AUDYT I KONTROLE SYSTEMÓW TELEINFORMATYCZNYCH ORAZ PROJEKTÓW IT W SEKTORZE ADMINISTRACJI PUBLICZNEJ

Anna KACZOROWSKA

Streszczenie: Celem artykułu jest przedstawienie prawnych i merytorycznych wytycznych do przeprowadzania kontroli systemów teleinformatycznych i projektów informatycznych w urzędach w świetle znowelizowanej ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne (dalej określanej jako UINF). Przy czym, zakres kontroli zasobów IT odniesiono do zakresu uwzględnionego w ustawie, gdyż konstytuuje ona e-działalność wszystkich jednostek administracji publicznej. W artykule wskazano również na metodykę COBIT w zakresie przeprowadzania audytów systemów teleinformatycznych w sektorze publicznym służących uporządkowaniu środowisk IT w urzędach. Zawarto tu także praktyczne wskazówki dla jednostek realizujących zadania publiczne w zakresie przeprowadzania audytu informatycznego w świetle obowiązujących przepisów prawa.

Słowa kluczowe: oprogramowanie interfejsowe, system teleinformatyczny, audyt informatyczny, kontroler, IT Governance.

1. Kontrola systemów teleinformatycznych i projektów IT w świetle znowelizowanej UINF

Na mocy ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne z 17 lutego 2005 r. (Dz. U. nr 64, poz. 565) [1] kontrola systemów teleinformatycznych tych jednostek nie była faktycznie przeprowadzana. Dopiero po 5-u latach, w nowelizacji (na podstawie ustawy z dnia 12 lutego 2010 r.; Dz. U. nr 40, poz. 230) przewidziano instrumenty prawne, które miałyby przyczyniać się do zapewnienia jednolitości, sprawności i bezpieczeństwa systemów teleinformatycznych, dzięki którym wykonywane są zadania publiczne.

Instrumentami, które przewiduje znowelizowana UINF [2] mają być:

- badanie zgodności oprogramowania interfejsowego z rozwiązaniami określonymi przez podmioty publiczne,
- kontrola przestrzegania przepisów ustawy.

W art. 3 § 11 UINF oprogramowanie interfejsowe zostało zdefiniowane jako: „oprogramowanie umożliwiające łączenie i wymianę danych w komunikacji pomiędzy systemami teleinformatycznymi".

Kontrolowana jest zatem ocena poprawności wdrożenia w oprogramowaniu interfejsowym rozwiązań (używanych przez podmioty publiczne do przekazywania danych innemu podmiotowi niebędącemu organem administracji rządowej), które podmiot publiczny ma obowiązek publikować w Biuletynie Informacji Publicznej lub udostępniać w inny sposób razem z testami akceptacyjnymi, z zastrzeżeniem, że podmiot publiczny może ich nie dostarczać, gdy w oprogramowaniu interfejsowym mają być stosowane

wyłącznie formaty danych oraz protokoły komunikacyjne i szyfrujące (podane w przepisach wydanych na podstawie art. 18 pkt. 1).

Testy akceptacyjne w sektorze administracji publicznej (w rozumieniu art. 3 § 12 UINF) to: „udokumentowane wartości danych wejściowych wprowadzanych do systemu teleinformatycznego i powiązanych z nimi wartości oczekiwanych danych wyjściowych, opisujące zestawy poprawnych odpowiedzi systemu teleinformatycznego na podawane dane wejściowe, pozwalające na sprawdzenie poprawności wdrożenia oprogramowania interfejsowego".

Badanie ma na celu ocenę, czy możliwe jest wykorzystywanie danego oprogramowania interfejsowego systemu teleinformatycznego do wykonywania zadań publicznych? Sprawdzane jest czy rozwiązania te obejmują zestawienia:

- stosowanych w oprogramowaniu interfejsowym struktur dokumentów elektronicznych,
- formatów danych,
- protokołów komunikacyjnych i szyfrujących.

Kontrola ma ustalić czy system teleinformatyczny podmiotu publicznego spełnia minimalne wymogi dla tego rodzaju systemów oraz czy jest zagwarantowana jego interoperacyjność na zasadach określonych w Krajowych Ramach Interoperacyjności. Ponadto, respektowane powinny być wymogi równego traktowania różnych rozwiązań informatycznych.

