MODUL PERKULIAHAN

EDP Audit

Program Audit Sistem Informasi

(*Information Systems Audit Program*)

Abstract

Modul ini mebahas tentang program audit sistem informasi. Program-program audit juga dapat membantu manajemen audit dalam perencanaan sumber daya. Program audit juga dapat meningkatkan konsistensi dalam tes yang dilakukan pada pengendalian umum untuk semua proses

Kompetensi

Mahasiswa mampu memahami tetang Program audit sistem informasi yang ada dan cara pengaplikasiannnya dalam proses audit berjalan.

Pengantar

Program-program audit diperlukan untuk melakukan audit secara efektif dan efisien. Program audit yang pada dasarnya adalah daftar pembanding dari berbagai tes yang harus auditor lakukan dalam lingkup audit mereka untuk menentukan apakah kontrol utama yang dimaksudkan untuk mengurangi risiko signifikan dapat berfungsi seperti yang dirancang. Berdasarkan hasil pengujian yang dilakukan, auditor harus mampu menentukan kecukupan pengendalian selama proses.

Manfaat Program Audit

Program-program audit juga dapat membantu manajemen audit dalam perencanaan sumber daya. Sebagai contoh, manajemen dapat memperkirakan jumlah total waktu yang diperlukan untuk melakukan audit berdasarkan perkiraan jumlah waktu yang diharapkan untuk melakukan setiap langkah-langkah dalam program audit. Manfaat lain dari program audit adalah dapat membantu mempromosikan konsistensi tes yang dilakukan dalam audit dari proses yang sama dari satu siklus ke berikutnya. Selama perencanaan dan persiapan audit, program audit yang digunakan selama audit sebelumnya biasanya dapat digunakan sebagai dasar untuk langkah-langkah yang akan dilakukan selama audit saat ini. Ini jelas tidak berlaku dalam kasus di mana proses tersebut belum pernah diaudit sebelumnya atau di mana proses tersebut telah berubah secara signifikan. Dalam kasus ini, program-program audit yang baru harus dibuat.

Program audit juga dapat meningkatkan konsistensi dalam tes yang dilakukan pada pengendalian umum untuk semua proses. Sebagai contoh, di banyak organisasi, administrator sistem keamanan melakukan penambahan, perubahan, dan penghapusan pengguna dan kemampuan akses mereka. Manajer departemen bertanggung jawab untuk otorisasi kemampuan akses yang diberikan kepada karyawan oleh administrator sistem keamanan tersebut. Dalam kasus ini, mungkin akan lebih praktis untuk menguji kemampuan sistem akses dari pengguna sebagai bagian proses atau departemen tertentu diaudit daripada mencoba untuk menguji kemampuan akses semua pengguna pada satu waktu. Jika departemen audit memilih untuk memeriksa kemampuan akses pengguna pada proses atau dasar departemen, akan sangat berguna untuk mengembangkan program audit standar untuk membantu memastikan bahwa auditor mengevaluasi kemampuan tersebut secara konsisten.

PROGRAM AUDIT SISTEM INFORMASI

Tampilan 3.1 menunjukkan program audit sistem informasi (SI) yang merupakan dasar dari bagian dua buku ini. Program audit dirancang untuk mengatasi risiko utama dari hampir semua sistem komputasi. Oleh karena itu, pernyataan tujuan dan langkah-langkah dalam program ini didesain bersifat umum. Jelas, sistem komputasi dapat memiliki banyak aplikasi yang berbeda yang dijalankannya, masing-masing dengan mengatur keunikan

sendiri pada pengendalian. Namun, semua pengendalian sekitar sistem komputasi sangat mirip.

TAMPILAN 3.1 PROGRAM AUDIT SISTEM INFORMASI

Tujuan: Untuk menilai kecukupan keamanan lingkungan, fisik, keamanan logis dan operasional kontrol yang dirancang untuk melindungi perangkat keras SI, perangkat lunak, dan data terhadap akses yang tidak sah dan perusakan disengaja atau tidak disengaja atau perubahan, dan untuk memastikan bahwa sistem informasi berfungsi dengan cara yang efisien dan efektif untuk membantu organisasi mencapai tujuan strategisnya.

Tes Kontrol Lingkungan (Bab 4 Sampai 6)

Langkah 1. Menilai kecukupan dan efektivitas kebijakan keamanan SI organisasi. Selain itu, menilai apakah persyaratan kontrol yang ditetapkan dalam standar keamanan SI organisasi secara memadai melindungi aset informasi organisasi. Minimal, standar harus menentukan kontrol berikut dan meminta mereka dikenakan menerapkan semua sistem informasi:

a) password perdananya harus diganti setelah sistem diinstal.
b) ada minimal panjang sandi dari delapan karakter atau lebih.
c) sandi memerlukan kombinasi dari karakter alfa dan numerik.
d) password ditutup di layar seperti yang dimasukkan.
e) file password dienkripsi sehingga tak seorang pun dapat membacanya.
f) ada kadaluarsa sandi dengan periode 60 hari atau kurang.
g) tiga kali atau kurang untuk masuk gagal diperbolehkan, kemudian ID pengguna ini ditangguhkan.
h) sesi pengguna dihentikan setelah periode tertentu tidak aktif (misalnya, lima menit atau kurang).
i) sesi masuk bersamaan tidak diperbolehkan.
j) prosedur yang diterapkan untuk menghapus user ID pengguna diakhiri pada waktu yang tepat.
k) pengguna dilatih untuk tidak berbagi atau mengungkapkan sandi dengan pengguna lain, mempostingnya di tempat kerja mereka, menyimpannya dalam berkas electronik, atau melakukan tindakan lain yang bisa mengungkapkan sandi mereka.

l) masuk yang gagal dan keamanan logis lainnya terkait peristiwa (misalnya, menambahkan dan menghapus pengguna, reset password, restart sistem) yang dicatat oleh sistem, dan catatan ditinjau secara teratur oleh petugas sistem keamanan.

m) ada prosedur cadangan dan pemulihan sepenuhnya yang dikembangkan dan diuji untuk membantu memastikan kembalinya bisnis yang terganggu dalam hal terjadi peristiwa bencana penuh atau sebagian.

n) sistem informasi yang baru harus dirancang untuk mengaktifkan kontrol tersebut dilaksanakan oleh administrator sistem keamanan. Sistem baru termasuk yang dikembangkan di rumah, yang dibeli dari vendor, dan sistem prosesor pihak ketiga. Dalam kasus vendor perangkat lunak dan prosesor pihak ketiga, persyaratan kontrol di atas harus ditetapkan sebagai persyaratan dalam kontrak.

Langkah 2. Untuk aplikasi organisasi jasa, periksa laporan terbaru tentang kebijakan dan prosedur yang ditempatkan dalam operasi di lokasi pengolahan data vendor seperti yang disiapkan oleh para auditor eksternal. Di Amerika Serikat, persyaratan format dan pengujian ditentukan oleh Pernyataan Standar Auditing 70 (SAS 70), yang dikeluarkan oleh American Institute of Certified Public Accountants. Laporan SAS 70 mungkin juga menggambarkan tes dari efektivitas kebijakan dan prosedur operasi jika vendor telah mengontrak auditor eksternal untuk melakukannya.

a) menilai kecukupan kontrol yang diuraikan dalam laporan dan menentukan apakah rekomendasi kontrol yang berlaku telah dilaksanakan di organisasi Anda.

b) jika berlaku, tentukan apakah jenis lain dari keamanan atau ada sertifikasi privasi (misalnya, TruSecure, SysTrust, WebTrust, BBBOnline, TRUSTe).

Langkah 3. Jika sistem dibeli dari dan didukung oleh penjual, menilai stabilitas keuangan dari sistem penjual menggunakan laporan keuangan audit terbaru yang disiapkan oleh auditor eksternal penjual. (Secara optimal, langkah ini harus dilakukan sebelum saat keputusan dibuat untuk membeli sistem. Jika tidak, sumber daya penting bisa terbuang pada sistem dimana penjual tidak akan ada lagi).

a) Pilih contoh faktur terakhir dari sistem penjual dan tentukan apakah biaya telah benar dicatat dan diklasifikasikan pada laporan keuangan organisasi Anda. Biaya biasanya diamortisasi selama masa perkiraan manfaat dari sistem.

b) untuk proyek pembangunan SI, tentukan apakah biaya pengembangan internal yang berlaku (misalnya, jam programmer) telah dikapitalisasi dan diamortisasi selama perkiraan masa manfaat dari sistem penggunaan internal sesuai dengan AICPA Statement of Position (SOP) 98-1 (tidak berlaku untuk perangkat lunak yang dijual ke pihak eksternal). Lihat Bab 15 untuk rincian tentang proyek-proyek pembangunan SI.

