AUDYT INFORMATYCZNY W JEDNOSTKACH SEKTORA FINANSÓW PUBLICZNYCH

Małgorzata PAŃKOWSKA

Streszczenie: W pracy przedstawiono uwarunkowania organizacyjno-prawne audytu wewnętrznego, ze zwróceniem szczególnej uwagi na audyt informatyczny. Wyeksponowano nowe zagrożenia w cyberprzestrzeni, których identyfikacja, kontrola, eliminowanie i prewencja mogą stanowić nowe wyzwania dla audytorów informatyki w jednostkach sektora finansów publicznych.

Słowa kluczowe: audyt wewnętrzny, audyt informatyczny, standardy audytu, zagrożenia biznesu elektronicznego, rozszerzone przedsiębiorstwo.

1. Uwarunkowania prawne rozwoju audytu w jednostkach sektora finansów publicznych

Zarządzanie aktywami instytucji społeczno-gospodarczej obejmuje procesy planowania i monitorowania zasobów materialnych i informacyjnych w trakcie ich eksploatacji. Efektywne wdrożenie zasad zarządzania aktywami pozwala uwzględnić obniżkę kosztów ogólnych i klarowne podstawy księgowości, oraz ustalić odpowiedzialność za zasoby. Prowadzi do redukcji popytu na nowe zasoby przez odpowiednie przystosowanie zasobów istniejących i maksymalizację potencjału usługowego istniejących zasobów. Procesy zarządzania zasobami materialnymi i informacyjnymi w organizacjach społeczno-gospodarczych wspomaga audyt wewnętrzny rozumiany jako niezależna i obiektywna ocena sposobu zarządzania i kontrolowania organizacji. Działania zarządcze zorientowane są głównie na ochronę majątku oraz wydajne i oszczędne korzystanie z zasobów organizacji. Audyt traktowany jest jako nowoczesny instrument zarządzania, wspomagających osiąganie celów organizacji, identyfikujący i oceniający ryzyko działalności, wykorzystywany dla tworzenia wartości dodanej i usprawnienia działalności.

Termin audyt pochodzi z łacińskiego słowa *słuchanie.* Audyt pojawił się ponad 2000 lat temu, najpierw w Egipcie, a następnie w Grecji, Rzymie i innych krajach, gdzie obywatele (a także niewolnicy), którym powierzono gromadzenie i dystrybucję funduszy publicznych byli proszeni o publiczne zaprezentowanie, przed odpowiednim urzędnikiem (audytorem) ustnego oświadczenia o wykorzystaniu tych funduszy [1]. Przyjmując jako kryterium klasyfikacji beneficjentów audytu można wyróżnić audyty zewnętrzne i wewnętrzne. Audyt zewnętrzny jest prowadzony przez ekspertów, organizację zewnętrzną wobec instytucji audytowanej. W przeciwieństwie do tego, audyty wewnętrzne wykonywane są przez jednostki wewnętrzne danej instytucji, zwykle są to powołani przez zarząd pracownicy. Audyt wewnętrzny prowadzony jest w zgodności z wymaganiami zarządu, który aprobuje plan audytów i dla którego generowane są raporty. W obu przypadkach audyt jest systematycznym badaniem i oceną dowodów, które są przedsiębrane dla zapewnienia, czy jednostki organizacji społeczno-gospodarczej dostatecznie dobrze prezentują podstawowe fakty i spełniają ustalone kryteria.

W Polsce audyt wewnętrzny został wprowadzony w 1998 r. ustawą o finansach

publicznych, stosownie do zaleceń Unii Europejskiej oraz rozporządzeń i komunikatów Ministra Finansów. Obecnie audyt wewnętrzny regulowany jest przepisami:

- ustawa z 30 VI 2005 o finansach publicznych (Dz.U. 2005 r, nr 249 poz. 2104 z późn.zm.),
- rozporządzenie Ministra Finansów z 24 VI 2006 r. w sprawie szczegółowego sposobu i trybu przeprowadzania audytu wewnętrznego (Dz.U. nr 112 poz. 765),
- rozporządzenie Ministra Finansów z 24 VI 2006 w sprawie trybu sporządzania oraz wzoru sprawozdania z wykonania planu audytu wewnętrznego (Dz.U. nr 112 poz. 764),
- komunikat nr 11 Ministra Finansów z 26 VI 2006 r. w sprawie ogłoszenia standardów audytu wewnętrznego w jednostkach sektora finansów publicznych (Dz.Urz.Min. Fin. Nr 7 poz. 56),
- komunikat nr 16/2006 Ministra Finansów z dnia 18 VII 2006 w sprawie ogłoszenia „Kodeksu etyki audytora wewnętrznego w jednostkach sektora finansów publicznych" i „Karty audytu wewnętrznego w jednostkach sektora finansów publicznych" (Dz. Urz.Min. Fin nr 9 poz. 70).