Intencją ustawodawcy było także, aby przepisy znowelizowanej UINF zapewniały prawidłową - kontrolowaną realizację projektów ustanowionych dla rozwoju społeczeństwa informacyjnego. Przedsięwzięcia informatyczne o publicznym zastosowaniu są wiec także przedmiotem kontroli przewidzianej przepisami UINF i powinna być przeprowadzana ocena ich prawidłowości, jeśli chodzi o legalność, gospodarność, celowość i rzetelność wydatkowania środków publicznych przyznawanych na dofinansowanie takich zamierzeń.

Celowości kontroli przewidzianych w UINF należy upatrywać w:

- dokonaniu obiektywnych ustaleń w kwestiach będących przedmiotem weryfikacji,
- wyjaśnieniu przyczyn, zakresu i skutków stwierdzonych nieprawidłowości oraz wskazaniu, kto jest za nie odpowiedzialny.

Podmiotami badanymi będą:

- organy administracji rządowej,
- organy kontroli państwowej i ochrony prawa,
- sądy,
- jednostki organizacyjne prokuratury,
- jednostki samorządu terytorialnego i ich organy,
- jednostki budżetowe i samorządowe zakłady budżetowe,
- fundusze celowe,
- samodzielne publiczne zakłady opieki zdrowotnej,
- Zakład Ubezpieczeń Społecznych, Kasy Rolniczego Ubezpieczenia Społecznego,
- Narodowy Fundusz Zdrowia,
- państwowe lub samorządowe osoby prawne utworzone na podstawie odrębnych ustaw w celu realizacji zadań publicznych.

Istnieje podmiotowe ograniczenie stosowania przepisów UINF (na podstawie art. 2 § 4) dotyczących kontroli zgodności oprogramowania interfejsowego w odniesieniu do:

- jednostek badawczo-rozwojowych,
- uczelni publicznych,
- Polskiej Akademii Nauk i tworzonych przez nią jednostek organizacyjnych,

- Rzecznika Praw Obywatelskich,
- Trybunału Konstytucyjnego,
- Sądu Najwyższego oraz sądów administracyjnych,
- Najwyższej Izby Kontroli,
- Krajowej Rady Radiofonii i Telewizji,
- Krajowego Biura Wyborczego,
- Instytutu Pamięci Narodowej - Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu,
- Generalnego Inspektora Ochrony Danych Osobowych,
- Komisji Nadzoru Finansowego,
- Generalnego Inspektora Informacji Finansowej.

Kontroli, co do zasady, nie podlegają podmioty wymienione wcześniej, ale wyjątkiem są tu „przypadki, w których w związku z realizacją zadań publicznych podmioty te są zobowiązane do przekazywania informacji podmiotom niebędącym organami administracji rządowej" [3]. Używany w takich sytuacjach system teleinformatyczny musi również spełniać minimalne ustawowe wymagania informatyczne. Jeśli podmiot publiczny powierzył lub zlecił realizację zadania publicznego innym podmiotom, to obowiązek zapewnienia minimalnych wymagań ciąży właśnie na nich a z tym związane jest przekazywanie informacji do lub od jednostek niebędących organami administracji rządowej.

Rodzaje oprogramowania interfejsowego podlegającego badaniu oraz metodykę, warunki i tryb sporządzania rzetelnego zestawu testów akceptacyjnych (z uwzględnieniem konieczności jednolitych warunków ich przygotowania), ma dopiero określić minister MSWiA poprzez wydanie stosownego rozporządzenia. W tym rozporządzeniu ma być również uwzględniony wzór oświadczenia o wyniku badania oraz weryfikacji badania.

W branży IT testowanie akceptacyjne to testy w środowisku użytkownika przeprowadzane przez producenta lub w postaci beta-testów przez samego użytkownika, jego dystrybutorów lub partnerów, zarówno na systemie informatycznym użytkownika, jak i na jego rzeczywistych danych.

W środowisku informatyków dba się również o to, aby osoba testująca nie była autorem kontrolowanego systemu, ponieważ mogłaby wówczas okazać się nieobiektywna. Testowaniem powinna się zajmować niezależna osoba, która by bez sentymentów znajdowała błędy.

W sektorze administracji publicznej badanie poprawności wdrożenia rozwiązań w oprogramowaniu interfejsowym przy wykorzystaniu testów akceptacyjnych udostępnionych przez podmiot publiczny, przeprowadza na własny koszt albo twórca oprogramowania interfejsowego, albo inny podmiot uprawiony, który posiada autorskie prawa majątkowe do tego oprogramowania. Kontrowersyjnie, dla ustawodawcy twórca oprogramowania i podmiot autorskich praw majątkowych, to mogą być dwa odrębne podmioty.