Langkah 4. Periksa perjanjian lisensi perangkat lunak penjual dan perjanjian apapun untuk pemeliharaan dan dukungan untuk memastikan bahwa mereka saat ini, menunjukka kebutuhan layanan, dan tidak mengandung atau menghilangkan kata-kata apapun yang dapat merugikan organisasi Anda. Bila dapat diterapkan, perjanjian juga harus meminta salinan kode sumber pemrograman dari perangkat lunak versi saat ini yang dapat disimpan dalam escrow oleh pihak ketiga yang independen sehingga tersedia bagi perusahaan Anda dalam acara penjual keluar dari bisnis atau peristiwa lain yang terjadi (misalnya, pelanggaran kontrak; perangkat lunak tidak lagi didukung oleh penjual).

Tes Kontrol Keamanan Fisik (Bab 7)

Langkah 5. Menilai kecukupan keamanan fisik atas perangkat keras sistem komputer dan media penyimpanan.

Langkah 6. Menentukan apakah cukup terlatih administrator keamanan sistem cadangan yang telah ditetapkan.

Langkah 7. Menilai kecukupan dan efektivitas dari rencana dimulainya kembali bisnis yang tertulis, termasuk hasil tes bencana tiruan yang telah dilakukan.

a. menilai kecukupan prosedur cadangan untuk perangkat lunak sistem dan data. Prosedur harus mencakup backup periodik yang diperlukan (harian, mingguan, bulanan), bentuk penyimpanan situs di lokasi aman, dan rotasi media cadangan.

b. verifikasi setidaknya satu alternatif dari serangkaian proses untuk masing-masing asumsi kunci (transportasi, komunikasi, kepegawaian, fasilitas pengolahan, dll).

Langkah 8. Menilai kecukupan pertanggungan asuransi atas perangkat keras, sistem operasi, aplikasi perangkat lunak dan data. Perangkat keras harus menutupi biaya penggantian. Biaya membuat perangkat lunak yang hilang dan data yang harus ditutupi. Secara optimal, cakupan harus meliputi pendapatan yang

hilang akibat langsung dari kegagalan perangkat keras dan hilangnya sistem operasi, aplikasi perangkat lunak, dan data selama acara tertutup.

Tes Kontrol Keamanan Logis (Bab 8)

Langkah 9. Menentukan apakah sandi pertama pada sistem telah berubah dan apakah kontrol ada yang dirubah secara periodik sesuai dengan kebijakan keamanan sistem komputasi, standar, atau pedoman yang diidentifikasi dalam langkah 1.

Langkah 10. Mengamati administrator keamanan sistem menandatangani dan mencetak daftar pengguna sistem saat ini dan kemampuan akses mereka. Selain itu, jika Anda dapat memperoleh akses sistem yang tepat, Anda dapat memperoleh daftar pengguna secara independen.

a. menilai kewajaran kemampuan akses yang ditugaskan pada setiap pengguna.
b. mengkonfirmasi bahwa ID pengguna karyawan yang diberhentikan ditangguhkan pada waktu yang tepat.
c. konfirmasi bahwa kemampuan akses sistem karyawan yang dialihkan disesuaikan secara benar.

Langkah 11. Mendokumentasikan dan menilai kewajaran dari standar keamanan pengaturan parameter sistem. Pengaturan harus sesuai dengan kebijakan sistem keamanan komputasi organisasi, standar, atau pedoman pengujian pada langkah 1. (Waspada terhadap fakta bahwa dalam beberapa sistem, pengaturan parameter pengguna individu menimpa standar keamanan pengaturan parameter sistem.)

Langkah 12. Menguji fungsi sistem kontrol keamanan logis (misalnya, penyamaran sandi, panjang sandi minimum, kadaluarsa sandi, ID pengguna yang ditangguhkan setelah berturut-turut berupaya masuk, log-on saat diperbolehkan, dan sesi habis waktu).

Langkah 13. Menentukan apakah file yang berisi sandi pengguna dienkripsi dan tidak dapat dilihat oleh siapa pun, termasuk administrator sistem keamanan.

Langkah 14. Menentukan apakah data sensitif, termasuk password, seluruh siklus hidup dienkripsi secara memadai, termasuk selama penyimpanan, transmisi melalui jaringan internal atau eksternal atau perangkat telekomunikasi, dan duplikasi pada media cadangan.

Langkah 15. Menilai kecukupan prosedur untuk memeriksa catatan sistem keamanan yang terkait kejadian (misalnya, berturut-turut berupaya masuk dengan tidak sah, sistem restart, perubahan kemampuan akses pengguna dan pengaturan parameter pengguna).

Langkah 16. Menilai kecukupan kontrol akses remote (misalnya, jaringan virtual pribadi [vpn], perangkat token [CRYPTOCard, SecurID, dll], otomatis tekan-kembali, lapisan aman soket [SSL]).

Tes Sistem Informasi Operasi Kontrol (Bab 9)

Langkah 17. Menentukan apakah tugas cukup terpisah dalam operasi daerah-daerah yang mendukung sistem informasi (misalnya, transaksi harus disahkan hanya oleh departemen asal, programmer tidak harus memiliki kemampuan untuk menjalankan program produksi, prosedur harus didokumentasikan secara memadai, dll).

Langkah 18. Menentukan apakah ada masalah perangkat lunak yang signifikan pada sistem. Menilai kecukupan, ketepatan waktu, dan dokumentasi dari upaya resolusi.

Langkah 19. Menilai kecukupan kontrol yang membantu memastikan operasi berfungsi secara efisien dan efektif untuk mendukung tujuan strategis dan operasi bisnis organisasi (misalnya, operator sistem harus memonitor pemrosesan CPU dan pemanfaatan kapasitas penyimpanan selama setiap hari untuk memastikan bahwa kapasitas cadangan yang memadai ada setiap saat).

1. Kontrol lingkungan
2. Kontrol keamanan fisik
3. Kontrol keamanan logis
4. Kontrol operasi SI

Kontrol lingkungan lebih umum daripada kontrol keamanan fisik atau logis. Mereka sering mendikte sejauh mana kontrol keamanan fisik dan logis dikerahkan. Kontrol lingkungan meliputi item seperti kebijakan keamanan SI, standar, dan panduan; struktur pelaporan dalam lingkungan pengolahan SI (termasuk operasi komputer dan pemrograman); kondisi keuangan organisasi layanan dan penjual; lisensi perangkat lunak penjual, pemeliharaan, dan perjanjian dan jaminan yang mendukung; dan status kebijakan dan prosedur sistem komputasi yang ditempatkan dalam operasi di organisasi pelayanan,

jika ada. (Lihat Tampilan 1.1 untuk model konseptual termasuk kontrol lingkungan. Kontrol lingkungan dibahas dalam bab 4 sampai 6.)

Kontrol keamanan fisik berkaitan dengan perlindungan atas perangkat keras komputer, komponen, dan fasilitas di mana mereka berada. Meskipun terbilang kontrol lingkungan, asuransi atas sistem komputer dan biaya untuk menciptakan kembali atau mengganti yang hilang atau program software rusak dan data akan dibahas dalam hubungannya dengan kontrol keamanan fisik karena sangat erat kaitannya. Bab 7 menggali berbagai aspek keamanan fisik.

Kontrol keamanan logis adalah yang telah dikerahkan di dalam sistem operasi dan aplikasi untuk membantu mencegah akses yang tidak sah dan perusakan disengaja atau tidak disengaja atas program dan data. Termasuk kemampuan akses sistem pengguna, profil akses sistem dan parameter serta mekanisme pencatatan. Kontrol keamanan logis dibahas secara lebih rinci dalam Bab 8.

Bab 9 didedikasikan untuk kontrol operasi sistem informasi, yang dirancang untuk membantu memastikan bahwa sistem informasi beroperasi secara efisien dan efektif. Kontrol ini meliputi penyelesaian yang tepat waktu dan akurat atas pekerjaan produksi, distribusi media output, pelaksanaan cadangan dan prosedur pemulihan, pelaksanaan prosedur pemeliharaan, dokumentasi dan resolusi masalah sistem, dan pemantauan unit pemroses sentral dan pemanfaatan kapasitas penyimpanan data.

Sepanjang bab 4 sampai 9, teori yang mendukung mengapa setiap langkah dalam program audit harus dilakukan disajikan dalam bagian pertama dari setiap bab. Bagian kedua dari setiap bab mencakup satu atau lebih deskripsi situasi dunia nyata yang menggambarkan bagaimana konsep-konsep yang diterapkan dalam praktek. Bab ini disajikan dalam urutan kemunculan program audit. Untuk memberikan keleluasaan kepada pembaca ketika menggunakan program audit sebagai referensi, setiap bab telah telah dirancang sebagai suatu modul independen.

