ZESZYTY NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO nr 833
Finanse, Rynki Finansowe, Ubezpieczenia nr 72 (2014)
s. 107–119

Bezpieczeństwo informacji – dylematy związane z realizacją obowiązku prowadzenia audytu wewnętrznego w jednostkach sektora finansów publicznych

Anna Myśko[*], **Ewelina Młodzik**[**]

Streszczenie: *Cel* – Celem artykułu jest przedstawienie praktycznych aspektów związanych z realizacją obowiązku prowadzenia corocznego audytu wewnętrznego w zakresie bezpieczeństwa informacji w jednostkach sektora finansów publicznych.
Metodologia badania – W artykule dokonano analizy porównawczej aktów prawnych regulujących tematykę bezpieczeństwa informacji w sektorze publicznym.
Wynik – Przedstawiona analiza problemowa stanowi próbę ujęcia i usystematyzowania terminologii związanej z bezpieczeństwem informacji, niezbędnej do realizacji obowiązku prowadzenia corocznego audytu wewnętrznego m.in. w jednostkach sektora finansów publicznych.
Oryginalność/Wartość – Zasygnalizowane przez autorki rozbieżności interpretacyjne mogą stanowić materiał pomocniczy dla osób odpowiedzialnych za konstrukcję systemu bezpieczeństwa informacji w jednostkach sektora finansów publicznych.

Słowa kluczowe: bezpieczeństwo informacji, bezpieczeństwo systemów informatycznych (teleinformatycznych), audyt bezpieczeństwa informacji, minimalne wymagania dla systemu teleinformatycznego

Wprowadzenie

Przepis § 20 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (DzU poz. 526, zwanego dalej: rozporządzeniem w sprawie Krajowych Ram Interoperacyjności) zobowiązał kierownictwo podmiotów publicznych do realizacji zadań w zakresie zarządzania bezpieczeństwem informacji. Wymogiem, który wywołał burzliwą dyskusję wśród audytorów wewnętrznych zatrudnionych w jednostkach sektora finansów publicznych stał się obowiązek zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji nie rzadziej niż raz na rok.

[*] mgr Anna Myśko, CGAP, audytor wewnętrzny w jednostkach sektora finansów publicznych; auditor wiodący systemu zarządzania bezpieczeństwem informacji wg normy PN-ISO/IEC 27001:2007.
[**] mgr Ewelina Młodzik, Uniwersytet Szczeciński, Wydział Nauk Ekonomicznych i Zarządzania, Instytut Rachunkowości, ewelina.mlodzik@wneiz.pl.

Z wypełnieniem obowiązku związanego z audytem bezpieczeństwa informacji pojawił się szereg wątpliwości dotyczących sposobu jego realizacji. Dla jednostek sektora publicznego pomocne stały się opublikowane na stronie Ministerstwa Finansów dokumenty, tj.: *Wspólne stanowisko Departamentu Informatyzacji Ministerstwa Administracji i Cyfryzacji oraz Departamentu Audytu Sektora Finansów Publicznych Ministerstwa Finansów odnośnie zapewnienia audytu wewnętrznego w zakresie bezpieczeństwa informacji* oraz *Wytyczne dotyczące prowadzenia audytu bezpieczeństwa informacji przez komórkę audytu wewnętrznego*.

1. Bezpieczeństwo informacji a bezpieczeństwo informatyczne. System informatyczny a system teleinformatyczny – problemy interpretacyjne

Informacja jest obecnie jednym z najcenniejszych zasobów współczesnej organizacji. Z punktu widzenia biznesowego informacje posiadają określoną wartość dla organizacji, dlatego powinny w celu zapewnienia ich bezpieczeństwa i ciągłości działania być chronione, co może okazać się niezbędne do osiągnięcia rentowności, zachowania płynności finansowej i zgodności działalności z przepisami prawa oraz utrzymania reputacji przez jednostkę.

Zasoby informacyjne jednostek przechowywane są zarówno w postaci tradycyjnej, np. papierowej, jak i w systemach informatycznych. Przetwarzanie informacji w warunkach stałego poszukiwania sposobów ograniczenia warunków niepewności podejmowanych decyzji, a zatem ograniczania ryzyka strat i dążenia tym samym do zwiększenia szans sukcesu, powoduje, że zasoby informacji są stale narażone na nieuprawniony dostęp, modyfikację, czy nawet częściową lub całkowitą utratę. Działania tego rodzaju mogą być dokonane zarówno z zewnątrz jednostki, jak i z wnętrza organizacji, zarówno świadomie, jak i nieświadomie (Pazio 2010: 176).

Bezpieczeństwo informacji jest istotne zarówno dla podmiotów sektora prywatnego, jak i jednostek sektora publicznego. W efekcie coraz większego uzależnienia od sieci Internet informacje są narażone na coraz to większą liczbę i różnorodność zagrożeń. Niezbędna jest więc implementacja odpowiednich środków bezpieczeństwa w celu ochrony informacji przed celowym lub nieumyślnym jej zmodyfikowaniem, zniszczeniem czy ujawnieniem.

