelemahan signifikan mempengaruhi lingkungan pengendalian internal di organisasi klien. Jika demikian, auditor internal harus merekomendasikan agar manajemen mengkomunikasikan urusannya ke organisasi jasa dan menentukan apakah

organisasi jasa telah mengimplementasikan perubahan yang diperlukan untuk mengatasi kelemahan kontrol.

Jika perubahan yang diperlukan tidak dilaksanakan, auditor internal harus merekomendasikan agar manajemen mempertimbangkan perubahan untuk penjual jasa lain yang tidak memiliki kelemahan kontrol yang signifikan yang dapat mempengaruhi lingkungan pengendalian internal organisasi kliennya. Jika organisasi jasa asli menyatakan bahwa kelemahan kontrol telah diperbaiki, auditor internal harus melakukan pengujian alternatif untuk mengkonfirmaskan perubahan. Auditor internal juga harus memastikan bahwa kelemahan kontrol yang sama tidak disebutkan dalam laporan auditor jasa berikutnya. Adanya kelemahan kontrol terus-menerus dalam organisasi jasa bisa mengindikasikan bahwa keseluruhan lingkungan kontrol lemah, sehingga meningkatkan resiko transaksi bisa semestinya diproses; pelayananan dapat mengalami gangguan; data dapat hilang, rusak, atau terungkap ke pihak yang tidak tidak berkepentingan; dan organisasi jasa bisa menderita kerugian yang cukup signifikan untuk mendorongnya keluar dari bisnis. Studi kasus 5.3 dan 5.4 menyajikan pendapat wajar dari dua organisasi jasa yang berbeda dengan auditor jasa mereka masing-masing.

STUDI KASUS 5.3

Pendapat Wajar Dari Organisasi Pelayananan Jaringan ATM

Selama audit internal atas layanan peralihan jaringan ATM ke banyak pemilik lembaga keuangan, laporan auditor jasa akan diuji dan terkait pendapat wajar berikut ini dicatat:

> Deskripsi yang menyertai kebijakan dan prosedur termasuk kontrol komputer umum yang berhubungan dengan pengolahan data dan pelayanan yang dipilih tetapi tidak termasuk tujuan kontrol sistem aplikasi untuk sistem aplikasi yang diproses oleh organisasi klien. Kami percaya bahwa ini tujuan kontrol ini, dan terkait kebijakan dan prosedur yang mungkin mencapai tujuan pengendalian ini, relevan kepada organisasi pengguna dan auditor pengguna yang berniat untuk mengandalkan kebijakan dan prosedur pengendalian untuk sistem aplikasi ini.
>
> Menurut pendapat kami, kecuali untuk hal yang dijelaskan dalam paragraf sebelumnya, deskripsi yang menyertai kontrol tersebut disajikan secara wajar, dalam semua aspek yang material, aspek yang relevan dari kebijakan dan prosedur organisasi klien yang telah ditempatkan dalam operasi pada (tanggal).

Dalam kasus khusus ini, chief executive officer (CEO) atas jasa peralihan ini biasanya dikenal tidak menyukai auditor dan tidak jauh dari masa pensiun. Dia kemungkinan besar yakin bahwa tujuan pengendalian yang ditentukan dalam laporan dan pengujian efektivitas operasi mereka cukup untuk keperluan pelayanan laporan auditor. Oleh karena itu, ia memilih untuk menerima pendapat wajar daripada tunduk pada rekomendasi auditor jasa dan menyertakan setidaknya deskripsi dari tujuan kontrol sistem aplikasi untuk sistem aplikasi yang diproses oleh organisasi layanan.

Laporan auditor jasa menggambarkan tujuan dan prosedur pengendalian di bidang organisasi dan administrasi; kartu produksi; penyelesaian jaringan; operasi komputer; akses dan keamanan fisik; akses dan keamanan logis; akuisisi, pengembangan, dan pemeliharaan sistem; dan manajemen sistem. Karena pendapat auditor jasa mengenai daerah kontrol adalah wajar, dan karena pengujian ekstensif dari pengolahan prosedur ATM internal dilakukan, auditor internal tidak menyarankan pemilik proses di organisasi klien untuk meminta organisasi jasa menjelaskan mengapa kontrol aplikasi tidak disertakan dalam lingkup laporan auditor jasa.

STUDI KASUS 5.4

Pendapat Wajar Dari Organisasi Jasa Kartu Kredit

Lembaga keuangan telah menggunaka organisasi jasa kartu kredit yang sama untuk lebih dari satu dekade. Lembaga keuangan menggunakan aplikasi kartu kredit yang disediakan oleh organisasi jasa seperti sumber pengolahan data pada pusat data organisasi jasa. Untuk periode tahun 1984 sampai 1995, laporan auditor jasa disusun pada tahun berikut: 1984, 1986, 1988, 1991, 1992, 1993, 1994 dan 1995. Pemeriksaan laporan-laporan ini menunjukkan bahwa auditor jasa telah mengeluarkan pendapat yang memenuhi syarat pada laporan berturut-turut dari tahun 1986 sampai 1991. Hal ini menarik untuk dicatat bagaimana kekurangan 3 angka dalam laporan tahun 1986 yang diselesaikan tetapi menyebabkan berbagai kekurangan yang baru pada tahun 1988, sebagai organisasi jasa masih dalam proses mempelajari bagaimana mengamankan mainframenya secara memadai dan menyebarkan perangkat lunak kontrol akses yang baru. Meskipun pendapat wajar yang dikeluarkan dalam tiga laporan auditor jasa berturut-turut, sebagian besar tujuan pengendalian dicapai oleh organisasi jasa dan mengidentifikasi kelemahan yang diperbaiki dari waktu ke waktu. Juga, kelemahan yang tidak dianggap sebagai indikasi bahwa keseluruhan lingkungan kontrol pada organisasi jasa mencurigakan. Ketika Anda membaca

kelemahan-kelemahan ini, pertimbangkan apakah kelemahan mungkin ada dalam organisasi Anda. Banyak kelemahan kontrol yang cukup umum dan bisa ada di hampir semua organisasi.

Kekurangan-kekurangan yang dicatat pada laporan auditor jasa tahun 1986

1. Bagian jaminan kualitas tidak meninjau output dari setiap produksi kartu plastik yang dijalankan baik yang pencetakan ataupun akurasi pengkodean. Tanpa jaminan kualitas atau ulasan lainnya, kartu kredit yang salah cetak atau dikodekan dapat didistribusikan ke pengguna lembaga pelanggan. Kemungkinan bercabang dari kesalahan pengkodean adalah batas penarikan harian terletak pada jalur 3 dari strip magnetik kartu yang bisa lebih besar daripada jumlah dimaksudkan.
2. Manual programmer menggambarkan berkas layout, catatan layout, panggilan rutin, dan informasi terkait lainnya yang tidak disiapkan secara konsisten. Setelah pengembangan awal, modifikasi atau penambahan program lebih sulit dan rentan terhadap kesalahan tanpa dokumentasi program rinci.
3. Meskipun organisasi jasa memiliki kebijakan mengotorisasi individu yang sesuai untuk membuat program atau modifikasi lain, hanya dasar proteksi password yang ada untuk memastikan bahwa kebijakan tersebut dipatuhi. Perangkat lunak aplikasi keamanan sistem, seperti RACF® atau ACF2®, tidak diinstal untuk membantu mencegah modifikasi yang tidak sah untuk perangkat lunak aplikasi, file data, atau sistem perangkat lunak.

Kekurangan-kekurangan yang dicatat dalam laporan 1988

1. Jadwal internal audit tidak ditaati dan daerah yang sebenarnya diaudit ditentukan secara subjektif. Laporan audit tidak selalu dikeluarkan tepat waktu, tanggapan manajemen tidak didokumentasikan, dan tindak lanjut audit untuk menentukan status pelaksanaan rekomendasi yang tidak dilakukan. Departemen audit internal tidak konsisten meninjau desain sistem, pengembangan, dan pemeliharaan kontrol untuk perubahan program. Personil audit sistem informasi tidak secara rutin menghadiri pertemuan dimana penambahan sistem dan penulisan ulang utama dari sistem mempengaruhi semua lembaga pengguna ditentukan.
2. Organisasi jasa tidak memiliki metodologi pengembangan sistem yang diterapkan secara konsisten pada tempat. Klien organisasi sign-off pada sistem sebelum pelaksanaan tidak diminta oleh organisasi jasa. Dokumentasi program tidak

disiapkan secara konsisten. Modifikasi program sering ditempatkan ke dalam produksi tanpa review pengawasan atau persetujuan pengguna.