Zgodnie z ustawą o finansach publicznych jednostki zobowiązane do wdrożenia audytu wewnętrznego to jednostki obsługujące najwyższe organy państwa, centralne jednostki administracji centralnej, urzędy wojewódzkie, urzędy skarbowe i celne, jednostki organizacyjne służby więziennej i prokuratury, fundusze celowe, ZUS i KRUS, NFZ, osoby prawne państwa, jednostki o znacznych przychodach i wydatkach. Do przeprowadzenia audytu wewnętrznego są zobowiązane tylko te jednostki samorządu terytorialnego, których przychody lub wydatki przekroczyły w poprzednim roku 40 mln złotych [2].

W literaturze z zakresu audytu wewnętrznego pojawiają się odwołania do standardów ISO: 9000, 9001, 9002, 9003, 9004, oraz ISO 10011 – wytyczne do przeprowadzania audytu systemu jakości. Dla ujednolicenia prac audytu Institute of Internal Audit (IIA) opracował standardy profesjonalnej praktyki audytu wewnętrznego, wśród których wyróżnia się:

- standardy atrybutów, określające cechy organizacji i osób przeprowadzających audyt,
- standardy działania, opisujące rodzaje czynności w ramach audytu wewnętrznego oraz określające kryteria jakościowe oceny,
- standardy wdrożenia, odnoszące się do określonych rodzajów zadań audytowych (na przykład audyt zgodności z prawem) [2].

W Polsce problematyką audytu wewnętrznego zajmują się: Polski Instytut Kontroli Wewnętrznej (PIKW) w Warszawie, który powstał w 1999 r. z inicjatywy Brytyjskiego Funduszu Know-How oraz Oddział Międzynarodowego Stowarzyszenia Audytu Wewnętrznego w Polsce (IIA).

Kontrola finansowa i audyt wewnętrzny stanowią elementy systemu kontroli wewnętrznej administracji publicznej realizowanej wewnątrz jej struktur. Użycie w ustawie z 1998 r, terminu audyt wewnętrzny miało na celu rozróżnienie od kontroli finansowej, która dotyczy procesów związanych z gromadzeniem i rozdysponowaniem środków publicznych oraz gospodarowaniem mieniem. 5 lipca 2002 r. definicję audytu rozszerzono w rozporządzeniu Ministra Finansów w sprawie szczegółowego sposobu i trybu przeprowadzania audytu wewnętrznego przez określenie zakresu działania audytora wewnętrznego. Artykuł 48 ust 1 ustawy z 2005 r. o finansach publicznych wprowadza

zmodyfikowaną definicję audytu wewnętrznego. Tamże audyt jest określany jako ogół działań obejmujących niezależne badanie systemów zarządzania i kontroli w jednostce, w tym procedur kontroli finansowej, w wyniku której kierownik jednostki uzyskuje obiektywną i niezależną ocenę adekwatności, efektywności i skuteczności tych systemów.

Audyt wewnętrzny nie może być utożsamiany z kontrolą wewnętrzną. Kontrola wewnętrzna bada stan faktyczny w porównaniu z założeniami, planami i wzorcami. Działania kontrolne mają charakter rozliczeniowy, a ich celem jest odkrycie i opisanie nieprawidłowości. Audyt wewnętrzny różni się od kontroli wewnętrznej metodami działania, zakresem niezależności, pełnionymi zadaniami, usytuowaniem organizacyjnym, formą działania, stosowanymi kryteriami oceny oraz efektami prac. Audyt wewnętrzny przyczynia się do usprawnienia kontroli, ocenia jej sprawność, ale służy wykazaniu słabych stron organizacji, identyfikacji ryzyka, oferowania sposobów działania i prezentacji kierunków kształtowania przyszłości. Pożądane jest, aby audyt wewnętrzny umożliwiał:

- rozszerzenie wiedzy fachowej i specjalistycznej, na przykład określonej w ustawie Sarbanes-Oxley (Sarbanes-Oxley Act, SOX),
- zdobycie umiejętności przewidywania przyszłych zdarzeń,
- określenie celów strategicznych przedsiębiorstwa i skoncentrowanie uwagi na obszarach krytycznych,
- jasne sformułownaie stanowisk w najbardziej wrażliwych obszarach.