Podstawowe atrybuty informacji związane z jej ochroną to (Pazio 2010: 176–177):

- poufność (tajność) – informuje o stopniu ochrony, przy czym stopień ten jest ustalany przez wytwórcę lub dostawcę informacji lub użytkownika, bądź odbiorcę informacji. Poufność oznacza, że informacja dostępna jest tylko osobom upoważnionym; poufność jest zatem stopniowalna;
- integralność – oznacza, że informacje są poprawne, nienaruszone i niezmanipulowane, czyli dokładne i kompletne;
- dostępność – informuje o zakresie i upoważnieniu osób mających dostęp do informacji i związanych z nią aktywów, gdy jest to potrzebne.

Określenie bezpieczeństwa informacji w jednostce będzie zależało w szczególności od ram prawnych, na podstawie których i w ramach których funkcjonuje dany podmiot. Do zasadniczych aktów prawnych regulujących problematykę bezpieczeństwa informacji w jednostkach sektora finansów publicznych należy zaliczyć:

1) Ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych,
2) Ustawę z dnia 6 września 2001 r. o dostępie do informacji publicznej,

3) Ustawę z dnia 18 września 2001 r. o podpisie elektronicznym,
4) Ustawę z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną,
5) Ustawę z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (zwaną dalej: Ustawą o informatyzacji działalności podmiotów realizujących zadania publiczne),
6) Ustawę z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych,
7) Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

W ujęciu K. Lidermana (2008: 12–13) ochrona informacji jest zagadnieniem szerokim i generalnie wiąże się z tzw. bezpieczeństwem informacyjnym obejmującym wszystkie formy wymiany, przechowywania i przetwarzania informacji. Natomiast tzw. bezpieczeństwo teleinformatyczne odnosi się do węższego zakresu form wymiany, przechowywania i przetwarzania informacji, ograniczonego do technicznych środków łączności (telefony stacjonarne i komórkowe, radiostacje, sieci i systemy komputerowe, itd.). Bezpieczeństwo teleinformatyczne dotyczy informacji przesyłanych i przetwarzanych w sieciach i systemach teleinformatycznych.

Analizując literaturę przedmiotu, w tym akty prawne, można zauważyć, że nierzadko pojęcie „bezpieczeństwo informacji" jest utożsamiane z pojęciem „bezpieczeństwo informatyczne" bądź „bezpieczeństwo teleinformatyczne". Dodatkową wątpliwość wzbudza stosowanie zamiennie terminu „system informatyczny" i „system teleinformatyczny". Nasuwa się zatem pytanie, czy „system informatyczny" należy traktować jako synonim „systemu teleinformatycznego".

Do pojęcia systemu informatycznego odwołują się przepisy ustawy o ochronie danych osobowych (Ustawa z dnia 29 sierpnia 1997 r.). W myśl art. 7 pkt 2a ww. ustawy przez system informatyczny należy rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

System informatyczny jest to zbiór powiązanych ze sobą elementów, którego funkcją jest przetwarzanie danych przy użyciu techniki komputerowej. Na systemy informatyczne składają się obecnie takie elementy jak sprzęt – głównie komputery oraz urządzenia służące do przechowywania danych, urządzenia służące do komunikacji między sprzętowymi elementami systemu, urządzenia służące do komunikacji między ludźmi a komputerami, urządzenia służące do odbierania danych z otoczenia zewnętrznego – nie od ludzi, np. kamery, skanery, czujniki elektroniczne (Wójcik 2011: 8).

Z kolei w ustawie o informatyzacji działalności podmiotów realizujących zadania publiczne, w ustawie o ochronie informacji niejawnych (Ustawa z dnia 5 sierpnia 2010 r.) oraz w ustawie o świadczeniu usług drogą elektroniczną (Ustawa z dnia 18 lipca 2002 r.) operuje się pojęciem systemu teleinformatycznego.

W świetle powyższych przepisów system teleinformatyczny to zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy – Prawo telekomunikacyjne (Ustawa z dnia 16 lipca 2004 r.).

Dla wyjaśnienia różnic między systemem informatycznym i systemem teleinformatycznym warto odwołać się w tym miejscu do zapisów *Rekomendacji D dotyczącej zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach*, zgodnie z którą na środowisko teleinformatyczne składa się infrastruktura teleinformatyczna jednostki wraz z wykorzystującymi ją systemami informatycznymi oraz eksploatowane w jednostce systemy informatyczne wspierające jego działalność, oparte na infrastrukturze teleinformatycznej zapewnianej przez podmioty zewnętrzne (Komisja Nadzoru Finansowego 2013: 7).

Infrastrukturę teleinformatyczną definiuje się jako zespół urządzeń i łączy transmisyjnych, obejmujący w szczególności platformy sprzętowe (w tym: serwery, macierze, stacje robocze), sieć teleinformatyczną (w tym: routery, przełączniki, zapory sieciowe oraz inne urządzenia sieciowe), oprogramowanie systemowe (w tym systemy operacyjne i systemy zarządzania bazami danych) oraz inne elementy umożliwiające bezawaryjną i bezpieczną pracę ww. zasobów (w tym zasilacze UPS, generatory prądotwórcze, urządzenia klimatyzacyjne), także te wykorzystywane w ośrodkach zapasowych jednostki (Komisja Nadzoru Finansowego 2013: 6).

Ze względu na znaczny postęp technologiczny system teleinformatyczny ułatwia działanie systemu informatycznego, ponieważ poszerza go o transmisję danych za pomocą elektronicznej sieci komunikacyjnej.