3. Manual programmer menggambarkan berkas layout, catatan layout, panggilan rutin, dan informasi terkait lainnya yang tidak disiapkan secara konsisten. Setelah pengembangan awal, modifikasi atau penambahan program lebih sulit dan rentan terhadap kesalahan tanpa dokumentasi program rinci.
4. Programmer dapat menulis dan mengotorisasi perubahan program mereka sendiri untuk ditempatkan ke dalam produksi tanpa review konsisten atau persetujuan. Setelah program yang ditujukan programmer untuk modifikasi, penyelesaian pengujian umumnya tergantung pada kebijaksanaan programmer. Pengujian validasi sistem tidak secara rutin dilakukan untuk memastikan bahwa kode sumber tidak sengaja dihapus atau sebaliknya tidak diubah.
5. Organisasi jasa tidak memiliki seseorang yang ditunjuk memiliki tanggung jawab untuk mengelola keamanan. Tidak diresmikan, prosedur keamanan terdokumentasi yang ada untuk penugasan kartu kunci yang memungkinkan akses ke daerah-daerah operasional yang kritis, akses ke sistem aplikasi oleh karyawan organisasi jasa melalui sistem keamanan rumah, atau kontrol akses programmer melalui perangkat lunak kontrol akses ACF2. Keamanan pelanggaran laporan tidak secara rutin ditinjau, password tidak secara rutin berubah, password karyawan diakhiri dan ditransfer serta kartu kunci tidak selalu dihapus atau diubah pada sistem yang sesuai secara tepat waktu, dan jumlah individu yang berlebihan mampu melakukan pemeliharaan sandi. Kelompok programmer berbagi User ID dan password yang sama untuk fungsi pembagian waktu, dengan demikian mengurangi tanggung jawab pribadi dalam penggunaan sistem. Organisasi jasa baru-baru ini telah menerapkan program fasilitas kontrol akses untuk mengontrol akses ke program dan data dalam lingkungan *batch* dan *time-sharing*. Namun, fasilitas control akses tidak dipasang pada pengujian komputer, dimana terhubung ke komputer produksi dan semua berkas disk.
6. Pita sistem dan produksi, yang diperlukan dalam kejadian pemulihan layanan pemrosesan data, tidak selalu dipertahankan di fasilitas penyimpanan luar. Rencana pemulihan bencana organisasi jasa tidak lengkap dan kurang detail di sejumlah daerah.
7. Programer sistem diberi akses yang tidak terbatas oleh Fasilitas Manajemen Sistem (SMF), terutama jejak audit di sistem operasi MVS® yang digunakan dalam

organisasi jasa. Fasilitas ini digunakan menjurnal berbagai macam aktivitas sistem, termasuk informasi perangkat lunak kontrol akses ACF2.

8. Tidak ada metode yang terdapat untuk mengotorisasi atau mendokumentasikan perubahan yang dilakukan oleh programmer sistem untuk daerah sensitif seperti Pustaka Parameter Sistem (SPL), yang berisi informasi penting untuk audit, kontrol, dan keamanan sistem operasi MVS.
9. Fasilitas Program Autorisasi (APF) yang disediakan oleh IBM untuk mengontrol akses pustaka program yang dapat menghindari semua mekanisme keamanan sistem operasi, termasuk perangkat lunak kontrol akses. Kebanyakan otorisasi pustaka APF dapat diakses hanya oleh programer sistem yang pekerjaannya adalah mempertahankan program-program di pusataka mereka. Namun, satu pengujian pustaka APF resmi dan juga memungkinkan pemrogram aplikasi dibatasi aksesnya. Akibatnya, ada kemungkinan bahwa programmer aplikasi dapat menjalankan program yang tidak sah.
10. Pustaka produksi untuk program aplikasi adalah APF yang berwenang dan berisi 25 program APF resmi, beberapa di antaranya sudah lama dan tidak terdokumentasi. Selama pemeriksaan kami, semua 25 dari program ini baik yang dihapus atau dipindah ke pustaka yang lebih tepat.
11. Untuk kinerja atau alasan lain, mainframe dirancang untuk memungkinkan program tertentu melewai keamanan standar MVS dan mekanisme kontrol. Dasar Tabel Properti Program berisi nama beberapa program yang tidak digunakan dalam organisasi jasa. Nama program ini diresmikan untuk melewati fungsi tertentu, seperti integritas dataset atau password MVS, dan untuk mengakses penyimpanan utama yang dimiliki oleh program lain. Karena program ini tidak ada di organisasi jasa, akan menjadi mungkin bagi seseorang untuk membuat sebuah program yang tidak sah, menetapkan nama dari salah satu program yang tidak digunakan dalam Tabel Properti Program, dan kemudian menjalankannya tanpa tergantung pada kontrol keamanan standar.
12. Tidak ada kebijakan yang mengharuskan pengguna mengubah sandi secara berkala.
13. ACF2 memiliki kemampuan untuk melindungi file rekaman dari akses yang tidak sah. Namun, fitur ini tidak digunakan oleh organisasi jasa. Jadi, memungkinkan programmer membaca pita produksi, membuat salinan dengan perubahan catatan tertentu, dan menggantikannya untuk pita produksi.

Kekurangan-kekurangan yang dicatat dalam laporan tahun 1991

1. Organisasi jasa tidak memiliki metodologi pengembangan sistem yang diterapkan secara konsisten pada tempat. Selain itu, persetujuan tertulis pengguna dari sistem sebelum pelaksanaan tidak selalu diperoleh oleh organisasi jasa, pendokumentasian program tidak disiapka secara rutin, dan modifikasi program yang terkadang ditempatkan dalam produksi tanpa review pengawasan atau persetujuan pengguna. Akibatnya, ada peningkatan risiko bahwa daerah sensitive pengguna bisa dilalui, fitur kontrol penting dapat terabaikan, dan program mungkin tidak diuji dengan benar atau dirancang untuk memenuhi spesifikasi pengguna.
2. Dokumentasi programmer menggambarkan berkas layout, catatan layout, panggilan rutin, dan informasi serta data terkait lainnya tidak disiapkan dengan rutin. Hasilnya, setelah sistem ini dikembangkan, modifikasi atau penambahan program lebih sulit dilakukan, dan perubahan tersebut cenderung mengandung kesalahan.
3. Programmer dapat menulis dan mengotorisasi perubahan program mereka sendiri untuk ditempatkan ke dalam produksi tanpa review atau persetujuan berkala. Setelah program yang ditujukan programmer untuk modifikasi, penyelesaian pengujian umumnya tergantung pada kebijaksanaan programmer. Rencana pengujian tidak disiapkan secara berkala, dan hasil pengujian tidak selalu ditinjau oleh anggota pengawas. Kelemahan-kelemahan ini meningkatkan risiko bahwa kode sumber bisa secara tidak sengaja dihapus atau sebaliknya tidak diubah.
4. Programer aplikasi memiliki akses tertulis ke berbagai sumber produksi, parameter, prosedur katalog, dan pustaka makro. Akses ini tidak dicatat oleh ACF2. Dengan demikian, pemrogram dapat membuat perubahan tidak sah untuk kode dasar, yang mungkin akan ditempatkan ke dalam produksi di lain waktu.
5. Rencana pemulihan bencana organisasi jasa telah dikembangkan hanya untuk mengatasi pengrusakan atas pusat data utama dan mainframe komputer IBM. Prosedur pemulihan jaringan tidak ditangani, atau prosedur dijelaskan di departemen kartu produksi dan pernyataan departemen produksi. Juga, rencana yang sudah ada tidak diuji selama 20 bulan.

Ketika laporan auditor jasa tidak mengungkapkan pendapat mengenai efektivitas operasi atas kebijakan dan prosedur di organisasi jasa, auditor internal harus merekomendasikan kepada pemilik proses di organisasi klien agar mereka menanyakan organisasi jasa mengapa auditor jasa tidak melakukan pengujian atas efektivitas operasi.

Alasan yang paling umum adalah organisasi jasa ini menghindari biaya tambahan yang akan dikenakan oleh auditor jasa untuk melakukan pengujian tambahan. Jika hal ini terjadi, auditor internal harus menilai tingkat risiko terkait dengan proses yang diaudit. Jika risiko dianggap tinggi, auditor harus merekomendasikan agat pemilik proses mengumpulkan permintaan untuk organisasi jasa dimana auditor jasa melakukan pengujian efektivitas operasi atas kebijakan dan prosedur di organisasi jasa. Jika organisasi jasa menolak, auditor internal harus bekerja dengan pemilik proses di organisasi klien untuk menentukan apakah risiko cukup signifikan untuk mempertimbangkan manfaat pelayanan dari organisasi jasa alternatif.

Pilihan lain untuk organisasi klien adalah mengirim auditornya sendiri ke fasilitas pengolahan organisasi jasa untuk melakukan audit kontrol yang berlaku umum. Sementara jenis audit tidak akan dirincikan dan tidak akan dapat diuji selama enam bulan, itu akan memberikan sejumlah keyakinan yang setidaknya kontrol dasar yang sedang dilakukan oleh organisasi jasa. Studi kasus 5.5 menjelaskan bagaimana organisasi klien melakukan audit singkat atas organisasi jasa swasta yang diadakan tidak memiliki perlakuan audit SAS 70.

