MODUL PERKULIAHAN

EDP Audit

MENGINDETIFIKASI SISTEM KOMPUTER

(*Identifying Computer System)*

Abstract

Nodul ini mebahas tentang sistem computer beserta komponen-komponen yang melikupinya. Cara kerja sistem computer dan aplikasi yang terkait dengan sistem computer tersebut. Dalam modul ini juga digambarkan beberapa kasus yang ada terkait dengan sistem computer.

Kompetensi

Mahasiswa mampu pememahami tetang sistem computer serta kasus-kasu yang terkait dengan sistem computer.

Pengantar

Sebelum melakukan setiap penilaian atas kontrol sistem komputasi, semua sistem komputasi yang digunakan oleh sebuah organisasi harus diidentifikasi. Membuat inventarisasi sistem komputasi adalah penting sehingga ukuran dan kompleksitas lingkungan sistem komputasi, atau "alam semesta," dalam sebuah organisasi dapat dinilai. Inventarisasi harus mencakup sistem yang telah dikembangkan secara internal seperti yang dibeli dari vendor. Itu juga harus mencakup sistem di mana data organisasi diproses oleh sistem komputer vendor eksternal (vendor ini sering dirujuk sebagai biro jasa, prosesor pihak ketiga, atau organisasi layanan). Inventaris sistem komputasi organisasi mungkin terbukti cukup menantang. Jangan terkejut jika jumlah sistem komputasi bisa mencapai ribuan.

Mengidentifikasi Sistem Komputer

PERSIAPAN

Dalam tujuan buku ini, sistem komputasi biasanya didefinisikan sebagai aplikasi komputer perangkat lunak yang melakukan fungsi bisnis; pendukung sistem manajemen database, jika ada; perangkat keras di mana ia berada dan yang menyediakan akses ke dalamnya; dan sistem operasi yang mengontrol perangkat keras. Sistem komputasi termasuk perangkat keras yang berada dalam sebuah organisasi atau di situs vendor serta program perangkat lunak yang dirancang dan dipelihara oleh programmer internal, dibeli dari dan dikelola oleh vendor, atau berada di situs prosesor pihak ketiga. Buku ini berfokus pada sistem komputasi yang telah atau harus memiliki beberapa bentuk keamanan yang dapat diaudit terkait dengan sistem. Bahkan meskipun dasar kalkulator dapat dianggap sebagai sistem komputer, mereka tidak signifikan dalam istilah risiko yang terkait dengan penggunaannya. Dengan demikian, mereka tidak dimasukkan dalam lingkup buku ini.

Setelah "alam semesta" dari sistem komputasi dalam sebuah organisasi yang telah diidentifikasi, sistem harus dikategorikan dengan kritis; pada dasarnya analisis risiko harus dilakukan pada mereka. Analisis risiko bisa dibuktikan sangat memakan waktu. Metode terbaik untuk mengevaluasi risiko sistem komputasi harus dapat ditentukan. Untuk beberapa hal mungkin dari segi nilai total dolar item yang diproses oleh sistem, sedangkan untuk yang lain mungkin jumlah item yang diproses, total kombinasi dari kriteria ini, atau beberapa faktor lain yang mungkin dianggap tepat. Metode yang paling tepat untuk industri, ukuran organisasi, dan jumlah dan kompleksitas sistem komputasi di organisasi harus ditentukan. Paket perangkat lunak dapat membantu dalam menjalankan analisis risiko. Meskipun perangkat lunak analisis risiko dapat berguna untuk mendapatkan peringkat risiko umum, penilaian manusia harus selalu dilakukana untuk membuat keputusan akhir untuk apa sistem risiko tertinggi dan harus diaudit berikutnya.

Salah satu cara untuk membuat inventarisasi dimulai dengan survei manajer dalam setiap kelompok kerja. Jika organisasi besar, formulir survei tertulis mungkin perlu dibuat dan dikirim ke manajer. Dalam organisasi kecil, menelepon manajer dan secara lisan meminta mereka informasi yang diperlukan mungkin cara yang lebih efisien untuk menyelesaikan survei.

Seperti istilah auditor menyiratkan, salah satunya sering dapat mengidentifikasi sistem komputasi, terutama yang sedang diusulkan atau mereka yang berada dalam tahap awal pengembangan, dengan apa yang orang dengar selama percakapan dengan orang lain

di organisasi atau bahkan melalui rumor. Studi kasus 2.1 menggambarkan situasi di mana aspek yang tidak diketahui dari sistem e-mail yang diidentifikasi melalui rumor perusahaan.

Cara lain untuk mengidentifikasi sistem komputasi adalah menggunakan beberapa macam program penelusuran jaringan yang mengidentifikasi semua file yang dapat dieksekusi. Alat ini juga membantu dalam mengidentifikasi pembajakan atau perangkat lunak lainnya yang tidak sah. Namun, metode ini akan tidak mengidentifikasi semua sistem prosesor pihak ketiga atau aplikasi berbasis internet. Optimalnya, kombinasi metode harus digunakan untuk mengidentifikasi semua sistem.

