AUDYTY BEZPIECZEŃSTWA

WSTĘP

Tradycyjny audyt skupiał się na przeglądzie dokumentacji finansowej organizacji i kontroli w celu sprawdzenia dokładności i integralności danych finansowych. Audytorzy zewnętrzni zazwyczaj skupiali się na kwestiach istotnych lub na poziomie makro, natomiast audytorzy wewnętrzni skupiali się przede wszystkim na kontrolach na poziomie transakcji, ochronie aktywów oraz sprawdzaniu adekwatności i ważności informacji. Zmiany w otoczeniu regulacyjnym na przestrzeni ostatnich kilku lat spowodowały jednak znaczne zwiększenie zakresu i głębokości tych obowiązków. Wraz ze zmianą otoczenia zakres, zakres, wiarygodność i jakość prac kontrolnych znacznie wzrosły pod względem ilości, głębokości i wiarygodności. Dlatego obecne środowisko biznesowe, zarówno globalne, jak i krajowe, w coraz większym stopniu wymaga rutynowych, okresowych audytów i inspekcji bezpieczeństwa, które obejmują zgodność z:

* Wymogi prawne; np. przepisy federalne Stanów Zjednoczonych, takie jak Sarbanes-Oxley (SOX), ustawa o przenośności i odpowiedzialności w ubezpieczeniach zdrowotnych (HIPAA) oraz ustawa Gramma-Leacha-Blileya (GLBA)

* Standardy branżowe, takie jak Payment Card Industry Data Security Standard (PCI DSS) dla organizacji akceptujących płatności kartami kredytowymi

* Standardy audytu, takie jak ISO 17799, ISO 27001 i ISO 27002, Zestawienie standardów audytu (SAS) 70 audytów, zarówno typu I, jak i typu II; oraz Oświadczenie w sprawie standardów usług atestacyjnych (SSAE) nr 16

Audyty te zazwyczaj dotyczą sieci, systemów hostów, łączności związanej z Internetem, urządzeń zabezpieczających i wykrywających, obiektów fizycznych i elementów związanych z polityką w sposób powtarzalny, ponieważ statyczna postawa może nieświadomie narazić organizację na niebezpieczeństwo. Kierownictwo organizacji może postrzegać te przeglądy i audyty z postawami wahającymi się od dwóch skrajności:

1. Stanowią koszt prowadzenia działalności gospodarczej, wymagany przez organ regulacyjny lub prawo rządowe.

2. Miło jest mieć, ale nie wydawaj za dużo pieniędzy.

Obie skrajności, szczególnie ta druga, ignorują wartość takich przeglądów dla organizacji, ponieważ wydatek może być głównym (lub jedynym) kryterium ocenianym przez wyższą kadrę kierowniczą. Sarah Abelow podsumowała wartość audytów technologii informatycznych (IT) w następujący sposób:

1. Zmniejsz ryzyko. Audyty IT zaplanowane i wykonane w oparciu o najlepsze praktyki pozwolą zidentyfikować i ocenić ryzyko w środowisku IT organizacji.… Po ocenie ryzyka można uzyskać jasną wizję tego, jaki kierunek należy obrać — zmniejszyć lub złagodzić ryzyko poprzez kontrole,

przenieść ryzyko poprzez ubezpieczenie lub po prostu zaakceptować ryzyko jako część środowiska operacyjnego…

2. Wzmocnij kontrole (i popraw bezpieczeństwo). W oparciu o oszacowane ryzyko, jak omówiono powyżej, następnym krokiem jest identyfikacja i ocena odpowiednich mechanizmów kontrolnych. Jeżeli kontrole zostaną ocenione jako źle zaprojektowane lub nieskuteczne, można podjąć działania naprawcze.

3. Przestrzegaj przepisów. Szerokie regulacje na poziomie federalnym i stanowym zawierają szczegółowe wymagania dotyczące bezpieczeństwa informacji. Audytor IT pełni kluczową funkcję, zapewniając spełnienie określonych wymagań, ocenę ryzyka i wdrożenie mechanizmów kontrolnych.... Dla organizacji niezwykle ważne jest posiadanie pewności, że wszystkie wymagania zostały spełnione.

4. Ułatwiać komunikację pomiędzy zarządzaniem biznesem a technologią. Audyt otwiera kanały komunikacji pomiędzy biznesem organizacji a zarządem technologii. Audytorzy spędzają czas na przeprowadzaniu wywiadów, obserwacji i testowaniu tego, co dzieje się w rzeczywistości i praktyce. Audyt może dostarczyć cennych informacji w formie pisemnych raportów i ustnych prezentacji. Kierownictwo wyższego szczebla musi wiedzieć z pierwszej ręki, jak funkcjonuje ich organizacja. Odwrotna komunikacja między wyższą kadrą kierowniczą a specjalistami ds. technologii jest również kluczowa. Cele i oczekiwania kierownictwa wyższego szczebla są komunikowane personelowi technologicznemu. Audytorzy mogą ułatwić tę komunikację poprzez udział w spotkaniach technicznych oraz poprzez przegląd bieżącego wdrożenia polityk, standardów i wytycznych....

5. Popraw zarządzanie IT. IT Governance Institute (ITGI) podaje następującą definicję: „Za zarządzanie IT odpowiada kadra kierownicza i zarząd i obejmuje kierownictwo, struktury organizacyjne i procesy, które zapewniają, że IT przedsiębiorstwa utrzymuje i rozwija strategie i cele organizacji. ” Przywództwo, struktury organizacyjne i procesy wymienione w definicji wskazują, że audytorzy IT są kluczowymi graczami. Audyt IT i ogólne zarządzanie IT koncentrują się na wartości, ryzyku i kontrolach wokół środowiska technologicznego organizacji. Audytorzy IT dokonują przeglądu wartości, ryzyka i kontroli we wszystkich kluczowych komponentach technologii — aplikacjach, informacjach, infrastrukturze i ludziach

Ponadto audyty IT i bezpieczeństwa mogą pomóc zapewnić, że organizacja nie stwarza nieświadomie ryzyka związanego z IT dla innych organizacji, niezależnie od tego, czy są one powiązane, zagraniczne, konkurencyjne, równorzędne czy niepowiązane, angażując się, nawet nieświadomie, w krajowe naruszenia bezpieczeństwa, szpiegostwo lub sabotaż przemysłowy, włamanie do komputera, naruszenie prywatności, spam lub nękanie z powodu nieodpowiednich kontroli. Niedawne zmiany w regulacjach i nadzorze rządowym ograniczyły szare strefy audytorów; oznacza to, że zmniejszono liczbę niejasności i wyjątków od wymogów dotyczących raportowania i zgodności. Być może w wyniku rosnącej świadomości społecznej na temat wycieków danych osobowych (PII) na uniwersytetach i w szkołach wyższych na całym świecie opracowano kilka programów studiów licencjackich i magisterskich, których celem jest szkolenie studentów w zakresie audytu IT, bezpieczeństwa i zgodności. Na koniec warto przypomnieć czytelnikom różnicę między audytem a oceną:

* Audyt to formalny proces, zwykle przeprowadzany przez certyfikowanego audytora, skupiający się na sprawdzeniu zgodności z określonymi politykami wewnętrznymi, zewnętrznymi standardami formalnymi i wymogami prawnymi. Raport z audytu zazwyczaj zawiera szczegółowe zestawienie, które dokładnie wymogi formalne zostały spełnione, a które nie.

* Ocena to proces nieformalny, zwykle przeprowadzany przez eksperta branżowego, który może, ale nie musi, być certyfikowany przez organizację zawodową, koncentrujący się na poprawie wydajności i skuteczności, często z wykorzystaniem nieformalnych najlepszych praktyk branżowych i wiedzy specjalistycznej osoby oceniającej. Sprawozdanie z oceny zazwyczaj zawiera szczegółową analizę niedociągnięć i konkretne zalecenia dotyczące konkretnych sposobów poprawy tego, co zostało poddane ocenie

Uwzględnienie wielu przepisów dotyczących bezpieczeństwa informacji.

Przepisy federalne i standardy branżowe w coraz większym stopniu uznają potrzebę zajęcia się kontrolami związanymi z bezpieczeństwem informacji. Jednakże ze względu na ciągły postęp technologiczny oraz różnorodność sprzętu i konstrukcji dostępnych do użycia, przepisy i standardy w dalszym ciągu niejasno określają, w jaki sposób konfiguracje zabezpieczeń powinny być wdrażane, testowane i monitorowane. Chociaż istnieje wielu różnych klientów z różnych branż, z różnymi przepisami, ustawodawstwem lub standardami specyficznymi dla danej branży, wszyscy z nich mają podstawowe źródło swoich najlepszych praktyk. W latach 80-tych Centrum Bezpieczeństwa Komputerowego Obrony rozpoczęło tworzenie szeregu standardów związanych z zabezpieczaniem systemów komputerowych dla podmiotów rządowych i podwykonawców. Seria dokumentów dotyczących konfiguracji, audytu i zabezpieczania systemów jest powszechnie nazywana „Serią Rainbow", ponieważ każda okładka w tej serii ma inny kolor. Systemy, które postępowały zgodnie z procedurami tej serii, uznano za systemy zaufane ze względu na sztywne wymagania dotyczące przestrzegania kryteriów konfiguracji zawartych w tej serii. Dokumenty Rainbow Series przekształciły się w dzisiejszy schemat oceny i walidacji wspólnych kryteriów (CCEVS), aby sprostać wymaganiom współczesnych systemów przetwarzania i systemów komputerowych; jednakże podstawy zabezpieczania i kontrolowania systemów i informacji pozostały częściowo niezmienne i zaczęto je określać jako najlepsze praktyki. Termin najlepsze praktyki jest niejasny, ale koncepcja obejmuje zestaw standardów, doświadczeń i raportów po działaniu (wyciągniętych wniosków), które mają pomóc w spełnieniu wymogów kontroli bezpieczeństwa informacji najczęściej oczekiwanych od zaufanych organizacji. Te najlepsze praktyki wywodzą się ze standardów opracowanych dla bezpiecznych lub zaufanych systemów. Obecnie najlepsze praktyki w zakresie zapewniania informacji wyewoluowały ze sztywnych wymagań standardów Rainbow Series. Najlepsze praktyki można obecnie znaleźć w różnych dokumentach, m.in.:

* Listy kontrolne audytu, które można uzyskać od Stowarzyszenia Audytu i Kontroli Systemów Informacyjnych (ISACA)

* Techniczne wytyczne dotyczące wdrażania bezpieczeństwa Agencji Systemów Informacyjnych Obrony (DISA-STIG)

* Seria publikacji specjalnych (SP) Narodowego Instytutu Standardów i Technologii (NIST) Wydziału Bezpieczeństwa Komputerowego – 800 dokumentów

Innym sposobem rozwiązania problemu wielu przepisów jest włączenie jednego z bardziej kompleksowych ram, takich jak cele kontroli informacji i technologii pokrewnych (COBIT), biblioteka infrastruktury technologii informatycznych (ITIL)7 oraz Międzynarodowa Organizacja Normalizacyjna (ISO) seria 27000 , przy czym wiele z nich polega na innych w zakresie zapewnienia odpowiednich kontroli w obszarach bezpieczeństwa informacji. Sekcje dotyczące bezpieczeństwa informacji różnią się pod względem typów ram, które należy uwzględnić, ale mają wartość, ponieważ identyfikują obszary, które powinny mieć ręczne lub technologiczne kontrole odnoszące się do tych obszarów. Na przykład federalna ustawa o zarządzaniu bezpieczeństwem informacji (FISMA) z 2002 r., ustawa Sarbanes-Oxley z 2002 r. oraz ustawa o przenośności i odpowiedzialności w ubezpieczeniach zdrowotnych z 1996 r. dotyczą polityki bezpieczeństwa, kontroli dostępu logicznego oraz metod obsługi i przechowywania danych Wrażliwa informacja. W przeszłości, jeśli potrzebna była pomoc w klasyfikacji informacji, punktem odniesienia lub standardem była Żółta Księga lub CSC-STD-003-85. Po odpowiednim sklasyfikowaniu informacji organizacja opracowała politykę klasyfikacji bezpieczeństwa informacji, która została zastosowana do zabezpieczenia danych w systemach informatycznych. Obecnie wymagania prawne i specyficzne dla danej branży czasami definiują, jakie informacje są krytyczne lub wrażliwe; dla wielu organizacji szukających odpowiedzi punktem wyjścia jest NIST SP 800-60, Przewodnik po mapowaniu typów informacji i systemów informatycznych na kategorie

bezpieczeństwa. Seria NIST SP 800 zapewnia bogactwo informacji wspierających skuteczne audyty IT i bezpieczeństwa.