STUDI KASUS 5.5

Organisasi Jasa Tanpa SAS 70

Organisasi jasa swasta yang besar menyiapkan laporan bulanan, pemberitahuan, dan berbagai surat promosi untuk beberapa organisasi perbankan terbesar di wilayah. Surat tersebut masing-masing berjumlah puluhan juta per bulan. Karena nama besar dan database alamat sangat berharga untuk perusahaan-perusahaan pemasaran komersial, pernyataan berisi informasi rahasia pribadi, dan biaya ongkos kirim bulanan mencapai jutaan, risiko terkait dengan pengendalian internal organisasi jasa menjadi signifikan. Organisasi jasa telah ada dalam bisnis selama 20 tahun dan mengalami pertumbuhan yang signifikan.

Auditor internal di salah satu klien organisasi perbankan melakukan audit atas proses persiapan laporan mereka. Salah satu langkah untuk menilai kecukupan kontrol atas permintaan dan pemeriksaan SAS 70 dari organisasi jasa. Para auditor belajar bahwa organisasi jasa memiliki laporan keuangan audit independen tetapi tidak dilakukan sesuai SAS 70. Para auditor memutuskan untuk melakukan audit fasilitas singkat karena organisasi jasa terletak di daerah geografis yang sama. Organisasi jasa menghubungi perwakilan (penyedia jasa) yang sangat bersedia menjadi tuan rumah para auditor klien untuk kunjungan singkat di tempat dan memberikan banyak dokumentasi dan informasi yang

bisa membantu dalam audit. Anehnya, tidak satu pun dari organisasi perbankan lainnya yang pernah diminta SAS 70 atau melakukan audit di tempat.

Auditor klien menyususun pertemuan dua jam awal dengan penyedia jasa, manajer pengolah data, dan seorang analis sistem. Sebelum pertemuan, para auditor memberikan penyedia jasa daftar yang diperlukan termasuk informasi:

- Laporan keuangan yang baru diaudit
- Sertifikat asuransi saat ini untuk tanggung jawab umum komersial, obligasi yang tepat, dan asuransi kendaraan komersial
- Kebijakan dan standar keamanan SI
- Rencana kembalinya bisnis/pemulihan bencana
- Prosedur pengendalian ongkos kirim

Pertemuan dimulai dengan meninjau dokumen di atas. Saat ini semua dan isinya dianggap memadai, meskipun penyedia jasa hanya akan mengijinkan pemeriksaan visual atas laporan keuangan yang diaudit karena diadakan secara pribadi. Mereka meberikan para auditor salinan atas surat pendapat CPA.

Para auditor bertanya pada manager pengolahan data dan analis sistem mengenai lingkungan sistem informasi (hardware dan sistem aplikasi) yang digunakan dalam penyusunan berbagai surat dan hubungan kontrol keamanan logis. Para auditor juga diberikan penjelasan singkat atas keberadaan beberapa kontrol sistem produksi. Tidak ada pengecualian yang dijalankan.

Terakhir, para auditor diberi wisara pengolahan data berkecepatan tinggi dan daerah pencetakan dimana semua pernyataan dan surat lain dicetak. Kontrol keamanan fisik termasuk akses elektronik tanda pengenal mengakses ke daerah terlarang dan kamera pengintai di semua pintu masuk dan teluk gudang pengiriman. Penyedia jasa tidak menggunakan kurir atau pengemudi truk eksternal, sehingga membantu memastikan kontrol internal atas persiapan dan pengiriman semua dokumen dari waktu download elektronik yang diterima dari klien sampai surat dikirim ke kantor pos Amerika Serikat.

Semua biaya ongkos kirim dibebankan ke meteran nomor unik kantor pos yang diberikan untuk setiap organisasi klien. Meteran bisa diisi oleh kantor pos saja menggunakan dana yang disediakan oleh penyedia jasa. Penyedia jasa memberitahu masing-masing klien atas perkiraan biaya pengiriman di setiap awal bulan. Klien perlu mentransfer jumlah perkiraan ongkos kirim ke penyedia jasa agar cadangan kecil tetap pada akhir bulan. Ongkos kirim pengendalian internal termasuk berbagai penyeimbangan dan pemisahan tugas prosedur dalam SI, persiapan laporan, dan daerah akuntansi.

Berdasarkan pengujian terbatas yang dilakukan dan resolusi beberapa pertanyaan-pertanyaan lanjutan, auditor klien menyimpulkan bahwa kontrol internal di organisasi jasa sudah memadai. Namun, dua kekurangan pengendalian internal yang signifikan dalam prosedur akuntansi internal untuk pengiriman dibayar dimuka di organisasi klien.

Pertama, klien telah telah memberikan jumlah yang diminta penyedia jasa setiap bulan. Bidang akuntansi akan mendebet rekening aset ongkos kirim dibayar dimuka dan kredit uang tunai pada awal bulan. Pada akhir bulan, akuntansi akan membuat entri akrual untuk biaya ongkos kirim di debit dan kredit ongkos kirim dibayar dimuka untuk perkiraan pengiriman biaya yang dikeluarkan. Penyedia jasa mengirimkan invoice bulanan untuk tenaga kerja dan biaya material yang berkaitan dengan persiapan pengiriman (jumlah ini dibebankan pada saat terjadinya). Faktur yang menunjukkan besarnya ongkos kirim digunakan untuk pengiriman yang berlaku tetapi tidak menunjukkan berapa jumlah tetap dalam perhitungan ongkos dibayar dimuka pada penyedia jasa.

Masalahnya adalah biaya akrual bulanan dimasukkan ke debit biaya dan kredit ongkos kirim belum disesuaikan dengan yang baru untuk mencerminkan peningkatan biaya ongkos kirim karena peningkatan yang stabil dalam jumlah surat dan tingkat ongkos kirim sebagai organisasi yang tumbuh. Hasilnya, jumlah dalam akun aset ongkos kirim meningkat sementara biaya ongkos kirim akrual relatif tidak berubah. Penyesuaian untuk biaya ongkos kirim debit dan ongkos kirim dibayar dimuka kredit sebesar $120.000 diperlukan untuk mengurangi jumlah akun ongkos kirim dibayar dimuka atas apa yang telah diperkirakan bidang akuntansi telah tersisa pada perhitungan ongkos kirim di penyedia jasa tersebut. Juga, biaya jumlah bulanan akrual harus ditingkatkan sebesar $10.000.

Masalah kedua adalah bahwa departemen akuntansi pernah berusaha untuk menyesuaikan besarnya ongkos kirim dibayar dimuka di general ledger dengan jumlah perhitungan ongkos kirim dibayar dimuka pada buku penyedia jasa. Dengan demikian, jika penyedia jasa membebankan lebih perhitungan ongkos kirim klien, pengolahan pengiriman klien lain atau dirinya untuk perhitungan organisasi klien, menggelapkan sebagian dana dari dana ongkos kirim klien yang diberikan sebelum perhitungan diisi ulang, atau memiliki masalah pengolahan yang habis jumlah perhitungannya tanpa mencap setiap amplop yang sebenarnya, organisasi klien tidak akan mampu mendeteksi dengan mudah, terutama dalam lingkungan dimana jumlah yang ditransfer ke penyedia jasa terus meningkat. Para auditor merekomendasikan agar departemen akuntansi melaksanakan prosedur rekonsiliasi. Ini diperlukan organisasi jasa untuk memulai memberikan jumlah saldo perhitungan ongkos kirim yang tersisa pada faktur bulanan untuk tenaga kerja dan

bahan. Setelah rekonsiliasi awal, tambahan $10.000 dalam biaya ongkos kirim yang dikeluarkan oleh organisasi klien untuk mengurangi jumlah akun ongkos kirim dengan perhitungan ongkos kirim yang sebenarnya di penyedia jasa. Para auditor juga merekomendasikan agar departemen akuntansi melaksanakan kontrol untuk menghitung ulang rata-rata biaya ongkos kirim per amplop pada masing-masing faktur.

GAMBARAN KEBIJAKAN DAN PROSEDUR SERTA INFORMASI LAIN YANGTERKAIT

Hal ini penting bagi auditor internal untuk membaca bagian laporan auditor jasa untuk mendapatkan pemahaman yang lebih baik dari organisasi jasa dan lingkungan kontrolnya. Cukup sering informasi ini dapat memberikan informasi yang lebih lengkap tentang organisasi jasa dan aplikasi dari pemilik proses di organisasi klien. Bagian ini biasanya mencakup gambaran umum operasi, gambaran elemen lingkungan kontrol, dan gambaran aliran transaksi.

Gambaran umum operasi biasanya terdiri dari gambaran narasi struktur perusahaan dari organisasi jasa, gambaran operasi perusahaan, dan gambaran umum dari setiap aplikasi yang berlaku. Bagan organisasi sering dimasukkan, atau dapat disediakan dalam lampiran.