PENTINGNYA KONTROL EFEKTIF DAN INTERNAL COSO

Pengendalian internal adalah salah satu yang paling penting dan mendasar konsep yang eksternal dan auditor internal dan profesional bisnis di semua tingkat harus mengerti. The Bisnis profesional membangun dan menggunakan pengendalian internal perusahaan; Auditor meninjau dan menguji operasional, itu, dan sistem keuangan dan proses dengan

tujuan untuk mengevaluasi mereka kontrol internal. Meskipun internal dan eksternal auditor memiliki tujuan yang berbeda, sebagian besar kami referensi dalam bab ini berlaku untuk IT auditor, yang memiliki besar tanggung jawab untuk memahami dan menilai kontrol internal yang berhubungan dengan IT. Meskipun telah ada banyak definisi yang sedikit berbeda pengendalian internal di masa lalu, COSO standar memberikan definisi yang tepat. Ia mengakui bahwa pengendalian internal melampaui hal-hal yang hanya akuntansi dan keuangan dan termasuk Semua proses perusahaan. Juga, karena itu begitu tertanam ke dalam hampir semua bisnis proses, pengendalian internal yang berhubungan dengan TI adalah sebagian besar dari pemahaman kami secara keseluruhan pengendalian internal. Enterprise unit atau proses memiliki kontrol internal yang baik jika itu:

1. Menyelesaikan misinya dinyatakan secara etis
2. Menghasilkan data yang akurat dan dapat diandalkan
3. Sesuai dengan hukum yang berlaku dan kebijakan perusahaan
4. Memberikan untuk ekonomis dan efisien penggunaan sumber daya
5. Menyediakan untuk sesuai pengamanan aset

Semua anggota perusahaan bertanggung jawab pengendalian internal di daerah mereka operasi dan operasi mereka secara efektif. Meskipun atau mungkin karena ini luas dan menjangkau seluruh pengendalian internal definisi, banyak bisnis profesional memiliki masalah dalam memahami sepenuhnya dan menerapkan konsep-konsep pengendalian internal. Melihat definisi kita sedikit berbeda, konsep pengendalian internal dan mendukung proses kontrol kembali ke prosedur dasar mekanik dan dokumen yang pernah ada seluruh sehari-hari kehidupan. Kontrol proses diperlukan untuk kegiatan di dalam dan di luar perusahaan hari ini, dan banyak konsep-konsep dasar dan prinsip-prinsip yang sama mana kontrol dilaksanakan. Sebuah mobil memberikan beberapa contoh dasar kontrol. Ketika Accelerator-aspeed kontrol — ditekan, mobil yang terjadi lebih cepat. Ketika rem — kontrol lain-tertekan, mobil melambat atau berhenti. Ketika kemudi roda dimatikan, kendaraan berubah. Sopir kontrol Mobil, dan semua tiga ini mewakili sistem pengendalian internal dasar mobil. Jika pengemudi tidak menggunakan atau tidak menggunakan akselerator, rem, atau roda kemudi, mobil akan beroperasi luar kendali.

Memperluas konsep ini hanya sedikit, tanda berhenti, lalu lintas arah tanda, atau gerbang penyeberangan mewakili hambatan semua kontrol eksternal untuk mobil dan driver. Pengemudi operator proses pengendalian internal yang berbasis mobil atau sistem tetapi memiliki sedikit keputusan otoritas atas pesan yang dikirim dari kontrol eksternal lampu lalu lintas. Dari perspektif pengendalian internal, perusahaan dapat dibandingkan

dengan kami contoh mobil. Ada banyak perusahaan sistem dan proses di tempat kerja, seperti sebagai akuntansi operasi, proses penjualan, dan sistem IT. Jika manajemen tidak beroperasi atau langsung proses ini dengan benar, perusahaan dapat beroperasi di luar kendali.

Semua anggota perusahaan harus mengembangkan pemahaman tentang yang sesuai sistem kontrol dan kemudian menentukan jika mereka benar terhubung untuk mengelola perusahaan. Sistem ini dirujuk sebagai sistem pengendalian internal perusahaan. Latar belakang standar pengendalian internal Meskipun konsep dan definisi pengendalian internal adalah cukup dipahami dengan baik hari ini, ini bukanlah benar sampai akhir 1980-an. Konsep umum mungkin telah difahami, tapi tidak ada perjanjian yang konsisten antara banyak tertarik tentang apa yang dimaksud oleh " baik kontrol internal." Awal definisi yang pertama datang dari AICPA dan digunakan oleh US Securities and Exchange Commission (SEC) untuk Bursa Act of 1934 memberikan titik awal yang baik. Meskipun telah ada perubahan atas bertahun-tahun, AICPA pertama di dikodifikasikan standar, disebut pernyataan pada audit Standards2 (SAS No. 1) didefinisikan praktek keuangan eksternal audit di Amerika Serikat selama bertahun-tahun. Definisi AICPA pengendalian internal telah tunduk perubahan dan reinterpretations selama bertahun-tahun. Selama 1970-an, SEC dan AICPA merilis banyak definisi pengendalian internal, dan perusahaan-perusahaan besar berwarna audit eksternal mengembangkan interpretasi yang produktif dan pedoman.
Hal-hal yang berubah di akhir 1970-an dan awal 1980-an, masa ketika ada banyak utama US perusahaan kegagalan karena faktor-faktor seperti inflasi tinggi dan resultan tinggi suku bunga. Perusahaan berkali-kali dilaporkan cukup penghasilan di mereka diaudit laporan keuangan, hanya untuk menderita keruntuhan keuangan tidak lama setelah rilis menguntungkan laporan keuangan. Beberapa kegagalan ini disebabkan oleh penipuan keuangan pelaporan, meskipun banyak lainnya karena inflasi tinggi atau ketidakstabilan perusahaan lain isu-isu. Namun demikian, beberapa anggota Kongres rancangan undang-undang untuk " memperbaiki " kegagalan bisnis dan audit ini potensi. Tagihan adalah sidang rancangan dan Kongres diadakan, tetapi undang-undang tidak disahkan. Dalam menanggapi keprihatinan ini serta kurangnya tindakan legislatif, Nasional Komisi pelaporan dibentuk. Ini terdiri dari lima organisasi profesi: IIA dan AICPA, disebutkan sebelumnya; Keuangan Eksekutif International (FEI), sebuah asosiasi manajer senior keuangan; Amerika Akuntansi Association (AAA); dan Institute of Management Accountants (IMA). AAA adalah sebuah organisasi profesional untuk akuntan akademik, dan IMA organisasi profesional akuntan manajerial atau biaya.

Komisi Nasional pelaporan kemudian disebut Treadway Komisi setelah nama ketua nya. Tujuan utama adalah untuk mengidentifikasi faktor penyebab yang memungkinkan pelaporan keuangan yang curang dan membuat rekomendasi untuk mengurangi insiden mereka. Laporan akhir Komisi Treadway, dikeluarkan pada tahun 1987, termasuk rekomendasi untuk manajemen, Direksi, Umum profesi akuntansi, dan others.3 itu juga disebut untuk manajemen laporan Efektivitas sistem pengendalian intern dan menekankan elemen-elemen kunci dalam apa mereka merasa harus systemof pengendalian internal, termasuk lingkungan pengendalian yang kokoh, kode perilaku, komite audit kompeten dan terlibat, dan fungsi audit internal yang kuat. Laporan Komisi Treadway lagi menunjukkan kurangnya definisi konsisten kontrol internal, menyarankan pekerjaan lebih lanjut diperlukan. Komite sama mensponsori Organisasi yang dikelola laporan Treadway yang kemudian mengontrak di luar spesialis dan meluncurkan sebuah proyek untuk mendefinisikan kontrol internal. Meskipun itu dikeluarkan no standar, Komisi Treadway dirilis kerangka pengendalian internal COSO, dibahas dalam bagian selanjutnya dan direferensikan di seluruh buku ini. Kerangka kerja COSO Pengendalian Internal Seperti disebutkan, COSO mengacu pada lima profesional audit dan akuntansi organisasi yang membentuk sebuah Komite untuk mengembangkan laporan pengendalian internal ini; judul resmi adalah Terpadu Control–Integrated Framework.4 seluruh buku ini, kita menyebutnya sebagai COSO pengendalian internal laporan atau kerangka. Hal ini kontras dengan COSO perusahaan risiko Manajemen (COSO ERM) enterprise resource management framework diperkenalkan di Bab 4. Pertama kali dirilis pada bulan September 1992, COSO internal kontrol laporan yang diusulkan kerangka umum untuk definisi pengendalian internal serta prosedur untuk mengevaluasi kontrol tersebut. Dalam jumlah yang sangat singkat tahun, kerangka pengendalian internal COSO telah menjadi standar yang diakui di seluruh dunia untuk pemahaman dan membangun pengendalian internal yang efektif di hampir semua sistem bisnis. Berikutnya paragraf memberikan penjelasan cukup rinci tentang Kerangka COSO pengendalian internal dan penggunaannya oleh auditor internal dan profesional bisnis untuk penilaian kontrol internal dan evaluasi.