Ustawa Gramma-Leacha-Blileya.

Ustawa o modernizacji usług finansowych z 1999 r., bardziej znana jako ustawa Gramma-Leacha-Blileya (GLBA), reguluje bezpieczeństwo osobistych informacji finansowych konsumentów oraz niepublicznych danych osobowych (NPI). Główne postanowienia GLBA dotyczą wymogów dotyczących prywatności informacji, ujawniania danych osobowych i finansowych osobom trzecim, zasad dotyczących ochrony informacji oraz zabezpieczeń przed użyciem pretekstu w celu nielegalnego zdobycia danych osobowych.9 Informacje finansowe mogą zawierać nazwy instytucji finansowych klientów, numery kont oraz informacje dotyczące sald i transakcji. NPI może obejmować datę urodzenia, numer ubezpieczenia społecznego, numer prawa jazdy, numery rachunków finansowych, salda, adres domowy, numery telefonów i tak dalej. GLBA reguluje również ujawnianie takich informacji osobom trzecim. Instytucje, na które GLBA ma wpływ, muszą ujawnić klientom w formie informacji o ochronie prywatności, kiedy i w jaki sposób ich dane są ujawniane. Ponadto instytucje muszą zapewnić klientom możliwość rezygnacji z udostępniania ich informacji niektórym stronom trzecim. Klienci nie mogą korzystać z przywileju rezygnacji w celu wstrzymania udostępniania swoich informacji organom ścigania prowadzącym autoryzowane dochodzenie. Regulacje GLBA chronią także konsumentów przed coraz częściej stosowaną formą inżynierii społecznej zwaną „pretekstem". Pretekst to czynność polegająca na posługiwaniu się fałszywymi oświadczeniami lub podszywaniem się w celu uzyskania dostępu do informacji innej osoby. Przykładem może być sprawca dzwoniący do instytucji finansowej i podający się za uprawnionego posiadacza rachunku z prośbą o dokonanie przelewu drogą telefoniczną. W przypadku braku bezpośredniej weryfikacji prawa jazdy lub innego tokenu, banki dopuszczają takie transakcje po zweryfikowaniu przez osobę dzwoniącą „znanych" informacji, takich jak data urodzenia, adres, numer ubezpieczenia społecznego, i tak dalej. GLBA sprawia, że preteksty są nielegalne i zachęca instytucje do stosowania bardziej rygorystycznych metod potwierdzania tożsamości klienta. Audyt wewnętrzny mający na celu określenie zgodności z GLBA chroni organizacje i zapewnia prawidłowe postępowanie z NPI. Ponieważ niewłaściwe obchodzenie się z danymi NPI lub nieupoważnione ich udostępnienie może prowadzić do przypadków oszustw i kradzieży tożsamości, instytucje, od których wymaga się wykorzystywania i przechowywania takich informacji, muszą bardzo skrupulatnie stosować swoje procesy bezpieczeństwa. Okresowe audyty procesów biznesowych i sieciowych kontrolujących przechowywanie, transmisję i wykorzystanie NPI pomogą w ostrzeganiu organizacji o słabych stronach ich bezpieczeństwa i będą dokumentować wysiłki należytej staranności w zakresie ochrony informacji o klientach.

Federalna ustawa o zarządzaniu systemami informacyjnymi.

FISMA ma wpływ na prawie wszystkie podmioty rządu USA i została utworzona w ramach ustawy o administracji elektronicznej (Public Law 107-347)10 uchwalonej przez 108. Kongres w 2002 r. i podpisanej przez ówczesnego prezydenta George'a W. Busha. W rezolucji uznano znaczenie bezpieczeństwa informacji dla interesów gospodarczych i bezpieczeństwa narodowego Stanów Zjednoczonych. Tytuł III ustawy o administracji elektronicznej upoważniał FISMA11 do wymagania od każdej agencji federalnej opracowania, udokumentowania i wdrożenia obejmującego całą agencję programu zapewniania informacji, który zapewniałby kontrolę bezpieczeństwa informacji i systemów wspierających działalność i aktywa agencji. Środek ten powinien również obejmować kontrole bezpieczeństwa usług lub systemów przetwarzania informacji, które są dostarczane lub zarządzane przez agencje zewnętrzne, wykonawców lub inne źródła. FISMA zdefiniowała, co należy uwzględnić w programie bezpieczeństwa informacji, aby był skuteczny:

* Okresowe oceny ryzyka, w tym wielkości szkód, które mogą wynikać z nieuprawnionego dostępu, użycia, ujawnienia, zakłócenia, modyfikacji lub zniszczenia informacji i systemów informatycznych wspierających działalność i aktywa organizacji (Wiele podmiotów korporacyjnych może odnosić się do jest to analiza wpływu na działalność biznesową [BIA].)

* Polityki i procedury oparte na informacjach dostarczonych w wyniku ocen ryzyka, które w opłacalny sposób redukują ryzyko bezpieczeństwa informacji do akceptowalnego poziomu i które zapewniają, że bezpieczeństwo informacji będzie uwzględniane w całym cyklu życia każdego systemu informacyjnego organizacji

* Podrzędne plany zapewnienia odpowiedniego bezpieczeństwa informacji dla sieci, obiektów, systemów informatycznych lub grup systemów informatycznych, stosownie do przypadku

* Szkolenie w zakresie świadomości bezpieczeństwa mające na celu informowanie personelu (w tym wykonawców i innych użytkowników systemów informatycznych wspierających działalność i aktywa organizacji) o zagrożeniach bezpieczeństwa informacji związanych z ich działalnością i ich obowiązkami w zakresie przestrzegania zasad i procedur organizacyjnych mających na celu ograniczenie tych zagrożeń ryzyko

*Będą przeprowadzane okresowe testy i ocena skuteczności polityk, procedur, praktyk i kontroli bezpieczeństwa informacji w zakresie bezpieczeństwa, z częstotliwością określoną przez poziom ryzyka, ale nie mniej niż raz w roku

* Proces planowania, wdrażania, oceny i dokumentowania działań zaradczych mających na celu usunięcie wszelkich braków w zasadach, procedurach i praktykach dotyczących bezpieczeństwa informacji organizacji

* Procedury wykrywania, raportowania i reagowania na incydenty bezpieczeństwa

* Plany i procedury zapewniające ciągłość działania systemów informatycznych wspierających działalność i aktywa organizacji

FISMA, wraz z ustawą o ograniczeniu formalności papierowych z 1995 r. i ustawą o reformie zarządzania technologiami informatycznymi z 1996 r. (ustawa Clingera-Cohena), wyraźnie kładzie nacisk na politykę opartą na ryzyku w celu zapewnienia opłacalnego bezpieczeństwa. Wspierając i wzmacniając to ustawodawstwo, Biuro Zarządzania i Budżetu (OMB) poprzez okólnik A-130, załącznik III, Bezpieczeństwo federalnych zautomatyzowanych zasobów informacyjnych12 wymaga, aby agencje wykonawcze w rządzie federalnym:

* Zaplanuj bezpieczeństwo

* Upewnij się, że odpowiednim urzędnikom przypisano odpowiedzialność za bezpieczeństwo

* Okresowo przeglądaj zabezpieczenia w swoich systemach informatycznych

* Autoryzuj przetwarzanie systemu przed operacjami i okresowo po nich

Te wymagania dotyczące zarządzania zakładają, że urzędnicy odpowiedzialnych agencji rozumieją ryzyko i inne czynniki, które mogą niekorzystnie wpłynąć na ich cele. Co więcej, urzędnicy ci muszą rozumieć status swoich programów bezpieczeństwa oraz środki kontroli bezpieczeństwa zaplanowane lub wdrożone w celu ochrony ich informacji i systemów informatycznych, aby móc podejmować świadome oceny i dokonywać inwestycji, które odpowiednio ograniczają ryzyko do akceptowalnego poziomu.

Ostatecznym celem jest prowadzenie codziennej działalności agencji i wypełnianie wyznaczonych jej zadań przy zachowaniu bezpieczeństwa proporcjonalnego do poziomu ryzyka, przy jednoczesnym uwzględnieniu skali szkód, które mogą wyniknąć z nieuprawnionego dostępu, wykorzystania, ujawnienia, zakłócenia , modyfikacji lub zniszczenia informacji. Jako kluczowy element projektu wdrożeniowego FISMA, NIST opracował również zintegrowane ramy ryzyka, które skutecznie łączą wszystkie standardy i wytyczne bezpieczeństwa związane z FISMA, w celu promowania rozwoju kompleksowych i zrównoważonych programów bezpieczeństwa informacji przez agencje

Ustawa o przenośności i odpowiedzialności w ubezpieczeniach zdrowotnych z 1996 r.

Ustawa o przenośności i odpowiedzialności w ubezpieczeniach zdrowotnych (HIPAA)15 42 USC 201 i nast. zawiera szczegółowe przepisy mające wpływ na bezpieczeństwo informacji: Biuro Praw Obywatelskich egzekwuje zasadę prywatności HIPAA, która chroni prywatność informacji zdrowotnych umożliwiających indywidualną identyfikację; zasada bezpieczeństwa HIPAA, która ustanawia krajowe standardy bezpieczeństwa informacji zdrowotnych chronionych w formie elektronicznej; zasada powiadamiania o naruszeniu ustawy HIPAA, która wymaga od podmiotów objętych nią i partnerów biznesowych dostarczania powiadomień w przypadku naruszenia niezabezpieczonych, chronionych informacji zdrowotnych; oraz postanowienia dotyczące poufności zawarte w Zasadach bezpieczeństwa pacjenta, które chronią informacje umożliwiające identyfikację wykorzystywane do analizowania zdarzeń związanych z bezpieczeństwem pacjenta i poprawy bezpieczeństwa pacjenta

Standardy bezpieczeństwa danych w branży kart płatniczych.