Celem wprowadzenia SOX w 2002 r. było przywrócenie zaufania inwestorów w USA przez zaostrzenie wymogów wobec uczestników rynku finansowego w zakresie efektywności kontroli wewnętrznej [3]. Ustawa SOX wprowadziła organ regulujący obszar audytu – Public Company Accounting Oversight Board (PCAOB), którego zadaniem jest między innymi generowanie standardów księgowych i audytorskich. W wyniku rozmów Komisji Europejskiej i PCAOB ustalono, że europejskie firmy audytorskie obsługujące przedsiębiorstwa notowane w USA będą podlegać wspólnej rejestracji zarówno w USA jak i w kraju pochodzenia, a Komisja Europejska będzie musiała zmodyfikować ustawodawstwo tak, aby było zgodne z ustawą Sarbanes-Oxley. W paragrafie 404 SOX określony został wymóg weryfikacji przez audytora zewnętrznego przyjętych przez przedsiębiorstwo rozwiązań w zakresie kontroli wewnętrznej i oceny efektywności kontroli dokonanej przez zarząd. Zgodnie z przyjętymi ustaleniami SOX zatwierdzony biznesowy dokument elektroniczny np. umowa po podpisaniu staje się rekordem [2]. Należy zatem zapewnić dostęp do aktualnej wersji dokumentu wszystkim uczestnikom procesu jego tworzenia. Należy też zagwarantować kontrole nad wersjami starszymi oraz zarządzanie prawami dostępu. Zachodzi konieczność zapewnienia integralności i nadzoru nad jego dysponowaniem. W odróżnieniu od zarządzania dokumentami, zarządzanie rekordami jest zbiorem ściśle zdefiniowanych reguł. Muszą być dobrze określone jednolite zasady kategoryzacji rekordów, budowy struktury katalogów do ich przechowywania. Niezbędne jest zdefiniowanie grupy użytkowników i nadanie im uprawnień do korzystania z rekordów oraz zasady dysponowania nimi. Wymagane są okresowe przeglądy zbiorów rekordów. SOX zobowiązuje korporacje notowane na giełdach w USA do traktowania dokumentów finansowych i poczty elektronicznej dotyczącej zagadnień finansowych i audytorskich jako rekordy, przechowywane bezpiecznie przez 7 lat. Wytyczne dotyczące zarządzania rekordami znalazły swój zapis w międzynarodowej normie ISO 15489 oraz w wytycznych Model of Requirements for Records Management przygotowanych przez Komisję Europejską. Szczegółowe regulacje są opracowywane przez poszczególne kraje europejskie.

2. Audyt informatyczny

W polskiej literaturze przedmiotu wyróżnia się najczęściej trzy rodzaje audytu wewnętrznego:

- audyt finansowy,
- audyt operacyjny,
- audyt informatyczny [2, 4, 5, 6, 7].

Audyt finansowy dotyczy sprawozdań finansowych zgodnie ze standardami (normami) rewizji finansowej. W audycie opiniowana jest wiarygodność sprawozdania finansowego, oceniana jest zgodność informacji podawanych w sprawozdaniu z dokumentacją źródłową, błędy w sprawozdaniu finansowym i pominięcia informacji. Audyt pozwala zbadać, czy sprawozdanie finansowe jest kompletne, prawidłowo sporządzone, czy transakcje są udokumentowane i zgodne z prawem, a działalność jest prowadzona oszczędnie, wydajnie i skutecznie. Audyt operacyjny obejmuje badanie oszczędności, wydajności i skuteczności systemów i jednostek organizacyjnych, ocenę efektywności zarządzania, czyli sposobu jak kierownictwo organizacji planuje swoje działania, a następnie kontroluje realizację planów.