Unsur lingkungan pengendalian adalah mereka yang harus di tempatkan di organisasi jasa untuk memberikan keyakinan memadai bahwa transaksi dan data organisasi klien diproses dengan akurat, tepat waktu dan aman. Beberapa laporan auditor jasa memberikan gambaran fungsi departemen kunci yang mendukung lingkungan pengendalian secara keseluruhan. Contoh departemen kunci tersebut meliputi Sumber Daya Manusia, Audit Internal, Dukungan Klien, Pengiriman Produk, Penelitian dan Pengembangan, dan Manajemen Produk. Laporan auditor jasa lainnya mungkin malah menggambarkan kebijakan dan prosedur sekitar tujuan pengendalian khusus yang ditentukan oleh manajemen organisasi jasa.

Gambaran aliran transaksi merupakan narasi tingkat tinggi tentang bagaimana aplikasi mengolah transaksi dan menghasilkan output laporan dan dokumen lainnya untuk organisasi klien. Flow chart dapat dimasukkan dalam bagian ini atau dalam lampiran.

Ikhtisar aplikasi merupakan gambaran narasi dari berbagai layanan atau fungsi yang dilakukan setiap aplikasi. Dalam beberapa kasus, aplikasi utama yang kompleks didukung

oleh satu atau lebih aplikasi sekunder. Jika demikian, ikhtisar dari aplikasi sekunder juga akan diberikan.

Prosedur perubahan program di organisasi jasa yang ada untuk membantu memastikan bahwa perubahan telah diotorisasi, didokumentasikan, diuji, dan ditempatkan ke dalam produksi. Prosedur ini dapat digambarkan dalam bentuk narasi dengan diagram alur yang menyertai atau mungkin hanya dimasukkan sebagai sebuah diagram alur dalam lampiran.

Tergantung pada industri mana organisasi jasa memberikan aplikasi, gambaran kebijakan dan prosedur yang memastikan kepatuhan peraturan mungkin diberikan. Format akan bervariasi dengan sifat hukum atau peraturan yang dijelaskan.

TUJUAN PENGENDALIAN SEPERTI YANG DITENTUKAN OLEH MANAJEMEN ORGANISASI JASA

Tujuan pengendalian ditentukan oleh manajemen organisasi layanan. Namun, auditor jasa memainkan peran penting dalam konsultasi dengan manajemen untuk memastikan bahwa tujuan pengendalian yang ditentukan mengatasi risiko utama yang terkait dengan operasi organisasi jasa. Setelah masing-masing tujuan kontrol dijelaskan secara rinci tentang kebijakan dan prosedur yang diakui berada di tempat untuk memastikan bahwa tujuan pengendalian tercapai. Manajemen organisasi jasa juga memberikan informasi ini. Untuk laporan auditor jasa yang meliputi opini auditor terhadap efektivitas operasi dari kebijakan dan prosedur yang ditempatkan dalam operasi, auditor jasa menentukan tes yang dilakukan untuk mendapatkan kewajaran, namun tidak mutlak, keyakinan atas efektivitas mereka. Tes ini biasanya mencakup pertanyaan dengan manajemen dan staf dari organisasi jasa, pengujian sampel dari transaksi individu, pemeriksaan atas kontrol akses sistem, penilaian pemisahan tugas, pengamatan operasi organisasi jasa, dan sebagainya.

Tampilan 5.1 sampai 5.4 menggambarkan beberapa jenis tujuan pengendalian yang dapat ditentukan dalam laporan auditor jasa di berbagai industri. Meskipun banyak risiko yang unik ada dalam setiap industri, beberapa tujuan pengendalian hampir serupa, meskipun organisasi jasa melayani industri yang berbeda. Hal ini karena banyak risiko yang terkait dengan sistem informasi tidak tergantung pada jenis informasi yang diproses atau perangkat keras yang diolah. Oleh karena itu, kontrol untuk mengurangi risiko tersebut sangat mirip.

TUJUAN KONTROL UNTUK ORGANISASI JASA PENGOLAH KARTU KREDIT

1. Pusat data dan fungsi klien harus terstruktur untuk mejaga pembagian tugas yang memadai.
2. Pusat data harus diatur untuk memberikan pembagian tugas dan fungsi yang memadai.
3. Audit internal harus memberikan peninjauan dan verifikasi dari operasi pengolah data elektronik.
4. Kebijakan dan prosedur administratif yang sesuai harus didokumentasikan.
5. Fungsi penjamin kualitas harus ada untuk meyakinkan kualitas layanan yang diberikan ke klien.
6. Program baru yang sedang dikembangkan dan perubahan pada program yang ada harus diotorisasi, diuji, disetujui, diimplementasikan dengan benar, dan didokumentasikan.
7. Perubahan perangkat lunak yang ada harus diotorisasi, diuji, disetujui, dan diimpelementasikan dengan benar.
8. Akses fisik ke perlengkapan komputer dan media penyimpanan harus dibatasi pada individu yang benar-benar berwenang.
9. Akses logis ke program produksi dan data dalam lingkungan mainframe hanya harus diberikan kepada individu yang benar-benar berwenang.
10. Pengolahan harus dijadwalkan dengan benar, dan penyimpangan harus diidentifikasi dan diatasi.
11. Pengiriman data antara organisasi jasa dan klien harus dilengkapi, akurat, dan aman.
12. Pengiriman data antara pusat data organisasi jasa harus dilengkapi, akurat, dan aman.
13. Informasi aplikasi kartu kredit harus diterima dari sumber terotorisasi.
14. Informasi aplikasi kartu kredit harus dicatat dengan lengkap, akurat, dan dalam kesesuaian dengan sepesifikasi klien.
15. Informasi output harus lengkap, akurat, dan didistribusikan berdasarkan spesifikasi klien.
16. Input secara online harus diterima dari sumber yang terotorisasi.
17. Spesifikasi klien yang sesuai harus digunakan untuk perhitungan yang diprogram.
18. Aktivitas pemegang kartu harus diposting ke akun yang benar secara lengkap dan akurat.
19. Informasi pernyataan pemegang kartu harus lengkap, akurat, dan didistribusikan sesuai dengan spesifikasi klien.

20. Nomor identifikasi anggota dan informasi pemberitahuan pengirim surat harus lengkap, akurat, dan didistribusikan sesuai dengan spesifikasi klien.
21. Laporan manajemen dan berkas data harus lengkap, akurat, dan didistribusikan sesuai dengan spesifikasi klien.
22. Informasi output ke sistem aplikasi lain harus lengkap dan akurat.
23. Permintaan produksi kartu harus diterima dari sumber terotorisasi.
24. Kartu harus diproduksi dengan lengkap dan akurat.
25. Akses kartu kosong harus dibatasi oleh anggota sah, dan inventaris harus dipertanggungjawabkan dengan benar.
26. Output produksi kartu harus didistribusikan berdasarkan spesifikasi klien.
27. Input harus secara lengkap dan akurat diterima dari sumber terotorisasi.
28. Transaksi pertukaran harus diproses dengan lengkap dan akurat berdasarkan spesifikasi klien dan asosiasi.
29. Nilai penyelesaian bersih harus akurat.
30. Laporan transaksi perdagangan harus lengkap dan akurat.
31. Output ke sistem aplikasi lain di organisasi jasa harus lengkap dan akurat.
32. Transaksi perdagangan harus diterima dengan lengkap dan akurat dari sistem perdagangan.
33. Informasi perdagangan harus diproses dengan lengkap, akurat, dan berdasarkan spesifikasi klien.
34. Informasi output harus lengkap, akurat, dan berdasarkan spesifikasi klien.
35. Prosedur administratif dan operasional harus dibentuk dalam pusat data organisasi jasa untuk menjamin kecukupan perlindungan dari asset fisik dan kelangsungan operasi.

TUJUAN KONTROL UNTUK ORGANISASI JASA PENGOLAH PENGGAJIAN

1. Aplikasi baru yang sedang dikembangkan dan perubahan pada perangkat lunak yang ada diotorisasi, diuji, disetujui, diimplementasikan dengan benar, dan didokumentasikan.
2. Perubahan pada perangkat lunak sistem yang ada dan impelementasi pada perangkat lunak baru diotorisasi, diuji, disetujui, diimplementasikan dengan benar, dan didokumentasikan.
3. Akses fisik ke perlengkapan komputer, media penyimpanan, alat yang dapat dijalankan, dan dokumentasi program dibatasi dengan individu yang benar-benar berwenang.