Oprogramowanie interfejsowe podlega badaniu przed jego pierwszym udostępnieniem do realizacji danego zadania publicznego przy wykorzystaniu systemu teleinformatycznego. Kontrola powinna również nastąpić po modyfikacji (oprogramowania interfejsowego systemu teleinformatycznego używanego przez ten podmiot do realizacji zadań publicznych) w zakresie stosowanych struktur dokumentów elektronicznych, formatów danych oraz protokołów komunikacyjnych i szyfrujących, przeprowadzonej po poprzednim badaniu.

Podmiot uprawniony do przeprowadzenia badania powinien poinformować podmiot publiczny o rodzaju, wersji, dacie wytworzenia i charakterystyce techniczno-funkcjonalnej oprogramowania interfejsowego oraz złożyć mu oświadczenie o wyniku kontroli. Z kolei podmiot publiczny, dla potwierdzenia wyniku otrzymanego badania może, we własnym zakresie, przeprowadzić jego weryfikację (wykorzystując testy akceptacyjne udostępnione podmiotowi uprawnionemu) i poinformować podmiot uprawniony o jej wynikach. W przypadku rozbieżności pomiędzy wynikami weryfikacji a badania przeprowadzonego przez podmiot uprawniony za rozstrzygający uznaje się wynik weryfikacji. Kosztami weryfikacji zostaje wówczas obciążony podmiot uprawniony.

Przy braku wspomnianego rozporządzenia ministra MSWiA szczegóły dotyczące przebiegu badania reguluje w dalszym ciągu rozporządzenie Ministra Nauki i Informatyzacji z dnia 19 października 2005 r. w sprawie testów akceptacyjnych oraz badania oprogramowania interfejsowego (Dz. U. nr 217, poz. 1836).

Podmiot publiczny może odmówić przyjęcia danych przekazywanych za pomocą oprogramowania interfejsowego, jeśli nie przejdzie ono pozytywnie testu akceptacyjnego, lub też zostało użyte do realizacji zadań publicznych, a nie zostało nigdy poddane takiemu badaniu. W UINF odmowa przyjęcia danych jest równoznaczna z nieprzekazaniem tych danych, a to może skutkować niewykonaniem określonych czynności w ramach realizacji zadań publicznych. Oprogramowania interfejsowego, które uzyskało w badaniu wynik negatywny, bo nie przeszło testu akceptacyjnego nie można używać do wykonywania zadań publicznych.

Powinność przeprowadzania kontroli przewidzianej w UINF spoczywa na: Prezesie Rady Ministrów (w przypadku projektów ponadsektorowych), wojewodach (w jednostkach samorządu terytorialnego i ich związkach oraz tworzonych lub prowadzonych przez te jednostki samorządowych osobach prawnych i innych samorządowych jednostkach organizacyjnych), organach administracji rządowej nadzorujących dany podmiot publiczny (w podmiotach publicznych podległych lub nadzorowanych przez organ administracji rządowej) oraz Ministrze Spraw Wewnętrznych i Administracji (w innych podmiotach publicznych realizujących swoje zadania przy wykorzystaniu systemu teleinformatycznego albo z użyciem środków komunikacji elektronicznej) odpowiednio do podległych im jednostek.

Prawo, ale i obowiązek kontroli oprogramowania interfejsowego przysługuje także ministrowi kierującemu działem administracji rządowej, dla którego ustanowiono projekt informatyczny.

W rozdziale 2 UINF na mocy art. 5 powołano Plan informatyzacji Państwa oraz projekty informatyczne o publicznym zastosowaniu. Plan ten jest aktem wykonawczym do UINF. Do końca 2010 r. obowiązuje Plan Informatyzacji Państwa na lata 2007-2010 (poprzez rozporządzenie Rady Ministrów z dnia 28 marca 2007 r.). W części drugiej planu zestawiono 23-y sektorowe i 5-ć ponadsektorowych projektów informatycznych ustanowionych dla realizacji określonych priorytetów i usług wraz z opisem przedsięwzięć uwzględniającym informacje o szacunkowych kosztach, możliwych źródłach finansowania i podmiotach odpowiedzialnych za ich realizację.