Na podstawie dotychczasowych rozważań należy zatem stwierdzić, że między systemem informatycznym a systemem teleinformatycznym nie należy stawiać znaku równości.

Kolejną problematyczną kwestią, która wymaga wyeksponowania, jest treść § 20 rozporządzenia w sprawie Krajowych Ram Interoperacyjności.

Jak wynika już z samej nazwy ww. rozporządzenia, regulacje w nim zawarte odnoszą się do zagadnień związanych z systemami teleinformatycznymi. Natomiast w § 20 ust. 2 wskazuje się na pojęcie bezpieczeństwa informacji. Należy domniemywać, że użycie terminu „bezpieczeństwo informacji" jest wynikiem bezpośredniego przeniesienia pojęć stosowanych w Polskiej Normie PN-ISO/IEC 27001, gdzie zdefiniowano pojęcie systemu zarządzania bezpieczeństwem informacji jako (Polski Komitet Normalizacyjny 2007: 9): część całościowego systemu zarządzania, oparta na podejściu wynikającym z ryzyka biznesowego, odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji.

Zgodnie z treścią rozporządzenia w sprawie Krajowych Ram Interoperacyjności (§ 20 ust. 2 pkt 14) zarządzanie bezpieczeństwem informacji realizowane jest w szczególności poprzez zapewnienie przez kierownictwo podmiotu publicznego okresowego audytu wewnętrznego w zakresie bezpieczeństwa, nie rzadziej niż raz na rok. Pojawia się jednak wątpliwość, czy audytorzy mają ograniczać badanie tylko do audytu systemu informatycznego (teleinformatycznego).

Następną kwestią wymagającą podkreślenia jest rozróżnienie pojęć „system informacyjny" i „system informatyczny".

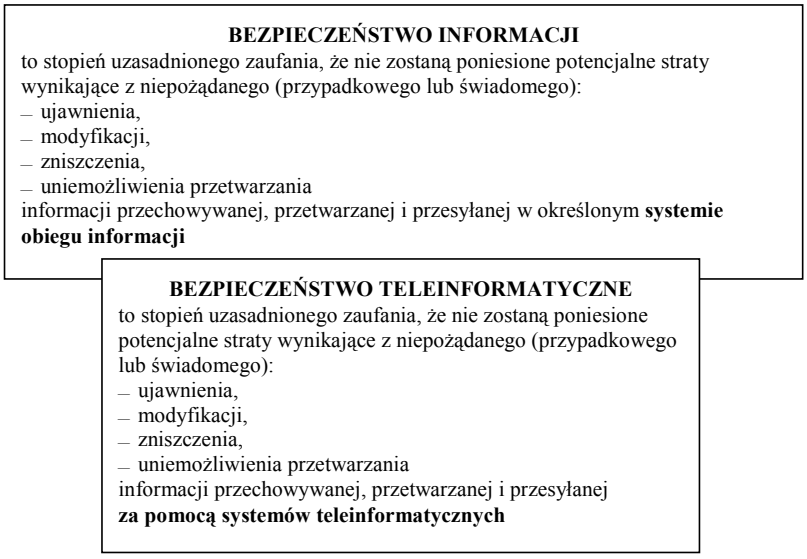
Jak wskazuje M. Kuraś, w ślad za rozprzestrzenianiem nowych technologii, w miejsce pojęcia „system informacyjny" pojawiło się nowe pojęcie „system informatyczny". Pojęcia te zdaniem autora nieustannie wiążą się z nieporozumieniami. Przyczyna tych błędów interpretacyjnych wynika w dużej mierze z niejednoznacznego rozumienia pojęcia „informacji", która bywa często traktowana jako jednoznaczna z pojęciem „dana".

„Dana" to reprezentacja fizyczna elementarnej części informacji. Jest wykorzystywana do rejestrowania informacji i jej przekazu. W praktyce języka codziennego zamiennie uży-

wa się pojęć „informacje" i „dane", w celu uproszczenia komunikacji, czego następstwem mogą być wskazane nieporozumienia (Kuraś: 3).

Słuszne wydaje się przywołanie za autorem definicji systemu informacyjnego w ujęciu W. Steinmüllera. System informacyjny został zdefiniowany przez W. Steinmüllera jako system społeczny, który współtworzą elementy przynależne do pięciu klas: dane, metody, technika (wykorzystywana technologia – wyposażenie techniczne), organizacja, ludzie. Przyjęcie takiego podejścia jednoznacznie wskazuje, że natura systemu informacyjnego nie pozwala go zakwalifikować do klasy systemów sztucznych (artefaktów). W oparciu o tę definicję można wnioskować, że system informatyczny nie jest synonimem systemu informacyjnego, gdyż jest on artefaktem (rozwiązaniem technicznym), który służy do wykonywania (w procesie automatycznym) pewnego podzbioru funkcji spośród ogółu oczekiwanych od systemu informacyjnego (Kuraś: 6).

Z kolei podążając za stanowiskiem K. Lidermana (2008: 12–13), trafne wydaje się stwierdzenie, że systemy teleinformatyczne są częścią obiegu informacji. Dla rozróżnienia powyższych pojęć autor wskazuje na następujące definicje terminu „bezpieczeństwo informacji" oraz terminu „bezpieczeństwo teleinformatyczne", zaprezentowane na rysunku 1.