Rada ds. Standardów Bezpieczeństwa Branży Kart Płatniczych została utworzona w 2006 roku w wyniku współpracy firm American Express, Discover Financial Services, JCB International, MasterCardWorldwide i Visa Inc. Rada ogłosiła

* Standard bezpieczeństwa danych kart płatniczych (PCI DSS) dla „akceptantów i podmiotów przechowujących, przetwarzających lub przesyłających dane posiadaczy kart”

* Standard bezpieczeństwa danych aplikacji płatniczych (PA-DSS) dla twórców oprogramowania

* Wymagania dotyczące bezpieczeństwa transakcji PIN (PTS) dla producentów sprzętu do odczytu kart.

Podstawowe cele PCI DSS podsumowano w tabeli celów i wymagań organizacji.

Na oficjalnej stronie dostępny jest szeroki zakres dokumentów dostępnych bezpłatnie (wymagana jest prosta rejestracja), w tym (stan na lipiec 2013 r.):

* Często zadawane pytania dotyczące stosowania z ROC [Raport dotyczący zgodności] Instrukcje raportowania dla PCI DSS v2.0

* Słownik v2.0

* Nawigacja po PCI DSS v2.0

* PCI DSS AOC — Sprzedawcy v2.0

* PCI DSS AOC — dostawcy usług v2.0

* Skrócona instrukcja obsługi PCI DSS wersja 2.0

* Podsumowanie zmian PCI DSS Wersja 1.2.1 do 2.0

* Formularz zamówienia skróconego referencji PCI

* Podejście priorytetowe dla PCI DSS wersja 2.0

* Narzędzie do podejścia priorytetowego w wersji 2.0

* Instrukcje raportowania ROC dla PCI DSS v2.0

* Podsumowanie zmian w stosunku do podejścia priorytetowego dla PCI DSS w wersji 1.2 do 2.0

* Podsumowanie opinii PCI DSS i PA-DSS 2012

Konkretne wytyczne można zintegrować ze wzorcami audytów dostosowanymi do wymagań każdej organizacji obsługującej dane kart kredytowych.

Publicznie dostępne publikacje dotyczące bezpieczeństwa.

NIST SP (SP) 800-53 wersja 1 to „Zalecane środki kontroli bezpieczeństwa dla federalnych systemów informatycznych". Celem SP 800-53 jest dostarczenie wytycznych dotyczących wyboru i określenia, jakie powinny być mechanizmy kontroli bezpieczeństwa systemów informatycznych wspierających agencje wykonawcze rządu federalnego. Wytyczne zostały opracowane, aby pomóc w osiągnięciu bezpiecznych wymagań systemowych poprzez:

* Ułatwienie bardziej spójnego, porównywalnego i powtarzalnego podejścia do wyboru i określania kontroli bezpieczeństwa systemów informatycznych

* Przedstawienie rekomendacji dotyczących minimalnych kontroli bezpieczeństwa systemów informatycznych sklasyfikowanych zgodnie z Federalną Normą Przetwarzania Informacji (FIPS) 199,21 Standardy kategoryzacji bezpieczeństwa federalnych systemów informacyjnych i informacyjnych

* Zapewnienie stabilnego, ale elastycznego katalogu kontroli bezpieczeństwa systemów informatycznych w celu zaspokojenia bieżących potrzeb organizacji w zakresie ochrony oraz wymagań przyszłych potrzeb ochrony w oparciu o zmieniające się wymagania i technologie

* Stworzenie podstaw do opracowania metod oceny i procedur określania efektywności kontroli bezpieczeństwa

Wytyczne zawarte w SP 800-53 mają zastosowanie do wszystkich federalnych systemów informacyjnych22 z wyjątkiem systemów określonych jako systemy bezpieczeństwa narodowego zgodnie z definicją zawartą w 44 sekcji 3542 USC.23 Wytyczne zostały szeroko opracowane z technicznego punktu widzenia w celu uzupełnienia podobnych wytycznych dla systemów bezpieczeństwa narodowego . Niniejsza publikacja ma na celu dostarczenie wskazówek agencjom federalnym wdrażającym minimalne wymagania bezpieczeństwa FIPS 200,24 dla systemów informacyjnych i informacyjnych firmy eder. Oprócz agencji rządu federalnego do stosowania niniejszych wytycznych, w stosownych przypadkach, zachęca się także władze stanowe, lokalne, plemienne i organizacje sektora prywatnego tworzące infrastrukturę krytyczną Stanów Zjednoczonych. Mechanizmy bezpieczeństwa w SP 800-53 zostały opracowane przy użyciu danych wejściowych z różnych źródeł, w tym NIST SP 800-26, Polityka Departamentu Obrony (DoD) 8500, dyrektorDyrektywy Central Intelligence (DCID) 6/3, normy ISO/IEC 17799, Głównego Biura Księgowego (GAO), Podręcznika audytu kontroli federalnego systemu informacyjnego (FISCAM) oraz Centrów usług zdrowotnych i społecznych (HHS) Medicare i Medicaid Services (CMS) Podstawowe wymagania bezpieczeństwa. Kontrole bezpieczeństwa obejmują ten temat:

* Kontrola dostępu

* Odpowiedzialność i audyt

* Świadomość i szkolenie

* Certyfikacja, akredytacja i ocena bezpieczeństwa

* Zarządzanie konfiguracją

* Planowanie awaryjne

* Identyfikacja i uwierzytelnianie

* Reagowania na incydenty

* Konserwacja

* Ochrona mediów

* Bezpieczeństwo personelu

* Ochrona fizyczna i środowiska

* Ocena ryzyka

* Planowanie bezpieczeństwa

* Ochrona systemu i komunikacji

* Integralność systemu i informacji

* Usługi systemowe i akwizycja

Ramy ryzyka

Poniższa lista ilustruje przykład tworzenia struktury audytu bezpieczeństwa, która opiera się na szerokiej gamie standardów audytu:

1. Skategoryzuj system informacyjny i informacje znajdujące się w tym systemie na podstawie wpływu. (FIPS 199iii i NIST SP 800-6026)

2. Wybierz początkowy zestaw kontroli bezpieczeństwa systemu informatycznego w oparciu o kategoryzację zabezpieczeń FIPS 199 i zastosuj wytyczne dotyczące dostosowywania, jeśli to konieczne, aby uzyskać punkt wyjścia dla wymaganych kontroli. (FIPS 200 i NIST SP 800-53)

3. Uzupełnij początkowy zestaw dostosowanych kontroli bezpieczeństwa w oparciu o ocenę ryzyka i warunków lokalnych, w tym specyficzne dla organizacji wymagania bezpieczeństwa, informacje o konkretnych zagrożeniach, analizy kosztów i korzyści oraz szczególne okoliczności. (NIST SP 800-53 i SP 800-3027)

4. Udokumentuj uzgodniony zestaw kontroli bezpieczeństwa w planie bezpieczeństwa systemu, w tym uzasadnienie organizacji dotyczące wszelkich udoskonaleń lub dostosowań w początkowym zestawie kontroli. (NIST SP 800-1828)

5. Wdrożyć zabezpieczenia systemu informatycznego

6. Ocenić mechanizmy kontroli bezpieczeństwa, stosując odpowiednie metody i procedury, aby określić stopień, w jakim mechanizmy zabezpieczeń są prawidłowo wdrożone, działają zgodnie z zamierzeniami i dają pożądany wynik w odniesieniu do spełnienia wymagań bezpieczeństwa systemu. (NIST SP 800-53A29)

7. Zezwolić na funkcjonowanie systemu informatycznego w oparciu o określenie ryzyka działalności organizacyjnej, majątku organizacyjnego lub osób fizycznych wynikającego z funkcjonowania systemu informacyjnego i podjęcie decyzji o akceptowalności tego ryzyka. (NIST SP 800-3730)

8. Na bieżąco monitorować i oceniać wybrane zabezpieczenia systemu informatycznego, w tym dokumentować zmiany w systemie, przeprowadzać analizy wpływu zmian na bezpieczeństwo związanych z nimi zmian oraz regularnie raportować stan bezpieczeństwa systemu odpowiednim osobom organizacyjnym.

Leczenie behawioralne

Terapia mająca na celu redukcję SIB zazwyczaj obejmuje wstrzymywanie stosowania wzmocnień po zachowaniu (wygaszanie), dostarczanie wzmocnień po pominięciu zachowania (zróżnicowane wzmocnienie innego zachowania), dostarczanie wzmocnień po właściwym zachowaniu (różnicowe wzmocnienie alternatywnego zachowania), dostarczanie wzmocnień niezależnych od zachowania (niewarunkowe wzmocnienie) lub jakąś kombinację tych podejść. Oprócz tych procedur inne metody leczenia SIB obejmują ogólne budowanie umiejętności poprzez procedury wzmacniania i podpowiedzi oraz kary. Krótki opis każdego podejścia oraz jego potencjalnych zalet i wad opisano poniżej w następujący sposób.

Wprowadzenie do ISO.

ISO32 to pozarządowa spółdzielnia zrzeszająca członków międzynarodowych, którzy współpracują w celu tworzenia, identyfikowania i publikowania standardów branżowych odnoszących się do biznesu i technologii. Członkostwo obejmuje ciała członkowskie, członków korespondentów i członków subskrybentów.

* Organizacja członkowska to grupa reprezentująca standardy przyjęte w danym kraju.

* Członkowie korespondenci reprezentują kraj, który nie ma jeszcze w pełni opracowanych standardów.

* Członkowie abonenci reprezentują kraje o gospodarkach rozwijających się.

Poziom członkostwa określa udział techniczny i polityczny oraz przywileje w zakresie głosowania, ale wszyscy członkowie są jednakowo reprezentowani w międzynarodowej normalizacji i są zachęcani do wnoszenia wkładu. Normy są opracowywane w oparciu o zainteresowanie branży; potrzeby dostawców, rządów i konsumentów; i inicjatywach ISO, jeśli widzi zainteresowanie rynku. Po uznaniu idei normy przez ISO komitety członkowskie rozpoczynają proces definiowania wymagań technicznych niezbędnych dla normy. W skład Komitetu wchodzą eksperci techniczni reprezentujący kraje zainteresowane potencjalnym nowym standardem. Po zdefiniowaniu wymagań technicznych zainteresowani członkowie i kraje pracują nad osiągnięciem porozumienia w sprawie szczegółowych specyfikacji normy. Kiedy ostateczne szczegóły zostaną zatwierdzone przez komisję, projekt międzynarodowej normy zostaje udostępniony do przeglądu. Ostateczne wydanie oficjalnej normy ISO wymaga zgody dwóch trzecich członków, którzy brali udział w procesie rozwoju i 75 procent wszystkich członków głosujących. Normy ustanowione przez ISO nie mają charakteru regulacyjnego; reprezentują wytyczne najlepszych praktyk, które są globalnie spójne dla danej branży lub linii biznesowej. Powszechna akceptacja i wdrażanie norm i wytycznych ISO jeszcze bardziej podnosi ich rangę jako wyróżników w danej branży. Podobnie jak normy ISO 9000 i ISO 14000 uznane na całym świecie za standardy odpowiednio Zarządzania Jakością i Zarządzania Środowiskiem, seria ISO 27000 szybko staje się akceptowana jako miara doskonałości w zarządzaniu bezpieczeństwem informacji.