Zmieniono art. 7 w UINF i usunięto z niego odwołanie do art. 8 i 9, które również uchylono, a dotyczyły one właśnie sektorowych i ponadsektorowych projektów informatycznych. Konsekwentnie, w znowelizowanej ustawie uchylono także inne artykuły (10 i 11) dotyczące tych projektów. Od 17 czerwca 2010 r., czyli od daty wejścia w życie nowego brzmienia większości artykułów UINF, nie powinno się zatem dzielić projektów na ponadsektorowe i sektorowe a dla realizacji bieżącego Planu Informatyzacji Państwa

ustanawiane są po prostu projekty informatyczne. Jednak dla zapewnienia kontynuacji realizacji ustanowionych wcześniej jako sektorowe czy też ponadsektorowe projektów określono (art. 25), kto będzie przeprowadzał ich kontrole. Realizacja ponadsektorowych projektów informatycznych ma być kontrolowana przez Prezesa Rady Ministrów a sektorowych przez ministra kierującego działem administracji rządowej, dla którego ustanowiono taki projekt.

Prawidłowość wydatkowania środków publicznych na dofinansowanie projektów informatycznych jest sprawdzana przez właściwą regionalną izbę obrachunkową, jeśli chodzi o jednostki samorządowe, a we wszystkich innych przypadkach przez Ministra Spraw Wewnętrznych i Administracji.

Niekorzystny wynik kontroli przestrzegania przepisów ustawy powoduje bardziej złożone konsekwencje proceduralne. Wyniki te są zawarte w protokole kontroli, który obejmuje podjęte ustalenia, w tym stwierdzone przypadki naruszenia przepisów UINF lub innych wydanych do niej aktów wykonawczych. Protokół podpisują zarówno kontroler jak i kierownik kontrolowanego podmiotu, któremu przysługuje prawo do zgłoszenia umotywowanych zastrzeżeń odnośnie ustaleń tam przedstawionych przed złożeniem podpisu. Jeśli kierownik kontrolowanego podmiotu publicznego odmówi podpisania protokołu kontroli, to powinien w terminie 3 dni roboczych (od dnia otrzymania protokołu) wyjaśnić (pisemnie) przyczyny odmowy. Zastrzeżenia zgłasza się formalnie – na piśmie, w przeciągu 7 dni roboczych od dnia otrzymania protokołu kontroli. Zasadne zastrzeżenia kierownika powodują konieczność zmiany lub rozszerzenia treści protokołu a także jeśli wskazują na potrzebę uzupełnienia czynności kontrolnych, to powinny one zostać podjęte. Gdy zastrzeżenia zostały zgłoszone i w protokole zaistniały określone naruszenia, to organ dokonujący kontroli sporządza wystąpienia pokontrolne, gdzie określa sposób oraz termin usunięcia naruszeń. Kontrolowanemu podmiotowi przysługuje wtedy 60 dni (od dnia otrzymania wystąpienia pokontrolnego) na zastosowanie się do zaleceń oraz zawiadomienie o ich wykonaniu a jeśli nie zostały one wykonane, to należy poinformować organ dokonujący kontroli dlaczego nie oraz kiedy to nastąpi. Bieg wskazanych 60-u dni ulega zawieszeniu na czas rozpatrzenia zastrzeżenia w odniesieniu do zaleceń pokontrolnych objętych zastrzeżeniem.

Podmiot kontrolowany może również wnieść zastrzeżenia do zaleceń do organu wyższego stopnia niż kontrolujący za pośrednictwem tego ostatniego. Jeśli kontrolującym jest Prezes Rady Ministrów lub minister, to zastrzeżenia w stosunku do zaleceń składane są bezpośrednio do nich i są przez nich rozpatrywane.

2. Kontrolerzy projektów informatycznych i systemów teleinformatycznych

Kontrolerem jest osoba wyznaczana przez organ dokonujący kontroli na podstawie wydanego przezeń imiennego upoważnienia. W art. 28 znowelizowanej UINF określono, kto może być kontrolerem projektów informatycznych i systemów teleinformatycznych. Na jego mocy uchylono przepisy dotyczące zdobywania uprawnień kontrolera poprzez udział w szkoleniu i uzyskanie świadectwa kwalifikacji w wyniku pozytywnego złożenia egzaminu przed komisją powołaną przez ministra MSWiA.

Obecnie kontrolerem może być osoba, która posiada certyfikat określony w rozporządzeniu wydanym na podstawie art. 28 § 3 ustawy i spełnia następujące wymagania:

- jest pełnoletnia i posiada wykształcenie wyższe,

- ma niczym nie ograniczoną zdolność do czynności prawnych oraz korzysta z pełni praw publicznych,
- nie była karana ani za umyślne przestępstwo, ani umyślne przestępstwo skarbowe,
- posiada obywatelstwo jednej z grup krajów takich jak: Unia Europejska, Konfederacja Szwajcarska, Europejskie Porozumienie o Wolnym Handlu (EFTA) – strony umowy o Europejskim Obszarze Gospodarczym, chyba że w odrębnych przepisach zastrzeżono, że jej zatrudnienie w jednostce kontrolowanej wymaga posiadania obywatelstwa polskiego.