Audyt informatyczny zajmuje się środowiskiem systemów przetwarzania danych i wykorzystaniem tych systemów. Audytorzy oceniają poufność, integralność, wiarygodność, bezpieczeństwo, dostępność informacji przechowywanych i przetwarzanych w systemach informatycznych. Audyt jest procesem zbierania i oceniania dowodów w celu określenia, czy systemy informatyczne i związane z nimi zasoby właściwie chronią majątek, utrzymują integralność danych i systemu, dostarczają odpowiednich i rzetelnych informacji, przyczyniają się do osiągnięcia celów organizacji i chronią organizację przed niepożądanymi zdarzeniami, pozwalają na wczesne wykrywanie zagrożeń i łagodzenie konsekwencji ich urealnienia. Zakres audytu informatycznego obejmuje wszystkie systemy informatyczne i związane z nimi zasoby (tj. budynki, systemy energetyczne, systemy kablowe, systemy klimatyzacyjne, które są niezbędne do funkcjonowania systemów informatycznych, wszystkie platformy systemowe, systemy bazodanowe, oprogramowanie użytkowe, sprzęt komputerowy, problemy związane z zarządzeniem licencjami oprogramowania, problemy związane z procesami zarządzania ryzykiem i procesem zapewnienia bezpieczeństwa systemów.

Audyt informatyczny może być traktowany jako samodzielne przedsięwzięcie lub jako element pomocniczy audytu finansowego lub operacyjnego. Należy pamiętać, że audyt informatyczny służy badaniu i ocenie sprawności i skuteczności systemu kontroli wewnętrznej dla różnych procesów występujących w przedsiębiorstwie. Celem jego prowadzenia jest usprawnienie funkcjonowania organizacji, w sensie większej sprawności procesów decyzyjnych i biznesowych.

Prace audytu informatycznego powinny spełniać określone standardy i przebiegać w sposób systematyczny, konsekwentny i uporządkowany. Audyt informatyczny, w aspekcie sposobu wykonania, nie różni się zasadniczo od innego rodzaju audytu. Występują w nim cztery podstawowe fazy: planowanie, ocena mechanizmów kontrolnych, testowanie i raportowanie. Zatem można przyjąć, że proces audytowy będzie przebiegał następująco:

- szacowanie ryzyka i wstępne planowanie audytu,
- zapoznanie się z audytowanym obszarem (zrozumienie natury procesów i rodzajów ryzyka),
- szczegółowe planowanie audytu,

- przeprowadzenie szczegółowych prac audytowych,
- ocena zaplanowanych i wdrożonych mechanizmów kontrolnych w aspekcie ich adekwatności wobec potrzeb,
- ocena zgodności istniejącej praktyki z planami i przewidywaniami, udzielenie odpowiedzi na pytanie, czy stosowane mechanizmy dobrze działają,
- testowanie dowodowe,
- przygotowanie i przekazanie raportu,
- działania poaudytowe, monitorowanie rekomendacji i zaleceń wynikających z raportu [5].

W Polsce brakuje uznanych, szeroko akceptowanych metodyk i standardów audytu informatycznego dla instytucji sektora publicznego. Audytorzy informatyki poszukują dobrych metodyk dotyczących organizacji pracy, pisemnych procedur postępowania w trakcie audytu, skutecznych sposobów prowadzenia audytu i uznanych standardów. Postępowanie audytowe musi być oparte na dowodach. Można przyjąć, że zarządzanie organizacją gospodarczą w oparciu o wyniki badania audytowego jest zarządzaniem opartym na dowodach (evidence-based management). Gromadzone w pierwszej części zadania audytowego dowody muszą spełniać pewne wymagania, czyli powinny być:

- dostateczne: oparte na faktach, adekwatne i przekonywujące na tyle, że inna kompetentna osoba dojdzie na ich podstawie do tych samych wniosków,
- wiarygodne: rzetelne i najlepsze jakie można było uzyskać przy użyciu właściwej techniki
- istotne: wspierające ustalenia audytora i ściśle powiązane z obiektami audytu,
- użyteczne: pozwalające na osiągnięcie celów audytu [4].

Narzędziami wspomagającymi audyt informatyczny są modele COBIT, ITIL i Val IT [8, 9]. Model COBIT (Control Objectives for Information and related Technology) został jako narzędzie zarządzania opublikowany przez Information Systems Audit and Control Foundation (ISACF) w 1996 r. COBIT jako produkt to metodologia ciągle aktualizowana i rozbudowywana o kolejne narzędzia. COBIT ma służyć jako pomoc w zarządzaniu, kontroli i audycie systemów informatycznych. COBIT jest standardem ISACA (Information Systems Audit and Control Association) i w wersji 4.1 zawiera 34 procesy służące do zarządzania zasobami informatycznymi, ujęte w następujących obszarach:

- obszar polityki technologii informacji (information technology, IT) (plan and organise) (10 procesów): definiowanie planu strategicznego IT, definiowanie architektury informacji, definiowanie polityki technologii, definiowanie procesów, relacji i organizacji IT, zarządzanie inwestycjami IT, komunikowanie celów i kierunku zarządzania, zarządzanie zasobami ludzkimi, zarządzanie ryzykiem informatycznym, zarządzanie jakością,
- obszar akwizycji i implementacji (acquire and implement) (7 procesów): identyfikacja rozwiązań IT, akwizycja i konserwacja oprogramowania użytkowego, akwizycja i konserwacja infrastruktury IT, zapewnienie eksploatacji, zakupy zasobów informatycznych drogą przetargów, zarządzanie zmianą, instalacja i akredytacja rozwiązań i zmian.
- dostawy i wspomaganie (deliver and support) (13 procesów): zarządzanie poziomem usług, zarządzanie relacjami z dostawcami, zarządzanie wykonaniem i możliwościami, gwarantowanie ciągłości, gwarantowanie bezpieczeństwa informacji, identyfikacja przydział kosztów i zarządzanie kosztami, trening i

edukacja użytkowników, pomoc, porada i konsultacje dla użytkowników, zarządzanie konfiguracją, zarządzanie problemami i incydentami, zarządzanie danymi, zarządzanie środowiskiem gospodarowania, zarządzanie operacjami,

- procesy monitorowania (monitoring)(4 procesy): monitorowanie i ocena procesów IT, monitorowanie i ocena kontroli wewnętrznej, zapewnienie regulującego audytu, zapewnienie ładu informatycznego [8].

Dla każdego z procesów określone zostały:

- cel biznesowy,
- kryteria oceny systemu zależne od realizacji procesu, wybrane z następującego zbioru: efektywność (effectiveness), wydajność (efficiency), poufność (confidentiality), wiarygodność (integrity), dostępność (availability), zgodność (compliance), niezawodność (reliability);
- kluczowe wskaźniki celu - definiujące miary umożliwiające ustalenie, w jakim stopniu zrealizowany został postawiony cel biznesowy,
- kluczowe wskaźniki wydajności - definiujące miary umożliwiające ustalenie jak intensywne są działania prowadzące do osiągnięcia celu biznesowego,
- krytyczne czynniki sukcesu - lista warunków, których spełnienie jest konieczne dla osiągnięcia celu biznesowego,
- zasoby konieczne do realizacji procesu - wybrane z następującego zbioru: ludzie (people), oprogramowanie (applications), technologie (technology), urządzenia (facilities), dane (data),
- 6-stopniowy model dojrzałości - każdy stopień modelu jest zdefiniowany w kategoriach właściwych dla danego procesu organizacyjnego,
- kluczowe mechanizmy kontrolne - zdefiniowane w postaci haseł,
- szczegółowe mechanizmy kontrolne - wytyczne dotyczące przebiegu procesu, związanych z nim mechanizmów kontrolnych, wskazujące osoby lub jednostki organizacyjne odpowiedzialne za ich realizację,
- wytyczne dotyczące poszczególnych działań procesu audytowego.

W chwili obecnej trwają prace nad uzupełnieniem standardu COBIT o wytyczne dotyczące zastosowania konkretnych, praktycznych mechanizmów kontrolnych w ramach poszczególnych procesów. W metodyce COBIT proponowana jest typowa procedura audytowa pochodząca z audytu finansowego, która obejmuje fazy takie jak: zapoznanie się z procesem IT, ocena mechanizmów kontrolnych, testy zgodności, wykazanie ryzyka niespełnienia celów kontrolnych i raportowanie. COBIT przedstawia rozpoznawalną i akceptowaną osnowę zarządzania i kontroli IT umożliwiającą organizacjom społeczno-gospodarczym wdrażanie koncepcji ładu informatycznego (IT governance).

Celem modelu ITIL (Information Technology Infrastructure Library) jest dostarczenie ram efektywnego zarządzania w następujących obszarach:

- strategiczne planowania zasobów IT dla potrzeb biznesu,
- powiązanie celów biznesu i wspierającej go technologii informatycznej,
- pozyskiwanie, wykorzystanie i utrzymywanie odpowiednich zasobów
- pomiar wydajności rozwiązań IT,
- redukcja całkowitego kosztu eksploatacji infrastruktury IT,
- wskazanie wartości rozwiązań IT w konkretnych obszarach organizacji,
- rozwijanie partnerstwa biznesowych w dziedzinie zarządzania IT,

- outsourcing IT,
- wykorzystanie IT dla osiągnięcia przewagi konkurencyjnej [10].