Seria ISO/IEC 27000

Bezpieczeństwo informacji i sieci stanowiło problem już od początków istnienia robaków i wirusów; jednakże dopiero w ciągu ostatnich 15–20 lat zdefiniowano struktury integrujące bezpieczeństwo z użytkowaniem sieci i zarządzaniem ryzykiem. Wprowadzenie standardu BS7799 i jego akceptacja przez ISO zapewniły administratorom długo potrzebne narzędzia do identyfikacji tych domen i zarządzania nimi. Ponadto regulacje takie jak ustawa Sarbanes-Oxley Act z 2002 r. (SOX), ustawa Gramm-Leach-Bliley Act (GLBA), ustawa o przenośności i odpowiedzialności w ubezpieczeniach zdrowotnych (HIPAA) oraz federalna ustawa o zarządzaniu bezpieczeństwem informacji (FISMA) określiły wymogi dotyczące zgodności, które są łatwiejsze do osiągnięcia dzięki wdrożeniu kompleksowego systemu zarządzania bezpieczeństwem informacji. Brytyjska norma 7799, reprezentująca najlepsze praktyki w zakresie bezpieczeństwa informacji, została po raz pierwszy opublikowana w lutym 1995 r. Ta trzyczęściowa norma obejmuje cele i kontrole bezpieczeństwa, a także metodologię rozwoju niezbędną do stworzenia systemu zarządzania bezpieczeństwem informacji (ISMS).

* BS7799: Część 1, Najlepsze praktyki w zakresie zarządzania bezpieczeństwem informacji

* BS7799: Część 2: Definiuje specyfikacje systemów zarządzania bezpieczeństwem informacji

* BS7799: Część 3, Wytyczne dotyczące zarządzania ryzykiem związanym z bezpieczeństwem informacji

W ostatniej dekadzie brytyjska norma 7799 była podstawą normy ISO 17799, a następnie serii ISO 27000, która w dalszym ciągu ewoluuje jako powszechnie akceptowana norma dotycząca zarządzania bezpieczeństwem informacji i wytycznych dotyczących procedur operacyjnych. Obie agencje (i ich zbiorowi członkowie) zrozumiały potrzebę kompleksowego programu działania , który uwzględniał potrzeby organizacji w zakresie zarządzania ryzykiem i audytu, definiując jednocześnie ramy dla programów i polityk wspierających tę koncepcję. Częściowe lub pełne wdrożenie tych standardów nie tylko przygotowuje organizacje do audytów i ocen ryzyka, ale może również pomóc im spełnić wymagania regulacyjne.

SZBI zdefiniowany w normie BS7799 i udoskonalony w normach ISO 17799 i ISO/IEC 27000 jest środkiem zapewniającym najlepsze środowisko nie tylko dla praktyk bezpieczeństwa, ale także dla obiektywnych audytów i ocen. Interpretacja modelu SZBI przez organizację i przestrzeganie go może być głównym wskaźnikiem klimatu bezpieczeństwa organizacji, a także wsparcia kierownictwa dla polityk i procedur. Programy wspierające funkcje ISMS muszą być promowane i wykorzystywane przez kierownictwo, aby pokazać ich znaczenie pracownikom i zachęcić do uczestnictwa. Audyty zazwyczaj składają się z fazy planowania, faktycznego procesu audytu i raportu końcowego dla komitetu ds. audytu, przedstawiającego szczegóły audytów lub ocen. W grudniu 2000 r. zrewidowano część 1 normy BS7799 (Najlepsze praktyki zarządzania bezpieczeństwem informacji) i opublikowano ją jako ISO 17799.37. Norma ISO 17799 obejmuje 10 dziedzin:

1. Planowanie ciągłości działania

2. Kontrola dostępu do systemu

3. Rozwój i utrzymanie systemu

4. Bezpieczeństwo fizyczne i środowiskowe

5. Zgodność

6. Bezpieczeństwo personelu

7. Organizacja bezpieczeństwa

8. Zarządzanie komputerem i operacjami

9. Klasyfikacja i kontrola aktywów

10. Polityka bezpieczeństwa

W 2005 roku ISO nawiązało współpracę z Międzynarodową Komisją Elektrotechniczną w celu wydania normy ISO/IEC 17799:2005. W tej wersji, zatytułowanej Technologia informacyjna — Techniki bezpieczeństwa — Kodeks postępowania w zakresie zarządzania bezpieczeństwem informacji, dodano cele i mechanizmy kontrolne dotyczące zarządzania bezpieczeństwem informacji, a także zaktualizowano poprzednią wersję, uwzględniając postęp w technologii (mobilnej i bezprzewodowej) oraz w aplikacjach i sposobach korzystania z Internetu . W normach BS7799 i ISO 17799 ustanowiono szeroko stosowane wytyczne dotyczące normy dotyczącej systemów zarządzania bezpieczeństwem informacji, ale ewolucyjna ścieżka opublikowanych norm sprawiła, że stały się one niemal przestarzałe. Zestaw norm ISO/IEC 2700039 nie tylko zawiera wytyczne norm BS7799 i ISO 1779940, ale także zapewnia dokładniejsze wyjaśnienie i zrozumienie każdej dziedziny poprzez podzielenie ich na wyraźnie odrębne standardy. Rodzina ISO/IEC ISMS obejmuje następujące normy międzynarodowe (stan na lipiec 2013 r.):

* ISO/IEC 27000:2009, Systemy zarządzania bezpieczeństwem informacji – przegląd i słownictwo

* ISO/IEC 27001:2005, Systemy zarządzania bezpieczeństwem informacji – Wymagania

* ISO/IEC 27002:2005, Kodeks postępowania w zakresie zarządzania bezpieczeństwem informacji

* ISO/IEC 27003:2010, Wytyczne dotyczące wdrażania systemu zarządzania bezpieczeństwem informacji

* ISO/IEC 27004:2009, Zarządzanie bezpieczeństwem informacji – pomiary

* ISO/IEC 27005:2011, Zarządzanie ryzykiem związanym z bezpieczeństwem informacji

* ISO/IEC 27006:2011, Wymagania dla organów zapewniających audyt i certyfikację systemów zarządzania bezpieczeństwem informacji

* ISO/IEC 27007:2011, Wytyczne dotyczące audytowania systemów zarządzania bezpieczeństwem informacji

* ISO/IEC 27010:2012, Wytyczne dotyczące zarządzania bezpieczeństwem informacji w komunikacji międzysektorowej i międzyorganizacyjnej

* ISO 27799:2008, Informatyka w służbie zdrowia – Zarządzanie bezpieczeństwem informacji w służbie zdrowia z wykorzystaniem ISO/IEC 27002

* ISO/IEC FDIS 27013, Wytyczne dotyczące zintegrowanego wdrażania norm ISO/IEC 27001 i ISO/IEC 20000-1

* ISO/IEC TR 27008:2011, Wytyczne dla audytorów dotyczące kontroli systemów zarządzania bezpieczeństwem informacji

* ISO/IEC TR 27015, Wytyczne dotyczące zarządzania bezpieczeństwem informacji w usługach finansowych

* ISO/IEC WD 27016, Zarządzanie bezpieczeństwem informacji, Ekonomika organizacji

* ITU-T X.1051 | ISO/IEC 27011:2008, Wytyczne dotyczące zarządzania bezpieczeństwem informacji dla organizacji telekomunikacyjnych w oparciu o ISO/IEC 27002

* ITU-T X.1054 | ISO/IEC FDIS 27014, Zarządzanie bezpieczeństwem informacji

Niektóre normy ISO są swobodnie dostępne w formie elektronicznej pod adresem http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html. Można je również nabyć w formie dokumentów elektronicznych lub drukowanych pod adresem http://www.iso.org/iso /home/store.htm ISO/IEC 27001 (Wymagania ISMS) ściśle wzoruje wytyczne Organizacji Współpracy Gospodarczej i Rozwoju (OECD)41 dotyczące bezpieczeństwa systemów i sieci informatycznych i opiera się na zasadzie „planuj – wykonaj – sprawdź – działaj" (cykl PDCA). Cykl PDCA, opracowany przez W. Edwardsa Deminga w latach pięćdziesiątych XX wieku, wymaga od menedżerów postrzegania procesów biznesowych jako znajdujących się w ciągłej pętli sprzężenia zwrotnego. Metoda ta pozwala menedżerom na pełniejsze zaangażowanie się w cały proces kontroli zmian i doskonalenia. Organizacje mogą wdrożyć niektóre lub wszystkie standardy ISO/IEC 27001 lub pójść o krok dalej w swoim programie, ubiegając się o certyfikację ISMS. Certyfikacja zapewnia zarówno audytorom, jak i interesariuszom pewność, że wdrożono kompleksowy program dotyczący bezpieczeństwa informacji i systemów biznesowych. Niezależnie od tego, czy organizacja stara się o uznaną certyfikację ISMS, czy nie, przyjęcie celów i kontroli przedstawionych w normie ISO/IEC 27001 ma kilka zalet. Jak stwierdzono wcześniej, posiadanie kompleksowego programu ISMS może w znacznym stopniu przyczynić się do zapewnienia zgodności w innych obszarach. SZBI z certyfikatem ISO/IEC 27001 zapewni zgodność z całym zakresem przepisów prawnych związanych z bezpieczeństwem informacji, w tym przepisami HIPAA, GLBA i FISMA, a także warunkami pomyślnego raportu Sarbanes-Oxley Sekcja 404. Udokumentowane zasady i programy ISMS, klimat bezpieczeństwa obejmujący zarówno kierownictwo, jak i pracowników, a także przestrzeganie zasad są nie tylko niezbędne, aby system zarządzania bezpieczeństwem informacji był skuteczny, ale zapewnią pomyślny, konstruktywny i skuteczny proces audytu

Standardy audytu bezpieczeństwa AICPA

Firmy i agencje rządowe znajdują się pod ciągłą presją poprawy wydajności i zmniejszenia kosztów operacyjnych. Ponadto inwestorzy i akcjonariusze zachęcają spółki publiczne do poprawy rentowności, przyczyniając się w niewielkim stopniu do outsourcingu IT w pierwszej dekadzie XXI wieku. Amerykańskie Biuro Statystyki Pracy zaczęło uwzględniać „kontrolę kosztów/obniżanie kosztów/zwiększanie rentowności" jako przyczynę masowych zwolnień, począwszy od badań z 2007 r.; odsetek respondentów podających ten wpis jako przyczynę zwolnień utrzymywał się na stabilnym poziomie i wynosił około 3% wszystkich zwolnień rocznych w latach 2007–2011. Outsourcing nie ograniczał się do spółek publicznych; agencje rządowe również zdecydowały się na outsourcing, aby ograniczyć koszty. Z danych Federalnego Biura Zarządzania i Budżetu Stanów Zjednoczonych za rok 2013 wynika, że około jedna trzecia wszystkich uznaniowych wydatków rządu USA została zlecona podmiotom zewnętrznym. W związku z dążeniem większej liczby firm do skupienia się na swoich kluczowych kompetencjach, zleca się na zewnątrz następujące typy funkcji biznesowych:

Obsługa roszczeń

Obsługa klienta i helpdesk

Przetwarzanie danych

Finansowe i księgowe

Zasoby ludzkie i plany świadczeń

Hosting internetowy

Członkowie kadry kierowniczej organizacji rozważających outsourcing muszą rozumieć zarówno korzyści, jak i ryzyko; muszą także ograniczać ryzyko do poziomu akceptowalnego dla ich organizacji. Amerykański Instytut Biegłych Księgowych (AICPA) zdefiniował trzy powszechnie stosowane standardy audytu bezpieczeństwa, omówione w następujących sekcjach:

SAS 70

SSAE 16

ISAE 3402 to międzynarodowa norma, z którą jest zgodny SSAE 16.