Zlikwidowano zatem szkolenia (podstawowe i uzupełniające) organizowane przez ministra właściwego do spraw informatyzacji i egzaminy państwowe a w ich miejsce zaproponowano, w drodze rozporządzenia, wykaz certyfikatów uprawniających do otrzymania statusu kontrolera. Chcąc spełnić wymagania w zakresie merytorycznych kompetencji kontrolera należy obowiązkowo posiadać stosowny certyfikat, z listy tych, uwzględnionych w wykazie.

Kontroler może przystąpić do przeprowadzenia kontroli dopiero po okazaniu dokumentu stwierdzającego jego tożsamość, legitymacji służbowej, upoważnienia oraz aktualnego poświadczenia bezpieczeństwa uprawniającego go do dostępu do informacji niejawnych stanowiących tajemnicę państwową w sytuacji, gdy kontrolą objęte będą systemy teleinformatyczne lub rejestry publiczne zawierające informacje i dane stanowiące tajemnicę państwową lub inną tajemnicę ustawowo chronioną. Upoważnienie poza imieniem i nazwiskiem kontrolera, serią i numerem jego dokumentu tożsamości oraz legitymacji służbowej powinno zawierać następujące dane: przedmiot i zakres kontroli we wskazanym podmiocie publicznym, przewidywany czas trwania kontroli, datę ważności i wydania upoważnienia oraz podpis organu dokonującego kontroli albo osoby przez ten organ upoważnionej.

Art. 27 i jego paragrafy traktują o prawach kontrolera. Realizując kontrolę ma on prawo do swobodnego poruszania się na terenie siedziby kontrolowanego podmiotu publicznego i w miejscu wykonywania zadań. Ma wgląd do dokumentów i materiałów dotyczących przedmiotu kontroli. Może żądać udzielania ustnych lub pisemnych wyjaśnień oraz sporządzania i to na koszt podlegającego kontroli uwierzytelnionych kopii, odpisów i wyciągów z dokumentów i różnych zestawień i obliczeń potrzebnych mu do obiektywnego ustalenia stanu faktycznego. Wśród uprawnień kontrolera są oględziny systemów teleinformatycznych używanych do realizacji zadań publicznych i korzystanie z pomocy biegłych w ramach wykonywania czynności kontrolnych.

W art. 29 podano rygory prawne mające zapewnić obiektywizm kontrolerów. Na podstawie § 1 tego artykułu „Kontroler podlega wyłączeniu z kontroli, z urzędu albo na wniosek, jeżeli wyniki kontroli mogą oddziaływać na jego prawa lub obowiązki, na prawa lub obowiązki jego małżonka albo osoby pozostającej z nim faktycznie we wspólnym pożyciu, krewnych i powinowatych do drugiego stopnia lub osób związanych z nim z tytułu przysposobienia, opieki bądź kurateli.” Powody, które zadecydowały o wyłączeniu kontrolującego obowiązują pomimo ustania małżeństwa, wspólnego pożycia, przysposobienia lub kurateli. Gdy istnieją uzasadnione wątpliwości, co do bezstronności kontrolera, to może on być wyłączony z kontroli w każdym czasie. Z wnioskiem o wyłączenie kontrolera może wystąpić on sam albo kontrolowany podmiot publiczny. Decyzję o wyłączeniu lub odmowie podejmuje Minister Spraw Wewnętrznych i Administracji, który obecnie kieruje działem administracji rządowej – informatyzacja.

Dodatkowo, na kontrolerze ciąży obowiązek zachowania w tajemnicy informacji uzyskanych podczas kontroli także wówczas, gdy zakończył już swoją pracę.

3. Certyfikaty uprawniające do kontroli

W projekcie rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie wykazu certyfikatów uprawniających do prowadzenia kontroli projektów informatycznych i systemów teleinformatycznych wymienione były tylko trzy certyfikaty: Certified Information System Auditor (CISA), Certified Information Security Manager (CISM), Europejski Certyfikat Umiejętności Zawodowych Informatyka (EUCIP Professional; specjalizacja Audytor Systemów Informacyjnych).