Rysunek 1. Bezpieczeństwo informacji a bezpieczeństwo informatyczne (teleinformatyczne)

Źródło: opracowanie własne na podstawie (Liderman 2008).

Bezpieczeństwo teleinformatyczne/informatyczne stanowi jeden z obszarów, który może zostać poddany badaniu w ramach audytu systemu bezpieczeństwa informacji w jednostce.

Zdaniem M. Gałacha (2005: 5) wdrożenie i utrzymywanie efektywnych zasad zarządzania bezpieczeństwem systemu informatycznego jest jednym z podstawowych elementów zapewnienia ochrony informacji przetwarzanych we współczesnej organizacji. Nieau-

toryzowany wypływ informacji, utrata danych czy uszkodzenie lub zniszczenie zasobów informatycznych, mogą narazić organizację na poważne problemy oraz straty finansowe (Forystek 2005: 155).

Oprócz systemów informatycznych/teleinformatycznych w podmiotach sektora publicznego zakres podmiotowy audytu bezpieczeństwa informacji można rozszerzyć o następujące zagadnienia:

1) ochrona danych osobowych,
2) ochrona informacji niejawnych,
3) udostępnianie informacji publicznej,
4) ochrona informacji objętych tajemnicą, np. skarbową.

Zasygnalizowane trudności interpretacyjne mogą wskazywać na potrzebę zachowania spójności między zapisami zawartymi w różnych aktach prawnych regulujących zagadnienia bezpieczeństwa informacji. Dodatkowo w celu ułatwienia realizacji zadania, polegającego na zapewnieniu okresowych audytów bezpieczeństwa informacji, zasadne jest sformułowanie jasnych wytycznych precyzujących w sposób dokładny zakres przedmiotowy audytu.

2. Propozycje rozwiązań organizacyjnych w zakresie prowadzenia audytu bezpieczeństwa informacji w jednostkach sektora finansów publicznych

Przechodząc do rozważań praktycznych, należy wskazać, że obowiązek wskazany w § 20 ust. 2 rozporządzenia w sprawie Krajowych Ram Interoperacyjności, dotyczący w szczególności (w pkt 14) zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji nie rzadziej niż raz na rok, ma być realizowany przez kierownictwo podmiotu publicznego. Przez podmiot publiczny należy rozumieć jeden z podmiotów zdefiniowanych w art. 2 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, np.: organy administracji rządowej, organy kontroli państwowej i ochrony prawa, sądów, jednostek organizacyjnych prokuratury, a także jednostek samorządu terytorialnego i ich organów, jednostki budżetowe i samorządowe zakłady budżetowe.

Rozważając kwestie organizacyjne prowadzenia corocznego audytu, należy wziąć pod uwagę:

- osoby lub podmioty, które będą go wykonywały,
- zakres przedmiotowy realizowanych audytów wewnętrznych.

Mając powyższe na względzie, można wskazać na możliwe do zastosowania w praktyce rozwiązania organizacyjne:

- organizacja audytu wewnętrznego systemu bezpieczeństwa informacji,
- certyfikacja systemu bezpieczeństwa informacji,
- zlecenie przeprowadzenia corocznego audytu wewnętrznego – bez certyfikacji systemu zarządzania bezpieczeństwem informacji,
- powierzenie prowadzenia corocznego audytu wewnętrznego systemu bezpieczeństwa informacji komórkom audytu wewnętrznego, o którym mowa w ustawie o finansach publicznych,
- forma prowadzenia corocznych obowiązkowych audytów bezpieczeństwa informacji oraz zakres przedmiotowy realizowanych audytów wewnętrznych.

W rozporządzeniu w sprawie Krajowych Ram Interoperacyjności wskazano jedynie na sam obowiązek prowadzenia corocznego audytu wewnętrznego, bez określania jakichkol-

wiek wymogów w zakresie sposobu oraz trybu realizacji czy też formy prowadzonych audytów oraz wymogów stawianych osobom, które miałyby realizować na rzecz podmiotu publicznego ww. zadanie.

Wobec powyższego należy wnioskować, że decyzję w zakresie doboru rozwiązań organizacyjnych (obejmujących m.in. sposób, formę oraz wykonawcę) stosowanych w zakresie realizacji obowiązku prowadzenia corocznego audytu wewnętrznego bezpieczeństwa informacji podejmuje kierownictwo jednostki.

Jest to bardzo istotne, ponieważ daje możliwość dostosowania rozwiązań organizacyjnych i zakresu merytorycznego do indywidualnej specyfiki każdego podmiotu publicznego realizującego zadania publiczne. Będzie się odbywało z uwzględnieniem zasobów, którymi dysponuje jednostka: kadrowych (zatrudnianie pracowników, którzy będą mogli przeprowadzić czynności audytowe) oraz finansowych (ewentualne decyzje związane ze zleceniem czynności na zewnątrz organizacji – outsourcing).

Jednym z rozwiązań organizacyjnych możliwych do zastosowania jest wdrożenie w jednostce systemu zarządzania bezpieczeństwem w oparciu o normę PN-ISO/IEC 27001[1] potwierdzonego uzyskaniem certyfikatu.

Zgodnie z brzmieniem § 20 ust. 3 rozporządzenia w sprawie Krajowych Ram Interoperacyjności, jeżeli system zarządzania bezpieczeństwem został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie polskich norm związanych z tą normą, wymagania określone w § 20 ust. 1 i 2 ww. rozporządzenia uznaje się za spełnione.

