„Zeszyty Teoretyczne Rachunkowości”
tom 100 (156), 2018, s. 131–165

Stowarzyszenie Księgowych
w Polsce

Propozycja rekomendacji dotyczącej kontroli wewnętrznej w rachunkowości w środowisku informatycznym

ELŻBIETA IZABELA SZCZEPANKIEWICZ *

Streszczenie

Opracowanie określonych regulacji i konkretne działania to podstawowy środek do zapewnienia bezpieczeństwa zasobów informatycznych rachunkowości w jednostkach gospodarczych. Jednostki w Polsce od 1995 roku stosują się do określonych zapisów ustawy o rachunkowości w tym zakresie. Badania autorki na temat aktualnego poziomu zapewnienia bezpieczeństwa zasobów informatycznych rachunkowości w jednostkach potwierdziły, że znacznie się on różni w poszczególnych sektorach i typach badanych jednostek. W artykule przyjęto hipotezę: jednostki, które przyjęły do stosowania dodatkowe regulacje (standardy, rekomendacje) dotyczące kontroli wewnętrznej mają skuteczniejszy system kontroli wewnętrznej w rachunkowości prowadzonej w środowisku informatycznym. Na podstawie zaprezentowanych wyników badań empirycznych hipoteza ta została pozytywnie zweryfikowana, ponieważ w jednostkach, w których obowiązują dodatkowe regulacje branżowe w tym zakresie kierownictwo bardziej angażuje się w zapewnienie bezpieczeństwa zasobów informatycznych rachunkowości. Podczas badań ankietowani wskazali, że oczekują opracowania dla nich regulacji (rekomendacji, wytycznych), które pomogą im doskonalić kontrolę wewnętrzną w tym obszarze. Celem artykułu jest przedstawienie autorskiej propozycji założeń do rekomendacji dotyczącej kontroli wewnętrznej w tym zakresie. Wprowadzenie takiej rekomendacji może pomóc kierownikom jednostek w projektowaniu nowych i doskonaleniu obecnych systemów kontroli wewnętrznej w rachunkowości prowadzonej w środowisku informatycznym. W artykule zaproponowano także autorski model systemu kontroli wewnętrznej, który został opracowany w wyniku analizy kilku wiodących koncepcji i regulacji światowych oraz krajowych, ogłoszonych w przedmiotowym zakresie. Metody badawcze wykorzystane w opracowaniu to analiza piśmiennictwa oraz regulacji w przedmiotowym zakresie, analiza wyników badań ankietowych i wnioskowanie.

Słowa kluczowe: IT, bezpieczeństwo informatyczne w rachunkowości, system kontroli wewnętrznej, standard kontroli wewnętrznej, zarządzanie ryzykiem.

Abstract

Proposals concerning development of internal control recommendations applicable to accounting systems in IT environments

Developing appropriate legal regulations and taking specific actions are the basic tools for ensuring accounting information resources security (AIRS) in business entities. Since 1995 businesses have been following appropriate provisions of the Accounting Act with regard to AIRS. However, the author’s research on the current level of AIRS assurance level in businesses showed that AIRS level varies considerably in various types of businesses. The following hypothesis is proposed in the paper: entities that endorse additional regulations (standards or recommendations) concerning internal control have a more

* Dr Elżbieta Izabela Szczepankiewicz, adiunkt, Uniwersytet Ekonomiczny w Poznaniu, Wydział Zarządzania, Katedra Rachunkowości, elzbieta.szczepankiewicz@ue.poznan.pl

ISSN 1641-4381 *print* / ISSN 2391-677X *online*

http://www.ztr.skwp.pl
DOI: 10.5604/01.3001.0012.7316

effective internal control system in the area of accounting in the IT environment. On the basis of the presented empirical results, this hypothesis was confirmed, as in entities which follow additional industry regulations in this respect, the management is more committed to ensuring the security of IT accounting resources. During the research, the respondents indicated that they expect to have regulations developed (recommendations, guidelines) that will help them improve internal control in this area. The objective of the paper is to present original contribution to developing a national internal control recommendation . The introduction of such a recommendation may help managers design new and improve existing internal control systems in the area of accounting in an IT environment. Research methods used by the author include analysis of literature and legislation, analysis of survey results and inference.

Keywords: IT, security of IT resources in accounting, internal control systems, internal control standards, risk management.

