DOI: 10.31648/sp.9284

Marcin Janik
Uniwersytet Śląski w Katowicach
ORCID: 0000-0002-6197-2722
kontakt@janikadwokat.pl

Stanisław Hady-Głowiak
Uniwersytet Ekonomiczny w Katowicach
ORCID: 0000-0002-1060-6984
stanislawhg@gmail.com

Bezpieczeństwo informacji jako zadanie jednostek sektora finansów publicznych

Wstęp

Ciągle zmieniająca się rzeczywistość, w tym zmiany organizacyjne i prawne oraz związane z tym ryzyka i zagrożenia wymagają zapewnienia odpowiedniego reagowania. Administracja publiczna stoi przed nowymi wyzwaniami, do których należy bez wątpienia cyfryzacja powodująca powstanie dodatkowych ryzyk i zagrożeń w tym obszarze. Brak zapewnienia skuteczności i efektywności funkcjonowania systemu zarządzania bezpieczeństwem informacji w jednostce może spowodować straty finansowe, wizerunkowe czy przeszkody w zachowaniu ciągłości działania i realizacji założonych celów i zadań. Mając powyższe na uwadze, celem niniejszego artykułu jest wskazanie roli audytu wewnętrznego w zapewnieniu wiarygodnej, niezależnej i obiektywnej oceny dotyczącej tego, czy system zarządzania bezpieczeństwem informacji w jednostce funkcjonuje prawidłowo, a jego poszczególne elementy wypełniają wymogi wynikające z obowiązujących przepisów i norm technicznych. Z drugiej strony zaś zwrócono uwagę na wiedzę i kwalifikacje audytora wewnętrznego w przedmiotowym zakresie oraz wymogi prawne i rolę funkcjonowania audytu wewnętrznego w jednostkach sektora finansów publicznych. Niniejszy artykuł składa się z trzech części i zakończenia. W pierwszym podrozdziale zanalizowano rolę audytu wewnętrznego w zakresie zapewnienia skuteczności i efektywności funkcjonowania systemu zarządzania bezpieczeństwem informacji w jednostce. W kolejnym scharakteryzowane zostały zasady funkcjonowania i rola audytu wewnętrznego jako niezależnego i obiektywnego narzędzia

zapewniającego i doradczego kierownika jednostki. W trzecim podrozdziale wskazano na wymogi prawne w zakresie kwalifikacji i kompetencji interpersonalnych audytora wewnętrznego w zapewnieniu okresowego audytu wewnętrznego w zakresie zarządzania bezpieczeństwem informacji.

Istota audytu wewnętrznego w zakresie zapewnienia skuteczności i efektywności funkcjonowania systemu zarządzania bezpieczeństwem informacji w jednostce

Podstawowym aktywem podlegającym ochronie w każdej organizacji jest informacja. Może przybierać formę papierową, elektroniczną czy głosową, analogicznie do sposobów jej przetwarzania. Coraz bardziej powszechna elektronizacja i cyfryzacja procesów zachodzących w administracji publicznej powoduje powstanie nowych podatności i wymaga odpowiedniego reagowania na wszelkie istniejące i pojawiające się ryzyka i zagrożenia oraz zapewnienia ciągłości działania systemów informatycznych służących do przetwarzania danych, jak również funkcjonowania organizacji zgodnie z obowiązującymi przepisami prawa oraz normami technicznymi. Tym samym audytorzy wewnętrzni powinni posiadać z jednej strony wiedzę i umiejętności praktyczne w zakresie właściwej interpretacji przepisów prawa i stosowania praktyk w dziedzinie bezpieczeństwa informacji, w tym umiejętności przeprowadzania skutecznego badania podatności systemów informatycznych na wszelkie zagrożenia. Z drugiej strony audytor wewnętrzny, jako niezależne i obiektywne narzędzie zapewniające i doradcze kierownika jednostki, powinien dawać zapewnienie, że systemy informatyczne użytkowane przez instytucję wypełniają wymogi wynikające z obowiązujących przepisów i norm technicznych. Nie można również zapomnieć o obowiązku spoczywającym na kierowniku jednostki sektora finansów publicznych w zapewnieniu okresowego audytu wewnętrznego. Obowiązek zapewnienia okresowego audytu wewnętrznego w zakresie zarządzania bezpieczeństwem informacji w jednostkach samorządu terytorialnego wynika z przepisów prawa. Potwierdzenie zgodności i skuteczności działania systemu zarządzania bezpieczeństwem informacji można uzyskać w wyniku przeprowadzonego audytu wewnętrznego [1].

Dopuszczenie do wystąpienia dysfunkcji w obszarze bezpieczeństwa informacji może spowodować w konsekwencji zniekształcenia w zachowaniu ciągłości działania i realizacji założonych celów i zadań. Mogą także pojawić się problemy w utrzymaniu reżimu dotyczącego zarządzania finansami jed-

[1] P. Sołtyk, *System zarządzania bezpieczeństwem informacji w jednostce samorządu terytorialnego przedmiotem oceny audytu wewnętrznego – wątpliwości interpretacyjne*, „Finanse Komunalne" 2016, nr 1–2, s. 126–133, Lex.

nostki, co negatywnie może wpłynąć na wynik finansowy, a w dalszej kolejności – na ocenę przez biegłego rewidenta lub komisji rewizyjnej. Brak skutecznej kontroli nad bezpieczeństwem informacji oznacza także możliwość wystąpienia poważnego ryzyka związanego z utratą danych liczbowych pochodzących z elektronicznych systemów przetwarzających dane. Może to być uzasadnionym problemem w procesie tworzenia stosownych analiz ekonomiczno-finansowych niezbędnych w zarządzaniu jednostką.

Należy pokreślić, że w każdej organizacji – niezależnie od formy prawnej – informacja stanowi podstawę do podejmowania decyzji zarządczych, przez co powinna być kompletna, dokładna, wiarygodna, elastyczna, szybko przetwarzana i ekspediowana na potrzeby kadry zarządzającej, a co najważniejsze – powinna być skutecznie chroniona zgodnie z wymaganiami stawianymi przez prawo[2]. Bezpieczeństwo informacji wiąże się nie tylko z technologią, ale dotyczy również ludzi i procesów. Wdrożenie ISO/IEC 27001 służy promowaniu kultury organizacyjnej, w tym świadomości znaczenia i zasad ochrony danych osobowych. Wiedza i świadomość pracowników w organizacjach funkcjonujących według standardów ISO/IEC 27001 ułatwia wykrywanie i zgłaszanie incydentów związanych z bezpieczeństwem danych[3].