Należy podkreślić, że za spełnienie wymagań uznaje się nie tylko samo ustanowienie zabezpieczeń oraz zarządzanie ryzykiem, ale także, co ważne, bieżące audytowanie.

Zgodnie z wymogami PN-ISO/IEC 27001 audytowanie jest wymagane. Wobec powyższego funkcjonowanie systemu zarządzania bezpieczeństwem poddawanego badaniu w rokrocznych audytach wewnętrznych prowadzonych w ramach ww. normy wyczerpuje obowiązek nałożony przepisami analizowanego rozporządzenia. Proces audytu stanowi element systemu zarządzania bezpieczeństwem ujętym w normie.

Wdrażanie oraz certyfikacja zgodności z wymaganiami normy jest dokonywana przez profesjonalne podmioty działające na rynku, posiadające stosowne akredytacje. W ramach posiadanego certyfikatu prowadzone są audyty tzw. pierwszej strony (wewnętrzne), drugiej strony (np. partnerów, kontrahentów) oraz trzeciej strony (audyty certyfikujące i recertyfikujące).

Na skutek certyfikacji podmiot jest poddany ciągłemu procesowi badania – audytowania, wobec czego nie ma konieczności podejmowania innych działań.

Podmioty zobowiązane mogą również podjąć decyzję o sposobie realizacji obowiązku prowadzenia corocznego audytu wewnętrznego z zakresu bezpieczeństwa informacji bez certyfikacji systemu zarządzania bezpieczeństwem informacji zgodnie z wymogami PN-ISO/IEC 27001. W tym przypadku można zdecydować się na zlecenie prowadzenia ww. audytów osobom lub podmiotom zewnętrznym lub osobom wewnątrz jednostki.

Ze względu na fakt, że rozporządzenie w sprawie Krajowych Ram Interoperacyjności nie wskazuje na minimalne kwalifikacje osób lub podmiotów, które mogłyby wykonywać

[1] Należy zaznaczyć, że we wrześniu 2013 r. została opublikowana nowa wersja ISO/IEC 27001:2013 zastępująca normę ISO/IEC 27001:2005.

audyty bezpieczeństwa informacji wskazane w § 20 ust. 2 pkt 4 ww. rozporządzenia, istotne jest, by przy wyborze wykonawców mieć na uwadze podstawowe zasady, tj.:

- niezależności i obiektywizmu – audytorzy nie powinni badać swojej własnej pracy, jest to szczególnie istotne w przypadku niewielkich jednostek organizacyjnych, gdzie kierownictwo może chcieć podjąć decyzję o powierzeniu realizacji ww. zadania np. informatykom lub osobom pełniącym funkcję administratora bezpieczeństwa informacji lub które na zlecenie tworzą procedury i realizują czynności związane z bezpieczeństwem informacji;
- znajomości metodologii związanej z prowadzeniem audytu – związanej z procesem audytowania;
- wiedzy i doświadczenia.

Na powyższe wskazuje również *Wspólne stanowisko Departamentu Informatyzacji Ministerstwa Administracji i Cyfryzacji i Departamentu Audytu Sektora Finansów Publicznych Ministerstwa Finansów odnośnie zapewnienia audytu wewnętrznego w zakresie bezpieczeństwa informacji*, w którym stwierdza się, że: „Kryteriami, jakimi należy się kierować przy wyborze osób/komórek organizacyjnych prowadzących audyt w zakresie bezpieczeństwa informacji, są: odpowiednie kwalifikacje, doświadczenie, znajomość metodyki audytu w zakresie bezpieczeństwa informacji, a także niezależność od obszaru audytowanego. W razie wątpliwości, przy wyborze osób/komórek organizacyjnych prowadzących ww. audyt można brać pod uwagę wymogi wskazane w normach wymienionych w § 20 ust. 3 rozporządzenia".

Użycie w treści rozporządzenia w sprawie Krajowych Ram Interoperacyjności sformułowania „audyt wewnętrzny" spowodowało wątpliwość interpretacyjną. Zagadnienie związane z realizacją ww. obowiązku mogło być bowiem postrzegane jako zadanie obligatoryjne, które można bezpośrednio przypisać do realizacji komórek audytu wewnętrznego funkcjonujących w strukturach jednostek sektora finansów publicznych lub zewnętrznych usługodawców audytu wewnętrznego.

Zgodnie z brzmieniem art. 272 ust. 1 ustawy o finansach publicznych (Ustawa z dnia 27 sierpnia 2009 r.): „Audyt wewnętrzny jest działalnością niezależną i obiektywną, której celem jest wspieranie ministra kierującego działem lub kierownika jednostki w realizacji celów i zadań przez systematyczną ocenę kontroli zarządczej oraz czynności doradcze. Ocena ta dotyczy w szczególności adekwatności, skuteczności i efektywności kontroli zarządczej w dziale administracji rządowej lub jednostce".