Rozporządzenie (Dz. U. nr 177 z 2010 r.; poz. 1195, s. 1) obowiązuje już od 24.09.2010 (po 14-o dniowym *vacatio legis*). Podany w załączniku do rozporządzenia wykaz ma uwzględniać zakres wiedzy specjalistycznej wymaganej od osób legitymujących się poszczególnymi certyfikatami i zakres kontroli określony w art. 25 UINF a także sankcjonuje jako upoważniające do bycia kontrolerem certyfikaty przedstawione w tabeli 1.

Tab. 1. Certyfikaty uprawniające do kontroli

Lp.	**Nazwa certyfikatu**	**Uwagi**
1.	Audytor systemu zarządzania bezpieczeństwem informacji według normy PN ISO/IEC 27001 lub jej odpowiednika międzynarodowego	
2.	Audytor systemu zarządzania usługami informatycznymi według normy PN ISO/IEC 20000 lub jej odpowiednika międzynarodowego	
3.	Audytor systemu zarządzania jakością według normy PN ISO/IEC 9001 lub jej odpowiednika międzynarodowego.	
4.	Certified Information System Auditor (CISA).	był w projekcie rozporządzenia
5.	Certified in the Governance of Enterprise IT (CGEIT)	
6.	Certified Internal Auditor (CIA)	
7.	Certified Information Systems Security Professional (CISSP).	
8.	Europejski Certyfikat Umiejętności Zawodowych Informatyka - EUCIP Professional specjalizacja Audytor Systemów Informacyjnych	był w projekcie rozporządzenia
9.	Systems Security Certified Practitioner (SSCP)	

Wśród zamieszczonych w rozporządzeniu certyfikatów nie znalazł się Certified Information Security Manager (CISM) proponowany w projekcie tego aktu wykonawczego. CISM, jako jedyny wśród certyfikatów wydawanych przez stowarzyszenie ISACA, jest adresowany do ludzi zajmujących się zarządzaniem bezpieczeństwem informacji. Informacje przechowywane w systemach teleinformatycznych jednostek realizujących zadania publiczne powinny być przecież szczególnie dobrze zabezpieczane.

4. Audyt systemów IT w sektorze publicznym

Jednostki administracji publicznej chcąc skontrolować poprawność rozwiązań zastosowanych w oprogramowaniu interfejsowym używanych systemów teleinformatycznych mogłyby skorzystać z usługi audytu informatycznego doceniając rolę i znaczenie usług IT w tym sektorze.

Początkowo w instytucjach publicznych pojmowano audyt informatyczny jako kontrolę legalności posiadanego oprogramowania a następnie myślano o nim w kontekście spełniania warunków ustawy o ochronie danych osobowych. Obecnie najlepiej byłoby, gdyby to pojęcie było ściśle wiązane z generowaniem wartości i ładu organizacyjnego IT.

Audyt informatyczny stwarza możliwość przewidywania różnych scenariuszy poprzez analizę ryzyka i zapobieganie wystąpieniu zidentyfikowanych zagrożeń.

Na pewno do czynników wysokiego ryzyka IT w instytucjach publicznych należy zaliczyć dobieranie rozwiązań informatycznych w sposób bezkierunkowy i chaotyczny pod władzą kolejnych kierownictw. Nie da się jednak, w krótkim czasie, zaprowadzić porządku w informatyzacji, która powstaje na bazie chaosu i bałaganu. ”Wszechogarniający chaos rodzi się wraz z radosną twórczością ustawodawcy, który ustalając priorytety, rzadko zwraca uwagę na przyszłe konsekwencje swoich pomysłów (ma komfort niezabierania głosu w określaniu sposobów realizacji strategii)” [5]. W cytacie chodzi o kolejny dokument - „Strategię rozwoju społeczeństwa informacyjnego w Polsce do roku 2013”, który Rząd RP przygotował w październiku 2008 r. . Mało jednostek z tego sektora ma zdefiniowaną strategię zarządzania czy opracowaną strategię informatyzacji, wyznaczającą kierunki i standardy jej rozwoju. Jeszcze mniej urzędów planuje politykę informatyzacji na podstawie strategii zarządzania i rozwoju jednostki. Najczęściej strategia informatyzacji istnieje tylko w głowie dyrektora IT a rzadziej kierownika urzędu.