Ministerstwo Finansów opracowało wytyczne dotyczące prowadzenia audytu w zakresie bezpieczeństwa informacji w przypadku powierzenia tego zadania komórce audytu wewnętrznego. W swoich wytycznych Ministerstwo Finansów zwróciło uwagę na to, że jeśli w podmiocie administracyjnym realizacja audytu wewnętrznego w zakresie bezpieczeństwa informacji zostanie powierzona komórce audytu wewnętrznego, to wtedy „przypisanie tego zadania powinno odbyć się w sposób formalny poprzez odpowiednie uzupełnienie karty audytu lub innych dokumentów wewnętrznych określających cel, zakres i uprawnienia audytu wewnętrznego w jednostce, o zapisy jednoznacznie wskazujące komórkę audytu jako odpowiedzialną za realizację tego zadania". Ponadto „audyt w zakresie bezpieczeństwa informacji powinien być prowadzony w formie zadań zapewniających. Realizacja audytu bezpieczeństwa informacji jako zadania zapewniającego następowałaby z uwzględnieniem wymogów określonych w ustawie o finansach publicznych, rozporządzeniu w sprawie przeprowadzania i dokumentowania audytu wewnętrznego oraz w Standardach audytu wewnętrznego"[4].

Jego celem jest ustalenie zgodności funkcjonowania tego sytemu z uregulowaniami wewnętrznymi – normami, politykami w zakresie bezpieczeństwa

---

[2] Ibidem.

[3] T. Soczyński, *Kompetencje i umiejętności inspektora ochrony danych a możliwe mechanizmy certyfikacji*, [w:] T. Wyka, M.A. Mielczarek (red.), *Administrator i inspektor ochrony danych osobowych*, Warszawa 2019.

[4] W. Dziomdziora, *Cyberbezpieczeństwo w samorządzie terytorialnym. Praktyczny przewodnik*, 2021, Lex.

informacji oraz rozpoznanie ewentualnych luk, które negatywnie mogą wpływać na bezpieczeństwo zarządzanej informacji. Zadaniem audytora wewnętrznego jest także ustalenie, czy kierownictwo jednostki w pełni respektuje wymagania prawne określone w rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznych oraz minimalnych wymagań dla systemów teleinformatycznych[5]. Zgodnie z § 20 ust. 1 KRI podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność. Analogicznie zastosowanie ma metodyka ISO/IEC 27001[6]. W świetle wymienionego aktu prawnego kierownik jednostki jest zobowiązany zapewnić warunki umożliwiające realizację i egzekwowanie działań wymienionych w § 20 ust. 2 pkt 1–14 KRI. Katalog ten nie jest zamknięty z uwagi na użycie w treści przywołanego przepisu sformułowania w „szczególności", co oznacza możliwości dopuszczenia do podejmowania także innych działań służących zapewnieniu skutecznego zarządzania bezpieczeństwem informacji. Brak skutecznej kontroli nad bezpieczeństwem informacji oznacza także możliwość wystąpienia poważnego ryzyka związanego z utratą danych liczbowych czerpanych z elektronicznych systemów przetwarzających zapisy w rachunkowości. Może to być uzasadnionym problemem w procesie tworzenia stosownych analiz ekonomiczno-finansowych pomocnych w zarządzaniu jednostką. Należy pokreślić, że w każdej organizacji – niezależnie od formy prawnej – informacja stanowi podstawę do podejmowania decyzji zarządczych, przez co powinna być kompletna, dokładna, wiarygodna, elastyczna, szybko przetwarzana i ekspediowana na potrzeby kadry zarządzającej, a nade wszystko powinna być skutecznie chroniona zgodnie z wymaganiami stawianymi przez prawo[7].

Bardzo istotne jest przeprowadzanie co najmniej raz w roku udokumentowanej analizy ryzyka w zakresie utraty integralności, dostępności lub poufności informacji oraz zapewnienie, aby osoby zaangażowane w proces zarzą-

[5] 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 (t.j. Dz.U. z 2017 r., poz. 2247), dalej jako KRI.

[6] ISO/IEC 27001 to międzynarodowa norma opracowana dla zarządzania bezpieczeństwem informacji. Norma ta określa wymagania dotyczące ustanowienia, wdrożenia, utrzymania i ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji w odniesieniu do organizacji. Norma obejmuje również wymagania dotyczące szacowania i postępowania z ryzykiem dotyczącym bezpieczeństwa informacji, dostosowanych do potrzeb organizacji. Wymogi określone w niniejszej normie międzynarodowej są ogólne i mają zastosowanie do wszystkich organizacji, niezależnie od typu, wielkości i charakteru.

[7] P. Sołtyk, *System zarządzania*..., s. 126–133.

dzania bezpieczeństwem informacji zostały wyposażone w stosowne certyfikaty, uprawnienia po uprzednim odbyciu specjalistycznych szkoleń. Nie należy zapomnieć o zapewnieniu odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na dbałości o aktualizację oprogramowania, zapewnieniu bezpieczeństwa plików systemowych oraz kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa. Ponadto podczas realizacji audytu w tym obszarze zadaniem audytora jest także wyrażanie niezależnej opinii o skuteczności działania systemów bezpieczeństwa informacji na podstawie rozwiązań wynikających z ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej[8], a także wymogów ustanowionych w ustawie z dnia 17 lutego 2005 r.[9] o informatyzacji działalności podmiotów realizujących zadania publiczne[10].

Zasady funkcjonowania i rola audytu wewnętrznego jako niezależnego i obiektywnego narzędzia zapewniającego i doradczego kierownika jednostki

Instytucja audytu wewnętrznego została wprowadzona do polskiego porządku prawnego w celu wzmocnienia ochrony wydatkowania środków Unii Europejskiej. Uznana za doniosłą dla utrzymania ładu finansów publicznych, objęta została reżimem odpowiedzialności za naruszenie dyscypliny finansów publicznych[11]. W administracji publicznej audyt wewnętrzny odgrywa przede wszystkim rolę niezależnego instrumentu wspomagającego skuteczność zarządzania. Dostarcza racjonalnego zapewnienia, że system kontroli zarządczej działa zgodnie z przyjętymi normami. Jednak aby audyt wewnętrzny wypełniał wydajnie i skutecznie swoje cele i zadnia, jego działalność powinna podlegać ocenie i bieżącemu monitorowaniu[12].

Zgodnie z art. 272 ust. 1 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych[13] audyt wewnętrzny jest działalnością niezależną i obiektywną, której celem jest wspieranie ministra kierującego działem lub kierownika jed-

---

[8] Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (t.j. Dz.U. z 2022 r., poz. 902).

[9] Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2021 r., poz. 2070 z późn. zm.).

[10] P. Sołtyk, *System zarządzania*…, s. 126–133.

[11] A. Kamedulska, *Zaniechanie prowadzenia audytu wewnętrznego w świetle naruszenia dyscypliny finansów publicznych*, „Finanse Komunalne" 2020, nr 3, s. 56–70, Lex.