4. Akses logis ke program dan data dibatasi dengan individu yang benar-benar berwenang.
5. Pengolahan harus dijadwalkan dengan benar dan penyimpangan harus diidentifikasi dan diatasi.
6. Pengiriman data penggajian antara kantor pusat organisasi jasa dan pusat data wilayah aman, lengkap, dan akurat.
7. Pengiriman data penggajian antara organisasi jasa dan organisasi klien aman, lengkap, dan akurat.
8. Data penggajian diterima dari sumber terotorisasi.
9. Data penggajian dicatat dengan lengkap dan akurat.
10. Spesifikasi hukum yang sesuai digunakan untuk mengolah perhitungan pengurangan gaji dan pemotongan pajak.
11. Kaset output, cek, laporan, dan pengiriman lengkap, akurat, dan didistribusikan berdasarkan spesifikasi klien.
12. Akses untuk tanda tangan digital atas tanda tangan klien yang berwenang dibatasi untuk individu yang berwenang, dan gambar digital diakses oleh pengolahan penggajian perusahan yang sesuai.
13. Pengeluaran dana deposit langsung diotorisasi, lengkap, dan akurat.
14. Laporan output lengkap, akurat, dan dan didistribusikan berdasarkan spesifikasi klien.
15. Prosedur administratif dan operasional dibentuk dalam pusat data wilayah untuk menjamin kecukupan perlindungan kelangsungan operasi dan meyakinkan perlindungan dari aset fisik (misalnya, dalam hal bencana).

TUJUAN KONTROL UNTUK ORGANISASI JASA JARINGAN ATM

1. Lembaga anggota patuh dengan peraturan operasi organisasi jasa dalam memberikan perlindungan akhir-ke-akhir yang memadai.
2. Manajemen senior harus memberikan pemisahan tugas dalam organisasi, seperti antara pengembangan dan operasi sistem, kontrol dan operasi kualitas, dan pelayanan dan pengembangan sistem pelanggan.
3. Fungsi internal audit ada sebagai mekanisme kontrol selama pemeriksaan dan evaluasi independen dari masalah keamanan dan kontrol manajemen.
4. Karyawan organisasi jasa dari integritas dan komptensi teritinggi meyakinkan

5. Informasi pemegang kartu dilindungi secara memadai terhadap pengungkapan yang tidak sah.
6. Transaksi diproses oleh organisasi jasa
7. Pengolahan dijadwalkan dengan benar, dan penyimpangan dari jadwal diidentifikasi dan diatasi.
8. Prosedur administratif dan operasional dibentuk dalam pusat data untuk meyakinkan penghindaran dari pelayanan yang terganggu dan kelangsungan operasi dalam kejadian pada gangguan panjang dari kemampuan pengolahan.
9. Akses fisik ke peerlengkapan enkripsi komputer, media penyimpanan, dan dokumentasi program dibatasi dengan individu yang benar-benar berwenang.
10. Akses fisik ke peerlengkapan produksi kartu, pengirim, kartu, dan media informasi dibatasi dengan individu yang benar-benar berwenang.
11. Akses logis ke sistem jaringan produksi dibatasi dengan individu yang benar-benar berwenang.
12. Nomor identifikasi anggota pemegang kartu dan kunci enkripsi tidak pernah diterima, diproses, dan dikirim dalam teks yang jelas.
13. Perubahan pada mainframe yang ada dan aplikasi komputer mikro diotorisasi, diuji, disetujui, diimplementasikan dengan jelas, dan didokumentasikan.
14. Perubahan semua database pada parameter lembaga pengguna diotorisasi dan dikontrol untuk melindungi integritas dan akurasi data.
15. Sumber sistem cukup memberikan pengolahan lanjutan untuk pengguna.

TUJUAN KONTROL UNTUK ORGANISASI JASA YANG MENYEDIAKAN APLIKASI SERBA GUNA UNTUK LEMBAGA KEUANGAN

Prosedur dan kebijakan kontrol memberikan keyakinan yang memadai atas efektivitas operasi berikut.

1. Perubahan sistem aplikasi diotorisasi, diuji, disetujui, diimplementasikan dengan benar, dan didokumentasikan.
2. Perubahan pada perangkat lunak sistem yang ada dan implementasi atas perangkat lunak sistem yang baru diotorisasi, diuji, disetujui, diimplementasikan dengan benar, dan didokumentasikan.

3. Akses fisik ke perlengkapan komputer, media penyimpanan, dan dokumentasi program dibatasi dengan individu yang benar-benar berwenang.
4. Akses logis ke program dan data dibatasi dengan individu yang benar-benar berwenang.
5. Transaksi akun deposit diotorisasi dengan benar.
6. Transaksi akun deposit diproses secara lengkap dan akurat.
7. Saldo akun deposit dihitung dengan benar.
8. Transaksi pinjaman diotorisasi berwenang.
9. Transaksi pinjaman diproses secara lengkap dan akurat.
10. Saldo akun pinjaman dihitung dengan benar.

PERTIMBANGAN KONTROL KLIEN

Dari perspektif organisasi klien, informasi yang paling penting yang terkandung dalam laporan auditor jasa adalah pertimbangan kontrol klien. Pertimbangan kontrol klien merupakan prosedur dimana organisasi jasa merekomendasikan agar setiap organisasi klien menerapkan. Kontrol ini melengkapi kontrol pada organisasi jasa untuk meningkatkan tingkat kontrol atas transaksi dan data organisasi klien. Kontrol pada organisasi klien dan organisasi jasa terdiri dari keseluruhan lingkungan pengendalian untuk proses yang sedang dievaluasi.

Dalam laporan auditor jasa, pertimbangan kontrol klien kadang-kadang digambarkan segera setelah setiap gambaran kebijakan dan prosedur serta pengujian dilakukan. Pertimbangan kontrol klien juga dapat dikelompokkan dalam bagian terpisah atau dalam sebuah matriks. Tampilan 5.5, 5.6, 5.7, dan 5.8 memberikan daftar pertimbangan kontrol klien yang sesuai dengan organisasi jasa dalam Tampilan 5.1 sampai 5,4, berturut-turut.Setiap tujuan kontrol tidak selalu memerlukan pertimbangan kontrol klien.

Ketika melakukan audit pada proses yang memanfaatkan organisasi jasa, auditor internal harus memeriksa laporan auditor jasa dan memastikan bahwa setiap pertimbangan kontrol klien telah dilaksanakan di organisasi klien. Jika tidak, auditor harus menentukan alasan pertimbangan kontrol klien yang tidak dilaksanakan, menilai potensi risiko jika kontrol terus diabaikan, dan kemudian membuat rekomendasi yang tepat berdasarkan informasi yang dikumpulkan.

PERTIMBANGAN KONTROL KLIEN UNTUK ORGANISASI JASA PENGOLAH KARTU KREDIT

1. Prosedur harus disusun untuk meyakinkan perubahan pada parameter proses diotorisasi, diimplementasikan, dan ditinjau secara tepat.
2. Prosedur harus disusun untuk meyakinkan transaksi diotorisasi secara tepat, lengkap, dan akurat.
3. Prosedur harus disusun untuk meyakinkan kesalahan data input benar dan ditinjau ulang.
4. Prosedur harus disusun untuk meyakinkan bahwa laporan output ditinjau oleh anggota klien yang berwenang dalam kelengkapan dan akurasi.
5. Prosedur harus disusun untuk meyakinkan bahwa output dari program seimbang secara berkala dengan total kontrol yang relevan.
6. Klien harus meninjau laporan aktivitas pencatatan online yang dihasilkan oleh sistem untuk semua perubahan yang dibuat parameter sistem dan transaksi yang masuk secara online untuk meyakinkan bahwa semua aktivitas sesuai dengan permintaannya.
7. Keamanan aplikasi harus digunakan untuk mengontrol fungsi yang mungkin dilakukan anggota klien. Seseorang dalam setiap tempat klien harus bertanggung jawab atas pemeliharaan dan pengawasan kontrol akses, dan hasil cetak kemampuan akses dari setiap terminal dan operator harus ditinjau secara berkala.
8. Klien bertanggung jawab untuk menyusun dan memelihara parameter kontrol dan meninjau laporan berkala untuk meyakinkan bahwa semua data telah diterima dan dicatat dengan lengkap dan akurat.
9. Laporan harian kelebihan kredit harus ditinjau untuk menentukan bahwa semua kelebihan telah tepat.
10. Kebijakan dan prosedur harus ditetapkan untuk memastikan bahwa laporan kegiatan kredit ditelaah untuk kelengkapan, akurasi, dan aktivitas yang tidak sah pada waktu yang tepat.
11. Prosedur hari akhir yang memadai harus ada untuk memverifikasi volume transaksi dan jumlah uang yang dilaporkan oleh aplikasi sesuai dengan catatan akuntansi internal organisasi klien. Kondisi kelebihan saldo dan pengecualian lain harus diteliti dan diselesaikan secara tepat waktu.
12. Klien harus memastikan bahwa mereka telah menerapkan prosedur dalam menanggapi tindakan yang direkomendasikan oleh organisasi jasa dalam pemulihan rencana ikhtisar bencananya.