Hampir setiap perusahaan publik memiliki struktur prosedur kontrol yang kompleks. Mengikuti format bagan organisasi klasik, mungkin ada tingkat senior dan Manajemen menengah di beberapa unit operasi atau dalam kegiatan yang berbeda. Dalam Selain itu, prosedur pengendalian mungkin agak berbeda di masing-masing level ini dan komponen. Sebagai contoh, satu unit dapat beroperasi dalam lingkungan bisnis yang diatur mana kontrol proses sangat terstruktur, sementara unit lain dapat beroperasi hampir seperti

kewirausahaan start-up dengan struktur yang jauh kurang formal. Tingkat yang berbeda manajemen perusahaan-perusahaan ini akan memiliki kendali yang berbeda keprihatinan perspektif. The pertanyaan " bagaimana Anda menggambarkan Anda sistem pengendalian internal?" mungkin menerima jawaban yang berbeda dari orang-orang di tingkat yang berbeda atau unit di masing-masing perusahaan ini komponen. COSO menyediakan gambaran yang sangat baik dari konsep multidimensi internal kontrol, mendefinisikan pengendalian internal dengan cara ini:

Pengendalian internal adalah proses, dipengaruhi oleh entitas Dewan Direksi, manajemen, dan personel lain, dirancang untuk memberikan jaminan yang wajar mengenai pencapaian tujuan dalam kategori berikut:

- Efektivitas dan efisiensi operasi
- Keandalan pelaporan keuangan
- Sesuai dengan hukum yang berlaku dan regulations5

Menggunakan definisi umum pengendalian internal, COSO menggunakan tiga dimensi kerangka kerja untuk menggambarkan sistem pengendalian internal dalam suatu perusahaan. Pameran 1.2 menggambarkan kerangka kerja COSO pengendalian internal ini sebagai model tiga dimensi dengan lima tingkat pada sisi menghadap ke depan dan tiga komponen utama pengendalian internal — efektivitas dan efisiensi operasional, keandalan pelaporan keuangan, dan kepatuhan dengan hukum yang berlaku dan peraturan — mengambil agak sama segmen model dengan irisan di atasnya. Sisi kanan pameran menunjukkan tiga segmen, tapi mungkin ada lebih, tergantung pada struktur perusahaan.

Masing-masing tingkat kerangka pengendalian internal COSO, dari pemantauan pada top-down lingkungan kontrol Internal, dibahas secara lebih rinci dalam bagian datang. Idenya di sini adalah bahwa ketika kita melihat lapisan aktivitas pengendalian internal yang tengah — seperti periode-akhir keuangan menutup — kita harus mempertimbangkan bahwa kontrol dari segi unit bisnis atau entitas atau divisi beberapa di sisi kerangka mana yang kontrol telah diinstal. Namun, dalam model tiga dimensi ini, setiap kontrol adalah berhubungan dengan semua orang lain di baris yang sama, tumpukan, atau kolom. Titik Kerangka COSO pengendalian internal adalah bahwa kita harus selalu mempertimbangkan setiap kontrol internal yang diidentifikasi dalam hal bagaimana komponennya berhubungan dengan elemen kontrol internal dalam rangka terkait lainnya. Dalam contoh akhir-of period kontrol internal dekat keuangan, perusahaan harus memiliki informasi dan link komunikasi melekat pada proses dekat keuangan, dan kontrol harus dipantau. Menjatuhkan ke tingkat, harus ada kegiatan penilaian risiko terkait dengan proses kontrol

keuangan itu, dan itu harus beroperasi di sesuai lingkungan pengendalian internal. Isu-isu kepatuhan dan operasi juga mengandung faktor untuk kontrol internal tertentu yang dapat berfungsi pada tingkat apapun di perusahaan organisasi. Semua IT auditor harus memiliki pemahaman yang kuat tentang pengendalian internal COSO kerangka kerja. Tidak peduli apa daerah ini di bawah review, IT auditor selalu perlu untuk meninjau dan Pertimbangkan pengendalian internal dalam jenis cara yang bertingkat dan tiga dimensi. Dimulai dengan pertama atau tingkat bawah menghadap ke depan, teks kita menggambarkan COSO internal kontrol kerangka secara lebih rinci.

Kontrol Lingkungan

Dasar dari Kerangka COSO pengendalian internal adalah apa COSO panggilan internal kontrol lingkungan, Yayasan untuk semua komponen lain dari pengendalian internal. Memiliki pengaruh pada masing-masing tiga tujuan dan semua kegiatan unit dan entitas. Kontrol lingkungan mencerminkan sikap secara keseluruhan, kesadaran, dan tindakan oleh Dewan Direksi, manajemen, dan lain-lain tentang pentingnya pengendalian internal di perusahaan. Ada banyak konsep-konsep dasar di sini, dan setiap perusahaan akan memiliki dasar kontrol internal yang unik sendiri. Enterprise sejarah dan budaya sering memainkan peran utama dalam membentuk ini internal kontrol lingkungan. Ketika suatu perusahaan secara historis telah memiliki manajemen yang kuat penekanan pada memproduksi produk-produk yang bebas dari kesalahan dan Kapan manajemen senior berkomunikasi pentingnya kualitas tinggi produk untuk semua tingkat organisasi, COSO kontrol lingkungan menjadi faktor pengendalian internal perusahaan utama. Konten dan format pesan dari chief executive officer (CEO) atau manajer senior lainnya dikenal sebagai nada di atas — manajemen pesan kepada semua pemangku kepentingan. Namun, jika manajemen senior memiliki reputasi mencari jalan lain di Polis pelanggaran, pesan negatif yang sama ini akan disampaikan ke tingkat lain di perusahaan. Nada positif di bagian atas oleh manajemen senior adalah elemen kunci yang kuat perusahaan kontrol lingkungan. IT auditor harus selalu mencoba untuk memahami dan mengevaluasi kontrol keseluruhan lingkungan saat melakukan hampir semua ulasan. Ketika lingkungan pengendalian internal adalah lemah, auditor hampir pasti akan menemukan kontrol tambahan perhatian daerah. The kontrol lingkungan terdiri dari komponen-komponen berikut. Integritas dan nilai-nilai etis. Jika perusahaan telah mengembangkan kuat kode etik yang menekankan integritas dan nilai-nilai etis, dan jika stakeholder muncul untuk mengikuti kode, Semua stakeholder akan memiliki jaminan bahwa perusahaan memiliki seperangkat nilai-nilai yang baik. Kode Etika

atau perilaku merupakan komponen penting dari organisasi pemerintahan. Internal audit kode etik yang dibahas dalam bab 3. Namun, bahkan jika Perusahaan memiliki kuat kode etik, prinsip-prinsip dapat melanggar melalui kebodohan Alih-alih oleh disengaja karyawan penyalahgunaan jabatan. Dalam banyak kasus, karyawan mungkin tidak tahu bahwa mereka melakukan sesuatu yang salah atau keliru percaya bahwa mereka tindakan berada dalam kepentingan terbaik perusahaan. Ketidaktahuan ini sering disebabkan oleh miskin manajemen senior moral bimbingan bukan oleh setiap individu karyawan maksud untuk menipu. Nilai dan kebijakan perusahaan harus dikomunikasikan ke semua organisasi tingkat. Meskipun selalu ada apel buruk dalam usaha apa pun, moral yang kuat pesan akan mendorong semua orang untuk bertindak dengan benar. Tujuan harus selalu mengirimkan pesan yang tepat atau sinyal seluruh perusahaan. Semua pemangku kepentingan, dan tentu saja semua auditor internal, harus memiliki pemahaman yang baik usaha mereka kode perilaku dan bagaimana ini diterapkan. Jika kode yang sudah ada keluar dari tanggal, jika tidak muncul untuk mengatasi masalah etis penting menghadapi suatu perusahaan, atau jika manajemen tidak muncul untuk dapat berkomunikasi kode dengan semua stakeholder pada berulang dasar, manajemen perlu bangun dan memperbaiki kekurangan ini. Kode perilaku menjelaskan aturan untuk perilaku beretika, dan manajemen senior harus mengirimkan pesan etika tepat seluruh perusahaan. Lainnya insentif dan godaan, namun, yang dapat mengikis kontrol lingkungan ini secara keseluruhan. Individu mungkin tergoda untuk terlibat dalam tindakan yang tidak jujur, ilegal atau tidak etis jika perusahaan mereka memberi mereka insentif yang kuat atau godaan untuk melakukannya. Sebagai contoh, perusahaan dapat membangun sangat target kinerja tinggi, tidak realistis untuk penjualan atau produksi kuota. Jika ada yang kuat hadiah untuk pencapaian tujuan kinerja ini — atau, lebih buruk, kuat ancaman untuk kehilangan target — karyawan dapat didorong untuk melakukan penipuan atau dipertanyakan praktek-praktek untuk mencapai tujuan tersebut.