[12] P. Sołtyk, *Problematyka oceny działalności audytu wewnętrznego w jednostkach samorządu terytorialnego w świetle postulatów standardów zawodowych*, „Finanse Komunalne" 2017, nr 1, s. 64–74, Lex.

[13] Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz.U. z 2023 r., poz. 1270 z późn. zm.), dalej jako u.f.p.

nostki w realizacji celów i zadań przez systematyczną ocenę kontroli zarządczej oraz czynności doradcze. Ocena, o której mowa w ust. 1, dotyczy w szczególności adekwatności, skuteczności i efektywności kontroli zarządczej w dziale administracji rządowej lub jednostce[14].

Zdaniem Anny Bartoszewicz nowy kształt definicji zmienił ideę audytu wewnętrznego z aspektu finansowo-rachunkowego i objął swym zakresem wszystkie obszary działania jednostki, skupiając się na realizacji celów całej organizacji. Stało się to za sprawą wprowadzenia do definicji audytu pojęcia kontroli zarządczej[15].

Z kolei Kazimiera Winiarska wskazuje, że rolą audytu wewnętrznego jest omówienie z kierownictwem celów, obowiązków, priorytetów, ograniczeń i sposobu postrzegania ryzyka, przeprowadzenie niezależnej oceny bezpieczeństwa, niezawodności i skuteczności ustaleń kierowniczych, rozważenie czynników mających wpływ na takie ustalenia, omówienie wyników, konkluzji i zaleceń oraz ułatwienie kierownikom znalezienia sposobu rozwiązania bieżących problemów, realizacji ich obowiązków i ustalenie trwałych podstaw przyszłych działań[16].

Bolesław R. Kuc nadaje pojęciu audytu dwa podstawowe znaczenia. W znaczeniu czynnościowym rozumie audyt jako zespół działań bardzo silnie powiązanych z realizacją wewnętrznych celów organizacji. Umiejętności diagnostyczne i kontrolne audytora mają upewnić kierownika, że przyjęte przez niego zasady i procedury funkcjonowania danej instytucji są efektywnie wdrażane, mówiąc innymi słowy skutecznie wykonywane[17].

Audyt wewnętrzny występuje w kontekście kontroli zarządczej w podwójnej roli – z jednej strony jest jednym ze standardów kontroli zarządczej, a z drugiej strony ma zadanie dokonywać systematycznej i uporządkowanej oceny funkcjonowania kontroli zarządczej[18]. Zgodnie z art. 68 ust. 1 u.f.p. kontrolę zarządczą w jednostkach sektora finansów publicznych stanowi ogół działań podejmowanych dla zapewnienia realizacji celów i zadań w sposób zgodny z prawem, efektywny, oszczędny i terminowy. Celem kontroli zarządczej jest zapewnienie w szczególności zgodności działalności z przepisami prawa oraz procedurami wewnętrznymi; skuteczności i efektywności działania; wiarygodności sprawozdań; ochrony zasobów; przestrzegania i promowania zasad etycznego postępowania; efektywności i skuteczności przepływu informacji; zarządzania ryzykiem.

---

[14] A. Kamedulska, op. cit., s. 56–70.

[15] A. Bartoszewicz, *Praktyka funkcjonowania audytu wewnętrznego w Polsce*, Warszawa 2011, s. 11.

[16] K. Winiarska, *Audyt wewnętrzny. Teoria i zastosowanie*, Warszawa 2019, s. 83.

[17] B. Kuc, *Kontrola – kontroling – audyt. 3w1. Podobieństwa i różnice*, Warszawa 2008, s. 248.

[18] P. Szulin, *Kontrola zarządcza jednostek samorządu terytorialnego. Monitorowanie – kontrola – audyt*, Warszawa 2021, s. 83.

W praktyce audyt wspiera kierownika poprzez zapewnienie, że konkretny obszar działalności działa prawidłowo lub ostrzega, że wymaga poprawy. Prawidłowe umocowanie audytu wynika z regulaminu organizacyjnego urzędu, w szczególności z jego obligatoryjnego elementu, jakim jest schemat organizacyjny[19].

Niezwykle istotną kwestią jest faktyczna i prawna podległość audytora wewnętrznego bezpośrednio kierownikowi jednostki, zgodnie z art. 282 ust. 1 u.f.p. Zdaniem Krzysztofa Czerwińskiego organizacja zespołu audytu wewnętrznego powinna być dostosowana do zadań, jakie ma realizować, a tworząc strukturę organizacyjną, należy wziąć pod uwagę potrzeby wynikające z konieczności zapewnienia nadzoru i kontroli jakości[20]. Umiejscowienie audytu wewnętrznego w strukturze organizacyjnej nie może być sprzeczne z regulacjami prawa, a także wytycznymi standardów zawodowych. Z uwagi na realizowany zakres zadań audyt wewnętrzny musi podlegać takiemu szczeblowi zarządzania w organizacji, który pozwoli mu skutecznie wypełniać jego obowiązki. Przede wszystkim chodzi tu o podległość organizacyjną, która umożliwi audytorowi swobodnie identyfikować czynniki ryzyka, w szczególności na potrzeby przygotowania rocznego planu pracy audytu. Należy podkreślić, że obecne regulacje prawa finansowego zobowiązują wójta, burmistrza, prezydenta miasta, a także przewodniczącego zarządu jednostki samorządu terytorialnego (dalej jako JST) do zapewnienia organizacyjnej odrębności komórki audytu wewnętrznego, a także ciągłości jego prowadzenia (art. 282 ust. 1 u.f.p.). Ignorowanie tych wymogów może negatywnie wpływać na bezstronne realizowanie obowiązków służbowych w trakcie samej fazy przygotowania audytora do całego procesu zadania zapewniającego, fazy realizacji zadania zapewniającego, jak również raportowania o jego wynikach. Z informacji o wynikach kontroli przeprowadzonej w 2011 r. przez Najwyższą Izbę Kontroli (dalej jako NIK) wynika, że „w 16 przypadkach w 80% audytorzy wewnętrzni, zgodnie z art. 280 u.f.p. podlegali bezpośrednio kierownikom jednostek, którzy zapewnili organizacyjną odrębność komórki audytu wewnętrznego"[21]. Z wyników kontroli NIK z 2 kwietnia 2020 r. wynika, że spośród 17 jednostek, w których audyt wewnętrzny prowadzony był przez audytorów zatrudnionych w urzędzie, w strukturze organizacyjnej 7 urzędów wyodrębniono samodzielną, podlegającą bezpośrednio kierownikowi jednostki, komórkę organizacyjną ds. audytu lub samodzielne stanowisko ds. audytu. Takie rozwiązanie w pełni sprzyjało zapewnieniu niezależności organizacyjnej. W 10 urzędach audyt wewnętrzny funkcjonował wspólnie ze służbami kontrolnymi w ramach jednej komórki organizacyjnej, przy czym w przypadku połowy z nich nie zostały

[19] J. Mielczarek, *Jak zatrudnić audytora w JST*, 2019, Lex.