Model ITIL dzięki zawartym w nim procesom może wspomagać audyt informatyczny i kontrolę realizacji procesów wykorzystania IT w organizacji. W modelu ITIL wyróżniono następujące grupy procesów:

- zarządzanie poziomem usług (service level management)(odbywa się to za pomocą mechanizmu SLA, dokumentującego wymagania klienta i definiującego cele dotyczące żądanego poziomu usług, a następnie monitorującego dotrzymywanie tych postanowień),
- zarządzanie pojemnością infrastruktury informatycznej (capacity management),
- zarządzanie sytuacjami krytycznymi i ciągłością procesów (contingency planning),
- zarządzanie dostępnością usług (availability management),
- zarządzanie kosztami (cost management) (zastosowanie modelu Total Cost of Ownership, TCO),
- zarządzanie incydentami (incident management, help desk),
- zarządzanie problemami jako proces przetwarzania wielu incydentów podobnych, w celu identyfikacji przyczyn powstałej usterki i wyeliminowania znanych błędów w infrastrukturze informatycznej,
- zarządzanie konfiguracją (configuration management),
- zarządzanie zmianami infrastruktury informatycznej w udokumentowany i zgodny z regułami biznesu sposób,
- zarządzanie wersjami oprogramowania (release management) [10].

W modelu VAL IT znalazły miejsce ważne zasady zarządzania inwestycjami informatycznymi [9]. Przyjęto, że przedmiotem zarządzania będą portfele inwestycyjne, a zarządzanie inwestycjami IT będzie obejmowało pełny zakres działań koniecznych dla osiągnięcia wartości biznesowej i pełny cykl życia ekonomicznego. Poza ty, w praktykach generowania wartości zostaną uwzględnione różne kategorie inwestycji, różne ewaluowane i zarządzane. Zostaną zdefiniowane i będą monitorowane kluczowe metryki uwzględniające zmiany i odchylenia. Praktyki generowania wartości będą angażowały wszystkich interesariuszy przedsięwzięć informatycznych i przypisywały im odpowiednią odpowiedzialność i rozliczalność (accountability) wobec wygenerowanych efektów i korzyści biznesowych. Praktyki generowania wartości będą stale monitorowane, ewaluowane i doskonalone.

3. Nowe obszary audytu informatycznego

Misją audytu technologii informatycznych według Committee of Sponsoring Organizations of the Treadway Commission (COSO) jest użycie odpowiednich narzędzi technicznych i wiedzy, ocena adekwatności i efektywności systemów kontroli skierowanych na ryzyko wynikające z zastosowania technologii w organizacji gospodarczej dla wspomagania osiągania celów ekonomicznych. Metodyka audytu jest zgodnie ze standardami ISACA (tj. COBIT, ITIL) oparta na analizie procesów biznesowych (tj. zakupy, kontraktowanie, obsługa klienta, rozliczenia, księgowość, sprzedaż, przetwarzanie informacji). Tradycyjne audyty systemów informatycznych koncentrowały uwagę a trzech głównych obszarach: zgodność z politykami rozwoju IT, przegląd struktur kontroli i badanie śladu rewizyjnego. W przeszłości audyt systemów informatycznych był traktowany

jako uzupełnienie audytu finansowego. Ze względu na rosnące znaczenie informacji i związanej z tym technologii w organizacjach społeczno-gospodarczych kwestia audytu staje się coraz ważniejsza i traktowana jest jako niezależna dyscyplina. W rezultacie globalizacji organizacje społeczno-gospodarcze muszą uporządkować swoje działania i korzystać z systemów, które są chronione i kontrolowane, a wszystko to dla zachowania pozycji rynkowej i właściwego wizerunku. Rozwój technologii informatycznych powoduje, że powstają stale nowe obszary audytu informatycznego w jednostkach sektora finansów publicznych. Można wskazać nowe dziedziny, którymi powinien objąć audyt informatyczny:

- kształtowanie świadomości użytkowników i odpowiedzialności za eksploatację i zabezpieczenie komputerów, edukacja w zagrożeń inżynierii społecznej,
- ochrona i odpowiedzialne gospodarowanie danymi osobowymi i sensytywnymi, ochrona prywatności obywateli, prewencja kradzieży tożsamości, ochrona przed cyberprzemocą (cyberbullying),
- zarządzanie treścią serwisów internetowych jednostek administracji publicznej (w tym BIP) z zachowaniem cenzury i swobody wypowiedzi, oraz przyzwoleniem na rozwój blogów osób pełniących funkcje społeczne,
- uniemożliwienie normalnego przetwarzania danych na serwerze przez nadmierne obciążanie go, co powoduje wstrzymanie działania i konieczność oczekiwania na wykonanie zadań (denial of service),
- przekierowanie użytkownika do spreparowanej strony internetowej, która wyglądem przypomina stronę poszukiwanej przez użytkownika instytucji, co może hakerowi przynieść poufne informacje osobiste i korzyści ekonomiczne (pharming and phishing),
- cyberprzestępstwa.