Ze względu na powyższe konieczne stało się wyjaśnienie powstałej wątpliwości, co nastąpiło we *Wspólnym stanowisku Departamentu Informatyzacji Ministerstwa Administracji i Cyfryzacji i Departamentu Audytu Sektora Finansów Publicznych Ministerstwa Finansów odnośnie zapewnienia audytu wewnętrznego w zakresie bezpieczeństwa informacji.* W ww. dokumencie wskazuje się, że: „Użycie w rozporządzeniu sformułowania «audyt wewnętrzny» nie miało na celu obligatoryjnego przypisania tego obowiązku komórkom audytu wewnętrznego, funkcjonującym w jednostkach sektora finansów publicznych na mocy przepisów Działu VI ustawy o finansach publicznych, zwanymi dalej komórkami audytu wewnętrznego".

Z powyższego wynika, że przypisanie tego obowiązku komórkom audytu wewnętrznego może nastąpić w oparciu o decyzję kierownictwa jednostki.

Podejmując decyzję o powierzeniu prowadzenia audytu wewnętrznego audytorom wewnętrznym jako stałego obszaru badania (corocznie), kierownictwo jednostki musi wziąć pod uwagę, że wyznaczenie stałego obszaru ryzyka do corocznego przeprowadzania zadań

może wpływać na ograniczenie realizacji zadań w innych obszarach ryzyka, z uwagi na ograniczone zasoby komórki audytu wewnętrznego. Wobec powyższego zasadne jest uzgodnienie z audytorem wewnętrznym powierzenia do realizacji ww. obowiązku i potwierdzenie powyższych ustaleń poprzez dokonanie odpowiednich zmian np. w *Karcie audytu wewnętrznego*, tj. dokumencie, który stanowi swego rodzaju umowę z kierownictwem w zakresie obowiązków i zadań wykonywanych przez funkcję audytu wewnętrznego w podmiocie.

Wytyczne dotyczące prowadzenia audytu bezpieczeństwa informacji przez komórkę audytu wewnętrznego, opracowane przez Ministerstwo Finansów, wskazują na najważniejsze zagadnienia, które należy wziąć pod uwagę przy przyjmowaniu realizacji ww. zadania przez komórki audytu wewnętrznego.

Podejście do sposobu przedmiotowego realizacji zadania audytowego będzie uzależnione od specyfiki jednostki. Minimalny wymagany przepisami zakres przedmiotowy został wskazany w § 20 ust. 2 rozporządzenia w sprawie Krajowych Ram Interoperacyjności. Obejmuje on 14 punktów. Badanie może polegać na zweryfikowaniu ich w praktyce.

Można również dokonać badania zgodności systemu zarządzania bezpieczeństwem informacji z normą PN-ISO/IEC 27001, która określa bardziej precyzyjne wymagania.

W przypadku wyznaczenia audytorów wewnętrznych do realizacji ww. obowiązków należy zaznaczyć, że mogą oni realizować zadania audytowe w formie zadań zapewniających, albo czynności doradczych.

Z punktu widzenia wykorzystania wyników prowadzonych czynności istotny jest fakt, że realizacja zadania zapewniającego kończy się sporządzeniem sprawozdania i przekazaniem go kierownikom komórek audytowanych oraz kierownikowi jednostki celem zapoznania się i wdrożenia. Kierownicy, co do zasady, zobligowani są do ustosunkowania się do treści sprawozdania i wdrożenia zaleceń. Natomiast w wyniku czynności doradczych audytor wewnętrzny może przedstawić opinie lub wnioski dotyczące usprawnienia funkcjonowania komórki lub jednostki. Jednakże wnioski i opinie przedstawiane przez audytora wewnętrznego nie są wiążące, co oznacza swobodę w zakresie podjęcia decyzji co do ich wykorzystania i wdrożenia.

W opinii Ministerstwa Finansów audyt w zakresie bezpieczeństwa informacji powinien być prowadzony w formie zadań zapewniających.

W zależności od obszaru objętego systemem zarządzania bezpieczeństwem informacji przedmiotem badania może być cały podmiot lub jego część. Należy mieć na uwadze, że każdy proces zarządzania bezpieczeństwem informacji będzie wyjątkowy, ze względu na specyfikę każdej jednostki: administracji rządowej, jednostki samorządu terytorialnego czy poszczególnej jednostki organizacyjnej samorządu terytorialnego, np. jednostki budżetowej (szkoły), samorządowego zakładu budżetowego (przedszkola) czy samorządowych osób prawnych (samorządowych osób prawnych utworzonych na podstawie odrębnych ustaw, działających jako samorządowe instytucje kultury, np. dom kultury, biblioteka publiczna).

Uwzględniając wielkość, zasoby i możliwości (ludzkie i finansowe), sposób prowadzenia audytu oraz wyniki analizy ryzyka, można rozważać wykonanie badania w poszczególnych obszarach bezpieczeństwa informacji, np. ochrony danych osobowych, ochrony informacji ustawowo chronionej, udostępniania informacji publicznej, itp.

3. Kontrola realizacji obowiązku prowadzenia audytów bezpieczeństwa informacji

Rozporządzenie w sprawie Krajowych Ram Interoperacyjności nie nakłada obowiązku kontrolowania zapewnienia prowadzenia corocznego audytu bezpieczeństwa informacji. Zatem powyższe będzie wykonywane przez zewnętrzne instytucje kontrolne, np. Najwyższą Izbę Kontroli, zgodnie z ogólnymi zasadami kontroli jednostek sektora finansów publicznych.

Na wewnętrzne potrzeby jednostek sektora finansów publicznych możliwe jest jednak ujęcie w ramach sprawowania kontroli zarządczej kontrolowania przeprowadzania corocznego audytu wewnętrznego systemu bezpieczeństwa informacji.