STUDI KASUS 2.1

Identifikasi dari sistem e-mail yang tidak diketahui

Selama proses audit surat elektronik perusahaan, tampak bahwa hanya ada dua metode yang tersedia di mana karyawan dapat mengirim dan menerima pesan elektronik. Sistem surat elektronik utama adalah bagian dari sebuah aplikasi mainframe dimana semua karyawan adalah akses yang ditugaskan. Beberapa pengguna juga merupakan akses yang ditugaskan untuk jaringan luas area perusahaan. Namun, permohonan surat elektronik tidak diinstal pada jaringan sejak sejumlah besar karyawan tidak menjadi pengguna jaringan.

Semua pengguna jaringan dapat mengirim dan menerima pesan elektronik sampai dengan 240 karakter panjang melalui fitur sistem operasi jaringan. Praktek ini dihambat oleh kelompok manajemen jaringan karena itu bisa mengganggu prosedur update file tertentu. Banyak karyawan menemukan fitur luas ini karena pesan akan muncul di layar kerja penerima dan memerlukan dia untuk mengklik "OK" sebelum melanjutkan pekerjaan, sehingga memastikan segera membaca kecuali penerima tidak pada tempat kerjanya, sehingga ada risiko bahwa seorang pejalan kaki dapat membaca pesan. Pesan sistem operasi ini juga kurang memberatkan pesan e-mail biasa karena mereka tidak dapat diambil setelah penerima mengklik "OK." (Seperti masalah catatan, itu mungkin membuat catatan permanen pesan ini dengan menekan tombol "Print Screen" sebelum mengklik "OK." Tindakan ini akan menyalin layar dan pesan ke clipboard Windows. Pertama buka aplikasi pengolah kata dan klik "Paste" untuk menyalin layar file yang dicetak. Pada saat itu, file dapat disimpan dan dicetak. Dengan demikian, pengirim dari jenis pesan ini mengatur risiko dari konten yang ada di pesan mereka kembali dibuat.)

Sejauh siapa pun di Departemen Audit Internal sadar pada waktu itu, akses internet surat elektronik hanya pada tahap perencanaan, dengan ketersediaan umum untuk semua staf lebih dari satu tahun lagi. Dekat akhir audit, manajer mendengar dari beberapa rekan bahwa beberapa daerah, termasuk semua para eksekutif, memiliki kemampuan untuk mengirim dan menerima pesan di internet. Hal itu kemudian ditemukan bahwa selain untuk para eksekutif, pengguna di empat departemen, termasuk pemasaran dan manajemen jaringan, ditugaskan akses surat elektronik internet. Kami lega, akses surat elektronik internet terbatas dalam perusahaan, file server yang dimiliki dipasang di luar lokasi penjual dan terhubung ke internet melalui mainframe vendor. Dengan demikian, vendor diasumsikan bertanggung jawab untuk menggelar firewall antara sistem dan internet. Untuk mengirim atau menerima pesan melalui internet, pengguna harus menghubungi file server jaringan luar dan tanda masuk. Risiko ini terutama terbatas dengan virus yang melekat pada setiap pesan yang dikirim ke pengguna dan kemudian didownload ke tempat kerja pengguna. Untungnya, risiko ini sudah cukup dikendalikan oleh aplikasi perangkat lunak pendeteksi virusi, yang dipasang pada seluruh area jaringan. Perangkat lunak pendeteksi virus diprogram untuk memeriksa semua file masuk karena virus yang ada di database virus. Selain itu, vendor perangkat lunak virus menyediakan update triwulan untuk membantu memastikan bahwa persediaan virus bisa cukup melindungi virus baru.

Tidak dipercaya bahwa ada setiap maksud untuk menipu Departemen Audit Internal. Namun, contoh ini menggambarkan bagaimana orang-orang di banyak organisasi kadang-kadang mungkin tidak berpikir untuk memberitahukan auditor internal atau eksternal dari sistem baru. Dalam kasus ini, kelompok manajemen jaringan dan pengguna rupanya tidak menganggap bahwa kelompok audit internal akan khawatir tentang risiko yang terkait dengan akses e-mail internet (misalnya, hacking, virus, penyelidikan, kerusakan data) dan kontrol untuk mengurangi resiko tersebut (misalnya, firewall, pemantauan sistem, pencatatan, software proteksi virus, prosedur cadangan). Dalam pikiran mereka, sistem adalah pelayananan baru yang dibuat tersedia secara terbatas untuk memilih karyawan sampai infrastruktur untuk perusahaan akses surat elektronik internet berada di tempat. Mereka percaya bahwa sistem ini memiliki risiko yang relatif rendah dan risiko dikurangi. Mereka tidak mempertimbangkan fakta bahwa itu adalah pekerjaan auditor independen sistem informasi (SI) untuk menilai risiko dan kecukupan terkait kontrol atas sistem komputasi, sebaiknya sebelum instalasi sistem.