Źródłem ryzyka informatycznego w sektorze administracji publicznej są także przestarzałe i nieskutecznie zabezpieczone systemy IT, przypisywanie odpowiedzialności za nietrafione decyzje deficytowi budżetowemu, administrowanie zamiast zarządzania, silnie zhierarchizowane struktury organizacyjne, niechęć do procesów, łączenie rozwiązań informatycznych systemowo sprzecznych na polecenie przełożonego, a także nieliczne przypadki zatrudniania w urzędach audytorów informatycznych.

Chcąc mieć przekonanie, że w świetle prawa panuje się nad funkcjonowaniem urzędu, w gestii którego znajduje się zazwyczaj mnóstwo informacji (przechowywanych w systemach informatycznych oczywiście z zachowaniem ich ochrony i bezpieczeństwa) należy wdrożyć skuteczną kontrolę zarządczą zgodną z międzynarodowymi standardami w tym zakresie, jak np. COSO, INTOSAL, Komisja Europejska. W tym celu można się posłużyć metodyką COBIT wykazując jednocześnie racjonalny stosunek do ryzyka i rzeczywiście zamierzając uporządkować środowisko IT w danej instytucji publicznej. Kontrolę zarządczą można wzmocnić poprzez audyt wewnętrzny. Jest on bowiem niezależny i obiektywny i ma na celu wspieranie ministra kierującego działem administracji lub kierownika jednostki w realizacji celów i zadań poprzez systematyczną ocenę kontroli zarządczej i doradztwo.

COBIT jest metodyką kontroli zarządczej uzupełniającą inne standardy takiej kontroli o uporządkowany zbiór wskazówek dotyczących informatyki. Główną jej zasada zakłada, że jednostka chcąc sobie zapewnić informacje potrzebne jej do osiągnięcia celów nie powinna, ale musi inwestować w zasoby IT, którymi należy zarządzać i je kontrolować za pomocą usystematyzowanego zbioru procesów.

Najwyższe kierownictwo danej instytucji publicznej może wykorzystywać COBIT dla ograniczania ryzyka i kontroli inwestycji w środowisku IT oraz osiągania z nich korzyści.

Kierownicy działów IT w urzędach powinni widzieć użyteczność tej metodyki w dostarczaniu kontrolowanych i zarządzanych usług informatycznych. Te podmioty mają wszak świadczyć usługi na drodze elektronicznej wykonując zadania publiczne.

Audytorom ta metodyka również się podoba, ponieważ dzięki niej mogą potwierdzać swoje opinie bazując na międzynarodowym standardzie i udzielać kierownictwu jednostki rad w zakresie wewnętrznych mechanizmów kontrolnych. COBIT pomaga audytorom w

przedstawieniu wyniku audytu i sformułowaniu opinii odnośnie skuteczności i efektywności kontroli zarządczej IT.

Dla osiągania przez instytucje założonych celów określa się w COBIT kryteria kontrolne podmiotu względem informacji. Biorąc pod uwagę ogólne wymagania dotyczące jakości, powiernictwa i bezpieczeństwa zdefiniowano siedem kryteriów, które muszą spełniać informacje:

- efektywność (effectiveness),
- wydajność (efficiency),
- poufność (confidentiality),
- integralność (integrity),
- dostępność (availability),
- zgodność (compliance),
- rzetelność (reliability).

W metodyce wyróżnia się łącznie 34-y procesy IT, które z kolei są pogrupowane w 4-y domeny odpowiadające obszarom odpowiedzialności: planowania, budowania, uruchamiania i monitorowania. COBIT przyporządkowuje każdemu spośród 34-ch procesów IT określone kryteria informacji (spośród 7-u wcześniej wymienionych).

W standardzie tym definiuje się wykonywane cyklicznie czynności IT niezbędne do osiągnięcia mierzalnego rezultatu. Czynności łączą się w procesy IT.

Wyróżnienie procesów IT stwarza możliwość do ustalenia zasobów będących ich właścicielami. „Dla każdego procesu metodyka przedstawia także wzorcową tabelę RACI – ról i odpowiedzialności dotyczących czynności IT, w której zostają określone osoby decyzyjne, odpowiedzialne, konsultowane i informowane" [6]. Szablonową tabelę trzeba jeszcze odnieść do struktury organizacyjnej i zakresów odpowiedzialności pracowników danego urzędu i odpowiednio ją do nich dopasować.