PERTIMBANGAN KONTROL KLIEN UNTUK ORGANISASI JASA PENGOLAH PENGGAJIAN

1. Klien harus memastikan bahwa prosedur yang tepat berada di tempat untuk mengontrol penggunaan ID pengguna dan sandi untuk mengakses dan mengirimkan informasi penggajian.
2. Klien harus meninjau laporan audit penggajian secara tepat waktu untuk memastikan bahwa semua informasi penggajian telah dicatat secara lengkap dan akurat. Klien juga harus meninjau bentuk pengaturan master file awal sebelum gaji pertama dijalankan untuk memastikan bahwa informasi tingkat karyawan dan tingkat perusahaan awal telah dicatat secara lengkap dan akurat .
3. Klien harus meninjau laporan audit penggajian secara tepat waktu untuk memastikan bahwa semua informasi penggajian telah diproses secara lengkap dan akurat.
4. Klien harus meninjau cek gaji sampel yang dihasilkan oleh organisasi jasa sebelum proses penggajian awal untuk menentukan bahwa semua informasi lengkap dan akurat, termasuk nama perusahaan, kode, logo, dan tanda tangan.
5. Klien bertanggung jawab untuk meninjau kelengkapan dan keakuratan atas semua laporan yang dihasilkan oleh aplikasi .
6. Prosedur harus disusun untuk memastikan bahwa akses ke komputer pribadi dan terminal terkendali.
7. Prosedur harus disusun untuk memastikan bahwa transaksi diotorisasi dengan tepat, lengkap, dan akurat .
8. Prosedur harus disusun untuk memastikan bahwa kesalahan input data diperbaiki dan ditinjau ulang.
9. Prosedur harus disusun untuk memastikan bahwa laporan output ditinjau oleh anggota klien yang berwenang atas kelengkapan dan akurasi.
10. Prosedur harus disusun untuk memastikan bahwa output dari program ini sesuai secara berkala dengan total kontrol yang relevan.

PERTIMBANGAN KONTROL KLIEN UNTUK ORGANISASI JASA PENGOLAH JARINGAN ATM

Organisasi klien bertanggung jawab atas :

1. Memverifikasi kepatuhan terhadap aturan operasi dari organisasi jasa dan persyaratan teknis.

2. Melakukan pemeriksaan latar belakang yang memadai bagi pengguna yang memiliki akses ke sistem dan proses organisasi jasa.
3. Prosedur administrasi keamanan dan pemeliharaan catatan untuk mengizinkan/mengakhiri akses karyawan ke sistem organisasi jasa.
4. Akurasi dan otentikasi informasi produksi kartu yang digunakan sebagai data input ke sistem produksi kartu organisasi jasa.
5. Verifikasi dan otentikasi semua laporan data output kartu produksi yang dihasilkan dan diterima dari organisasi jasa.
6. Memastikan bahwa nomor identifikasi pribadi (PIN) yang terlambat tepat dari mailing kartu mereka yang terkait.
7. Mengembalikan praktek pengirim untuk menjamin keamanan dan kontrol yang tepat selama penghancuran kartu yang dikembalikan dan PIN dikeluarkan untuk pelanggan.
8. Meninjau dan menyesuaikan aktivitas jurnal transaksi ATM dengan yang dilaporkan oleh organisasi jasa.
9. Memverifikasi laporan penyelesaian dan prosedur untuk memastikan bahwa penyesuaian diterapkan dengan cara yang sesuai dan tepat waktu.
10. Meninjau dan memvalidasi total penyesuaian penyelesaian bersih dan mencatat debit/kredit ke rekening penyelesaian secara tepat waktu.
11. Pemberitahuan tepat waktu ke divisi bantuan organisasi jasa dari masalah operasi antara lembaga mereka dan organisasi jasa.
12. Memelihara dan menguji rencana pemulihan bisnis mereka sendiri.
13. Prosedur administrasi keamanan dan pemeliharaan catatan untuk mengizinkan/mengakhiri akses karyawan ke sistem organisasi layanan.
14. Memverifikasi kepatuhan terhadap aturan operasi organisasi jasa, persyaratan teknis, dan standar lain untuk enkripsi PIN dan manajemen kunci .
15. Menetapkan prosedur otentikasi pengguna yang sesuai untuk mengontrol enkripsi aktivitas manajemen kunci (penciptaan, perubahan, penghapusan).

PERTIMBANGAN KONTROL KLIEN UNTUK ORGANISASI JASA YANG MENYEDIAKAN APLIKASI SERBA GUNA UNTUK LEMBAGA KEUANGAN

1. Modem di lokasi lembaga keuangan klien harus selalu dinonaktifkan kecuali akses remote diperlukan. Lembaga klien harus secara teratur menelaah laporan akses internet untuk memastikan bahwa akses jarak jauh telah disetujui dan dilakukan oleh anggota organisasi jasa.

2. Prosedur lembaga klien harus disusun untuk memastikan bahwa karyawan memiliki akses aplikasi yang sesuai berdasarkan tanggung jawab pekerjaan mereka. Selain itu, prosedur harus disusun untuk memastikan bahwa perubahan pada staf dan/atau tanggung jawab pekerjaan mengakibatkan revisi keamanan tepat waktu. Laporan perubahan otorisasi perlu dikaji secara berkala untuk memastikan bahwa akses ditetapkan dengan benar. Sistem otorisasi harus dibatasi pada anggota yang berwenang. Sandi harus diubah secara berkala dan terstruktur untuk menjaga integritas mereka. Akses pada kemampuan transaksi sensitif harus dibatasi pada anggota yang berwenang. Hanya anggota yang berwenang yang harus diberi sandi sistem pengawas dan diizinkan untuk melakukan fungsi administrasi sistem.
3. Jurnal transaksi harian dan laporan sistem lainnya harus ditinjau secara teratur.
4. Akses ke transaksi akun deposito dan transaksi pemeliharaan file harus dibatasi pada anggota yang berwenang. Laporan otorisasi sistem perlu dikaji secara berkala untuk memastikan bahwa akses ditetapkan dengan benar.
5. Semua dokumentasi yang diperlukan untuk membuka rekening baru harus diperoleh, ditinjau, dan disetujui oleh staf selain mereka yang melakukan fungsi teller. Laporan rekening baru harus dibandingkan dengan tingkat rinci untuk semua dokumentasi akun baru untuk memastikan entri data akurat.
6. Bunga yang dibayar dan laporan yang diposting harus ditinjau untuk memastikan kewajaran perhitungan.
7. Dokumen pendukung dari pinjaman yang disetujui juga harus dijaga untuk dibandingkan dengan laporan yang dihasilkan komputer untuk memastikan bahwa semua pinjaman yang disetujui tersebut telah dicatat dengan benar. Rincian transaksi pemeliharaan file harus dibandingkan dengan dokumen sumber. Prosedur harus dikembangkan untuk mengawasi kredit bermasalah dan transaksi yang hilang, pengumpulan dan investigasi pinjaman yang hilang, dan pemulihan dari pinjaman yang hilang. Laporan pinjaman bermasalah harus ditinjau berkala dan dimulai tindakan untuk meminimalkan kerugian pinjaman.
8. Rekonsiliasi pengguna harian harus dilakukan antara dokumentasi pembayaran pinjaman, catatan pembantu kredit, dan saldo teller. Neraca saldo yang dihasilkan sistem juga harus disesuaikan ke buku besar.
9. Prosedur harus ditetapkan untuk memantau laporan bermasalah, memulai penyelidikan tepat waktu atas kredit bermasalah, dan mengevaluasi kecukupan atas cadangan kerugian pinjaman. Pinjaman yang hilang juga harus diawasi.

10. Laporan akrual bunga pinjaman harus dianalisis secara berkala untuk kewajaran. Pilihan biaya harus ditinjau untuk memastikan bahwa mereka sesuai dengan kebijakan lembaga klien.
11. Akses sistem untuk fungsi buku besar harus dibatasi pada anggota yang berwenang, dan laporan buku besar harus ditinjau secara berkala.
12. Lembaga klien harus meninjau perubahan pada tabel sistem dan parameter untuk memastikan bahwa mereka sesuai dengan kebijakan saat ini.

ALTERNATIF UNTUK SAS 70-JENIS AUDIT

Dengan perkembangan internet dan e-commerce, kebutuhan meningkat untuk alternatif ke SAS 70-jenis audit tradisional. SAS 70-jenis audit tradisional biasanya besar dalam ruang lingkup, yang memakan waktu, dan lebih cocok untuk organisasi besar yang melakukan proses transaksi bervolume tinggi untuk beberapa klien komersial. Mereka dirancang untuk memberikan informasi rinci dan keyakinan kepada auditor dari organisasi klien tentang pengendalian di organisasi jasa yang mungkin mempengaruhi laporan keuangan organisasi klien. Informasi rinci mencakup uraian dari lingkungan SI, prosedur pengujian yang dilakukan oleh auditor jasa, dan hasil pengujian.