[20] Por. K. Czerwiński, *Audyt wewnętrzny*, Warszawa 2004, s. 24, cyt. za: P. Sołtyk, *Problematyka oceny...*, s. 64–74.

[21] P. Sołtyk, *Problematyka oceny...*, s. 64–74.

określone mechanizmy zapewnienia niezależności audytu wewnętrznego, w szczególności bezpośredniej podległości audytu wewnętrznego kierownikowi jednostki, czego wymaga art. 280 u.f.p. Jednocześnie w trzech spośród takich jednostek audytorom przypisano zadania wykraczające poza zadania audytu wewnętrznego. Działaniem takim naruszony został art. 272 ust. 1 u.f.p., według którego audyt wewnętrzny stanowi działalność niezależną i obiektywną służącą wspieraniu kierownika jednostki w realizacji celów i zadań przez systematyczną ocenę kontroli zarządczej oraz czynności doradcze[22].

Zgodnie z art. 275 audyt wewnętrzny prowadzi: 1) audytor wewnętrzny zatrudniony w jednostce albo 2) usługodawca niezatrudniony w jednostce, zwany dalej usługodawcą. Art. 274 wymienia podmioty, w których audyt prowadzony jest obligatoryjnie, a także w innych jednostkach sektora finansów publicznych, w których została przekroczona w planie finansowym tzw. kwota progowa. Obecnie kwota ta wynosi 40 000 zł. Audyt prowadzi się także w JST, jeżeli ujęta w uchwale budżetowej JST kwota dochodów i przychodów lub kwota wydatków i rozchodów przekroczyła wysokość 40 000 zł (art. 274 ust. 3 u.f.p.)[23].

Przepisy ustawy o finansach publicznych ustanawiają obowiązek prowadzenia audytu wewnętrznego w stosunku do ustawowo wymienionych jednostek sektora finansów publicznych bądź też wskazują, że są to jednostki, w których prowadzenie audytu jest uzależnione od wysokości określonych kwot. O ile w stosunku do pierwszej grupy jednostek nie ma wątpliwości, czy powinny one być objęte audytem wewnętrznym – z uwagi na ich powołanie wprost przez ustawodawcę (bezwarunkowo), o tyle w drugim przypadku występują pewne wątpliwości co do podstawy i zakresu wyznaczenia determinantów obowiązku w obszarze prowadzenia audytu wewnętrznego. Wyznaczników tegoż obowiązku należy doszukiwać się przede wszystkim w orzecznictwie[24].

Analiza przepisu art. 275 u.f.p. wskazuje, że ustawodawca posłużył się w tym zakresie alternatywą rozłączną „albo", co oznacza, iż obie te formy wykonywania audytu nie mogą być w danej jednostce sektora finansów publicznych stosowane jednocześnie. Regulacje prawne, wychodząc naprzeciw deficytu audytorów wewnętrznych w JST, stwarzają możliwość realizacji audytu przez usługodawcę. Jednak taka forma audytu może być prowadzona tylko w JST o niewielkim potencjale finansowym przedstawionym w budżecie[25].

---

[22] Najwyższa Izba Kontroli, *Audyt wewnętrzny w jednostkach samorządu terytorialnego*, Warszawa 2020, s. 9, https://www.nik.gov.pl/kontrole/wyniki-kontroli-nik/kontrole,20344.html (data dostępu: 28.10.2023).

[23] P. Sołtyk, *Usługodawca zewnętrzny audytu wewnętrznego w jednostkach samorządu terytorialnego*, „Finanse Komunalne" 2014, nr 4, s. 45–51, Lex.

[24] A. Kamedulska, op. cit., s. 56–70.

[25] P. Sołtyk, *Usługodawca zewnętrzny...*, s. 45–51.

W JST audyt wewnętrzny może być prowadzony przez usługodawcę, jeżeli ujęta w uchwale budżetowej kwota dochodów i przychodów lub wydatków i rozchodów jest niższa niż 100 000 zł[26]. Zgodnie z tym przepisem naruszeniem dyscypliny finansów publicznych jest zaniechanie prowadzenia audytu wewnętrznego w jednostce sektora finansów publicznych do tego zobowiązanej, wskutek niezatrudniania audytora wewnętrznego albo niezawierania umowy z usługodawcą.

Do naruszenia dyscypliny finansów publicznych określonego w art. 18a ustawy z dnia 17 grudnia 2004 r. o odpowiedzialności za naruszenie dyscypliny finansów publicznych[27] konieczne jest łączne spełnienie trzech przesłanek:

1) zaniechanie prowadzenia audytu wewnętrznego w jednostce sektora finansów publicznych,

2) niezatrudnianie audytora wewnętrznego albo niezawarcie umowy z usługodawcą,

3) związek przyczynowy pomiędzy okolicznościami wymienionymi w pkt 1 i 2[28].

W latach 2013–2016 liczba przypisanych czynów z art. 18a wspomnianej ustawy kształtowała się następująco: w 2013 r. – 10; 2014 r. – 6; 2015 r. – 6 oraz w 2016 r. – 14 czynów[29]. Z kolei w latach 2016–2019 na podstawie wyników kontroli NIK w 3 jednostkach zlecono prowadzenie audytu wewnętrznego usługodawcy, mimo braku przesłanek określonych w art. 278 ust. 3 u.f.p. (tj. ujęta w uchwale budżetowej jednostki kwota dochodów lub wydatków przekraczała 100 000 zł)[30]. Zasadą ogólną jest dopuszczalność prowadzenia audytu przez audytora-pracownika w każdej jednostce sektora finansów publicznych. Natomiast w odniesieniu do niektórych, wyraźnie wskazanych w przepisach jednostek audyt – zamiast przez audytora zatrudnionego – może być prowadzony przez audytora-usługodawcę. Użycie w przepisie spójnika „albo" wyklucza jednoczesne zatrudnienie w jednostce audytora wewnętrznego i zawarcie umowy z usługodawcą[31]. NIK zauważyła, że niezachowanie ciągłości wykonywania zadań audytowych wynikało, według kierowników jednostek kontrolowanych, z niemożności „znalezienia" audytorów na rynku oraz z ich wysokich wymagań finansowych. Z informacji uzyskanych z wszystkich urzędów JST zobowiązanych do prowadzenia audytu wewnętrznego z pięciu województw,

---

[26] M. Jastrzębska, *Zarządzanie ryzykiem w działalności jednostek samorządu terytorialnego i jego związki z kontrolą zarządczą oraz audytem wewnętrznym*, „Finanse Komunalne" 2010, nr 7–8, s. 5–18, Lex.

[27] Ustawa z dnia 17 grudnia 2004 r. o odpowiedzialności za naruszenie dyscypliny finansów publicznych (Dz.U. z 2021 r., poz. 289 z późn. zm.).