MANFAAT INVENTARIS SISTEM KOMPUTASI

Setelah selesai, inventarisasi sistem komputasi dapat memberikan beberapa manfaat yang berguna. Pertama, seperti disebutkan sebelumnya, akan membantu dalam menilai ukuran dan kompleksitas lingkungan sistem komputasi dalam organisasi. Beberapa sistem yang salah satunya tidak menyadari komputer dapat diidentifikasi. Beberapa manfaat dari inventaris sistem komputasi yang dikenakan organisasi memiliki risiko yang signifikan karena relatif mudah dan cepat dimana sistem baru dapat dibeli atau dikembangakan secara internal di lokasi pengguna akhir. Sering manajer dalam tempat pengguna akhir terlalu sibuk atau mungkin sengaja lalai untuk menginformasikan Departemen Audit atau pihak penting lainnya dari pengembangan sistem komputasi baru.

Manfaat kedua inventaris sistem komputasi adalah dapat membantu mengidentifikasi area kerja dimana data yang sama atau yang mirip sedang disimpan dan digunakan. Dalam kasus ini, mungkin ada peluang untuk menggabungkan sumber penyimpanan data dan sumber pengolahan data, berpotensi akan mengurangi biaya dan menigkatkan efisiensi.

Manfaat ketiga adalah inventaris dapat membantu manajemen audit internal dan eksternal dalam merencanakan apakah sistem komputasi untuk memeriksa dan dalam penganggaran sumber daya manusia dan dollar yang diperlukan untuk melakukan pengujian. Studi kasus 2.2 menjelaskan situasi di mana inventaris sistem komputasi dikembangkan dan dimanfaatkan.

STUDI KASUS 2.2

Perisapan dan pemanfaatan inventaris sistem komputasi

Beberapa tahun yang lalu, sebagai auditor SI lembaga keuangan, manajer audit eksternal meminta semua daftar sistem komputasi di organisasi yang memiliki beberapa bentuk keamanan logis yang terkait dengan mereka. Auditor eksternal berencana menggunakan inventaris ini untuk memastikan bahwa audit internal dirancang untuk menilai kecukupan kontrol dan keamanan atas sistem berisiko tinggi yang dilakukan secara teratur. Auditor eksternal juga melakukan tes independen tambahan untuk memungkinkan mereka membuktikan kecukupan dan efektivitas pengendalian umum atas sistem berisiko tinggi ini, dengan demikian membantu mereka mendapatkan jaminan bahwa risiko

kesalahan material dalam pernyataan keuangan adalah minimal. Setiap tahunnya auditor eksternal meminta inventaris diperbarui.

Inventaris sistem komputasi adalah alat yang sangat berguna dalam mempersiapkan rencana audit internal sistem informasi tahunan. Baru-baru ini, daftar menjadi item yang menarik untuk manajemen di Divisi SI organisasi karena membantu mengidentifikasi aplikasi sistem komputasi yang berdiri sendiri yang mungkin menjadi kandidat jaringan, sehingga mengurangi pengulangan data dan biaya perangkat lunak. Biaya lisensi multiuser yang mungkin untuk jaringan perangkat lunak, sebagai contoh, 20 pengguna yang berbarengan, biasanya lebih ekonomis daripada pembelian 20 salinan pengguna single dengan perangkat lunak yang sama.

Daftar juga termasuk sistem komputasi yang dijadwalkan agar diganti atau sistem baru yang sedang dikembangkan. Sekali lagi, Manajemen Divisi SI tertarik dengan sistem ini karena beberapa organisasi pengguna akhir mungkin telah mempertimbangkan pembelian dan/atau pemasangan sistem untuk memenuhi kebutuhan sistem yang ada yang mungkin telah dapat diatasi.

Tampilan 2.1 ini memberikan contoh dari bagian inventaris sistem komputasi yang tampak seperti di lembaga keuangan. Hal itu telah diurutkan berdasarkan jenis sistem operasi atau platform dimana sistem komputasi berada, nama pemilik proses departemen, dan aplikasi bisnis. Biasanya, kolom lain menunjukkan nama dimana sistem ini yang umumnya dikenal akan terdaftar. Namanya biasanya adalah nama produk sebenarnya, layanan, penjual, atau pengembang. Namun, karena namanya biasanya merek dagang atau dengan kata lain dilindungi, kolom dihilangkan dari tampilan. Daftar ini tidak berarti komprehensif, tetapi ini dimaksudkan untuk memberi gambaran pembaca tentang luas berbagai sistem operasi, sistem manajemen database, dan aplikasi yang mungkin mereka hadapi.