Wprowadzenie do audytów SSAE 16

Oświadczenie o standardach audytu nr 70 (SAS 70): Organizacje usługowe zostało pierwotnie opracowane przez Amerykański Instytut Biegłych Księgowych (AICPA) w celu raportowania usług finansowych i było kluczową metodą zapewniającą, że firma rozważająca świadczenie usług outsourcingowych usługi spełniały wymogi bezpieczeństwa. Potrzeba raportowania na temat kontroli bezpieczeństwa występująca w branży audytu bezpieczeństwa doprowadziła do zastąpienia SAS 70 Oświadczeniem w sprawie standardów usług atestacyjnych nr 16 (SSAE 16), Reporting on Controls at a Service Organisation, które zastąpiło wytyczne dla audytorów usług w SAS 70 dla wszystkich takich zobowiązań kończących się 15 czerwca 2011 r. lub później. SSAE 16 został również „opracowany z zamiarem i celem aktualizacji standardu raportowania amerykańskich organizacji usługowych, tak aby odzwierciedlał on nowy standard raportowania międzynarodowych organizacji usługowych i był zgodny z nim – ISAE 3402”. Oprócz tego, że SSAE 16 jest używany do oceny dostawców outsourcingu, można go stosować podczas współpracy z firmami, które mogą mieć dostęp do zasobów IT i danych, zwłaszcza danych osobowych (PII) o klientach. W tej sekcji opisano dwa typy audytów SSAE 16 i ich elementy składowe.

Terminologia związana z audytami SSAE 16:

Organizacja usługowa — firma, która będzie przetwarzać informacje lub transakcje w imieniu organizacji użytkownika

Audytor usług – wyznaczony przez organizację usługową w celu przeprowadzenia audytu SSAE 16 i dostarczenia poświadczenia wyników audytu

Organizacja użytkownika — firma, która zleciła usługi na zewnątrz i jest klientem organizacji usługowej

Audytorzy użytkowników — wewnętrzna lub zewnętrzna grupa audytorów, która świadczy usługi audytu organizacji użytkownika

SOC – kontrole organizacji usługowej; istnieją trzy typy raportów SOC

MSAE 16 definiuje standardy zawodowe stosowane przez biegłego rewidenta usług, który będzie oceniał kontrole wewnętrzne wdrożone przez organizację usługową. Audyt SSAE 16 dostarcza miarodajnych wskazówek, które umożliwiają organizacji usługowej ujawnienie procesów i działań kontrolnych potencjalnym klientom i audytorom zewnętrznym; informacje prezentowane są w standardowym formacie raportowania. Istnieją trzy różne typy (SOC-1, -2 i -3) oraz dwa różne poziomy audytów SSAE 16 (typ I i typ II).

* SOC-1: Kontrole w organizacji usługowej, które są istotne dla kontroli wewnętrznej jednostki korzystającej z organizacji usługowej w zakresie sprawozdawczości finansowej; mogą one obejmować

zarówno kontrolę informatyczną, jak i finansową. Z tego raportu mogą korzystać wszystkie typy organizacji usługowych; centra danych mogą stosować tego typu raporty zamiast SOC-2, jeśli dokonane zostaną przeglądy jednej lub większej liczby kontroli związanych z finansami.

* SOC-2: Raport ściśle ukierunkowany na IT z wcześniej ustalonymi kontrolami i zorganizowanymi w kategorie bezpieczeństwa, dostępności, integralności przetwarzania, poufności i prywatności. Organizacja usługowa może zdecydować się na skupienie audytu na wybranych kategoriach; należy sprawdzić wszystkie kontrole w wybranej kategorii/kategoriach. Zwykle dotyczą one centrów danych, dostawców usług internetowych i ASP.

* SOC-3: Podobnie jak SOC-2, niniejszy raport koncentruje się na usługach i zasadach zaufania; np. audyt zaufania internetowego. Jeżeli organizacja usługowa zdecyduje się na włączenie zasady prywatności do zakresu audytu, uwzględnione zostaną kryteria dotyczące treści informacji o ochronie prywatności. Zwykle obejmuje to informacje na temat gromadzenia informacji, wyborów, jakie mają poszczególne osoby w odniesieniu do swoich danych osobowych, bezpieczeństwa informacji oraz sposobu, w jaki te osoby mogą kontaktować się z organizacją usługową w przypadku zapytań, skarg lub sporów.

Każdy raport zawiera kilka kluczowych sekcji:

* List z opinią od firmy CPA.

* Twierdzenie kierownictwa dotyczące opisu systemu organizacji usługowej i odpowiedniości projektu kontroli; jeżeli raport jest typu II, wówczas stwierdzenie obejmuje także skuteczność działania kontroli w osiąganiu celów kontroli.

* Opis kontroli i środowiska kontroli.

* Wyniki badań kontroli.

* Kluczowe organizacje podrzędne (np. outsourcing IT), których działalność wpływa na kontrole.

Zasadnicza różnica pomiędzy audytem typu I SSAE 16 a audytem typu II polega na tym, że audyt typu I sprawdza skuteczność projektu kontroli i testuje jedną próbną transakcję dla każdej kontroli; to, aby udowodnić, że projekt sterowania działa prawidłowo w co najmniej jednym przypadku. W przypadku audytu typu II testuje się projekt kontroli oraz skuteczność kontroli w okresie audytu. Z powodu tych testów audyty typu II są droższe, ale zapewniają szczegółowy raport oraz zapewniają większą wartość i niezawodność użytkownikom organizacji usługowych. Audyt SSAE 16 rozpoczyna się od przeprowadzenia przez audytora usług wstępnej oceny ryzyka i oceny systemu przetwarzania oraz kontroli przetwarzania systemów transakcyjnych, a także przeglądu zasad i procedur regulujących system i procesy IT. Następnie audytor opracowuje zakres prac (SOW), który zostanie przedstawiony organizacji usługowej, zawierający datę zakończenia, szczegóły audytu, zakres audytu i koszt. Zespół audytowy SSAE 16 będzie zwykle zarządzany przez CPA; CPA musi zapoznać się z raportem z audytu i pracą oraz podpisać opinię. Osoba ta będzie głównym kontaktem z kadrą kierowniczą klienta i będzie poświadczać wyniki audytu. Zespół audytowy wykonujący daną pracę może składać się z jednej osoby lub zespołu od dwóch do czterech audytorów. Kierownik techniczny jest odpowiedzialny za ocenę i testowanie systemów i urządzeń sieciowych. Jeżeli przeprowadzany jest audyt SOC-1, może istnieć od dwóch do pięciu celów kontroli związanych z IT, a w ramach każdego celu kontroli może być testowanych od jednego do piętnastu kontroli. Zazwyczaj testowanie mechanizmów kontrolnych jest bardziej szczegółowe, więc jeśli zawiedzie określony mechanizm kontrolny (np. nie wyłączy natychmiast dostępu zakończonego użytkownika), nie spowoduje to niepowodzenia innych połączonych razem elementów kontrolnych (np. jeśli przydzielanie użytkowników — dodawać,

zmieniać lub usuwać użytkowników — jest wyświetlany jako pojedyncza kontrolka, a nie trzy kontrolki). W przypadku audytu SOC-1 organizacja usługowa jest odpowiedzialna za identyfikację i zatwierdzenie celów kontroli i mechanizmów kontrolnych; audytor usług często dostarcza informacji na temat najlepszych praktyk i kontroli, które zazwyczaj są testowane. W przypadku raportów SOC-2 i SOC-3 kontrole są z góry ustalone, a organizacja usługowa może wybrać, które z kluczowych kategorii mają zostać poddane przeglądowi podczas audytu. Oprócz przeglądu konfiguracji sprzętu i oprogramowania, zazwyczaj uwzględniane są zasady i procedury IT, które podlegają ocenie, przeglądowi i weryfikacji. Na etapie instruktażu zostaną przeprowadzone rozmowy z kadrą kierowniczą, w tym administratorami systemów i sieci, w celu ustalenia sposobu wykonywania określonych zadań; przykładowa pozycja zostanie wówczas przetestowana w celu sprawdzenia, czy projekt kontroli jest skuteczny (tj. czy kontrola działa w przypadku przykładowej transakcji). Na przykład: kto zatwierdza formularz wniosku o utworzenie konta użytkownika i jak formularz przechodzi przez proces zatwierdzania? Administratorzy systemu lub aplikacji zostaną poproszeni o wyjaśnienie, czym się zajmują od momentu otrzymania formularza wniosku o założenie konta do momentu utworzenia konta. Audytor wykorzysta informacje zebrane podczas rozmów w celu ustalenia, czy przestrzegane są zasady i procedury dotyczące konta oraz czy są one odpowiednie dla środowiska klienta. Krótki przegląd tego, co audytor sprawdziłby pod kątem zasad dotyczących żądań użytkowników i sposobu raportowania wyników:

* Zasady prywatności. Wszyscy użytkownicy, którzy potrzebują nowego konta komputerowego lub modyfikacji istniejącego konta w dowolnym systemie w firmie, będą zobowiązani do wypełnienia formularza żądania konta użytkownika UA-09.

* Warunki i procedury. Polityka żądań konta użytkownika „IT-23, 1 listopada 2011 r.”. Wszystkie prośby o założenie nowego konta lub modyfikację istniejącego konta należy składać na formularzu UA-09.

* Procedura testowa. Przeprowadź przykładowy przegląd formularzy żądań użytkowników i przejrzyj formularze pod kątem prawidłowych podpisów autoryzowanych i kompletności. Przeprowadzaj wywiady z upoważnionymi sygnatariuszami pod kątem zgodności z polityką dotyczącą żądań użytkowników; upewnij się, że użytkownikom przydzielane są tylko role zgodne z najmniejszymi uprawnieniami na ich stanowisku pracy.

* Wyniki testu. Zbieraj próbki statystyczne formularzy wniosków użytkowników i przeprowadzaj wywiady z przełożonymi osób składających wnioski, aby ustalić, czy zażądano i zatwierdzono najmniejsze uprawnienia potrzebne do wykonywania ich pracy. Sprawdź formularze pod kątem kompletności i dokładności informacji.

* Analiza wyników testów. Audytor przedstawi zarówno pozytywne, jak i negatywne wyniki testów wraz z komentarzem. Próbka pozytywnych lub negatywnych wyników testu:

* Pozytywny wynik testu. Wszystkie sprawdzone formularze zostały wypełnione zgodnie z Polityką dotyczącą żądań konta użytkownika „IT-23 z dnia 1 listopada 2011 r.”, a wszystkie rozmowy wykazały, że wszystkie zasady i procedury były prawidłowo przestrzegane. Nie stwierdzono żadnych rozbieżności.

* Negatywny wynik testu. Po zapoznaniu się z Formularzem żądania założenia konta użytkownika i rozmowach z przełożonymi i upoważnionymi sygnatariuszami ustalono, że nie zastosowano się do Polityki dotyczącej żądań założenia konta użytkownika „IT-23 z dnia 1 listopada 2011 r.”. Użytkownicy otrzymali uprawnienia wykraczające poza to, co było wymagane do wykonywania ich pracy.

Wyjątki i ustalenia są zgłaszane w końcowym raporcie SSAE 16 przesyłanym do kierownictwa w następujący sposób:

* Jeżeli audytor uzna to za istotne, zgłasza wyjątek wraz z opisem wyjątku.