[28] A. Kamedulska, op. cit., s. 56–70.

[29] P. Sołtyk, *Problematyka oceny...*, s. 64–74.

[30] Najwyższa Izba Kontroli, *Audyt wewnętrzny...*, s. 9.

[31] D. Fleszer, *Audyt wewnętrzny i jego rola w zarządzaniu jednostką sektora finansów publicznych*, „Finanse Komunalne" 2014, nr 5, s. 57–68, Lex.

na terenie których prowadzona była kontrola NIK: łódzkiego, podkarpackiego, świętokrzyskiego, wielkopolskiego oraz zachodniopomorskiego (531 jednostek), wynika, że w 14% z nich nie prowadzono audytu w ogóle, natomiast w 18% pozostałych jednostkach, mimo zatrudnienia audytora lub zlecenia tego typu usługi, nie wykonano żadnego zadania zapewniającego w roku[32].

Pierwsza forma oznacza, że audytor wewnętrzny zostaje zatrudniony w jednostce. Wymóg, że audytor wewnętrzny ma być zatrudniony, oznacza, iż musi on pracować na podstawie stosunku pracy. Nie może to być np. umowa cywilnoprawna (np. zlecenia, o dzieło). Należy przy tym miejscu dodać, że zgodnie z art. 281 u.f.p. rozwiązanie stosunku pracy ani zmiana warunków płacy i pracy kierownika komórki audytu wewnętrznego ministerstwa oraz jednostki w dziale nie może nastąpić bez zgody właściwego komitetu audytu. Celem powyższej regulacji jest wprowadzenie mechanizmu, który ma zabezpieczyć niezależność kierownika komórki audytu wewnętrznego i wzmocnić jego pozycję w relacjach z kierownikiem jednostki (dyrektorem generalnym urzędu)[33].

W literaturze został przedstawiony pogląd, że zachowanie obiektywizmu audytora jest szczególnie trudne, zwłaszcza kiedy musi on dokonywać oceny działań współpracowników i przedstawiać kierownikowi jednostki słabości kontroli zarządczej. Skomplikowanie tego działania wynika z konieczności zachowania sprawiedliwego osądu oraz profesjonalnego obiektywizmu przy jednoczesnej otwartości i właściwie prowadzonej komunikacji[34].

W przypadku usługodawcy zewnętrznego przeprowadzanie audytu następuje bez konieczności nawiązywania stosunku pracy z audytorem, co ma wymierne korzyści finansowe w szczególności w niewielkich organizacjach publicznych zobligowanych do prowadzenia audytu. W odniesieniu do JST taka forma audytu wewnętrznego może zostać zastosowana, pod warunkiem że ujęta w uchwale budżetowej JST kwota dochodów i przychodów oraz kwota wydatków i rozchodów jest niższa niż 100 000 zł. W przypadku gdy kwota ta będzie równa lub wyższa niż 100 000 zł, wówczas kierownik jednostki jest zobowiązany do zatrudnienia audytora wewnętrznego. Istotną cechą budżetu samorządowego jest dynamiczny poziom zachodzących w nim zmian poprzez alokację zasobów. Jeżeli w trakcie wykonywania budżetu okaże się, że jest ona równa lub wyższa niż 100 000 tys. zł, wówczas istnieje prawny obowiązek wprowadzenia do jednostki audytu. Przepisy ustawy o finansach publicznych nie wyznaczają sztywnie punktu, w jakim czasie ma nastąpić realizacja tego obowiązku. Jedynym uprawnionym podmiotem do podjęcia decyzji o wprowadzeniu audytu jest kierownik jednostki, który – stosownie do treści art. 276 u.f.p. – odpowiada za wykonywanie zadań audytu wewnętrznego[35].

[32] Najwyższa Izba Kontroli, *Audyt wewnętrzny*..., s. 10.
[33] J. Mielczarek, op. cit.
[34] P. Szulin, op. cit., s. 83.
[35] P. Sołtyk, *Usługodawca zewnętrzny*..., s. 45–51.

Istnieje dowolność w wyborze rodzaju umowy, jaka może zostać zawarta z usługodawcą – może więc to być umowa cywilnoprawna (zlecenie lub o dzieło). Ustawodawca sformułował warunek, zgodnie z którym umowa z usługodawcą musi zostać zawarta na okres co najmniej roku. Wśród koniecznych elementów umowy należy wymienić postanowienia zawierające gwarancje prowadzenia czynności audytowych zgodnie z wymogami prawa. Warto też odnieść się do obowiązku stosowania standardów audytu wewnętrznego przez usługodawcę. Jest to zasadne, ponieważ regulacje w treści art. 273 ust. 2 u.f.p. zobowiązują audytora wewnętrznego, aby prowadząc audyt, kierował się wskazówkami zawartymi w standardach audytu wewnętrznego. Podkreślenia wymaga fakt, że regulacje ustawy o finansach publicznych nie dają delegacji prawnej Ministrowi Finansów do przeprowadzania oceny w przedmiocie działalności audytu wewnętrznego w JST.

Ważnym punktem umowy jest określenie zasad postępowania z dokumentami przekazanymi usługodawcy w trakcie czynności audytowych, a także tymi dokumentami, które zostały wytworzone przez osobę realizującą zadanie audytowe. Generalnie celem jest zapewnienie ochrony przed nieupoważnionym rozpowszechnieniem dokumentów, a także ich uszkodzeniem lub zniszczeniem. Dostępność do dokumentów i zarządzanie w szczególności finansowo-księgowymi dokumentami muszą być precyzyjnie określone w treści umowy, chociażby z uwagi na wymogi ustawy z dnia 29 września 1994 r. o rachunkowości[36]. Zlecając realizację audytu w formie usługodawcy niezatrudnionego w jednostce, należy zastosować przepisy normujące zasady dokonywania wydatków publicznych. Otóż na tle art. 44 ust. 3 pkt 1 u.f.p. wydatki powinny być dokonywane w sposób celowy i oszczędny z zachowaniem zasady uzyskiwania najlepszych efektów z danych nakładów. Te ogólne unormowania prawne mogą skłaniać do podjęcia próby przeprowadzenia przez decydentów samorządowych pogłębionej analizy w przedmiocie skuteczności oraz efektywności prac usługodawcy w relacji do angażowanych środków publicznych na ten cel [37].