PENILAIAN RISIKO

Sekarang sistem komputasi dalam suatu organisasi telah teridentifikasi, yang memiliki informasi yang diperlukan untuk mulai melakukan penilaian risiko lingkungan SI. Tambahan data mengenai jumlah dolar, volume transaksi, dan informasi lainnya harus diperoleh untuk mengaktifkan peringkat dari sistem komputasi dari yang paling berisiko hingga yang kurang berisiko. Itu adalah ide yang baik untuk merekam semua informasi demografis sistem komputasi dalam spreadsheet, database, atau aplikasi perencanaan audit

lainnya. Sistem komputasi kemudian dapat diurutkan dengan berbagai kriteria, seperti sebagai pemilik proses, volume dolar, sistem operasi, dan jenis aplikasi. Seringkali hal ini dapat membantu efisiensi dan efektivitas audit dengan membantu dalam menentukan audit yang perlu dilakukan dan urutan di mana mereka harus lakukan. Sebagai aplikasi perangkat lunak over-the-counter yang disebutkan sebelumnya, khusus untuk membantu dalam proses penilaian risiko. Namun, perangkat lunak tersebut tidak berarti persyaratan. Sebuah spreadsheet atau aplikasi database yang dikembangkan secara internal mungkin cukup memadai.

Periksa kolom aplikasi deskripsi dalam Tampilan 2.1. Anda akan melihat beberapa sistem komputasi yang sangat berisiko tinggi. Sebagai contoh, sistem transfer menyajikan risiko tunggal tertinggi yang dihadapi lembaga keuangan.[1] Transaksi otomatis kliring rumah (ACH) juga merupakan proses yang berisiko tinggi. Di AS banyak lembaga-lembaga keuangan, transfer dan transaksi ACH diproses melalui satu komputer pribadi (PC) berbasis aplikasi yang dikembangkan dan disebarluaskan oleh US Federal Reserve. Sistem berisiko tinggi lain pada daftar inventaris termasuk sistem telekomunikasi, sistem pengolahan cek masuk dan keluar, dan sistem automatic teller machine (ATM).

Kadang-kadang bahkan sistem yang tampaknya jelas dapat menimbulkan risiko yang signifikan. Sebagai contoh, laporan kredit permintaan tempat kerja tercantum dalam Tampilan 2.1 munkgin di permukaan, tampaknya memerlukan keamanan minimal. Namun, jika terminal ini tidak dijamin secara memadai, baik secara fisik atau secara logis, pengguna yang tidak sah dapat meminta laporan kredit melalui terminal. Karena kebanyakan database laporan kredit perusahaan merekam pernyataan oleh organisasi kreditor, orang yang memperoleh informasi kredit oleh pengguna yang tidak sah bisa mengetahui bahwa laporan kredit yang tidak sah namanya telah diminta oleh organisasi kreditor tertentu. Orang tersebut mungkin kemudian berhasil menuntut organisasi kreditor atas pelanggaran privasi jika dia dapat membuktikan bahwa pernyataan yang tidak sah adalah hasil dari pengendalian internal yang buruk. Studi kasus 2.3 menjelaskan situasi laporan kredit yang tidak sah yang diperoleh di lembaga keuangan.

STUDI KASUS 2.3

Laporan kredit tidak sah

Seorang karyawan di sebuah lembaga keuangan ditemukan meminta laporan kredit tidak sah melalui sebuah terminal yang tidak ada kontrol keamanan fisik atau logisnya untuk mencegah akses tersebut. Terminal berada di bangunan yang tidak dibatas dan user

ID dan password tidak diharuskan untuk memulai permintaan laporan kredit. Memanfaatkan kesempatan ini, karyawan meminta laporan kredit baru pada mantan partnernya dengan bunga yang diiginkan. Laporan kredit tidak sah teridentifikasi oleh orang yang melanggar ketika ia mengajukan kredit dan diberitahu bahwa telah ada pertanyaan terbaru dari lembaga keuangan. Penyelidikan berikutnya oleh lembaga keuangan mengungkapkan bahwa karyawan memiliki kesempatan dan motif untuk meminta laporan kredit tidak sah. Singkatnya karyawan dihentikan, meskipun kerusakan telah dilakukan. Untungnya bagi lembaga keuangan, orang yang melanggar tidak menuntut.

Berdasarkan hasil penilaian risiko, sistem komputasi berisiko tertinggi dapat dipilih dan audit kontrol mereka dapat dilakukan. Program audit yang disajikan dalam bab 3 ini dirancang untuk membantu seseorang mendapatkan kenyamanan yang memadai bahwa kontrol utama atas sistem komputasi telah dikerahkan dan bahwa kontrol tersebut berfungsi cukup memadai untuk melindungi perangkat keras komputer, perangkat lunak, dan data dalam organisasi terhadap akses yang tidak sah dan kehancuran atau perusakan disengaja atau tidak disengaja.