* Audytor rozważy wszelkie kontrole łagodzące lub reakcje kierownictwa na wyjątek.

* Jeżeli w opinii audytora ustalenie ma wpływ na cele kontroli, wówczas zostanie zgłoszone z zastrzeżeniem i potencjalnym wpływem; w przeciwnym razie zostanie to zgłoszone jako wyjątek.

Wnioski z audytów SSAE 16. Podsumowując, audyt SSAE 16 nie daje 100-procentowej gwarancji pewności, że wszystkie kontrole i procesy związane z bezpieczeństwem zostały poprawnie zaprojektowane i wdrożone; w końcu organizacja usługowa wybiera kontrole, które mają zostać przetestowane w ramach zadania SOC-1. W przypadku zleceń SOC-2 lub SOC-3 uwzględniono cele i kontrole o dużej wartości; jednakże nie obejmują one wszystkich możliwych kontroli. Niemniej jednak audyt SSAE 16 zapewnia wysoki poziom pewności, że ryzyko zostało ocenione i złagodzone.

Wyniki audytu SSAE 16 mogą również dostarczyć informacji na temat obszarów lub dalszych badań. Główną zaletą audytu SSAE 16 jest to, że można go wykorzystać do spełnienia wymagań sprawozdawczych w zakresie raportowania zgodnie z sekcją 404 SOX, pomóc w spełnieniu wymogów GLBA i HIPAA oraz może zapewnić korzyści jako narzędzie marketingowe dotyczące jakości usług.

Normy ISAE 3402

Międzynarodowy standard usług atestacyjnych (ISAE) nr 3402, Raporty atestacyjne dotyczące kontroli w organizacji usługowej to międzynarodowy standard, zgodnie z którym zatwierdzono SSAE 16: [ISAE 3402] został wydany w grudniu 2009 r. przez Międzynarodowe Standardy Audytu i Atestacji Board (IAASB), która jest częścią Międzynarodowej Federacji Księgowych (IFAC). ISAE 3402 został opracowany w celu zapewnienia międzynarodowego standardu pewności umożliwiającego księgowym publicznym wydawanie raportów do wykorzystania przez organizacje użytkowników i ich audytorów (audytorów użytkowników) na temat kontroli w organizacji usługowej, które mogą mieć wpływ na działalność organizacji użytkownika lub być jej częścią system kontroli wewnętrznej nad sprawozdawczością finansową.50 Ernst & Young opisuje ISAE 3402 w broszurze z 2013 roku w następujący sposób: Chociaż wiele firm od lat zleca część swojej pracy outsourcingowi, outsourcing z dnia na dzień staje się coraz bardziej popularny. Jest to szczególnie spowodowane zwiększoną globalizacją, ewolucją technologiczną i potrzebą ujednolicenia procesów biznesowych. Outsourcing to dowolne zadanie, operacja, praca lub proces, który może zostać wykonany przez pracowników w organizacji użytkownika, ale zamiast tego jest zlecany stronie trzeciej (organizacji usługowej) lub innej spółce należącej do grupy na określony czas. Oto kilka przykładów dla sektora finansowego:

* Zarządzający aktywami, którzy świadczą usługi zarządzania aktywami dla różnych stron w ramach spółki należącej do grupy.

* Administratorzy emerytur, którzy wykonują administrację funduszami emerytalnymi.

* Firmy zajmujące się obsługą roszczeń, które świadczą usługi likwidacji szkód dla dużych ubezpieczycieli.

Powszechne stosowanie outsourcingu wymaga od organizacji lepszego zarządzania ryzykiem związanym ze zlecanymi usługami. Mówiąc dokładniej, organizacja użytkowników wymaga pewnego stopnia pewności, że organizacja usługowa posiada ugruntowane ramy kontroli wewnętrznej, które działają skutecznie. Nowe regulacje, organy regulacyjne i rady nadzorcze wymagają także szczególnej kontroli procedur zlecanych na zewnątrz

USTAWA SARBANES-OXLEYA

W tej sekcji skupiono się na praktycznych aspektach zgodności z SOX w świecie rzeczywistym i przedstawiono koncepcje, z którymi praktyk z pewnością się zetknie. Sarbanes-Oxley to ustawa o sprawozdawczości finansowej wprowadzona do prawa Stanów Zjednoczonych w lipcu 2002 r. Była to odpowiedź rządu USA na szereg poważnych błędów w rachunkowości spółek publicznych, w tym Enron i WorldCom. SOX ma na celu ograniczenie oszustw i konfliktów interesów przy jednoczesnym zwiększeniu przejrzystości finansowej i zaufania publicznego do rynku i systemów kontroli wewnętrznej firm. Ustawa ma na celu zachęcanie do uczciwości i uczciwości w sprawozdawczości finansowej oraz przerzucanie odpowiedzialności bezpośrednio na właścicieli, menedżerów i kadrę kierowniczą. Ustawa wymaga, aby członkowie kadry kierowniczej poświadczyli, że „są odpowiedzialni za ustanowienie i utrzymywanie kontroli wewnętrznej" oraz „zaprojektowali takie kontrole wewnętrzne, aby zapewnić, że istotne informacje dotyczące spółki i jej skonsolidowanych spółek zależnych zostaną ujawnione takim członkom kierownictwa przez inne osoby w tych jednostek, w szczególności w okresie, w którym sporządzane są raporty okresowe." SOX dopuszcza możliwość zarówno postępowania cywilnego, jak i karnego. Zatem nieprzestrzeganie przepisów może skutkować karami grzywny, więzienia lub obiema karami w przypadku tych, którzy nie zapewnią dokładności sprawozdawczości finansowej swojej organizacji. Mając na uwadze, że SOXcur ma zastosowanie wyłącznie do spółek notowanych na giełdzie, których kapitalizacja rynkowa (lub dług publiczny) przekracza 75 milionów dolarów, wiele spółek wycofało się z amerykańskich giełd lub powróciło do statusu prywatnego, aby uniknąć ujęcia w ustawie. Co ważniejsze, wiele spółek spoza USA uważa obecnie, że SOX ma zastosowanie, ponieważ one same lub ich spółki zależne są notowane na amerykańskich giełdach. Zgodność jest konieczna dla całej organizacji, a nie tylko dla notowanej na giełdzie spółki zależnej. Tym samym, począwszy od skromnych początków, ustawa ta osiągnęła obecnie penetrację rynku światowego. SOX mógł pierwotnie być czynnikiem zapewniającym przestrzeganie rygorystycznych przepisów; jednakże w ciągu dziesięciu lat od jej uchwalenia „zgodność z normą SOX przestała być jedynie obowiązkiem regulacyjnym. Dziś postrzega się go w kontekście szerszego programu zarządzania, ryzyka i zgodności (GRC), który jest ściśle zintegrowany z procesem podejmowania decyzji strategicznych, dostosowany do celów biznesowych i możliwy dzięki technologii. W najlepszym interesie organizacji leży zaprojektowanie i wdrożenie kompleksowego programu zarządzania, ocena i wdrożenie wewnętrznych procesów i kontroli oraz wyznaczenie celów wykraczających poza samą zgodność z przepisami. Całość działań związanych z zapewnieniem zgodności powinna być powtarzalna, ponieważ zapewnienie zgodności nie jest działaniem jednorazowym; raczej będzie ono powtarzane corocznie przez cały okres istnienia organizacji (lub do czasu istotnej zmiany lub uchylenia prawa).

Sekcja 404

SOX składa się z kilku sekcji; większość wykracza poza zakres tego rozdziału. Z punktu widzenia specjalisty ds. zapewnienia informacji jednakże sekcja 404 jest najważniejsza i najczęściej omawiana. Jest to obszar, który bezpośrednio zajmuje się wpływem technologii informatycznych na sprawozdawczość finansową oraz adekwatność i skuteczność powiązanych kontroli wewnętrznych.

Artykuł 404 brzmi następująco:

SEK. 404. ZARZĄDZANIE <<UWAGA: 15 USC 7262.>> OCENA KONTROLI WEWNĘTRZNEJ.

(a) Wymagane zasady. – Komisja określi zasady wymagające, aby każde sprawozdanie roczne wymagane zgodnie z sekcją 13(a) lub 15(d) ustawy o giełdzie papierów wartościowych z 1934 r. (15 USC 78m lub 78o(d)) zawierało kontrolę wewnętrzną raport, który:

(1) określać odpowiedzialność kierownictwa za ustanowienie i utrzymanie odpowiedniej struktury kontroli wewnętrznej i procedur dotyczących sprawozdawczości finansowej; I

(2) zawierają ocenę, na koniec ostatniego roku obrotowego emitenta, skuteczności struktury kontroli wewnętrznej i procedur emitenta w zakresie sprawozdawczości finansowej.

(b) Ocena kontroli wewnętrznej i sprawozdawczość. – W odniesieniu do oceny kontroli wewnętrznej wymaganej na mocy podsekcji (a), każda zarejestrowana publiczna firma audytorska, która przygotowuje lub wydaje sprawozdanie z badania dla emitenta, poświadcza dokonaną ocenę i składa sprawozdanie na jej temat przez kierownictwo emitenta. Zaświadczenie sporządzone na mocy niniejszego podsekcji powinno zostać sporządzone zgodnie ze standardami dotyczącymi usług atestacyjnych wydanymi lub przyjętymi przez Radę. Żadne takie zaświadczenie nie będzie przedmiotem odrębnego zlecenia.

W związku z powszechnym poleganiem na IT w systemach zarządzania finansami i operacjami, obecnie w przemyśle amerykańskim przyjmuje się, że konieczne są odpowiednie i skuteczne kontrole wewnętrzne, szczególnie w przypadku systemów wspierających istotne procesy biznesowe

Osiągnięcie zgodności

Do zgodności z SOX należy podchodzić poprzez identyfikację kluczowych procesów w organizacji, dokumentowanie sposobu ich wdrażania i kontrolowania oraz definiowanie lub charakteryzowanie metod raportowania ich sukcesu lub niepowodzenia. Ochrona musi obejmować cały cykl życia systemu, a procesy wewnętrzne muszą obejmować projekty, projektowanie, architekturę, rozwój systemu, dostawę i operacje. Audytor będzie szukał jedynie oceny kluczowych procesów, adekwatności powiązanych kontroli oraz tego, czy procesy te były przestrzegane i kontrole zostały wykonane, zgodnie ze stwierdzeniem.

Ramy kontroli

Na szczęście ciężka praca związana z wyborem ram kontroli i oceny została już wykonana. Amerykańska Komisja Papierów Wartościowych i Giełd (SEC) nakazuje stosowanie ram kontroli wewnętrznej zalecanych przez COSO59, a Rada ds. Rachunkowości i Nadzoru Spółek Publicznych (PCAOB)60 popiera wybór SEC opisany szczegółowo w jej standardzie audytu nr 5 „Audyt kontroli wewnętrznej nad Sprawozdawczość wykonywana w powiązaniu z badaniem sprawozdań finansowych.