Zgodnie z brzmieniem art. 68 ust. 2 ustawy o finansach publicznych: „Celem kontroli zarządczej jest zapewnienie w szczególności m.in.: zgodności działalności z przepisami prawa oraz procedurami wewnętrznymi; ochrony zasobów; przestrzegania i promowania zasad etycznego postępowania; efektywności i skuteczności przepływu informacji; zarządzania ryzykiem".

Uwzględniając dwa poziomy funkcjonowania kontroli zarządczej w sektorze finansów publicznych, należy wskazać, że kierownik każdej jednostki w ww. sektorze odpowiada za jej funkcjonowanie (I poziom kontroli zarządczej). Zgodnie z Komunikatem nr 23 Ministra Finansów z dnia 16 grudnia 2009 r. w sprawie standardów kontroli zarządczej dla sektora finansów publicznych: „W ramach administracji rządowej i samorządowej powinna funkcjonować kontrola zarządcza odpowiednio na poziomie działu administracji rządowej, a także jednostki samorządu terytorialnego (II poziom kontroli zarządczej). Za funkcjonowanie kontroli zarządczej na tym poziomie odpowiada odpowiednio minister kierujący danym działem administracji rządowej oraz wójt (burmistrz, prezydent miasta), starosta albo marszałek województwa w przypadku samorządu terytorialnego. Minister jest odpowiedzialny za zapewnienie adekwatnego, skutecznego i efektywnego systemu kontroli zarządczej w ministerstwie (jako kierownik jednostki) oraz w dziale administracji rządowej (jako minister kierujący działem). Wójt (burmistrz, prezydent miasta), starosta oraz marszałek województwa jest odpowiedzialny za zapewnienie adekwatnego, skutecznego i efektywnego systemu kontroli zarządczej w urzędzie gminy (urzędzie miasta), starostwie powiatowym lub urzędzie marszałkowskim, a także w jednostce samorządu terytorialnego".

Monitorowanie wywiązywania się z corocznej realizacji audytu wewnętrznego systemu bezpieczeństwa informacji możliwe jest na każdym z ww. poziomów kontroli zarządczej.

Ponadto należy zwrócić uwagę na specyfikę jednostek „podsektora samorządowego", która wynika z jego samorządności i zróżnicowania wielkości tworzących go jednostek organizacyjnych. W tym przypadku wójt (burmistrz, prezydent miasta), starosta oraz marszałek województwa jest kierownikiem jednostki na II poziomie kontroli zarządczej i musi zwrócić uwagę na funkcjonowanie systemu kontroli zarządczej w całej podległej mu jednostce. W tym przypadku zaleca się kierownikom jednostek samorządu terytorialnego dokonanie przeglądu realizacji przedmiotowego obowiązku prowadzenia audytów bezpieczeństwa informacji przez kierowników jednostek organizacyjnych samorządu terytorialnego.

W zależności od konstrukcji systemu kontroli zarządczej w danej jednostce samorządu terytorialnego działania można ograniczyć minimalnie np. do zebrania informacji od poszczególnych kierowników jednostek organizacyjnych w zakresie obowiązku realizacji, ze względu na wrażliwe elementy systemu kontroli zarządczej, jakimi są w szczególności:

- zapewnienie ciągłości działania,
- ochrona zasobów,
- mechanizmy kontroli dotyczące systemów informatycznych służące zapewnieniu bezpieczeństwa danych i systemów informatycznych.

Należy także zaznaczyć, że pomimo braku wskazania w przepisach prawa obowiązku kontrolowania zapewnienia prowadzenia corocznego audytu bezpieczeństwa informacji, przepisy ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne nakładają obowiązek kontroli działania systemów informatycznych używanych do realizacji zadań publicznych, a także określają minimalne wymagania stawiane osobom lub podmiotom przeprowadzającym ww. kontrolę. Zgodnie z ww. regulacją kontroli systemów informatycznych używanych do realizacji zadań publicznych dokonują:

- w jednostkach samorządu terytorialnego i ich związkach oraz w tworzonych lub prowadzonych przez te jednostki samorządowych osobach prawnych i innych samorządowych jednostkach organizacyjnych – co do zasady właściwy wojewoda,
- w podmiotach publicznych podległych lub nadzorowanych przez organy administracji rządowej – organ administracji rządowej nadzorujący dany podmiot publiczny,
- w podmiotach publicznych niewymienionych w powyższych punktach – minister właściwy do spraw informatyzacji.

Należy zaznaczyć, że w stosunku do jednostek samorządu terytorialnego i ich związków oraz w tworzonych lub prowadzonych przez te jednostki samorządowych osobach prawnych i innych samorządowych jednostkach organizacyjnych kontrola może dotyczyć wyłącznie systemów teleinformatycznych oraz rejestrów publicznych, które są używane do realizacji zadań zleconych z zakresu administracji rządowej. W pozostałych przypadkach kontrola przeprowadzana jest na wniosek zgodnie z przepisami prawa.