Kwalifikacje i kompetencje interpersonalnych audytora wewnętrznego w zapewnieniu okresowego audytu wewnętrznego w zakresie zarządzania bezpieczeństwem informacji

Ustawodawca w art. 279 ust. 1 u.f.p. zastrzega, że o usługę audytu (lub jej wykonanie) może ubiegać się osoba fizyczna, która spełnia kryteria kwalifikacyjne przewidziane dla audytora wewnętrznego. Ponadto kierownik jed-

[36] Ustawa z dnia 29 września 1994 r. o rachunkowości (t.j. Dz.U. z 2023 r., poz. 120 z późn. zm.).
[37] P. Sołtyk, *Usługodawca zewnętrzny...*, s. 45–51.

nostki może zlecić usługę realizacji audytu osobie fizycznej prowadzącej działalność gospodarczą, spełniającej ww. wymogi dla audytora. W dalszej kolejności usługodawcą może być spółka cywilna, spółka jawna, spółka partnerska, spółka komandytowa, spółka komandytowo-akcyjna lub osoba prawna, która zatrudnia osobę spełniającą wymogi kwalifikacyjne przewidziane dla audytora wewnętrznego[38].

Audyt wewnętrzny wykonują zarówno osoby z organizacji, jak i spoza niej, dlatego stosuje się Międzynarodowe standardy praktyki zawodowej audytu wewnętrznego (zob. komunikat Ministra Rozwoju i Finansów z dnia 12 grudnia 2016 r. w sprawie standardów audytu wewnętrznego dla jednostek sektora finansów publicznych)[39].

Standard zawodowy oznaczony numerem 2010 – *Planowanie* głosi, że zarządzający audytem wewnętrznym musi opracować plan oparty na analizie ryzyka, określający priorytety działań audytu wewnętrznego zgodnie z celami organizacji. Ponadto inny standard zawodowy, oznaczony 2010.A1, stanowi, że plan zadań audytu wewnętrznego musi opierać się na udokumentowanej ocenie ryzyka, przeprowadzonej co najmniej raz w roku. Oznacza to, że roczny plan pracy komórki audytu wewnętrznego jest opracowywany po uprzednim przeprowadzeniu analizy ryzyka. Planowanie pracy opartej na wynikach analizy ryzyka w audycie wewnętrznym jest gwarantem zachowania obiektywizmu i niezależności przy obejmowaniu obszarów do badania. Na podstawie przytoczonych regulacji prawnych można więc wysnuć ogólny wniosek, że w obszarze zarządzania bezpieczeństwem informacji należy identyfikować czynniki ryzyka związane z tym systemem, a następnie poddawać je analizie ryzyka. Z wytycznych zaprezentowanych przez Ministerstwo Finansów wynika, że realizacja audytu o tematyce bezpieczeństwa informacji powinna następować zgodnie z wymogami określonymi w u.f.p., a także przepisów rozporządzenia Ministra Finansów z dnia 4 września 2015 r. w sprawie audytu wewnętrznego oraz informacji o pracy i wynikach tego audytu[40] z uwzględnieniem Standardów zawodowych audytu wewnętrznego[41].

Od audytora wewnętrznego oczekuje się także innych wymagań, do których należy zaliczyć:

1) obiektywizm – co oznacza, że działanie audytu wewnętrznego musi być niezależne, a audytorzy wewnętrzni muszą zachować obiektywizm podczas wykonywania swej pracy (standard zawodowy oznaczony nr 1100 *Niezależność i Obiektywizm*);

2) bezstronność – która polega na tym, że audytorzy muszą być bezstronni i wolni od uprzedzeń, muszą również unikać jakichkolwiek konfliktów in-

[38] Ibidem.

[39] J. Mielczarek, op. cit.

[40] Rozporządzenie Ministra Finansów z dnia 4 września 2015 r. w sprawie audytu wewnętrznego oraz informacji o pracy i wynikach tego audytu (t.j. Dz.U. z 2018 r., poz. 506).

[41] P. Sołtyk, *System zarządzania*..., s. 126–133.

teresów, do czego nakłania standard zawodowy nr 1120 *Indywidualny obiektywizm*;

3) staranność zawodową – co oznacza, że zadania audytorskie muszą być wykonywane z biegłością zawodową oraz z należytą starannością, co wynika ze standardu oznaczonego nr. 1200 *Biegłość oraz należyta staranność zawodowa*;

4) wiedzę – co zobowiązuje, aby audytorzy wewnętrzni posiadali wiedzę, umiejętności oraz kwalifikacje potrzebne do wykonywania ich indywidualnych obowiązków. Audytorzy muszą ciągle dążyć do zdobywania wiedzy oraz umiejętności praktycznych. Wysokie kwalifikacje w tej profesji są niezbędne do wykonywania swoich obowiązków, o czym stanowi standard zawodowy nr 1210 *Biegłość*;

5) staranność zawodową – co oznacza, że audytorzy muszą wykazywać staranność i umiejętność oczekiwane od odpowiednio rozważnego i kompetentnego audytora wewnętrznego. Należyta staranność zawodowa nie oznacza nieomylności, co wynika ze standardu nr 1220 *Należyta staranność zawodowa*;

6) rozwój zawodowy – który zmusza audytora do poszerzania swojej wiedzy, umiejętności oraz kwalifikacji drogą stałego doskonalenia zawodowego, co wynika z treści standardu zawodowego oznaczonego nr 1230 *Ciągły rozwój zawodowy*.

Wykonywanie profesji audytora wewnętrznego wymaga także, aby przestrzegał on zasad etycznych obowiązujących w organizacji publicznej. Ogólnie problematyka respektowania wartości etycznych w jednostkach sektora finansów publicznych została przedstawiona w grupie A „Środowisko wewnętrzne" poszczególnych elementów kontroli zarządczej. Ogólnie wymaga się, aby audytorzy w relacjach służbowych zachodzącymi między innymi audytorami, a także pracownikami organizacji publicznej postępowali w sposób godny i uczciwy. Warto podkreślić, że takiego postępowania wymaga się nie tylko od osób wykonujących zawód audytora, lecz od całego personelu pracowniczego[42].

Wśród cech osobowych pożądanych od osoby zatrudnionej na stanowisku audytora wewnętrznego należy wyróżnić:

1) dynamizm działania – różnorodność i tempo pracy wymagają intelektualnego wysiłku i pracowitości w sytuacjach, gdy warunki pracy bywają niekomfortowe, pod presją czasu, ze szczególną dbałością o pozytywny wizerunek;

2) równowaga rzeczy osądzonych – powinien zachowywać się swobodnie, wypowiadać swoje zdanie, ale bez napastliwości z zachowaniem wywarzonej krytyki, zachowywać emocjonalną równowagę, być odpornym na naciski. Na koniec brać odpowiedzialność za swoje oceny;

3) otwartość na nowe rozwiązania – powinien mieć zupełnie obiektywne spojrzenie na zagadnienia, które bada, będąc otwartym na nowości i oryginalne rozwiązania w zakresie zaleceń poaudytowych;

---

[42] Idem, *Usługodawca zewnętrzny...*, s. 45–51.