COSO. Sponsorem projektu COSO „Wewnętrzna kontrola – zintegrowane ramy (2013)" było konsorcjum składające się z:

* Amerykańskie Stowarzyszenie Księgowych (AAA)

* Amerykański Instytut Biegłych Księgowych (AICPA)

* Międzynarodowe Dyrektorzy Finansowi (FEI)

* Instytut Audytorów Wewnętrznych (IIA)

* Instytut Księgowych Zarządzających (IMA)

Streszczenie omawia zmiany w ramach od pierwotnej wersji z 1992 r., w tym:

* Oczekiwania dotyczące nadzoru zarządczego

* Globalizacja rynków i operacji

* Zmiany i większe skomplikowanie biznesu

* Wymagania i złożoność przepisów prawnych, zasad, regulacji i standardów

* Oczekiwania dotyczące kompetencji i odpowiedzialności

* Stosowanie i poleganie na rozwijających się technologiach

* Oczekiwania dotyczące zapobiegania i wykrywania oszustw.

Według COSO „Kontrola wewnętrzna to proces realizowany przez zarząd, kierownictwo i inny personel jednostki, mający na celu zapewnienie wystarczającej pewności co do osiągnięcia celów związanych z działalnością operacyjną, raportowaniem i zgodnością".

Podsumowanie wykonawcze kontynuuje:

Definicja ta odzwierciedla pewne podstawowe pojęcia. Kontrola wewnętrzna to:

* Nastawiony na osiągnięcie celów w jednej lub większej liczbie kategorii – operacje, raportowanie i zgodność

* Proces składający się z bieżących zadań i działań – środek do celu, a nie cel sam w sobie

* Wpływ na nie mają ludzie — nie tylko podręczniki, systemy i formularze zasad i procedur, ale także ludzie i działania, jakie podejmują na każdym poziomie organizacji, aby wpłynąć na kontrolę wewnętrzną

* Możliwość zapewnienia wystarczającej pewności – ale nie całkowitej pewności – kierownictwu wyższego szczebla i radzie dyrektorów jednostki

* Możliwość dostosowania do struktury podmiotu – elastyczność w zastosowaniu dla całego podmiotu lub dla konkretnej spółki zależnej, oddziału, jednostki operacyjnej lub procesu biznesowego.

„Pięć zintegrowanych elementów" kontroli wewnętrznej w ramach COSO można podsumować w następujący sposób:

* Środowisko kontroli: „… [Z]estaw standardów, procesów i struktur, które stanowią podstawę do przeprowadzania kontroli wewnętrznej w całej organizacji.…"

* Ocena ryzyka: Ocena prawdopodobieństwa zidentyfikowanych szkodliwych zdarzeń w kontekście biznesowym organizacji.

* Działania kontrolne: działania „[p]rewencyjne lub detektywistyczne" podejmowane w celu ograniczenia ryzyka przy jednoczesnym osiągnięciu celów korporacyjnych.

* Informacja i komunikacja: Organizacje potrzebują aktualnych, dokładnych danych na temat wszystkich aspektów działalności, w tym monitorowania pod kątem kontroli wewnętrznych. „Komunikacja to ciągły, iteracyjny proces dostarczania, udostępniania i uzyskiwania niezbędnych informacji".

* Działania monitorujące: „Oceny bieżące… dostarczają aktualnych informacji. Odrębne oceny, przeprowadzane okresowo, będą miały różny zakres i częstotliwość w zależności od oceny ryzyka, skuteczności bieżących ocen i innych względów zarządczych. Wyniki ocenia się na podstawie ustalonych kryteriów

przez organy regulacyjne, uznane organy ustanawiające standardy lub kierownictwo i radę dyrektorów, a braki są komunikowane kierownictwu i radzie dyrektorów, w stosownych przypadkach."

COBIT. ISACA pierwotnie nosił nazwę Audyt systemów informatycznych i stowarzyszenie Kontroli; ISACA zdefiniowała praktyczne ramy, na podstawie których można wyprowadzić kluczowe procesy i kontrole działań związanych ze zgodnością z SOX, wykorzystując ramy COBIT (Cele kontroli w zakresie informacji i technologii pokrewnych). ISACA opisuje zasady leżące u podstaw ram w następujący sposób:

COBIT 5 opiera się na pięciu kluczowych zasadach zarządzania i zarządzania IT w przedsiębiorstwie:

* Zasada 1: Spełnianie potrzeb interesariuszy

* Zasada 2: Kompleksowa obsługa przedsiębiorstwa

* Zasada 3: Stosowanie jednolitych, zintegrowanych ram

* Zasada 4: Umożliwianie podejścia holistycznego

* Zasada 5: Oddzielenie zarządzania od zarządzania

ISACA opisuje zalety COBIT 5 w następujący sposób:

COBIT 5 pomaga przedsiębiorstwom każdej wielkości:

* Utrzymywanie wysokiej jakości informacji w celu wspierania decyzji biznesowych

* Osiągaj cele strategiczne i realizuj korzyści biznesowe poprzez efektywne i innowacyjne wykorzystanie IT

* Osiągnij doskonałość operacyjną poprzez niezawodne i wydajne zastosowanie technologii

*Utrzymuj ryzyko związane z IT na akceptowalnym poziomie

* Optymalizacja kosztów usług i technologii IT

* Wspieranie zgodności z odpowiednimi przepisami prawa, regulacjami, umowami i politykami

Ramy COBIT 5 opisują siedem kategorii czynników umożliwiających:

1. Zasady, polityki i ramy są narzędziem umożliwiającym przełożenie pożądanego zachowania na praktyczne wskazówki dotyczące codziennego zarządzania.

2. Procesy opisują zorganizowany zestaw praktyk i działań mających na celu osiągnięcie określonych celów i wytwarzają zestaw wyników wspierających osiągnięcie ogólnych celów związanych z IT.

3. Struktury organizacyjne są kluczowymi podmiotami decyzyjnymi w przedsiębiorstwie.

4. Kultura, etyka i zachowanie jednostek i przedsiębiorstwa są bardzo często niedoceniane jako czynniki sukcesu w zarządzaniu i działaniach zarządczych.

5. Informacje są potrzebne, aby organizacja działała i była dobrze zarządzana, ale na poziomie operacyjnym informacja jest często kluczowym produktem samego przedsiębiorstwa.

6. Usługi, infrastruktura i aplikacje obejmują infrastrukturę, technologię i aplikacje, które zapewniają przedsiębiorstwu przetwarzanie i usługi w zakresie technologii informatycznych.

7. Do pomyślnego zakończenia wszystkich działań oraz do podejmowania właściwych decyzji i podejmowania działań naprawczych potrzebne są ludzie, umiejętności i kompetencje.

COBIT to kompleksowy framework do zarządzania zarządzaniem ryzykiem i kontrolą IT, obejmujący cztery domeny, 34 procesy IT i 215 celów kontrolnych. Chociaż ma szerszy cel niż tylko zajęcie się zgodnością z SOX, COBIT eliminuje wiele domysłów, sugerując 12 z 34 dostępnych standardowych procesów do włączenia do wdrożenia SOX:

1. Zakup i konserwacja oprogramowania aplikacyjnego. (AI2) Dostarczanie aplikacji biznesowych, zarówno niestandardowych, jak i gotowych, powinno być zgodne z wymaganiami biznesowymi.

2. Pozyskaj i utrzymaj infrastrukturę technologiczną. (AI3) Infrastruktura technologiczna powinna stanowić podstawę świadczenia usług wymaganych przez biznes i być zgodna ze standardami organizacyjnymi.

3. Włącz operacje. (AI4) Wspieranie efektywnego wykorzystania technologii poprzez transfer wiedzy, uzgodniony poziom usług i odpowiednio zintegrowane rozwiązania

4. Zainstaluj i akredytuj rozwiązania i zmiany. (AI7) Przed dostawą należy upewnić się, że dostarczone systemy odpowiadają zamierzonemu celowi i że po instalacji działają zgodnie z oczekiwaniami.

5. Zarządzaj zmianami. (AI6) Zapewnij skuteczny, formalny system zarządzania zmianami w celu ograniczenia błędów i defektów, które mogą mieć wpływ na pomyślne operacje i procesy biznesowe.

6. Definiuj i zarządzaj poziomami usług. (DS1) Dostosuj kluczowe procesy biznesowe do dostarczania technologii w zestawie znaczących dokumentów definiujących usługi, z mechanizmem raportowania interesariuszom na temat wydajności i osiągnięcia poziomów usług.

7. Zarządzaj usługami stron trzecich. (DS2) Zapewnienie świadczenia niezbędnych usług stron trzecich w celu wspierania działalności biznesowej, zachowując jednocześnie przejrzystość w odniesieniu do kosztów, korzyści i ryzyka.

8. Zapewnij bezpieczeństwo systemów. (DS5) Maksymalizuj integralność i dostępność systemów oraz poufność przechowywanych w nich danych, minimalizując jednocześnie wpływ luk w zabezpieczeniach poprzez stosowanie skutecznych polityk, standardów i procedur bezpieczeństwa.

9. Zarządzaj konfiguracją. (DS9) Utrzymuj dokładne i łatwo dostępne repozytorium informacji o konfiguracji aplikacji i systemu, podstawowych standardach i ich odmianach.

10. Zarządzaj problemami i incydentami. (DS8, DS10) Zapewnia formalne zarządzanie problemami i incydentami dla wszystkich operacji, w tym identyfikację problemów, analizę pierwotnych przyczyn i kompleksowe rozwiązywanie problemów.

11. Zarządzaj danymi. (DS11) Zapewnij wypróbowane i przetestowane systemy tworzenia kopii zapasowych, odzyskiwania i usuwania danych.

12. Zarządzaj środowiskiem fizycznym i operacjami. (DS12) Kontroluj dostęp do obiektów i zasobów obliczeniowych, aby zmniejszyć prawdopodobieństwo zakłóceń w działalności w wyniku wycieku danych lub kradzieży aktywów.

Specyficzna analiza może wymagać dodania dalszych procesów, a w ramach każdego procesu dodania lub usunięcia określonych kontroli w celu dalszego dostosowania ram dla każdej organizacji. Wybór procesów i kontroli musi zostać uzgodniony we współpracy z funkcją audytu wewnętrznego i audytorami zewnętrznymi przed przyjęciem konkretnych ram.

Testowanie

Równie ważne dla wyboru procesu i sterowania jest uzgodnienie planu i harmonogramu testów, w szczególności liczby testów i powiązanej wielkości próbek. W przypadku większości organizacji zasoby nie są nieograniczone. Jest prawdopodobne, że oprócz normalnego obciążenia pracą pracownicy zostaną poproszeni o przejęcie odpowiedzialności za pewną część działań SOX. Zatem osiągnięcie równowagi pomiędzy zgodnością a liczbą kontroli związanych z każdym procesem ma kluczowe znaczenie, ponieważ testowane będą kontrole przez cały rok, a wyniki testów wspierają proces certyfikacji SOX. Zmniejszenie liczby testów lub wielkości próbek może bezpośrednio wpłynąć na rzetelność i jakość wyników oraz pozytywnie wpłynąć na wydajność i produktywność personelu. Chociaż testowanie będzie prawdopodobnie postrzegane jako uciążliwe, większość działań kontrolnych należy traktować jak zwykle, a zatem codzienne procesy powinny dostarczyć większości dowodów wymaganych do testowania. Ta sekcja koncentruje się na znaczeniu i wpływie IT na szerszy cel, jakim jest zgodność z SOX, ale nie wszystkie procesy, nawet w organizacji IT, mają charakter techniczny. Wiele z nich to spotkania na poziomie dyrektorów, tablice incydentów, fora naprawcze, spotkania dotyczące ryzyka projektu itd., a wszystkie mogą stanowić część procesu objętego SOX i dlatego należy je przetestować. Testowanie zazwyczaj można podzielić na dwie kategorie: badanie i dyskusję. Badanie wymaga, aby reprezentatywna próbka dowodów wskazująca, że kontrola działa prawidłowo, została zebrana i zweryfikowana jako dokładna. Dyskusja wymaga potwierdzenia zrozumienia procesu i związanych z nim kontroli w drodze spotkań indywidualnych lub grupowych pomiędzy odpowiedzialnymi pracownikami. Wielkość próbek będzie zależeć od populacji testowej i częstotliwości pobierania próbek, a także prawdopodobnie od znaczenia pożądanego stopnia dokładności i precyzji wyników dla poziomów ufności statystycznej.