Uwagi końcowe

Zakres badania systemu bezpieczeństwa informacji będzie zależał w szczególności od ram prawnych, na podstawie których i w ramach których funkcjonuje dany podmiot. W administracji publicznej szczególnie istotne są obszary związane z ochroną danych osobowych (Ustawa z dnia 29 sierpnia 1997 r. wraz z aktami wykonawczymi), tajemnicą ustawowo chronioną (Ustawa z dnia 5 sierpnia 2010 r. wraz z aktami wykonawczymi), udostępnianiem informacji publicznej (Ustawa z dnia 6 września 2001 r. wraz z aktami wykonawczymi), tajemnicą skarbową i inne.

Wdrożenie obowiązku prowadzenia audytów bezpieczeństwa jest istotne ze względu na możliwość sprawowania bieżącej weryfikacji w zakresie skuteczności, efektywności, adekwatności systemu zarządzania bezpieczeństwem informacji, a nie tylko bezpieczeństwa informatycznego w jednostce.

Literatura

Forystek M. (2005), *Audyt informatyczny*, InfoAudit, Warszawa.

Gałach A. (2005), *Zarządzanie bezpieczeństwem systemu informatycznego – uniwersalna lista kontrolna*, ODDK, Gdańsk.

Komunikat nr 23 Ministra Finansów z dnia 16 grudnia 2009 r. w sprawie standardów kontroli zarządczej dla sektora finansów publicznych, Dz. Urz. nr 15, poz. 84.

Kuraś M., *System informacyjny – System informatyczny. Co poza nazwą różni te dwa obiekty?*, http://www.uci.agh.edu.pl/uczelnia/tad/PSI11/art/SI-vs-SIT.pdf. [27.06.2014].
Liderman K. (2008), *Analiza ryzyka i ochrona informacji w systemach komputerowych*, PWN, Warszawa.
Pazio N. (2010), *Polityka bezpieczeństwa jako element zarządzania ryzykiem operacyjnym*, w: *Zarządzanie ryzykiem działalności organizacji*, red. J. Monkiewicz, L. Gąsiorkiewicz, Wydawnictwo C.H. Beck, Warszawa.
Polski Komitet Normalizacyjny (2007), *Polska Norma PN-ISO/IEC 27001:2007. Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania*, Warszawa.
Praktyczne aspekty audytu wewnętrznego (2004), red. H. Grocholski, Instytut Rachunkowości i Podatków, Warszawa.
Rekomendacja D dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach (2013), Komisja Nadzoru Finansowego, Warszawa.
Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, DzU poz. 526.
Rozporządzenie Ministra Finansów z dnia 1 lutego 2010 r. w sprawie przeprowadzania i dokumentowania audytu wewnętrznego, DzU nr 21, poz. 108.
Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych, DzU z 2013 r. poz. 885 z późn. zm.
Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, DzU z 2002 r. nr 101, poz. 926 z późn. zm.
Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej, DzU z 2014 r. poz. 782.
Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, DzU nr 144, poz. 1204 z późn. zm.
Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, DzU z 2013 r. poz. 235 ze zm.
Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, DzU nr 182, poz. 1228.
Wójcik W. (2011), *Systemy teleinformatyczne*, Politechnika Lubelska, Lublin, http://bc.pollub.pl/Content/676/systemy.pdf [27.06.2014].
Wspólne stanowisko Departamentu Informatyzacji Ministerstwa Administracji i Cyfryzacji i Departamentu Audytu Sektora Finansów Publicznych Ministerstwa Finansów odnośnie zapewnienia audytu wewnętrznego w zakresie bezpieczeństwa informacji, Ministerstwo Finansów, http://www.mf.gov.pl/ministerstwo-finansow/dzialalnosc/finanse-publiczne/kontrola-zarzadcza-i-audyt-wewnetrzny/audyt-wewnetrzny-w-sektorze-publicznym/metodyka-i-dobre-praktyki/ [27.06.2014].
Wytyczne dotyczące prowadzenia audytu bezpieczeństwa informacji przez komórkę audytu wewnętrznego, Ministerstwo Finansów, http://www.mf.gov.pl/ministerstwo-finansow/dzialalnosc/finanse-publiczne/kontrola-zarzadcza-i-audyt-wewnetrzny/audyt-wewnetrzny-w-sektorze-publicznym/metodyka-i-dobre-praktyki/ [27.06.2014].

SECURITY OF INFORMATION – DILEMMAS OF REALISATION OF THE NECESSITY OF CONDUCTING INTERNAL AUDIT IN UNITS OF THE PUBLIC FINANCE SECTOR

Abstract: *Purpose* **–** Presentation of practical aspects of realisation of the necessity of conducting the annual internal audit in the area of information security in units of the public sector.
Design/Methodology/approach **–** Comparative analysis if law regulations related to information security in the public sector.
Findings – The presented problem analysis is a try at describing and systematizing terminology related to information security, necessary for realisation of the necessity of conducting the annual internal audit, in units of the public finance sector.
Originality/value – The discrepancies signalised by the authors may be used as a supplementary material for persons responsible for the construction of the information security system in units of the public finance sector.

Keywords: information security, IT system security, audit of information security, minimal requirements for IT systems

Cytowanie

Myśko A., Młodzik E. (2014), *Bezpieczeństwo informacji – dylematy związane z realizacją obowiązku prowadzenia audytu wewnętrznego w jednostkach sektora finansów publicznych*, Zeszyty Naukowe Uniwersytetu Szczecińskiego nr 833, „Finanse, Rynki Finansowe, Ubezpieczenia" nr 72, Szczecin, s. 107–119, www.wneiz.pl/frfu.