Fungsi audit internal yang kuat adalah komponen utama dari kontrol COSO lingkungan. Jika internal audit menemukan bahwa manajemen menempatkan batasan pada fungsi audit, CAE harus mengingatkan manajemen senior kepentingan internal audit sebagai bagian dari struktur kontrol secara keseluruhan internal perusahaan dan, lebih penting, harus berkomunikasi masalah ini ke Dewan Direktur komite audit. Komitmen untuk kompetensi. Sebuah perusahaan kontrol lingkungan dapat serius terkikis jika sejumlah besar posisi penuh dengan orang-orang yang kekurangan keterampilan kerja yang diperlukan. Dibutuhkan suatu perusahaan untuk menentukan tingkat kompetensi yang dibutuhkan untuk berbagai pekerjaan tugas dan untuk menerjemahkan kebutuhan tersebut

ke tingkat pengetahuan dan keterampilan yang diperlukan. Dengan menempatkan orang-orang yang tepat dalam pekerjaan yang tepat dan memberikan pelatihan yang memadai bila diperlukan, perusahaan adalah memuaskan COSO kontrol lingkungan komponen ini penting. Dewan Direksi dan Komite Audit. Kontrol lingkungan sangat banyak dipengaruhi oleh tindakan sebuah perusahaan Direksi dan komite audit. Papan yang aktif dan mandiri adalah komponen penting dari kontrol COSO lingkungan. Dengan menetapkan kebijakan tingkat tinggi dan meninjau perilaku perusahaan secara keseluruhan, Dewan dan komite audit memiliki tanggung jawab utama untuk menetapkan nada ini di atas.

Manajemen filsafat dan beroperasi gaya. Filosofi dan operasi gaya manajemen senior memiliki pengaruh yang besar atas sebuah perusahaan kontrol lingkungan. Beberapa manajer tingkat atas sering mengambil signifikan risiko tingkat perusahaan dalam usaha bisnis atau produk mereka baru sementara yang lain sangat berhati-hati atau konservatif. Beberapa manajer tampaknya beroperasi dengan kursi celana mereka sementara yang lainnya meyakini bahwa segala sesuatu harus benar disetujui dan didokumentasikan. Beberapa mungkin mengambil sangat agresif pendekatan dalam mereka interpretasi pajak dan peraturan pelaporan keuangan sementara orang lain pergi oleh buku. Komentar ini tidak berarti bahwa satu pendekatan selalu baik dan buruk lainnya. Filosofi manajemen dan operasional gaya pertimbangan ini adalah bagian dari sebuah perusahaan kontrol lingkungan. Meskipun tidak ada satu set styles dan filosofi terbaik untuk semua perusahaan, faktor-faktor seperti struktur organisasi yang kuat dan efektif kebijakan sumber daya manusia penting ketika mempertimbangkan komponen lain dari pengendalian internal dalam suatu perusahaan. Struktur organisasi. Komponen kontrol internal struktur organisasi menyediakan kerangka kerja untuk perencanaan, pelaksanaan, pengendalian, dan kegiatan pemantauan membantu mencapai tujuan secara keseluruhan. Faktor lingkungan kontrol ini berkaitan dengan bagaimana fungsi dikelola dan diatur. Struktur organisasi adalah aspek penting dari perusahaan kontrol lingkungan, tapi tidak ada satu struktur menyediakan apapun pilihan internal kontrol lingkungan.

Struktur organisasi adalah cara atau pendekatan untuk upaya individu pekerjaan keduanya ditetapkan dan terintegrasi untuk pencapaian tujuan secara keseluruhan. Setiap usaha perlu sebuah rencana yang efektif dari organisasi, dan kelemahan dalam kontrol organisasi dapat memiliki efek meresap seluruh lingkungan kontrol total. Meskipun jelas garis otoritas, namun, perusahaan kadang-kadang memiliki built-in inefisiensi yang dapat menjadi lebih besar dari waktu ke waktu sebagai mereka memperluas, menyebabkan prosedur pengendalian untuk memecah. Tugas dari otoritas dan tanggung jawab.

Penetapan otoritas dan tanggung jawab dalam lingkungan kontrol mirip dengan struktur organisasi komponen baru saja dibahas. Struktur organisasi perusahaan mendefinisikan tugas dan integrasi usaha kerja total. Pada dasarnya adalah tugas dari otoritas cara tanggung jawab didefinisikan dalam deskripsi pekerjaan formal dan disusun secara persyaratan bagan organisasi perusahaan. Meskipun pekerjaan tugas dapat pernah benar-benar melarikan diri beberapa tanggung-jawab yang saling tumpang tindih atau bersama, lebih tepatnya tanggung-jawab ini dapat dinyatakan, semakin baik. Kegagalan dengan jelas mendefinisikan tanggung jawab otoritas dan tempat kerja sering menyebabkan kebingungan dan konflik antara individu dan kelompok kerja upaya.

Kebijakan sumber daya manusia dan praktik. Penutup praktik sumber daya manusia (SDM) personil menyewa, orientasi, pelatihan, evaluasi, dan konseling, mempromosikan, kompensasi, dan mengambil tindakan perbaikan yang tepat. Meskipun perusahaan HR fungsi harus memadai diterbitkan kebijakan dan bimbingan bahan, yang sebenarnya praktek harus mengirim pesan yang kuat kepada karyawan mengenai diharapkan tingkat pengendalian internal kepatuhan, etika perilaku, dan kompetensi. Tingkat yang lebih tinggi karyawan yang secara terbuka penyalahgunaan atau mengabaikan kebijakan SDM cepat mengirim pesan lain tingkat di perusahaan. Themessage tumbuh louderwhen bahkan karyawan tingkat rendah disiplin untuk melanggar kebijakan yang sama sementara semua orang tampak cara lain di pelanggar tingkat yang lebih tinggi.

Efektif HR Kebijakan dan prosedur adalah komponen penting dalam kontrol keseluruhan lingkungan. Pesan dari atas struktur perusahaan kuat akan mencapai sedikit Jika perusahaan tidak memiliki kuat HR Kebijakan dan prosedur di tempat. IT audit harus selalu mempertimbangkan unsur HR kontrol lingkungan ketika meninjau Bagian lain dari kerangka pengendalian internal. Ringkasan. Sama seperti fondasi yang kuat diperlukan untuk bangunan gedung bertingkat, kontrol lingkungan menyediakan dasar untuk komponen lain dari internal kontrol. Perusahaan yang membangun struktur pengendalian internal yang kuat yang harus memberikan perhatian khusus untuk menempatkan batu- bata dasar yang kokoh dalam dasar lingkungan kontrol ini. Tentu saja, IT auditor harus menjaga konsep ini, seperti efektif HR Kebijakan, di pikiran ketika menilai kontrol internal. Apakah lingkungan pengendalian internal COSO tidak memerlukan serangkaian " melakukan debet sama kredit?" jenis aturan akuntansi tetapi kuat secara keseluruhan perusahaan-lebar kebijakan yang efektif.

Penilaian Risiko

Tingkat berikutnya di atas dasar kontrol pada Kerangka COSO pengendalian internal penilaian risiko. Kemampuan perusahaan untuk mencapai tujuannya dapat berisiko karena berbagai faktor internal dan eksternal. Memahami dan mengelola risiko lingkungan merupakan elemen dasar dari Yayasan pengendalian internal, dan perusahaan harus memiliki proses di tempat untuk mengevaluasi risiko potensial yang dapat mempengaruhi pencapaian yang berbagai tujuan. Komponen ini penilaian risiko memiliki fokus pada pengendalian internal dalam suatu perusahaan dan memiliki fokus yang lebih sempit daripada Kerangka COSO ERM dibahas dalam bab 4.

Penilaian risiko COSO pengendalian internal harus menjadi proses yang memandang ke depan yang dilakukan di semua tingkat dan hampir seluruh kegiatan dalam perusahaan. COSO menjelaskan penilaian risiko sebagai proses tiga langkah:

1. Memperkirakan pentingnya risiko.
2. Menilai kemungkinan atau frekuensi risiko yang terjadi.
3. Pertimbangkan bagaimana risiko harus dikelola, dan menilai tindakan apa yang harus diambil.

Ini proses penilaian risiko COSO menempatkan tanggung jawab pada manajemen untuk menilai apakah risiko yang signifikan dan, jika demikian, untuk mengambil tindakan yang tepat. COSO internal kontrol juga menekankan bahwa analisis risiko tidak proses teori tetapi sering sangat penting

entitas keberhasilan ekonomi dan operasional. Sebagai bagian dari penilaian yang internal kontrol, manajemen harus mengambil langkah-langkah untuk menilai risiko yang dapat mempengaruhi keseluruhan perusahaan serta risiko atas berbagai kegiatan perusahaan atau entitas. Berbagai risiko, disebabkan oleh sumber-sumber internal atau eksternal, dapat mempengaruhi perusahaan. Elemen penilaian risiko pengendalian internal COSO kerangka merupakan area dimana telah ada banyak kesalahpahaman dan kebingungan karena demikian pula bernama Kerangka COSO ERM dibahas dalam bab 4. Komponen penilaian risiko mencakup kerangka pengendalian internal COSO penilaian risiko dalam individu perusahaan. Kerangka kerja COSO ERM mencakup seluruh entitas dan seterusnya. Ini adalah benar-benar dua terpisah tetapi berkaitan, dan satu bukanlah pengganti yang lain.