Tapi banyak penyedia jasa, seperti penyedia jasa aplikasi kecil atau perusahaan hosting situs web, tidak dapat memberikan SAS 70-jenis audit atau menyewa staf audit internal SI. Dalam kasuslain, organisasi penyedia non-jasa yang bergerak dalam e-commerce atau kegiatan komersial berbasis internet lainnya menginginkan keyakinan independen bahwa sistem internal mereka handal dan aman, dan mereka ingin mengkomunikasikan status keamanannya kepada pelanggan mereka dan pemegang saham untuk mengatasi masalah keamanannya. Beberapa organisasi hanya ingin keyakinan independen bahwa sistem mereka handal dan aman, di luar tim keamanan SI mereka atau bahkan auditor internal SI yang melaporkan.

Untuk menjawab kebutuhan tersebut, beberapa jenis "sertifikasi" telah dikembangkan. Sangat memungkinkan organisasi yang memenuhi standar sertifikasi untuk mengirim sertifikasi elektronik atau segel di situs Web mereka. Bagian berikut menjelaskan secara singkat lima dari sertifikasi umum: TruSecure, SysTrust, WebTrust, BBBOnline, dan TRUSTe.

TruSecure®

TruSecure Corporation (dahulu ICSA dan awalnya dikenal sebagai NCSA) adalah pemimpin dunia dalam solusi jaminan keamanan untuk organisasi yang terhubung ke internet. TruSecure adalah salah satu organisasi pertama yang menawarkan jasa sertifikasi situs. Kriteria utama untuk sertifikasi TruSecure adalah:

- Penggunaan mekanisme keamanan fisik dan logis yang memadai yang mengatasi keinginan klien "postur keamanan". Mekanisme keamanan meliputi: kontrol akses ditulis dan diimplementasikan, antivirus, firewall, kebijakan dan prosedur backup dan redundansi.
- Dokumentasi penggunaan atas kontrol akses standar, mekanisme enkripsi, dan persetujuan atas penggunaan data yang memastikan kerahasiaan semua transaksi akhir dan lalu lintas sesi.
- TruSecure mengevaluasi situs dokumentasi, verifikasi di tempat, pengujian remote, dan pemeriksaan kepatuhan tahunan di tempat berbeda.

Salah satu aspek unik dari sertifikasi TruSecure adalah bahwa menyediakan sejumlah kecil atas asuransi untuk website bersertifikat dalam hal pelanggaran keamanan. Untuk informasi lebih lanjut tentang sertifikasi TruSecure, lihat situs webnya di www.trusecure.com.

SysTrust℠

SysTrust adalah jasa yang dikembangkan bersama oleh American Institute of Certified Public Accountant (AICPA) dan Canada Institute of Chartered Accountants (CICA) yang membolehkan akuntan publik yang berkualitas dengan keterampilan SI yang diperlukan untuk memberikan jaminan bahwa sistem klien sebenarnya dapat diandalkan. SysTrust Versi 1.0 dirilis pada tahun 1999, dan Versi 2.0 dikeluarkan pada tahun 2000. SysTrust memiliki 4 prinsip dan 58 kriteria yang terorganisir :

- Ketersediaan. Sistem ini tersedia untuk operasi dan digunakan pada waktu yang ditetapkan dalam pernyataan atau perjanjian tingkat layanan. Prinsip ini membutuhkan pengujian dari 12 kriteria rinci yang dikelompokkan ke dalam 3 kategori.
- Keamanan. Sistem dilindungi dari akses fisik dan logis yang tidak sah. Prinsip ini membutuhkan pengujian dari 19 kriteria rinci yang dikelompokkan ke dalam 3 kategori.
- Integritas. Pengolahan sistem yang lengkap, akurat, tepat waktu, dan diotorisasi. Prinsip ini membutuhkan pengujian dari 14 kriteria rinci yang dikelompokkan ke dalam 3 kategori.

- Maintainability. Sistem ini dapat diperbarui bila diperlukan dengan cara terus menyediakan ketersediaan sistem, keamanan, dan integritas. Prinsip ini membutuhkan pengujian dari 13 kriteria rinci yang dikelompokkan ke dalam 3 kategori.

Prinsip-prinsip dan kriteria SysTrust dapat diterapkan untuk semua jenis sistem . SysTrust mendefinisikan sistem sebagai infrastruktur perangkat keras, perangkat lunak, orang, prosedur, dan data yang menghasilkan informasi dalam konteks bisnis. Seperti dengan SAS 70-jenis audit, auditor mengeluarkan opini kepada SysTrust. Opini SysTrust mungkin wajar tanpa pengecualian atau wajar. Bertentangan dengan SAS 70-jenis audit, organisasi klien tidak menerima rincian tentang lingkungan SI, prosedur pengujian, dan hasil pengujian.

Untuk informasi lebih lanjut tentang jasa SysTrust, lihat website AICPA (www.aicpa.org) atau website CICA (www.cica.ca). Juga, Boritz dkk. telah menerbitkan sebuah artikel yang sangat bagus dalam memperkenalkan jaminan SysTrust baru service.[14]

WebTrust℠

WebTrust adalah keluarga dari jasa yang dikembangkan bersama oleh AICPA dan CICA yang membolehkan akuntan publik berkualitas dengan keterampilan SI yang diperlukan untuk memberikan jaminan bahwa website klien yang melakukan transaksi perdagangan bisnis ke konsumen atau bisnis ke bisnis elektronik memenuhi standar untuk satu atau lebih dari berbagai prinsip. Surat pendapat wajar tanpa pengecualian harus diperoleh dari auditor sebelum segel WebTrust dapat ditampilkan pada website klien.

WebTrust Versi 1.0 dirilis pada tahun 1997 dengan situs web pertama penghasil segel pada musim semi tahun 1998. Versi 2.0 dikeluarkan pada tahun 1999, dan Versi 3.0 pada tahun 2000. Versi 3.0 membolehkan auditor untuk mengeluarkan opini dan segel yang sesuai dengan prinsip individu atau kombinasi dari prinsip.

Suatu entitas harus mampu menunjukkan lima prinsip WebTrust 3,0. Kriteria rinci dalam setiap prinsip tersebut disusun dalam empat bidang: pengungkapan, kebijakan, prosedur, dan pemantauan.

- Prinsip Privasi On-line. Entitas mengungkapkan praktik privasi, sesuai dengan praktik privasi tersebut, dan memlihara kontrol yang efektif untuk memberikan keyakinan memadai bahwa informasi pribadi yang diperoleh sebagai hasil dari perdagangan elektronik dilindungi sesuai dengan praktik privasi yang diungkapkannya.

- Prinsip Keamanan. Entitas mengungkapkan praktik keamanan kunci, sesuai dengan praktik keamanan tersebut, dan memlihara kontrol yang efektif untuk memberikan keyakinan memadai bahwa akses ke sistem perdagangan elektronik dan data dibatasi hanya untuk individu yang berwenang sesuai dengan praktik keamanan yang diungkapkannya.
- Praktek Bisnis/Prinsip Integritas Transaksi. Entitas mengungkapkan praktik bisnis untuk perdagangan elektronik, mengeksekusi transaksi sesuai dengan praktik-praktik tersebut, dan memelihara kontrol yang efektif untuk memberikan keyakinan memadai bahwa transaksi perdagangan elektronik diproses secara lengkap, akurat, dan sesuai dengan praktik bisnis yang diungkapkan.
- Prinsip Ketersediaan. Entitas mengungkapkan praktik ketersediaan, sesuai dengan praktik ketersediaan tersebut, dan memelihara kontrol yang efektif untuk memberikan keyakinan memadai bahwa sistem perdagangan elektronik dan data yang tersedia sesuai dengan praktik ketersediaan yang diungkapkannya.
- Prinsip Kerahasiaan. Entitas mengungkapkan praktik kerahasiaannya, sesuai dengan praktik-praktik kerahasiaan tersebut, dan memelihara kontrol yang efektif untuk memberikan keyakinan memadai bahwa akses ke informasi yang diperoleh sebagai hasil dari perdagangan elektronik dan ditetapkan sebagai kerahasian yang dibatasi untuk individu yang berwenang, sekelompok orang, atau badan sesuai dengan praktik kerahasiaan yang diungkapkannya.

Selain sertifikasi ini, otoritas sertifikasi (CA) bisa mendapatkan segel WebTrust khusus, yang memiliki tiga prinsip.

- Pengungkapan Praktik Bisnis. Para CA mengungkapkan kunci dan sertifikat manajemen siklus hidup bisnisnya dan praktik informasi privasi dan memberikan jasa sesuai dengan praktik yang diungkapkannya.
- Layanan Integritas. Para CA memelihara kontrol yang efektif untuk memberikan keyakinan memadai bahwa informasi pelanggan telah mendapat otentikasi (untuk kegiatan pendaftaran yang dilakukan oleh ABC-CA) dan integritas kunci dan sertifikat yang dikelolanya didirikan dan dilindungi di seluruh siklus hidup mereka.
- Kontrol lingkungan. Para CA memelihara kontrol yang efektif untuk memberikan keyakinan memadai bahwa pelanggan dan informasi pihak terkait dibatasi untuk individu yang berwenang dan dilindungi dari penggunaan yang tidak ditentukan dalam pengungkapan praktik bisnis CA, kelangsungan kunci dan operasi manajemen

sertifikat dipertahankan, dan pengembangan sistem CA, pemeliharaan, dan operasi telah diotorisasi dan dilakukan untuk memelihara integritas sistem CA dengan baik.