4) analiza i synteza – powinien potrafić budować dobrą strukturę intelektualną, czyli umiejętność analizy pozwalającej określić problemy, syntezy dla ich rozwiązywania;

5) komunikacja – powinien cechować się poprawną umiejętnością werbalizacji myśli prostym językiem, wysławiając się lub na piśmie. Powinien posiadać łatwość docierania do ludzi, traktując jako wartość nadrzędną prawo do ochrony informatorów. Warto, aby kierownik dobrze zastanowił się, jakiej osoby szuka, które kompetencje i umiejętności są kluczowe na stanowisku audytora w jego urzędzie, z których można ewentualnie zrezygnować, jakie cechy interpersonalne sprawią, że osoba ta będzie jak najlepiej dopasowana do kultury organizacyjnej jednostki[43].

Nie sposób nie wspomnieć tutaj o kryteriach certyfikacji audytorów wewnętrznych w odniesieniu do systemu zarządzania bezpieczeństwem informacji, tj.: 1) PN-EN ISO/IEC 19011 Wytyczne dotyczące audytowania systemów zarządzania; 2) ISO/IEC 27006 Technika informatyczna – Techniki bezpieczeństwa – Wymagania dla jednostek prowadzących audyt i certyfikację systemów zarządzania bezpieczeństwem informacji.

Certyfikat kompetencji wydany przez jednostkę certyfikującą zgodnie z zasadami normy PN-EN ISO/IEC 17024 wskazuje, że wymieniona osoba spełnia wymagania certyfikacyjne. Kryteria certyfikacji dla osób ubiegających się o certyfikat kompetencji audytora wewnętrznego systemu zarządzania bezpieczeństwem informacji wymagają: wykształcenia minimum średniego, co najmniej rocznego stażu pracy zawodowej, co najmniej rocznego stażu pracy związanej z bezpieczeństwem informacji, ukończenia cyklu szkoleń według wymaganego programu, zdania egzaminu końcowego, doświadczenia zdobytego podczas pełnego procesu audytu[44].

Certyfikacja audytora wiodącego Systemu Zarządzania Bezpieczeństwem Informacji wg normy PN-EN ISO/IEC 27001:2022 pozwoli audytorowi na nabycie kompetencji zgodnych z normą ISO 27001, umożliwiających przeprowadzania audytów pierwszej, drugiej i trzeciej strony w roli audytora wiodącego. Uzyskanie wskazanej certyfikacji pozwoli na nabycie stosowej wiedzy, umiejętności i kompetencji do planowania i realizacji audytu zgodnie z wymogami normy ISO 27001, w tym oceny skuteczności działania Systemu Zarządzania Bezpieczeństwem Informacji, wskazania niezgodności, dokumentowania oraz wydania stosownych rekomendacji i działań korygujących dal kierownika jednostki w tym zakresie. W celu uzyskania certyfikacji kandydat musi wykazać się nie tylko znajomością normy ISO 27001, ale też wiedzą i doświadczeniem w zakresie techniki informatycznej, bezpieczeństwa informacji i audytowania, a wykaz certyfikatów uprawniających do przeprowadzenia audytu, uwzględ-

[43] J. Mielczarek, op. cit.
[44] T. Soczyński, op. cit.

niając zakres wiedzy specjalistycznej wymaganej od osób legitymujących się poszczególnymi certyfikatami, został określony w rozporządzeniu Ministra Cyfryzacji zgodnie z art. 15 ust. 8 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[45]. Certyfikat Audytora Wiodącego Systemu Zarządzania Bezpieczeństwem Informacji wg ISO/IEC 27001 znajduje się w wykazie certyfikatów określonym w rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu[46]. Ważne, że większość certyfikatów na rynku posiada akredytację Polskiego Centrum Akredytacji, a utrzymanie ważności certyfikacji (certyfikat zwykle ma określony okres ważności) wymaga potwierdzenia realizacji audytów zgodnie z normą celem przedłużenia jego ważności.

Kwestia dobrej znajomości metodyki audytu w obszarze bezpieczeństwa informacji odgrywa ważną rolę w formułowaniu rekomendacji odnośnie do działania systemu zarządzania bezpieczeństwem informacji. Tak więc kierownik jednostki, podejmując decyzję o przeprowadzaniu przez personel własnej komórki audytu wewnętrznego o tematyce bezpieczeństwa informacji, powinien brać pod uwagę kwalifikacje, a także posiadanie umiejętności praktycznych w realizacji audytu. Jeżeli się okaże, że pracownicy komórki audytu wewnętrznego nie mają niezbędnych kwalifikacji do rzetelnej i obiektywnej oceny, istnieje możliwość zlecenia realizacji audytu bezpieczeństwa informacji przez ekspertów w tej dziedzinie spoza jednostki[47].

Jak słusznie stwierdzono we wspólnym stanowisku Departamentu Informatyzacji Ministerstwa Administracji i Cyfryzacji oraz Departamentu Audytu Sektora Finansów Publicznych Ministerstwa Finansów, „ustawodawca nie określił sposobu, trybu, rodzaju audytu, ani też osób czy komórek organizacyjnych, którym należałoby powierzyć prowadzenie ww. audytu. Zatem decyzja co do tego, komu zostanie powierzone prowadzenie omawianego audytu, spoczywa na kierownictwie podmiotu". Ponadto Ministerstwo Finansów oraz Ministerstwo Administracji i Cyfryzacji określiły kryteria służące wyborowi w ramach danego podmiotu publicznego osób lub komórek organizacyjnych, które powinny być odpowiedzialne za przeprowadzanie audytu w zakresie bezpieczeństwa informacji. Kryteria te są następujące:

– odpowiednie kwalifikacje,
– doświadczenie,
– znajomość metodyki audytu w zakresie bezpieczeństwa informacji,
– niezależność od obszaru audytowanego[48].

---

[45] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. z 2023 r., poz. 913 z późn. zm.).

[46] Rozporządzenie Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu (t.j. Dz.U. z 2018 r., poz. 1999).

[47] P. Sołtyk, *System zarządzania*..., s. 126–133.

[48] W. Dziomdziora, op. cit.

W przypadku komórki audytu wewnętrznego, w której jest zatrudniony tylko jeden audytor lub gdy realizacja obowiązku prowadzenia audytu następuję poprzez usługodawcę niezatrudnionego w jednostce, przyjęcie jednego obszaru do oceny pod nazwą zarządzanie bezpieczeństwem informacji do przeprowadzania nie rzadziej niż raz na rok może destabilizować pracę audytora przy realizacji ewaluacji w innych obszarach działalności jednostki[49].