Kegiatan Pengawasan

Lapisan berikutnya up dalam rangka pengendalian internal COSO disebut kegiatan pengawasan. Ini adalah proses dan prosedur yang membantu memastikan bahwa tindakan diidentifikasi untuk Alamat risiko dilakukan. Kegiatan pengawasan ada di semua tingkat dan, dalam banyak kasus, mungkin tumpang tindih satu sama lain. Mereka adalah elemen penting untuk bangunan dan kemudian membangun pengendalian internal perusahaan yang efektif. Mengidentifikasi Kerangka COSO pengendalian internal serangkaian kegiatan yang umumnya diklasifikasikan sebagai manual, itu, atau manajemen kontrol; mereka juga dijelaskan dalam hal apakah mereka pencegahan, perbaikan, atau kegiatan pengawasan detektif. Meskipun tidak ada satu set definisi pengendalian internal benar untuk semua situasi, COSO internal kontrol merekomendasikan ini mengontrol aktivitas untuk perusahaan:

- Top-level ulasan. Manajemen dan auditor internal, di berbagai tingkatan, seharusnya meninjau hasil kinerja mereka, kontras hasil tersebut dengan anggaran, Statistik yang kompetitif, dan pengukuran patokan lainnya. Tindakan manajemen untuk menindaklanjuti hasil Tinjauan top-level ini dan mengambil tindakan korektif mewakili aktivitas key control.
- Langsung fungsional atau aktivitas manajemen. Para manajer pada berbagai tingkatan harus meninjau laporan operasional dari sistem kontrol mereka dan mengambil tindakan korektif sebagai tepat. Banyak sistem manajemen telah pengecualian laporan meliputi ini kegiatan pengawasan. Misalnya, sistem keamanan IT harus memiliki mekanisme untuk melaporkan upaya akses yang tidak sah, dengan aktivitas kontrol untuk menindaklanjuti melaporkan peristiwa dan mengambil tindakan korektif yang tepat. Beberapa kegiatan ini link erat dengan perpustakaan infrastruktur teknologi informasi (ITIL) terbaik praktek-praktek yang dibahas dalam Bab 7.
- Pengolahan informasi. Sistem IT sering mengandung kontrol untuk memeriksa kepatuhan di daerah-daerah tertentu dan kemudian melaporkan pengecualian pengendalian internal. Pengecualian tersebut item harus menerima tindakan korektif oleh prosedur sistem otomatis, dengan operasional personil, atau oleh manajemen. Kegiatan pengawasan lainnya mencakup kontrol atas pengembangan sistem baru atau melalui akses ke file data dan program.
- Kontrol fisik. Perusahaan harus sesuai kontrol atas fisik yang aset, termasuk perlengkapan, persediaan, dan negotiable efek. Aktif Program periodik fisik

persediaan merupakan kontrol yang sering signifikan kegiatan di sini, dan IT auditor dapat memainkan peran utama dalam memantau kepatuhan di sini.

- Indikator kinerja. Manajemen harus berhubungan set data, keduanya operasional dan keuangan, ke satu sama lain dan mengambil sesuai analitik, investigasi, atau tindakan korektif. Proses ini merupakan usaha yang penting kontrol aktivitas yang dapat juga memenuhi persyaratan pelaporan keuangan dan operasional.
- Pemisahan tugas. Tugas harus dibagi atau terpisah antara berbagai orang-orang untuk mengurangi risiko kesalahan atau tindakan yang tidak pantas. Dasar ini internal prosedur kontrol harus di layar radar hampir setiap IT auditor.

Kegiatan pengawasan yang disorot di sini mewakili hanya sejumlah kecil dari banyak kegiatan pengawasan dilakukan dalam kursus normal bisnis tetapi melibatkan kebijakan membangun apa yang harus dilakukan dan prosedur untuk mempengaruhi mereka. Meskipun kontrol kegiatan kadang-kadang dapat disampaikan hanya secara lisan, mereka harus dilaksanakan serius, jujur, dan secara konsisten. Pengakuan ini dan komunikasi kegiatan pengawasan adalah pesan yang kuat untuk auditor internal meninjau seperti pengendalian internal kegiatan. Meskipun perusahaan mungkin memiliki penutup diterbitkan kebijakan tertentu Area, harus ada prosedur pengendalian internal yang didirikan untuk mendukung kebijakan itu. Prosedur yang sedikit digunakan kecuali ada fokus yang tajam pada kondisi yang Kebijakan ini ditujukan. Semua terlalu sering, perusahaan dapat membangun sebuah pengecualian laporan sebagai bagian dari sistem otomatis sementara laporan pengecualian tersebut menerima sedikit lebih dari sepintas Manajemen Diperiksa oleh penerimanya. Namun, tergantung pada jenis kondisi dilaporkan, pengecualian tersebut harus menerima tindakan lanjutan yang tepat, yang mungkin berbeda tergantung pada ukuran perusahaan dan aktivitas dilaporkan dalam laporan pengecualian.

Kegiatan pengawasan ini harus erat berkaitan satu sama lain untuk mengidentifikasi risiko dari COSO komponen penilaian risiko pengendalian internal. Kontrol internal kontrol proses, dan tepat kegiatan harus diinstal ke alamat diidentifikasi risiko. Kegiatan pengawasan tidak boleh dipasang hanya karena mereka tampaknya menjadi hak hal yang harus dilakukan, bahkan jika ada tidak ada risiko yang signifikan di daerah mana aktivitas kontrol akan dipasang. Kadang-kadang kegiatan pengawasan mungkin di tempat yang mungkin sekali disajikan beberapa kontrol risiko kekhawatiran, meskipun kekhawatiran yang memiliki sebagian besar pergi. A kontrol kegiatan harus tidak dibuang karena sudah tidak ada sejarah dari kontrol pelanggaran, tetapi manajemen kebutuhan untuk

mengevaluasi kembali risiko relatif ini secara berkala. Semua kegiatan pengendalian internal harus memberikan kontribusi terhadap keseluruhan struktur kontrol, dan IT auditor harus diingat konsep ini ketika mereka meninjau pengendalian internal dan membuat rekomendasi. Kerangka kerja COSO pengendalian internal menekankan bahwa kontrol prosedur diperlukan lebih dari semua signifikan sistem IT: operasional, keuangan, dan kepatuhan yang terkait. Pengendalian internal COSO memecah informasi sistem kontrol ke wellrecognized Umum dan aplikasi kontrol. Kontrol umum berlaku untuk banyak informasi sistem berfungsi untuk membantu memastikan prosedur memadai pengendalian atas semua aplikasi. Kunci keamanan fisik pada pintu pusat server itu adalah seorang Jenderal kontrol untuk semua aplikasi yang berjalan dalam fasilitas tersebut. IT kontrol umum dibahas dalam Bab 6. Aplikasi kontrol, dibahas dalam bab 10, juga penting ini daerah kontrol untuk mengevaluasi keseluruhan kecukupan kontrol internal. COSO internal dokumen kerangka kerja kontrol diakhiri dengan sebuah diskusi tentang perlu mempertimbangkan dampak berkembang teknologi; ini harus selalu dipertimbangkan ketika mengevaluasi itu kegiatan pengawasan. Karena pengenalan cepat teknologi baru, apa baru hari ini akan segera digantikan oleh sesuatu yang lain.

Komunikasi Dan Informasi

Kerangka COSO pengendalian internal di pameran 1.2 menjelaskan paling pengendalian internal komponen sebagai lapisan, satu di atas lain, dimulai dengan kontrol lingkungan seperti Yayasan. Sebagai cara lain untuk melihat kerangka, pameran 1.3 menjelaskan Kerangka kerja COSO sebagai model berbentuk limas dengan informasi dan komunikasi komponen sebagai elemen sisi yang membentang di seluruh komponen lainnya. Sebagai bagian penting kerangka pengendalian internal, informasi dan komunikasi yang terkait tetapi komponen yang berbeda. Informasi yang tepat, didukung oleh sistem TI, harus dikomunikasikan atas dan ke bawah perusahaan dalam cara dan kerangka waktu yang memungkinkan orang-orang untuk melaksanakan tanggung jawab mereka. Selain komunikasi formal dan informal sistem, perusahaan harus memiliki prosedur yang efektif untuk berkomunikasi dengan pihak internal dan eksternal. Sebagai bagian dari evaluasi pengendalian internal, ada kebutuhan untuk memahami aliran ini informasi dan komunikasi di perusahaan. Perusahaan membutuhkan informasi di semua tingkatan untuk mencapai operasional, keuangan, dan tujuan kepatuhan. Sebagai contoh, perusahaan membutuhkan informasi untuk mempersiapkan laporan keuangan yang dikomunikasikan kepada investor luar serta biaya internal dan informasi pasar eksternal preferensi untuk

membuat keputusan pemasaran yang benar. Ini informasi harus mengalir baik dari tingkat atas dari perusahaan ke tingkat yang lebih rendah juga dari tingkat yang lebih rendah kembali ke tingkat atas. Pengendalian internal COSO mengambil luas pendekatan konsep sistem informasi, mengakui bahwa mereka dapat manual, otomatis, atau bahkan konseptual. Salah satu sistem informasi ini dapat berupa formal atau informal. Biasa percakapan dengan pelanggan, atau pemasok dapat menjadi sangat penting sumber informasi dan tipe informal sistem informasi. Efektif Perusahaan harus memiliki sistem informasi di tempat untuk mendengarkan permintaan pelanggan dan / atau keluhan dan untuk meneruskan informasi pelanggan-dimulai sesuai personil. Pengendalian internal COSO juga menekankan pentingnya menjaga informasi dan mendukung sistem sesuai dengan kebutuhan perusahaan secara keseluruhan. Sistem informasi beradaptasi untuk mendukung perubahan pada berbagai tingkatan. IT auditor, misalnya, sering mengalami kasus mana aplikasi itu dilaksanakan tahun sebelumnya untuk mendukung kebutuhan yang berbeda. Meskipun kontrol yang mungkin telah baik, sistem mungkin tidak mendukung perusahaan kebutuhan saat ini. Pengendalian internal COSO mengambil pandangan luas jenis sistem dan menunjukkan kebutuhan untuk memahami proses manual dan otomatis teknologi.