Pengantar CobiT

Kata yang tidak biasa bagi banyak orang, CobiT merupakan akronim yang menjadi semakin diakui oleh auditor, profesional TI, dan banyak manajer perusahaan. CobiT adalah kerangka pengendalian internal yang penting yang dapat berdiri sendiri tapi penting dukungan alat untuk mendokumentasikan dan memahami COSO dan SOx pengendalian internal dan mengenali nilai itu aset dalam suatu perusahaan. Umum atau pengetahuan tentang CobiT harus IT auditor persyaratan.

CobiT standar dan kerangka kerja yang dikeluarkan dan secara teratur diperbarui oleh itu Governance Institute (ITGI) dan organisasi profesional mereka erat afiliasi, Audit sistem informasi dan Control Association (ISACA). ISACA lebih terfokus di atasnya audit sementara ITGI's penekanan adalah pada proses penelitian dan pemerintahan. ISACA juga mengelola pemeriksaan Certified informasi sistem Auditor (CISA) dan penunjukan profesional serta baru Certified informasi sistem pengelola (CISM) dan bersertifikat dalam pemerintahan dari perusahaan itu (CGEIT) sertifikasi dan pemeriksaan. Target sertifikasi bersertifikat informasi keamanan manajer (CISM) Manajer keamanan TI dan mempromosikan kemajuan profesional yang ingin diakui untuk itu pemerintahan yang

berhubungan dengan pengalaman dan pengetahuan mereka. Auditrelated ini sertifikasi profesional dibahas dalam bab 30. ISACA awalnya dikenal sebagai EDP Auditor Association (EDPAA), sebuah kelompok profesional yang dimulai pada tahun 1967 oleh auditor internal yang merasa bahwa organisasi profesional saat mereka, Institut Auditor Internal (IIA), tidak memberikan perhatian yang cukup kepada kepentingan sistem TI dan kontrol teknologi sebagai bagian dari kegiatan internal audit. Kami memiliki hampir lupa bahwa EDP pernah berdiri untuk pemrosesan data elektronik, hari hampir kuno

istilah itu. Dari waktu ke waktu, perusahaan profesional ini memperluas fokus dan menjadi ISACA, sementara IIA juga memiliki panjang karena masalah memeluk kuat teknologi. EDPAA, awalnya upstart IT audit profesional organisasi, mulai mengembangkan bahan-bahan bimbingan profesional audit tak lama setelah pembentukannya. Sama seperti EDPAA berkembang menjadi dihormati ISACA dan sekarang ITGI, aslinya IT audit standar menjadi set yang sangat baik dari tujuan pengendalian internal yang berkembang untuk CobiT, sekarang dalam versi 2007 4.1 edition.1 dengan hampir semua proses perusahaan hari ini terikat Fasilitas berhubungan dengan itu, pemahaman tentang luas keseluruhan tata kelola TI penting. The Kerangka cobiT ini sering digambarkan sebagai sebuah pentagon meliputi lima luas dan saling berhubungan daerah kontrol internal, seperti yang digambarkan dalam pameran 2.1. Pameran menunjukkan CobiT's bidang penekanan yang diatur di sekitar konsep inti penting tata kelola TI:

1. Strategis keselarasan. Upaya harus berada di tempat untuk menyelaraskan operasi dan kegiatan dengan semua operasi perusahaan lain. Upaya-upaya ini termasuk membangun hubungan antara operasi bisnis perusahaan dan rencana itu serta proses untuk mendefinisikan, mempertahankan, dan memvalidasi hubungan kualitas dan nilai.
2. Nilai pengiriman. Proses harus berada di tempat untuk memastikan bahwa hal itu dan operasi lainnya unit memberikan manfaat yang dijanjikan seluruh siklus pengiriman dan dengan strategi yang mengoptimalkan biaya sementara menekankan nilai-nilai intrinsik dan aktivitas terkait.
3. Manajemen risiko. Manajemen, di semua tingkat, harus memiliki pemahaman yang jelas nafsu makan suatu perusahaan untuk risiko, persyaratan kepatuhan, dan dampak risiko yang signifikan. ITU dan operasi lainnya memiliki mereka sendiri dan bersama risiko tanggung jawab manajemen yang dapat secara individual atau bersama-sama mempengaruhi seluruh perusahaan.

4. Sumber daya manajemen. Dengan penekanan pada itu, harus ada optimal investasi, dan manajemen yang tepat, penting sumber daya itu, aplikasi, informasi, infrastruktur, dan orang-orang. Pengaturan IT yang efektif tergantung pada optimasi pengetahuan dan infrastruktur.
5. Kinerja pengukuran. Proses harus berada di tempat untuk melacak dan memantau strategi implementasi, penyelesaian proyek, penggunaan sumber daya kinerja proses, dan pelayanan pengiriman. IT governance mekanisme harus menerjemahkan implementasi strategi ke dalam tindakan dan pengukuran untuk mencapai tujuan ini.