W Polsce uchwalono 29 sierpnia 1997 ustawę o ochronie danych osobowych. Ustawa ta chroni prawa osób fizycznych, których dane są lub mogą być przetwarzane w zbiorach danych oraz określa zasady przetwarzania danych osobowych. Za dane osobowe, zgodnie z ustawą, uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Nie ma, niestety, zgodności wśród specjalistów od ochrony danych osobowych, jak rozumieć pojęcie przetwarzania danych poza zbiorem np. w plikach tekstowych, plikach edytorów, arkuszach kalkulacyjnych czy na stronach internetowych.

Dane wrażliwe (sensytywne) to takie, które ujawniają pochodzenie etniczne, poglądy polityczne, przekonania religijne, przynależność do grupy dochodowej, pochodzenie rasowe i etniczne, jak również dane o stanie zdrowia, kodzie genetycznym, nałogach i życiu seksualnym. Danymi sensytywnymi dysponują urzędy gminne, urzędy pracy i kontroli skarbowej, a banki i firmy ubezpieczeniowe chciałyby mieć do takich danych dostęp. Systemy informatyczne przetwarzające dane sensytywne powinny mieć budowę modułową, a przedmiotem badania audytowego jest ochrona dostępu do połączeń i kontrola ewidencji osób uprawnionych. Ustawowo powinien być ograniczony dostęp do danych sensytywnych, a wymienione instytucje mogą mieć jedynie dostęp do swoich modułów a nie do megazbioru. Poddanie serwisu internetowego i serwisu BIP audytowi pozwala na uzyskanie obiektywnej i kompleksowej oceny dotyczącej funkcjonowania zgodnie z obowiązującymi standardami i przepisami prawa. Wnioski z audytu ułatwiają usunięcie ewentualnych błędów lub braków w treści serwisu internetowego gminy i sugerują działania, jakie należałoby podjąć w celu uzyskania oczekiwanej przez lokalną

społeczności internautów funkcjonalności i dostępności serwisu wirtualnej społeczności lokalnej. Internetowe serwisy społecznością są wyrazem e-Demokracji i e-Partycypacji mieszkańców w gospodarowaniu gminą czy regionem. Wyróżnia się dwie ważne kwestie dla cenzury online – swoboda wypowiedzi i seks [11]. Ogólnie ujmując, każdy ma prawo wyrażania opinii, jednakże doświadczenie takiej swobody, powiązane z odpowiedzialnością może być zależne od formalności i ograniczeń, które są konieczne nawet w państwie demokratycznym dla ochrony zdrowia i morale, dla ochrony reputacji i praw innych, dla zapobiegania ujawnieniu informacji poufnej, dla zachowania autorytetu i bezstronności sądu. Prawo do swobodnego wyrażania się nie może być i nie powinno być uważane za najważniejsze. Swoboda wyrażania się nie oznacza, że inni muszą tego słuchać. Nawet najbardziej tolerancyjni liberałowie uważają pewne wyrażenia jako pozostające w konflikcie z prawami innych. Przeciwieństwem swobodnego wyrażania jest cenzura. Źródłem jej jest państwo, ale również instytucje pozarządowe i organizacje komercyjne mogą działać jako cenzorzy. Wyróżnia się dwa aspekty cenzury: wstrzymywanie prezentera od wyrażenia swoich pomysłów i uniemożliwianie słuchaczowi odbioru informacji. Jedną z najważniejszych tendencji w ostatnich latach jest rozwój międzynarodowych korporacyjnych cenzorów rywalizujących w ograniczaniu swobody korzystania z Internetu, np. przedsiębiorstwa telewizji kablowej zmierzają ku temu by przeobrazić Internet w kontrolowane medium transmisji takie jak radio i telewizja, zwracając uwagę by technologie wspomagały te działania. Wiele różnych metod jest stosowanych dla ograniczania i regulowania dostępu do Internetu np. licencjonowanie treści i oprogramowania, filtrowanie treści, nadzór publikacji elektronicznych, polityki podatkowe, propagowanie autocenzury. Konwencja Rady Europy dotycząca cyberprzestępstw wyróżnia:

- wykroczenia przeciw poufności, integralności i dostępności danych komputerowych i systemów, np. bezprawny dostęp do systemów, nielegalny podsłuch transmitowanych danych, niewłaściwe użycie urządzeń,
- wykroczenia tj. sprzeniewierzenia lub fałszerstwa (counterfeiting)
- wykroczenia związane z treścią – zasadniczo w pornografią dziecięcą,
- wykroczenia związane z naruszeniem praw autorskich i praw pokrewnych,
- wykroczenia podrzędne i sankcje – wspomaganie i nakłanianie innych do popełnienia przestępstwa [11].

Niestety dostęp do Internetu rozwija nie tylko relacje wirtualnych społeczności lokalnych i więzi ekonomiczne instytucji publicznych, ale sprzyja włamaniom, dystrybucji złośliwego i szpiegowskiego oprogramowania. Stowarzyszenie ISACA proponuje sześcioetapowe postępowanie wobec każdego z wyżej wymienionych zagrożeń obejmujące: działania preincydentalne, działania bezpośrednie po wystąpieniu zdarzenia, działania drugorzędne i uzupełniające, gromadzenie dowodów audytu, przygotowanie środków zaradczych i ocena [12]. Współcześnie przedsiębiorstwa, ale także instytucji administracji publicznej, organizacje rządowe i pozarządowe łączą się silnie więziami komunikacji internetowej w struktury sieciowe otwarte i bardzo elastyczne (extended enterprises), a to niestety sprzyja rozwojowi zagrożeń bezpieczeństwa informacji i ludzi.

4. Wnioski

Potrzeba wprowadzenia audytu wewnętrznego wyniknęła z konieczności rozszerzania instrumentów kontrolnych i nadzorczych w celu wzmocnienia racjonalności, przejrzystości

i odpowiedzialności za wszelkie działania podejmowane w sferze zarządzania i wydatkowanie środków publicznych. Audyt finansowy wymaga uzupełnienia o inne rodzaje audytu (w tym audyt procesów informatycznych) dla kompleksowej oceny gospodarowania. Nowe technologie informatyczne stwarzają nowe możliwości przetwarzania danych, ale też pożądane są ciągle nowe środki i sposoby zabezpieczenia informacji generowanej przez instytucje publiczne.

Literatura

1. Porter B., Simon J., Hatherly D.: Principles of External Auditing, J.Wiley & Sons Publication, Chichester, 2008.
2. Winiarska K.: Audyt wewnętrzny, Difin, Warszawa, 2008.
3. Governance of Extended Enterprise, Bridging Business and IT Strategies, IT Governance Institute, J.Wiley & Sons, Hoboken, New Jersey, 2005.
4. Czerwiński K.: Audyt wewnętrzny, InfoAudit, Warszawa, 2005.
5. Forystek M.: Audyt informatyczny, InfoAudit, Warszawa, 2005.
6. Molski M Łacheta M. Przewodnik audytora systemów informatycznych, Helion Gliwice, 2007.
7. Otręba M.: Klasyfikacja audytu wewnętrznego, w: Metody i procedury audytu wewnętrznego w jednostkach sektora finansów publicznych, Kostur A (red.) Wydawnictwo Akademii Ekonomicznej w Katowicach, Katowice, 2007, s.63-69.
8. COBIT Mapping, Mapping of ITIL v 3 With COBIT 4.1 IT Governance Institute Rolling Meadows, USA, 2008, http://www.isaca.org
9. IT Governance Implementation Guide, Using COBIT and VAL IT, IT Governance Institute, Rolling Meadows, USA, 2008, http://www.isaca.org
10. Lotko A.: Wybrane koncepcje i modele zarządzania technologią i usługami informatycznymi, w: Organizacja i Kierowanie nr 2(116), 2004, s.35-50.
11. Adams A.A., McCrindle R.J.: Pandora's Box, Social and professional issues of the information age, J.Wiley & Sons, Ltd. Chichester. 2008.
12. Cybercrime: Incident Response and Digital Forensics, Internal Control Questionnaires, ISACA Serving IT Governance Professionals, 2005, http://www.isaca.org

Dr Małgorzata PAŃKOWSKA
Katedra Informatyki
Akademia Ekonomiczna
40-226 Katowice, ul. Bogucicka 3
tel./fax.: (0-32) 257 7277
e-mail: pank@ae.katowice.pl