Zakończenie

Obowiązek zapewnienia okresowego audytu wewnętrznego w zakresie zarządzania bezpieczeństwem informacji w jednostkach sektora finansów publicznych, w tym w JST, wynika wprost z przepisów prawa. Potwierdzenie zgodności i skuteczności działania systemu zarządzania bezpieczeństwem informacji można uzyskać w wyniku przeprowadzonego audytu wewnętrznego. Należy podkreślić, że zaniechanie prowadzenia audytu wewnętrznego w jednostce sektora finansów publicznych lub niezatrudnianie audytora wewnętrznego albo niezawarcie umowy z usługodawcą może prowadzić do naruszenia dyscypliny finansów publicznych określonego w art. 18a ustawy z dnia 17 grudnia 2004 r. o odpowiedzialności za naruszenie dyscypliny finansów publicznych. W JST audyt wewnętrzny może być prowadzony przez usługodawcę, jeżeli ujęta w uchwale budżetowej kwota dochodów i przychodów lub wydatków i rozchodów jest niższa niż 100 000 zł. Istotą jest zapewnienie przez kierownika jednostki wyznaczonemu audytorowi gwarancji niezależności i obiektywizmu, jak również poszerzania i zdobywania odpowiednich kwalifikacji potwierdzających wiedzę i doświadczenie w audytowanym obszarze. W pierwszym przypadku mocno podkreślono wymogi wynikające zgodnie z art. 282 ust 1 u.f.p. i wytyczne standardów zawodowych, wskazujące na niezwykle istotną kwestię dotyczącą podległości audytora wewnętrznego bezpośrednio kierownikowi jednostki, mając na uwadze dostosowanie struktury organizacyjnej jednostki do zadań, jakie ma realizować komórka audytu wewnętrznego, oraz potrzeb wynikających z konieczności zapewnienia nadzoru i kontroli jakości. W myśl art. 279 ust. 1 u.f.p. o usługę audytu (lub jej wykonanie) może ubiegać się osoba fizyczna, która spełnia kryteria kwalifikacyjne przewidziane dla audytora wewnętrznego, a do prowadzenia audytu w obszarze bezpieczeństwa uprawnia m.in. certyfikat Audytora Wiodącego Systemu Zarządzania Bezpieczeństwem Informacji wg ISO/IEC 27001 potwierdzający wiedzę, umiejętności i kompetencje do planowania i realizacji audytu zgodnie z wymogami wskazanej normy.

[49] P. Sołtyk, *System zarządzania*..., s. 126–133.

Mając powyższe na uwadze, audytorzy powinni wyróżniać się bezstronnością i obiektywizmem, posiadaniem stosownej wiedzy i kwalifikacji zawodowych, dynamizmem działania i umiejętnościami komunikacji. Wskazane cechy pozwolą w sposób obiektywny dokonać niezależnej opinii o skuteczności działania systemu zarządzania bezpieczeństwem informacji, w tym oceny poziomu bezpieczeństwa w systemach teleinformatycznych i ich zgodności z odpowiednimi normami i politykami bezpieczeństwa lub innego istotnego obszaru. Pozwolą również na wskazanie niezgodności, właściwe dokumentowanie zadania zapewniającego, na wydanie stosownych rekomendacji i działań korygujących dla kierownika jednostki.

Wykaz literatury

Bartoszewicz A., *Praktyka funkcjonowania audytu wewnętrznego w Polsce*, CeDeWu, Warszawa 2011.

Czerwiński K., *Audyt wewnętrzny*, InfoAudit, Warszawa 2004.

Dziomdziora W., *Cyberbezpieczeństwo w samorządzie terytorialnym. Praktyczny przewodnik*, 2021, Lex.

Fleszer D., *Audyt wewnętrzny i jego rola w zarządzaniu jednostką sektora finansów publicznych,* „Finanse Komunalne" 2014, nr 5, Lex.

Jastrzębska M., *Zarządzanie ryzykiem w działalności jednostek samorządu terytorialnego i jego związki z kontrolą zarządczą oraz audytem wewnętrznym*, „Finanse Komunalne" 2010, nr 7–8, Lex.

Kamedulska A., *Zaniechanie prowadzenia audytu wewnętrznego w świetle naruszenia dyscypliny finansów publicznych*, „Finanse Komunalne" 2020, nr 3, Lex.

Kuc B., *Kontrola – kontroling – audyt. 3w1. Podobieństwa i różnice*, Wyd. PTM, Warszawa 2008.

Mielczarek J., *Jak zatrudnić audytora w JST*, 2019, Lex.

Najwyższa Izba Kontroli, *Audyt wewnętrzny w jednostkach samorządu terytorialnego*, Warszawa 2020, https://www.nik.gov.pl/kontrole/wyniki-kontroli-nik/kontrole,20344.html.

Soczyński T., *Kompetencje i umiejętności inspektora ochrony danych a możliwe mechanizmy certyfikacji*, [w:] T. Wyka, M.A. Mielczarek (red.), *Administrator i inspektor ochrony danych osobowych*, Wolters Kluwer, Warszawa 2019.

Sołtyk P., *Problematyka oceny działalności audytu wewnętrznego w jednostkach samorządu terytorialnego w świetle postulatów standardów zawodowych*, „Finanse Komunalne" 2017, nr 12, Lex.

Sołtyk P., *System zarządzania bezpieczeństwem informacji w jednostce samorządu terytorialnego przedmiotem oceny audytu wewnętrznego – wątpliwości interpretacyjne*, „Finanse Komunalne" 2016, Lex.

Sołtyk P., *Usługodawca zewnętrzny audytu wewnętrznego w jednostkach samorządu terytorialnego*, „Finanse Komunalne" 2014, nr 4, Lex.

Szulin P., *Kontrola zarządcza jednostek samorządu terytorialnego. Monitorowanie – kontrola – audyt*, Wolters Kluwer, Warszawa 2021.

Winiarska K., *Audyt wewnętrzny. Teoria i zastosowanie*, Difin, Warszawa 2019.

Summary

Security information as a task of public finance sector units

Keywords: law, internal audit, information security management system, independence and objectivity, certification.

The article presents issues concerning the principles of functioning and the role of internal audit in public finance sector units as an independent and objective tool ensuring and consulting the unit manager. In addition, the purpose of this work is to indicate the obligation of public finance sector units to ensure periodic implementation of internal audits and their role in the field of security information management and the required qualifications of auditors in this regard. Failure to ensure the effectiveness and efficiency of the security information management system in the unit may cause financial and image losses or obstacles in maintaining business continuity and implementation of the assumed goals and tasks. The role of the audit is to support the head of the unit by ensuring that a specific area of activity works properly or requires improvement, and the obligation to carry out periodic internal audits in the field of security information management in public units results from the provisions of law. The essence is that the head of the unit should provide the designated auditor the guarantee of independence and objectivity, as well as expanding and acquiring appropriate qualifications confirming knowledge and experience in the audited area. In the area of security information, it is worth it emphasizing the certification of the lead auditor of the Security Information Management System according to the PN-EN ISO/IEC 27001:2022 standard, confirming the required knowledge and experience in the field of security information, IT technology and auditing.