Lima masalah pengendalian internal lima CobiT ini adalah elemen kerangka CobiT dan menetapkan pemerintahan. Kerangka CobiT adalah alat yang efektif untuk mendokumentasikan itu dan semua kontrol internal lain. Bab ini terlihat kerangka kerja ini semakin luas perspektif menggunakan CobiT untuk membantu dalam proses governance IT manajemen, perusahaan, dan audit internal. Bagian berikut memberikan gambaran keseluruhan dari kerangka CobiT dan elemen-elemen kunci untuk menghubungkan bisnis dengan tujuan IT melalui kontrol utama dan efektif pengukuran metrik. Selain itu, bab menjelaskan pemetaan CobiT standar dengan kerangka pengendalian internal COSO, dibahas dalam Bab 1, dengan informasi teknologi praktik terbaik Perpustakaan (ITIL) infrastruktur diperkenalkan dalam Bab 7, dan untuk keseluruhan ini dan tata kelola perusahaan. Unsur-unsur dan kunci komponen tata kelola TI dibahas juga. Kerangka CobiT adalah mekanisme yang efektif untuk mendokumentasikan dan memahami pengendalian internal di semua tingkat. Meskipun CobiT pertama kali mulai terutama sebagai satu set bahan " IT audit" bimbingan, itu adalah alat yang jauh lebih kuat hari ini.

KERANGKA cobiT

Proses dan mendukung aplikasi perangkat lunak dan perangkat keras mereka adalah kunci komponen dalam usaha apa pun hari ini. Apakah kecil ritel bisnis dengan kebutuhan untuk menjaga melacak persediaan dan payemployees, atau sebuah perusahaan Fortune 50 besar, semua membutuhkan berbagai set saling berhubungan dan seringkali kompleks itu proses yang erat dengan bisnis mereka operasi. Maksudnya, proses bisnis perusahaan dan sumber daya TI mereka mendukung harus bekerja dalam berbagi informasi hubungan. ITU tidak dapat dan pasti tidak boleh memberitahu operasi bisnis apa jenis proses-proses TI dan sistem untuk melaksanakan, tetapi memberikan informasi untuk membantu mempengaruhi

keputusan bisnis. Pada hari-hari awal komputer sistem, sering ITmanagers merasa mereka punya banyak jawaban dan mempromosikan solusi sistem bisnis mereka, kadang-kadang dengan hasil yang sangat kontraproduktif. Namun, hubungan ini telah berubah hari ini; Operasi itu dan bisnis umumnya harus memiliki Reksa dekat hubungan bersama persyaratan dan informasi. Auditor internal harus memahami kebutuhan dan persyaratan berbagi informasi di kedua sisi. Seperti telah dibahas dalam Bab 1 dalam rangka pengendalian internal COSO, memiliki tanggung jawab atas serangkaian lain daerah terkait proses yang diaudit oleh atau melalui petunjuk audit didirikan, diukur oleh serangkaian langkah-langkah indikator kinerja dan kegiatan, dan dibuat efektif melalui kegiatan tujuan. Semua ini juga mudah dapat menjadi bagian dari CobiT, kontrol kerangka termasuk TI dan bisnis proses. Bab 1 menggambarkan Kerangka COSO pengendalian internal dan kepentingannya di mendefinisikan SOx kontrol internal. IT auditor mungkin bertanya, " saya memahami dan menggunakan COSO kontrol internal. Mengapa kerangka lain?" Jawabannya di sini adalah bahwa CobiT menyediakan pendekatan alternatif untuk mendefinisikan dan menjelaskan pengendalian internal yang memiliki lebih dari itu penekanan dari Kerangka COSO pengendalian internal murni. Informasi dan mendukung Proses-proses TI sering merupakan aset yang paling berharga untuk semua perusahaan hari ini, dan manajemen memiliki tanggung jawab besar untuk menjaga yang mendukung aset, termasuk mereka sistem otomatis. Manajemen, pengguna, dan IT auditor semua perlu memahami ini informasi terkait proses dan kontrol yang mendukung mereka. Kombinasi Proses amd pengendalian internal yang berfokus pada efektivitas dan efisiensi itu sumber daya, proses, dan persyaratan bisnis secara keseluruhan. 2.2 Pameran menggambarkan ini prinsip CobiT, dengan kebutuhan bisnis yang mendorong permintaan sumber daya TI dan sumber daya tersebut memulai proses dan informasi enterprise dalam terus-menerus, cara melingkar. Manajemen harus tertarik pada kualitas, biaya, dan tepat pengiriman berhubungan dengan sumber daya yang komponennya kontrol adalah sama seperti COSO elemen kontrol internal yang dibahas dalam Bab 1. Pengendalian internal terhadap sumber daya TI yang sangat banyak didasarkan pada efektifitas dan efisiensi ketergantungan ini ini komponen.