Audyt i certyfikacja

Będą działać co najmniej dwa niezależne procesy audytu: wewnętrzny i zewnętrzny. Audyt wewnętrzny odbędzie się po zakończeniu testowania SOX jako ostateczny punkt kontrolny zapewniający jakość, czy organizacja spełnia wymagania. Wszelkie zidentyfikowane luki w muszą zostać naprawione lub oficjalnie potwierdzone w ramach formalnego procesu ryzyka przed przybyciem audytorów zewnętrznych.

Audyt zewnętrzny

Audyt zewnętrzny odbędzie się pod koniec roku i będzie ostatecznym sprawdzianem zgodności. Niedopuszczalne jest czekanie z podjęciem działań naprawczych do czasu, aż funkcja audytu zewnętrznego zidentyfikuje lukę. Wszelkie obszary niezgodności na tym etapie zostaną oficjalnie zgłoszone i mogą zostać uwzględnione w ostatecznym piśmie do kierownictwa.

Harmonogram

Wymagania dotyczące certyfikacji różnią się w zależności od organizacji, chociaż oczywiście wymagany będzie co najmniej roczny certyfikat. Wiele organizacji certyfikuje

kwartalnie lub co miesiąc w ramach innego procesu związanego z SOX lub kontroli i wykorzystuje te certyfikaty do uzupełnienia swojej końcowej deklaracji rocznej (patrz Załącznik 54.4).

Wniosek Sarbanesa-Oxleya

Działania związane ze zgodnością z SOX nie powinny być odosobnione w organizacji. Należy je uważać za część szerszego programu zarządzania ryzykiem, najlepiej takiego, który jest wspierany przez wbudowaną, proaktywną i świadomą ryzyka kulturę kontroli. Co więcej, nigdy nie zaleca się wdrażania

programu zgodności, którego celem jest po prostu spełnienie wymogów regulacyjnych. W rzeczywistości program, który od początku został zaprojektowany tak, aby wykraczał poza obecne przepisy i umożliwiał dostosowanie się do zmian w istniejących lub całkowicie nowych przepisach, stanowi znacznie mądrzejszą inwestycję czasu i wysiłku.

RAMY TECHNICZNE AUDYTÓW IT.

Najlepsi audytorzy IT zmagają się z rzeczywistością akceptowalnego ryzyka i niejasnymi kontrolami, szukając solidnych ram, które pomogą im w audycie. Dobre badania i dobre ramy mogą pomóc w ustaleniu pytań do wielu wyjątkowych lub nowych audytów, z którymi nie spotykano się w przeszłości. Trzy przydatne modele, omówione poniżej, można zastosować z perspektywy wysokiego szczebla, aby upewnić się, że uwzględniono wszystkie istotne kwestie. Oprócz modeli ogólne najlepsze praktyki pomagają uzupełnić podstawy techniczne, aby mieć pewność, że audyt wykryje wszelkie istotne niedociągnięcia w kluczowych mechanizmach kontrolnych.

Ramy 1: Ludzie, procesy, narzędzia i środki.

Pierwsza użyteczna struktura — Ludzie, Procesy, Narzędzia i Miary (PPTM) — jest prosta koncepcyjnie, ale jej szeroki zakres pozwala szybko poznać często pomijane krytyczne procesy i ważne kontrole. Weź losowo wybraną aplikację, o której nic nie wiadomo, i zastosuj w niej koncepcje PPTM, aby ją zrozumieć i opracować szereg kontroli do przetestowania oraz przydatnych informacji do zebrania.

1. Ludzie tworzą aplikację, wprowadzają do niej dane i wykorzystują dane wyjściowe lub miejsce przechowywania danych obsługiwanych przez aplikację. Ludzie to komponent, który dotyka aplikacji lub z niej korzysta, dlatego powinien mieć elementy sterujące regulujące interakcję. Na przykład, w jaki sposób osoby są uwierzytelniane lub autoryzowane jako administratorzy lub użytkownicy aplikacji?

2. Procesy otaczają działanie aplikacji. Jakie procesy regulują standardowe praktyki operacyjne i jak można je zweryfikować?

3. Narzędzia to fizyczne kontrole, takie jak inne aplikacje, które mogą łączyć się z aplikacją lub zapewniać jakość lub walidację aplikacji. Inne rodzaje kontroli narzędzi obejmują sprawdzanie platformy, z której korzysta aplikacja. Jakie fizyczne kontrole istniały podczas wdrożenia lub są obecnie stosowane, aby upewnić się, że aplikacja znajduje się w bezpiecznym środowisku?

4. Miary są często pomijanymi wskaźnikami, chociaż reprezentują jedne z najbardziej przydatnych danych w dokładnych audytach. Mogą zweryfikować, czy aplikacja spełnia swoją funkcję wspierając przypisaną jej rolę biznesową. Metryki mogą na przykład raportować wydajność operacyjną aplikacji i stopień jej skalowania w celu zaspokojenia potrzeb klienta w miarę upływu czasu.

Ramy 2: KROK. STRIDE, akronim oparty na uporządkowanej liście zagadnień pokazanej poniżej, obejmuje sześć obszarów ryzyka wspólnych dla różnych technologii. Podobnie jak PPTM, STRIDE pomoże zrozumieć, w jaki sposób obszar ryzyka może odgrywać rolę w technologii podlegającej audytowi, a następnie znaleźć mechanizmy kontrolne łagodzące to ryzyko. Twórcy projektu Open Web Application Security Project (OWASP, www.owasp.com) stanowią doskonały przykład zastosowania STRIDE w aplikacjach internetowych.

1. S — Spoofing opisuje ryzyko, że każdy użytkownik przyjmie tożsamość innego użytkownika lub zamaskuje bezpośrednio lub pośrednio atrybuty innego użytkownika. Na przykład użytkownik logujący się do serwisu bankowego zasadniczo nie powinien mieć możliwości przyjęcia tożsamości innego użytkownika.

2. T – Manipulowanie danymi opisuje potrzebę walidacji danych wejściowych, walidacji procesu i walidacji wyników. Należy stale chronić integralność danych, a w niektórych przypadkach chronić je przed manipulacją, szyfrowaniem lub niezależną weryfikacją.

3. R – Odrzucenie opisuje scenariusz, w którym użytkownik może zasugerować, że transakcja nigdy nie miała miejsca. Do tej sytuacji prowadzą złe ścieżki audytu. Niezaprzeczalność to kontrola chroniąca przed odrzuceniem. Obejmuje podpisanie wiadomości datą i godziną jako niepowtarzalnym, nie powtarzalnym momentem.

4. I — Ujawnianie informacji opisuje dodatkowe mechanizmy kontrolne zapobiegające przedostawaniu się informacji z systemu do nieupoważnionych stron lub programów.

5. D — Odmowa usługi opisuje stan, w którym aplikacja lub technologia może zostać złośliwie lub przypadkowo usunięta z usługi. Jeśli stanowi to problem, należy wdrożyć mechanizmy kontrolne, takie jak systemy nadmiarowe, kopie zapasowe i środki zapobiegające zdarzeniom typu „odmowa usługi".

6. E — Podniesienie uprawnień opisuje sytuację, w której użytkownik złośliwie lub przypadkowo uzyskuje uprawnienia administracyjne.

Ramy 3: PDIO. PDIO — Planuj, projektuj, wdrażaj i eksploatuj — czerpie z procesów zarządzania projektami Cisco System i opisuje cykl życia technologii. Struktura ta może być bardzo wydajna, szczególnie w połączeniu z PPTM. Administratorzy zajmują się ludźmi, procesami, narzędziami i środkami na każdym etapie planowania, projektowania, wdrażania i operacji projektu. Na PDIO można spojrzeć z makroperspektywy, aby zrozumieć cały nowy projekt, lub z mikroperspektywy, aby zrozumieć każdy mniejszy element. Szerokie zrozumienie audytu jest oznaką doskonałego wyniku, który dostarcza klientom niezwykle cennych i przydatnych informacji, dzięki czemu mogą wzmocnić swoje kontrole.

Ogólne najlepsze praktyki.

Ta krótka lista typowych najlepszych praktyk powinna pomóc w dodatkowych kontrolach podczas testowania. Jest to szczególnie pomocne podczas audytu nowej technologii, która nie posiada jeszcze odpowiedniego programu audytu.

1. Zastosuj głęboką obronę, aby mieć wielowarstwową kontrolę.

2. Stosuj pozytywny model bezpieczeństwa. Domyślnie odmawiaj działań i zezwalaj tylko na zaufany lub łagodny podzbiór dostępnych opcji. Negatywne modele bezpieczeństwa domyślnie ufają wszystkiemu i próbują odkryć, kiedy zablokować niewłaściwe zachowanie.

3. Bezpieczne awarie, aby ludzie, sprzęt, dane i procesy biznesowe były bezpieczne.

4. Uruchom z najniższymi uprawnieniami, aby uniemożliwić użytkownikom zwiększanie ich uprawnień powyżej poziomu niezbędnego do wykonywania ich pracy.

5. Unikaj bezpieczeństwa poprzez zaciemnienie. Spróbuj ukryć dane lub opcje. Bezpieczeństwo przez zaciemnienie to technologia umożliwiająca kompromis.

6. Zadbaj o proste bezpieczeństwo. Zbyt złożone systemy są trudne w administrowaniu i często nie są zabezpieczone.

7. Wykrywaj włamania i prowadź dzienniki. Powinna istnieć ścieżka audytu dla wszystkiego, co ważne.

8. Nigdy nie ufaj infrastrukturze i usługom, szczególnie tym pochodzącym z rozwiązania zarządzanego przez stronę trzecią, w przypadku których mogą obowiązywać inne zasady i praktyki bezpieczeństwa niż organizacja, która je stworzyła.

9. Ustal bezpieczne ustawienia domyślne. Domyślne bezpieczne wartości i działania zamiast domyślnych mniej bezpiecznych wartości i działań. Innym częstym błędem jest nieokreślenie ważnej wartości, co powoduje późniejsze problemy z technologią lub aplikacją.

10. Stosuj otwarte standardy, bo są one dokładniej testowane niż technologie autorskie. Szyfrowanie w zarządzaniu prawami cyfrowymi jest przykładem złamania kilku rzekomo bezpiecznych prywatnych szyfrów lub systemów kryptograficznych.

Wnioski dotyczące ram technicznych

Ramy mogą być cennym atutem podczas zbliżania się do audytu technicznego, umożliwiając szybkie określenie obszarów, w których audyt będzie najbardziej wymagający i gdzie zgodność może być najskuteczniejsza.