COBIT 4.1 jest obecnie na świecie uznawana za standard budowy ładu informatycznego, czyli IT Governance w organizacjach. Ład organizacyjny w IT ma spowodować, że wykorzystywanie informatyki w instytucjach będzie wspierało osiąganie ich celów i realizację ich strategii. Błędy popełnione na poziomie zarządzania IT Governance spowodują, że będzie jeszcze trudniejszy do ogarnięcia nieład zinformatyzowany. Pojęcie IT Governance występuje w standardach audytu wewnętrznego, realizowanego na mocy znowelizowanej ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. nr 157, poz. 1240). Dodatkowo, Minister Finansów określił standardy kontroli zarządczej obowiązujące w sektorze finansów publicznych (w komunikacie nr 23 z dnia 16 grudnia 2009 r.), które pozostając w zgodzie z takimi jak COSO czy INTOSAL, mają także uwzględniać specyficzne zadania i warunki działania konkretnych urzędów.

Stałym wynikiem audytu IT powinien być raport o stanie informatyzacji jednostki składany kierownikowi urzędu przez kierownika (czy dyrektora) IT. Profesjonalny audyt informatyczny w ostatecznym rozrachunku, przy rozumieniu wzajemnych potrzeb i oczekiwań pomiędzy audytorem IT i kierownikiem jednostki, ma pomóc w podejmowaniu inwestycji, opartych na racjonalnym osądzie. Nie może to być badanie, w którym kontrolowani nie upatrują żadnych wartości a jedynie widzą skutki w postaci kar regulaminowych lub kodeksowych.

5. Wnioski

Badanie poprawności wymaganych rozwiązań w oprogramowaniu interfejsowym systemu teleinformatycznego dokonywane jest przez jego twórcę albo inny podmiot

posiadający autorskie prawa majątkowe do tego oprogramowania. Mogą zatem zachodzić uzasadnione wątpliwości co do obiektywizmu podmiotów wykonujących badanie.

Zastąpienie egzaminu państwowego międzynarodowymi certyfikatami budzi dezaprobatę. W sytuacji, gdy mała liczba osób przystępowała do egzaminu państwowego lepszym rozwiązaniem byłoby dodanie określonych certyfikatów predestynujących do bycia kontrolerem i utrzymanie uprawnień uzyskanych poprzez pozytywne złożenie egzaminu przed komisją państwową.

Kontrolę realizacji projektów informatycznych o publicznym zastosowaniu należy przeprowadzać dopiero wówczas, gdy jest się wyposażonym w zbiór najlepszych praktyk ITIL, najnowszą wersję Cobit 4.1, normy ISO/IEC 20000 (jedyna oficjalna norma w obszarze zarządzania usługami informatycznymi) i 27001 (norma międzynarodowa określająca wymogi dotyczące systemów zarządzania bezpieczeństwem informacji) i np. w metodykę zarządzania projektami PRINCE2 ze względu na jej światowy rodowód w sektorze publicznym. Można również zamówić audyt IT jako usługę zewnętrzną u profesjonalnego audytora IT posiadającego doświadczenie zawodowe poparte certyfikatami (CISA, CISM, CGEIT, CRISC) oraz potrafiącego zarządzać ryzykiem w projektach informatycznych. Są to fundamentalne podstawy dla dobrze wydatkowanych pieniędzy na audyt IT.

Audyt informatyczny powinien pełnić skuteczną i wiarygodną rolę diagnostyczną a także usprawniającą i doradczą dla kontrolowanej jednostki. Dzięki niezależnej i profesjonalnej formie takiego badania, przeprowadzonego zgodnie z najlepszymi praktykami można bowiem potwierdzić skuteczność, efektywność i wiarygodność funkcjonowania obszaru IT kontrolowanego podmiotu.

Literatura

1. Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne z dnia 17 lutego 2005 r. .
2. Znowelizowana ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne na podstawie ustawy z dnia 12 lutego 2010 r. .
3. Malczewska A.: Nadchodzi kontrola. IT w administracji, wrzesień, 2010, str. 13-15.
4. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji w sprawie wykazu certyfikatów uprawniających do prowadzenia kontroli projektów informatycznych i systemów teleinformatycznych z dnia 10 września 2010 r.
5. Welenc P.: Spojrzenie na audyt informatyczny. IT w administracji, wrzesień, 2010, str. 20-22.
6. Karczewska J.: Metodyka audytów systemów IT. IT w administracji, wrzesień, 2010, str. 18-19.

Dr Anna KACZOROWSKA
Katedra Informatyki
Wydział Zarządzania
Uniwersytet Łódzki
90-237 Łódź, ul. Matejki 22/26
Tel./fax.: (0-42) 635 50 45 / 635 50 17
e-mail: annak@wzmail.uni.lodz.pl