Tata kelola TI adalah konsep kunci yang tidak sangat ditekankan sebagai elemen CobiT sebelum SOx. Ini adalah konsep pengendalian internal penting hari ini dengan bermain ITGI peran kepemimpinan yang kuat. Seperti dijelaskan di pentagon tata kelola TI di pameran 2.1, CobiT mendefinisikan governance sebagai serangkaian bidang utama mulai dari menjaga fokus strategis keberpihakan dari pentingnya risiko dan kinerja pengukuran

ketika mengelola ITU sumber daya. Kita sebut ini IT governance pentagon lagi ketika kita melakukan navigasi melalui kerangka CobiT.

CobiT memandang pengendalian internal dari tiga itu dimensi: sumber daya, proses, dan informasi kriteria, dijelaskan dalam kubus CobiT digambarkan dalam pameran 2.3. Mirip dengan COSO pengendalian internal kerangka kubus dibahas dalam Bab 1 dan Bab 4 di Kerangka COSO ERM, model CobiT ini memandang IT kontrol dari tiga dimensi perspektif. Itu adalah, masing-masing komponen pada satu permukaan berkaitan dengan dua lainnya menghubungkan dimensi. Namun, menghadap depan CobiT's dimensi dengan deskripsi yang bergambar Diagram aliran proses kadang-kadang takut dari orang-orang non-IT dari mempertimbangkan CobiT. The non–it cerdas profesional- dan ada banyak — mungkin melihat diagram proses pada wajah CobiT kubus dan memutuskan pendekatan ini harus terlalu teknis. Hal ini tidak di Semua benar. Kami menjelaskan dan menerangkan kerangka CobiT dan mengapa ini bisa berharga untuk memahami SOx pengendalian internal dan meningkatkan IT audit dan tata kelola praktek-praktek dalam bagian selanjutnya. Kubus cobiT komponen Sumber daya TI Sisi sumber daya IT kerangka kubus tiga dimensi CobiT mewakili semua perusahaan IT aset, termasuk orang-orang, sistem aplikasi, menginstal teknologi, itu Fasilitas, dan nilai data. Sisi kanan dari kerangka kubus mewakili keprihatinan yang diperlukan dan pertimbangan untuk semua sumber daya yang diperlukan untuk kontrol Administrasi perusahaan IT dan sumber daya. Baik secara perorangan maupun sebagai kelompok, ini sumber daya yang harus dipertimbangkan ketika mengevaluasi kontrol di lingkungan itu:

- Aplikasi yang terdiri dari baik otomatis pengguna sistem dan manual atau otomatis prosedur untuk memproses informasi
- Informasi, termasuk data input, output, dan diproses, untuk digunakan oleh bisnis proses
- Teknologi dan fasilitas infrastruktur komponen termasuk hardware, operasi sistem, database, Jaringan, dan lingkungan yang rumah dan mendukung mereka
- Kunci dan personil khusus untuk merencanakan, mengatur, memperoleh, menerapkan, mendukung, memantau dan mengevaluasi Layanan Kami telah memulai Deskripsi CobiT kami dari sisi kanan kubus CobiT,

Tapi pengendalian internal pertimbangan selalu harus dipertimbangkan dalam hal bagaimana mereka

berhubungan dengan komponen lain pada sisi kubus CobiT juga dengan orang lain dalam hal ini perspektif tiga dimensi. Intinya di sini adalah bahwa sumber daya TI harus selalu dianggap sebagai komponen kunci untuk tata kelola TI dan pengendalian internal.

Proses-proses TI

Dimensi kedua dan menghadap ke depan kubus CobiT merujuk kepada proses-proses TI dan terdiri dari tiga segmen: domain, proses dan kegiatan. Domain adalah pengelompokan Kegiatan itu yang sesuai untuk organisasi area tanggung jawab, dengan empat khusus domain daerah didefinisikan dalam CobiT:

1. Perencanaan dan perusahaan. Daerah domain ini meliputi strategi dan taktik yang memungkinkan untuk berkontribusi pada terbaik dan mendukung tujuan-tujuan bisnis perusahaan. Jenis IT visi strategis pesan harus dikomunikasikan seluruh perusahaan-pesan dari misi dan apa itu berusaha untuk mencapai untuk keseluruhan perusahaan.
2. Akuisisi dan implementasi. Solusi IT perlu diidentifikasi, dikembangkan, atau diperoleh dan kedua dilaksanakan dan terintegrasi dengan proses bisnis. Ini domain daerah meliputi perubahan dan pemeliharaan sistem yang ada.
3. Pengiriman dan dukungan. Daerah domain ini meliputi pengiriman sebenarnya diperlukan Layanan, alat aplikasi dan infrastruktur. Proses sebenarnya aplikasi data dan kontrol ditutupi dalam domain ini.
4. Pemantauan dan evaluasi. Wilayah ini meliputi proses kontrol, termasuk kualitas dan kepatuhan pemantauan, serta evaluasi eksternal dan internal audit prosedur.