Pemantauan

Pemandangan Piramida pengendalian internal COSO menunjukkan komponen pemantauan sebagai Capstone, tingkat atas komponen pengendalian internal COSO. Meskipun internal sistem kontrol akan bekerja secara efektif dengan dukungan yang tepat dari manajemen, kontrol prosedur dan hubungan informasi dan komunikasi harus di tempat untuk memantau semua kegiatan lain. Pemantauan telah lama peran IT auditor, yang melakukan ulasan untuk menilai kepatuhan terhadap prosedur didirikan; Namun, COSO sekarang mengambil pandangan yang lebih luas dari prosedur pengendalian ini pemantauan. COSO pengendalian internal mengakui bahwa prosedur pengendalian dan sistem lain berubah dari waktu ke waktu. Apa yang tampak agar efektif ketika itu pertama kali dipasang tidak mungkin yang efektif di masa depan karena mengubah kondisi, prosedur baru, atau faktor-faktor lain.

Proses pemantauan harus berada di tempat untuk menilai efektivitas didirikan komponen kontrol internal dan untuk mengambil tindakan korektif saat yang tepat. Ini komponen kontrol internal tidak dapat dikesampingkan hanya untuk audit internal sementara Manajemen tampaknya tetap tidak menyadari potensi masalah kontrol lainnya.

An perusahaan perlu menetapkan berbagai kegiatan untuk mengukur efektivitas pemantauan mereka juga seperti melalui terpisah evaluasi pengendalian internal didirikan kegiatan pengawasan internal sedang berlangsung untuk memantau kinerja dan mengambil tindakan korektif bila diperlukan. Banyak fungsi bisnis rutin dapat digolongkan sebagai kegiatan pengawasan dan Pengendalian internal COSO memberikan contoh-contoh ini komponen penting dari pengendalian internal:

- Operasi manajemen fungsi normal. Manajemen normal ulasan selama operasi dan laporan keuangan yang penting pemantauan kegiatan yang sedang berlangsung, Tapi perhatian khusus harus diberikan untuk melaporkan pengecualian dan pengendalian internal penyimpangan. Pengendalian internal ditingkatkan jika laporan ditinjau secara teratur dan tindakan korektif dimulai untuk melaporkan pengecualian.
- Komunikasi dari pihak luar. Eksternal komunikasi monitor, seperti nomor telepon keluhan pelanggan, mereka penting, dan perusahaan perlu memonitor pesan dari panggilan ini dan melakukan perbaikan tindakan berdasarkan panggilan saat yang tepat.
- Struktur perusahaan dan kegiatan-kegiatan pengawasan. Manajemen senior harus selalu meninjau ringkasan laporan dan mengambil tindakan korektif, tetapi tingkat pertama pengawasan sering memainkan peran yang lebih penting dalam pemantauan. Langsung pengawasan kegiatan administrasi, misalnya, harus secara rutin meninjau dan memperbaiki tingkat rendah kesalahan dan meyakinkan kinerja karyawan administrasi. Hal ini juga daerah di mana pentingnya memadai pemisahan tugas penting, dan membagi tugas antara karyawan memungkinkan mereka untuk melayani sebagai cek pemantauan pada satu sama lain.
- Persediaan fisik dan aset rekonsiliasi. Periodik persediaan fisik, Apakah stock gudang, negotiable efek atau aset itu, adalah penting kegiatan pemantauan. Inventarisasi tahunan di toko ritel, misalnya, mungkin menunjukkan penurunan signifikan barang dagangan. Alasan yang mungkin untuk penurunan ini bisa pencurian, menunjuk ke kebutuhan kontrol keamanan yang lebih baik.

Ini adalah hanya beberapa contoh COSO pengendalian internal kegiatan pemantauan. Ini jenis prosedur yang sering di tempat di banyak usaha tetapi yang tidak dianggap sebagai kegiatan pemantauan yang sedang berjalan. Fungsi atau proses yang ulasan aktifitas usaha secara teratur dan kemudian menunjukkan potensi tindakan korektif dapat dianggap sebagai kegiatan pemantauan. Kerangka kerja COSO pengendalian internal

menunjukkan pentingnya terus-menerus kegiatan pemantauan dan juga menunjukkan bahwa " mungkin berguna untuk melihat segar dari waktu ke waktu " efektivitas pengendalian internal melalui evaluasi terpisah. Frekuensi dan sifat ulasan terpisah ini sangat tergantung pada sifat perusahaan dan pentingnya risiko itu harus mengontrol. Manajemen dapat untuk memulai periodik evaluasi pengendalian internal yang seluruh, tetapi kebanyakan evaluasi harus dimulai untuk menilai kontrol spesifik daerah. Sering ulasan ini dimulai ketika telah ada akuisisi, perubahan dalam bisnis atau aktivitas lain yang signifikan. COSO juga menekankan bahwa evaluasi ini dapat dilakukan oleh garis langsung manajemen melalui penilaian ulasan tamu. IT audit tidak harus melakukan ini Ulasan kecuali jika diminta, dan cukup waktu mungkin berlalu sebelum internal audit mungkin Jadwal penilaian jenis review di daerah operasi. Namun, bertanggung jawab Manajemen harus mempertimbangkan penjadwalan dan melakukan tugas pribadi pada teratur dasar. Jenis review yang dihasilkan secara internal dapat menunjukkan potensi masalah kontrol dan menyebabkan operasi manajemen untuk mengambil tindakan korektif. Karena penilaian ini Ulasan biasanya tidak seperti yang komprehensif sebagai normal audit internal, tindak lanjut Ulasan harus diluncurkan jika masalah berpotensi signifikan ditemui melalui penilaian terbatas ulasan.

Proses evaluasi pengendalian internal. COSO internal kontrol bimbingan bahan garis proses evaluasi untuk mengkaji pengendalian internal. Penilai harus pertama mengembangkan pemahaman tentang desain sistem, menguji kontrol utama, dan kemudian mengembangkan kesimpulan berdasarkan hasil tes. Ini adalah benar-benar itu proses audit. COSO internal kontrol ini juga menyebutkan pembandingan sebagai pendekatan alternatif. Pembandingan adalah proses membandingkan enterprise proses dan prosedur pengendalian dengan rekan perusahaan. Perbandingan dibuat dengan perusahaan serupa atau terhadap industri diterbitkan Statistik. Pendekatan ini nyaman untuk beberapa tindakan tetapi penuh dengan bahaya untuk lain-lain. Sebagai contoh, hal ini cukup mudah untuk patokan ukuran, tingkat kepegawaian, dan rata-rata kompensasi fungsi penjualan terhadap perusahaan-perusahaan yang sebanding pada umumnya sama industri; Namun, penilai mungkin mengalami kesulitan dalam mencoba untuk membandingkan lain faktor karena banyak perbedaan kecil yang membuat semua usaha yang unik. Rencana Aksi evaluasi. Pengendalian internal COSO mengakui bahwa banyak sangat efektif prosedur informal dan tidak terdokumentasikan. Banyak dari kontrol ini tercatat, Namun, dapat diuji dan dievaluasi dalam cara yang sama seperti yang didokumentasikan. An tingkat dokumentasi membuat setiap evaluasi pengendalian internal lain efisien dan memfasilitasi

karyawan pemahaman tentang bagaimana proses bekerja, tapi seperti dokumentasi ini tidak selalu penting. IT auditor enterprise meninjau 's internal sistem kontrol keuangan selalu meminta untuk melihat dokumentasi sistem sebagai bagian dari mereka Tinjauan kerja. Jika proses yang ada informal, tercatat, tapi diakui sebagai efektif, tim review akan perlu mempersiapkan dokumentasi aksi sendiri untuk menjelaskan Bagaimana proses bekerja dan sifat kontrol internal. Pelaporan kekurangan Pengendalian Internal. Ketika kekurangan pengendalian internal yang diidentifikasi — baik melalui proses dalam sistem pengendalian internal itu sendiri, pemantauan kegiatan atau peristiwa lain eksternal — mereka harus dilaporkan ke tingkat yang sesuai manajemen perusahaan. Pertanyaan kuncinya untuk IT audit evaluator adalah untuk menentukan whatshouldbe melaporkan, giventhemanydetails thatmay beencountered, dan towhomthe Laporan harus diarahkan. Pengendalian internal COSO menyatakan bahwa " semua kekurangan pengendalian internal yang dapat mempengaruhi entitas yang mencapai tujuannya harus dilaporkan kepada mereka yang dapat mengambil tindakan diperlukan." Pernyataan ini pengendalian internal COSO akal tapi sering sulit untuk menerapkan. Themodern perusahaan, nomatter howwell terorganisir, sering bersalah berbagai pengendalian internal kesalahan oromissions.COSOinternal kontrol menunjukkan bahwa semua ini harus diidentifikasi dan dilaporkan dan bahwa bahkan tampaknya kecil kesalahan harus menyelidiki untuk memahami jika mereka disebabkan oleh kekurangan kontrol secara keseluruhan. The COSO pengendalian internal laporan menggunakan contoh dari seorang karyawan mengambil beberapa dolar dari dana kas kecil. Meskipun ini bisa dipandang sebagai minormatter karena ukuran kecil pencurian, itu masih harus dilihat sebagai terobosan kontrol secara keseluruhan pada beberapa tingkatan.