Untuk informasi lebih lanjut tentang keluarga jasa WebTrust, lihat website AICPA (www.aicpa.org) atau website CICA (www.cica.ca).

BBBOnline®

BBBOnline menawarkan dua sertifikasi website, satu untuk keandalan dan satu untuk privasi. Berikut ini adalah persyaratan umum dari setiap program:

Persyaratan Program BBBOnline Keandalan

- Menjadi anggota dari Better Business Bureau (BBB) dimana perusahaan berpusat.
- Memberikan BBB informasi mengenai kepemilikan perusahaan dan manajemen dan alamat jalan dan nomor telepon dimana ia melakukan bisnis, yang dapat diverifikasi oleh BBB dalam kunjungan ke lokasi fisik perusahaan.
- Berbisnis minimal satu tahun (pengecualian dapat dibuat jika bisnis baru adalah sebuah perputaran atau divisi dari bisnis yang sudah ada, yang dikenal dan memiliki catatan yang positif dengan BBB).
- Memiliki catatan penanganan keluhan yang memuaskan dengan BBB.
- Setuju untuk berpartisipasi dalam program pengaturan diri periklanan BBB dan memperbaiki atau menarik iklan online ketika ditantang oleh BBB dan ditemukan tidak mendukung atau tidak sesuai dengan pedoman iklan anak-anak. (BBB tidak mengiklankan online sebelum jelas atau disetujui. Program peninjauan iklan lokal dan nasional dijelaskan di situs BBB, dan keluhan tentang iklan online yang dibawa oleh konsumen, pesaing, atau pejabat publik yang mungkin diajukan secara online dengan BBB.)
- Setuju untuk mematuhi Kode Praktek Bisnis Online BBB dan bekerjasama dengan setiap permintaan BBB dalam memodifikasi situs web untuk membawanya sesuai dengan kode.
- Menanggapi segera untuk semua keluhan konsumen.
- Setuju untuk penyelesaian sengketa, atas permintaan konsumen, untuk sengketa yang belum terselesaikan yang melibatkan produk konsumen atau jasa.

Persyaratan Kelayakan Program BBBOnline Privasi

Persyaratan kelayakan program privasi dikelompokkan ke dalam tujuh kategori:

1. Permulaan: termasuk umum, kelayakan, dan persyaratan kontrak
2. Pernyataan Privasi
3. Berbagi informasi
4. Penghargaan & persetujuan
5. Akses dan koreksi
6. keamanan
7. Program anak: ada persyaratan tambahan untuk situs yang diarahkan pada anak usia di bawah 13 tahun.

Untuk informasi lebih lanjut tentang sertifikasi BBBOnline, lihat situs web BBBOnline di www.bbbonline.com.

TRUSTe™

TRUSTe adalah organisasi swasta nirlaba independen yang memiliki misi untuk membangun kepercayaan pengguna dan keyakinan di internet dan, dalam melakukannya, mempercepat pertumbuhan dalam industri internet. Ini didirikan oleh Electronic Frontier Foundation (EFF) dan CommerceNet Consortium, yang bertindak sebagai independen, berisi entitas kepercayaan. Program privasi TRUSTe mencoba untuk menjembatani kesenjangan antara keprihatinan pengguna atas privasi dan keinginan website untuk informasi mandiri pengungkapan standar . Perbedaan dua masalah TRUSTe "trustmarks."

TRUSTe (Standard)

Website anggota harus mematuhi prinsip privasi yang ditetapkan dan setuju untuk mematuhi pengawasan TRUSTe yang berlangsung dan prosedur penyelesaian masalah pelanggan. Prinsip privasi mewujudkan praktek informasi yang adil disetujui oleh Departemen Perdagangan AS, Federal Trade Commission, dan organisasi dan asosiasi terkemuka yang mewakili industri. Prinsip-prinsip tersebut antara lain:

- Adopsi dan implementasi kebijakan privasi yang memperhitungkan kecemasan konsumen atas pembagian informasi pribadi secara online .
- Pemberitahuan dan pengungkapan pengumpulan informasi dan praktik penggunaan.
- Penghargaan dan persetujuan, memberikan pengguna kesempatan untuk melakukan kontrol atas informasi mereka.
- Keamanan data, kualitas, dan langkah-langkah akses untuk membantu melindungi keamanan dan keakuratan informasi pribadi

Semua website yang menanggung trustmark TRUSTe harus mengungkapkan pengumpulan informasi pribadi mereka dan praktik privasi dalam sebuah pernyataan privasi langsung, umumnya hubungan dari halaman beranda. Lebih dari satu trustmark dapat ditampilkan jika praktik privasi informasi pribadi bervariasi dalam situs.

Persyaratan Segel TRUSTe Privasi Anak

Website diarahkan pada anak usia di bawah 13 tahun harus memenuhi semua persyaratan program reguler dan juga harus tidak melakukan hal-hal berikut :

- Mengumpulkan informasi kontak online dari seorang anak usia di bawah 13 tahun tanpa izin orang tua sebelum diverifikasi atau pemberitahuan langsung orang tua dan dimaksudkan menggunakan informasi ini, harus mencakup kesempatan bagi orangtua untuk mencegah penggunaan informasi dan partisipasi dalam kegiatan ini. Dimana izin orang tua sebelumnya tidak diperoleh, informasi kontak online hanya akan digunakan untuk langsung menanggapi permintaan anak dan tidak akan digunakan untuk kembali menghubungi anak untuk tujuan lain.
- Mengumpulkan informasi kontak pribadi offline dari anak usia di bawah 13 tahun tanpa persetujuan izin orang tua sebelumnya.
- Mendistribusikan kepada pihak ketiga informasi pribadi yang dikumpulkan dari anak usia di bawah 13 tahun tanpa persetujuan izin orang tua sebelumnya.
- Memberikan kemampuan bagi anak usia di bawah 13 tahun di depan umum atau mendistribusikan informasi kontak pribadi tanpa persetujuan izin orang tua sebelumnya, dan melakukan upaya terbaik untuk melarang anak dari meengumumkan informasi kontak.
- Mengajak anak usia di bawah 13 tahun dengan prospek permainan khusus, hadiah, atau kegiatan lain untuk membocorkan informasi lebih dari yang diperlukan untuk berpartisipasi dalam kegiatan tersebut.

Situs ini juga harus menempatkan pemberitahuan yang mencolok dimana informasi pribadi yang dikumpulkan, meminta anak untuk memohon izin orang tua untuk menjawab pertanyaan. Untuk informasi lebih lanjut tentang sertifikasi TRUSTe, lihat situs web Electronic Frontier Foundation di www.eff.org .

Daftar Pustaka

1. American Institute of Certified Public Accountants, *Codification of Statements on Auditing Standards, Service Organizations*, AU Section 324 (March 31, 1993): Paragraph 24(a).
2. *Ibid*., Paragraph 53.
3. Canadian Institute of Chartered Accountants, *Opinions on Control Procedures at a Service* Organization, Section 5900 (July 1, 1987): Paragraph 6(b).
4. *Ibid*., Paragraph 7(a)(b).
5. *Ibid*., Paragraph 13.
6. Faculty of Information Technology of the Institute of Chartered Accountants in England and Wales, *Reports on the Processing of Transactions by Service Organizations*, Technical Release FIT 1/94 (September 1994): Part 1, Paragraph 25.
7. Financial Reporting and Auditing Group of the Institute of Chartered Accountants in England and Wales, *Reports on Internal Controls of Investment Custodians Made Available to Third Parties*, Technical Release FRAG 21/94 (May 1994): Paragraph
8. (2)(3).
9. Ibid., Appendix III, 16 (F).
10. Additional information on Australian auditing standards may be requested from the Australian Accounting Research Foundation, Level 10/600 Bourke Street, Melbourne, Victoria 3000, Australia.
11. Auditing Standards Board of the Australian Accounting Research Foundation, Invitation to Comment, "Reporting on Internal Controls" (April 1996): 6–7.
12. Auditing Standards Board of the Australian Accounting Research Foundation, Auditing Guidance Statement 1026 (January 1997): 6.
13. Financial Reporting and Auditing Group of the Institute of Chartered Accountants in England and Wales, Technical Release FRAG 21/94: Appendix III, 16 (F).
14. American Institute of Certified Public Accountants, AU Section 324: Paragraph 53.
15. Efrim Boritz et al., "Reporting on Systems Reliability," *Journal of Accountancy* (November 1999): 75–87.