Dalam suatu perusahaan itu, proses untuk mengidentifikasi dan membangun aplikasi baru — disebut tradisional sistem pengembangan siklus hidup (SDLC) prosedur — dilihat sebagai bagian dari CobiT implementasi domain, dan jaminan kualitas dapat dipandang sebagai Bagian dari domain pemantauan. Untuk perencanaan dan perusahaan domain, CobiT menunjukkan proses ini spesifik:

- Mendefinisikan sebuah rencana strategis TI.
- Menentukan informasi arsitektur.
- Menentukan arah teknologi.
- Menentukan perusahaan IT dan hubungan.
- Mengelola investasi IT.
- Mengkomunikasikan tujuan manajemen dan arah.
- Mengelola sumber daya manusia.

- Memastikan kepatuhan dengan persyaratan eksternal.
- Menilai risiko.
- Mengelola proyek.
- Mengelola kualitas.

Proses individu adalah tingkat berikutnya ke bawah. Mereka adalah serangkaian kegiatan bergabung dengan istirahat alam kontrol. Akhirnya, kegiatan adalah tindakan-tindakan yang diperlukan untuk mencapai terukur hasil. Kegiatan memiliki siklus hidup sedangkan tugas-tugas diskrit. Kita dapat memikirkan proses siklus hidup (SDLC) pengembangan sistem sebagai siklus mana aplikasi baru dirancang, dilaksanakan, dioperasikan dari waktu ke waktu, dan kemudian diganti dengan proses perbaikan.

Kebutuhan bisnis

Dimensi ketiga model CobiT terdiri dari kebutuhan bisnis. Ini tujuh komponen harus dipertimbangkan ketika mengevaluasi semua kebutuhan bisnis dan dengan pertimbangan diberikan untuk yang diperlukan berikut sumber daya dan unsur-unsur kriteria proses:

1. Efektivitas
2. Efisiensi
3. Kerahasiaan
4. Integritas
5. Ketersediaan
6. Kepatuhan
7. Keandalan

Semua sistem keseluruhan IT atau proses harus dievaluasi dengan pertimbangan yang diberikan kepada satu atau lebih bidang tujuh kriteria ini. Penekanan akan bervariasi, tetapi semua itu proses harus memiliki unsur-unsur dari satu atau lebih dari kriteria ini. Misalnya, untuk aplikasi tertentu itu, IT auditor mungkin khawatir tentang kerahasiaan dan integritas kontrol. Bisnis fungsi biasanya menetapkan persyaratan tersebut untuk keperluan umum bisnis mereka. Untuk itu aplikasi, setiap atribut ini dibahas secara lebih rinci pada bagian berikutnya sebagai serta dalam Bab 8 pada perencanaan dan melakukan itu umum kontrol audit. Mirip dengan model internal control COSO kubus dari bab 1 dan COSO kerangka kerja perusahaan risiko dibahas dalam bab 4, kubus CobiT menyajikan yang efektif cara untuk memahami hubungan antara kebutuhan bisnis, proses-proses TI, dan sumber daya. Sifat tiga dimensi model menekankan hubungan salib dan saling ketergantungan antara

bisnis dan proses-proses TI. Dalam dunia bergantung pada itu kita, ini adalah cara yang berguna untuk auditor IT untuk melihat dan memahami pengendalian internal. CobiT adalah kaya — kadang-kadang hampir terlalu kaya — serangkaian proses untuk berfokus pada bisnis dan TI tujuan dan kontrol utama, dan untuk mengidentifikasi metrik kunci pengukuran. Bagian selanjutnya membahas CobiT dalam beberapa detail, tetapi pembaca disarankan untuk berkonsultasi dengan ITGI CobiT referensi bahan-bahan di www.isaca.org untuk informasi lebih lanjut.

Daftar Pustaka

1. Jack Champlain, "Is Your Wire Transfer System Secure?" *Internal Auditor Journal* (June 1995): 56–59.
2. IT Governance Institute, CobiT—Governance, Control and Audit for Information and Related Technology, 4th ed. (Rolling Meadows, IL: Author, 2000).
3. IT Governance Institute, CobiT 4.1 (Rolling Meadows, IL: Author, 2007).
4. Capability Maturity Model1 Integration (CMMI) is a Carnegie Mellon University–developed process improvement approach that provides organizations with the essential elements of effective processes. It canbe used toguide process improvement across a project, a division, or an entire organization.
5. IT Governance Institute, IT Control Objectives for Sarbanes-Oxley, 2nd ed. (Rolling Meadows, IL: Author, September 2006).
6. IT Governance Institute, ITAFTM: A Professional Practices Framework for IT Assurance (Rolling Meadows, IL: Author, 2008).