Jumlah moneter mungkin tidak signifikan, tetapi pengendalian internal COSO mendesak yang masalah diselidiki daripada diabaikan, karena " seperti memaafkan jelas dari penggunaan pribadi uang entitas yang bisa mengirim pesan yang tidak diinginkan untuk karyawan." Sebelum SOx, auditor eksternal secara teratur menerapkan konsep materialitas ketika melakukan tinjauan dan memutuskan bahwa beberapa kesalahan dan penyimpangan yang sangat kecil bahwa mereka bukanlah bahan auditor eksternal keseluruhan kesimpulan. Dalam tahun pertama Tinjauan SOx kepatuhan dengan pedoman audit standar No. 2 (sebagai 2) asli, pesan dari auditor eksternal banyak adalah bahwa materialitas masalah tidak boleh dianggap — kesalahan adalah sebuah kesalahan. Pendekatan ini disebabkan banyak manajer bertanya-tanya mengapa auditor eksternal mereka mengangkat isu-isu pada apa yang mereka merasa adalah hal-hal kecil. Dengan aturan 5 sebagai dibahas kemudian dalam bab, materialitas dan risiko relatif sekarang harus

dipertimbangkan ketika mengevaluasi efisiensi dan efektivitas pengendalian internal. COSO pengendalian internal bimbingan menyimpulkan dengan membahas kepadanya untuk laporan pengendalian internal kekurangan dalam perusahaan. Dalam satu paragraf, pengendalian internal COSO memberikan bimbingan yang berguna untuk evaluasi.

Temuan pada kekurangan pengendalian internal biasanya harus dilaporkan tidak hanya untuk individu yang bertanggung jawab untuk fungsi atau aktivitas yang terlibat, yang di posisi untuk mengambil tindakan korektif, tetapi juga untuk setidaknya satu tingkat manajemen di atas orang yang secara langsung bertanggung jawab. Proses ini memungkinkan individu untuk memberikan dukungan yang diperlukan atau pengawasan untuk mengambil tindakan korektif, dan untuk berkomunikasi dengan orang lain di perusahaan yang kegiatannya mungkin akan terpengaruh. Mana Temuan memotong melintasi batas-batas organisasi, pelaporan harus menyeberang sebagai baik dan diarahkan ke tingkat cukup tinggi untuk memastikan tindakan yang tepat. Perusahaan juga harus mengembangkan prosedur pelaporan sehingga semua internal mengontrol kekurangan yang ditemui melalui IT audit ulasan operasi terus-menerus dilaporkan sesuai tingkat perusahaan. Pelaporan manajemen dan monitoring adalah aspek yang sangat penting dari pengendalian internal. Internal audit memiliki peran utama dalam proses melalui audit ulasan dan harus menyadari perlunya pengawasan lainnya proses ketika meninjau dan mengevaluasi kontrol internal. Dimensi yang lain dari Kerangka COSO Pengendalian Internal Kadang-kadang kita lupa bahwa Kerangka COSO pengendalian internal harus ditinjau ulang dan dievaluasi sebagai model tiga dimensi, ditampilkan dalam pameran 1.2. Selain menghadap ke depan dimensi model tersebut meliputi kegiatan pengawasan, mencakup sisi kanan entitas atau aktivitas, dan sisi atas atau dimensi rangka kubus covers tiga dimensi dari semua kontrol internal:

1. Efektivitas dan efisiensi operasi
2. Pemenuhan dengan hukum yang berlaku dan peraturan
3. Keandalan pelaporan keuangan Setiap dari daerah-daerah kontrol yang baru saja dibahas — dari kontrol lingkungan untuk memantau — juga harus dipertimbangkan sehubungan dengan yang lain dua dimensi.

Mengenai sisi kanan dimensi, pengendalian internal harus diinstal dan dievaluasi di semua unit di perusahaan. Ini tidak berarti bahwa kegiatan kontrol yang, seperti biaya proses persetujuan, harus identik di semua unit, seperti di perusahaan Kantor pusat atau kantor penjualan di lokasi geografis yang jauh. Namun, harus ada seperangkat konsisten proses kontrol seluruh perusahaan dengan pertimbangan yang diberikan untuk risiko relatif

dan cakupan operasi. Pengendalian internal harus konsisten, tapi mereka harus diterapkan tepat di masing-masing unit operasi.

Dimensi atas Kerangka COSO pengendalian internal ini bahkan lebih penting. Dikatakan bahwa kegiatan pengawasan internal harus diinstal di semua perusahaan yang mengoperasikan unit sehubungan dengan tiga faktor pengendalian internal: keandalan operasi, peraturan kepatuhan, dan efektivitas pelaporan keuangan. Melihat pengendalian internal dari ini tiga dimensi sudut pandang, ada Mei selalu menjadi beberapa variasi tapi kerangka harus di bawah pengendalian internal yang mendasar dan konsisten. Pertimbangkan contoh Fasilitas anak perusahaan di negara Asia Tengah, jauh dari pusatnya US. Negara prosedur persetujuan biaya dapat dikenakan undang-undang setempat, dan proses lainnya mungkin agak berbeda karena komunikasi jarak atau perbedaan dalam sistem TI lokal. Namun, pengendalian internal yang masih harus dilaksanakan dengan cara yang menjamin kehandalan dalam pelaporan keuangan sebagai hasil dilaporkan ke kantor pusat perusahaan. Semua pertimbangan pengendalian internal harus dipertimbangkan dalam hal COSO threedimensional kubus. Maksudnya, kontrol harus dipertimbangkan dalam hal tempat yang sesuai di Perusahaan secara keseluruhan dan hubungannya dengan daerah kontrol tiga tujuan yang baru saja dibahas. Konsep ini menyediakan itu auditor dengan cara yang ampuh untuk melihat pengendalian internal dari perspektif total. Kerangka kerja COSO pengendalian internal yang terus menjadi penting standar dan set bimbingan bahan untuk mengukur dan mengevaluasi kontrol internal.

Kerangka kerja COSO pengendalian internal menjadi standar di seluruh dunia membangun dan mengembangkan kontrol internal yang efektif. Ini adalah proses yang terus-menerus di masing-masing tiga dimensi. Di sisi menghadap ke depan dari model, komponen pemantauan di atas adalah nilai kecil kecuali kontrol internal proses di tempat semua jalan ke bawah untuk Yayasan lingkungan pengendalian internal. Demikian pula, efektif internal kontrol harus dipasang di semua tingkat unit organisasi, dan masing-masing kontrol tersebut harus sensitif terhadap pengendalian internal atas menghadap tiga elemen.

Daftar Pustaka

1. More information on the total roles and responsibilities of internal audit in today's enterprise can be found in Robert Moeller, Brink's Modern Internal Auditing, 7th ed. (Hoboken, NJ: John Wiley & Sons, 2009).
2. Statement on Auditing Standards No. 1, Codification of Auditing Standards and Procedures, AICPA, Professional Standards.
3. National Commission on Fraudulent Financial Reporting, Report of the National Commission on Fraudulent Financial Reporting (1987).
4. Internal Control—Integrated Framework, www.coso.org/publications.htm Note: This reference is for the COSO internal controls report, which can be ordered through the AICPA at www.cpa2biz.com.
5. AICPA-published COSO internal control standards are described in the Statement on Auditing Standards (SAS) numbers 103, 105, 106, 107, 109, 110, and 112.
6. See Robert Moeller, Sarbanes-Oxley Internal Controls: Effective Auditing with AS5, CobiT, and ITIL (Hoboken, NJ: John Wiley & Sons, 2008).
7. COSO, Guidance on Monitoring Internal Control Systems (2009). www.coso.org/documents/ COSO_Guidance_On_Monitoring_Intro_online1.pdf.
8. Here we are presenting only a high-level summary of SOx requirements. See Moeller, Sarbanes-Oxley Internal Controls, for much more information. As a public document, the text of the law can be found in many Web locations. One source is http://fl1.findlaw.com/news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley 072302.pdf.