Wprowadzenie

Współczesną rachunkowość trudno sobie wyobrazić bez wykorzystania najnowszych rozwiązań informatycznych. Zasięg interakcji rachunkowości jednostki gospodarczej z otoczeniem ulega ciągłemu rozszerzaniu. Jeszcze kilka lat temu[1] prowadzenie rachunkowości ograniczano do cyberprzestrzeni organizacyjnej jednostki, a jej zasoby informatyczne były narażone na czynniki ryzyka związane z funkcjonowaniem wewnętrznych struktur organizacji. W kolejnych latach wiele jednostek, z coraz większym zaufaniem do najnowszych rozwiązań w zakresie zapewnienia bezpieczeństwa przesyłanych informacji, zdecydowało się na wprowadzenie swojej rachunkowości do cyberprzestrzeni globalnej. Jeszcze kilka lat temu były to tylko interakcje związane z korzystaniem z usług bankowości internetowej i utrzymywaniem w czasie rzeczywistym stałych relacji z kontrahentami (w tym: gromadzenie zamówień, zlecanie dostaw), jak również innymi interesariuszami w dowolnym miejscu na świecie. Obecnie można prowadzić rachunkowość w cyberprzestrzeni globalnej. Związane jest to na przykład z możliwością: technologicznego integrowania (konsolidowania) rachunkowości (w tym sprawozdawczości) filii czy oddziałów jednostki (np. korporacji, banków) funkcjonujących w dowolnym miejscu na świecie; wynajmowania oprogramowania do prowadzenia biznesu w modelu usług ASP (*Application Service Provider*)[2], czy też korzystania

[1] Wiele jednostek, prowadząc rachunkowość wyodrębniało pojedyncze komputery, na których instalowano poszczególne podsystemy rachunkowości (system finansowo-księgowy, kadrowo-płacowy, rejestry sprzedaży i in.). Dla zapewnienia ochrony danych i ksiąg rachunkowych komputerów do obsługi rachunkowości nie podłączano do Internetu. Natomiast inne, zazwyczaj większe jednostki budowały lokalne sieci wewnętrzne, aby integrować poszczególne podsystemy (moduły) z systemem finansowo-księgowym, a komputer, z którego zlecano internetowe przelewy bankowe zawsze funkcjonował poza tą siecią.

[2] Idea usług w tym modelu polega na wykorzystywaniu dzierżawionego oprogramowania za pośrednictwem Internetu przez te jednostki, które chcą korzystać z najnowszych, bieżąco aktualizowanych aplikacji bez ponoszenia kosztów na zakup licencji własnych systemów. Jednostka może wynająć np. system wspomagający zarządzanie przedsiębiorstwem klasy ERP II albo tylko system informatyczny rachunkowości (z modułami dziedzinowymi), bądź tylko jeden wybrany moduł (np. system kadrowo-płacowy). Niektóre internetowe biura rachunkowe oraz ich klienci od kilku lat korzystają z wydzierżawionych aplikacji do prowadzenia rachunkowości *online*.

z usług internetowych biur rachunkowych[3]. Współczesna rachunkowość jednostek coraz szerzej funkcjonuje w krajowej cyberprzestrzeni publicznej. Jednostki poza krajową bankowością elektroniczną, realizują wynikające z przepisów prawa nowe obowiązki wobec urzędów administracji publicznej (ZUS, US, GUS), organów rejestrowych (KRS) i organów nadzoru (KNF, GPW i in.).

W ostatnich latach coraz więcej jednostek rozważa również przetwarzanie i przechowywanie danych z rachunkowości w technologii chmury (*cloud computing*) (Szczepankiewicz, 2017) i wykorzystania w przyszłości w interakcjach z innymi podmiotami takich technologii cyfrowych, takimi jak *business analytics, big data, digital tax returns*, które dotychczas realizowały potrzeby wewnętrzne zarządów dużych firm. Wiele jednostek opracowuje już plany na najbliższą przyszłość, aby wykorzystać szanse związane z najnowszymi technologiami cyfrowymi, nad którymi intensywnie pracują firmy informatyczne. W niedalekiej przyszłości jednostki będą powszechnie prowadzić rozliczenia podatkowe, składać deklaracje i sprawozdania (w tym np. e-sprawozdania finansowe do urzędów skarbowych), wykorzystywać oprogramowanie wspomagające e-fakturowanie w relacjach online z kontrahentami. Coraz powszechniej będą wynajmować oprogramowanie w serwisie ASP, prowadzić księgi rachunkowe działające w środowisku rozproszonym (tzw. *distributed ledgers*), przygotowywać i automatycznie przesyłać rozliczenia z wykorzystaniem kryptowalut, wykorzystywać technologię sztucznej inteligencji do prowadzenia e-analiz eksperckich, a nawet korzystać z przeprowadzenia w trybie online audytu finansowego. Obecnie wdrażane w niektórych dużych jednostkach nowe technologie cyfrowe[4] takie jak na przykład: *Big Data*[5], *Robo Advisor*[6], *Artificial Intelligence*[7], *FinTech*[8], *Algo Trading*[9], *Blockchain*[10] i inne, będą miały

[3] Powszechne i tanie jest zlecenie prowadzenia konkretnego obszaru rachunkowości np. spraw kadrowo-płacowych albo rejestrów podatkowych, w tym sporządzanie plików JPK do urzędu skarbowego.

[4] Wdrożenie nowych technologii cyfrowych (Jajuga, 2017) pozwoli jednostkom poszerzyć zasięg działania w otoczeniu, umożliwi skuteczniejsze zarządzanie relacjami z otoczeniem oraz wewnątrz jednostki, ułatwi dostęp do aktualnej informacji z wewnątrz i z otoczenia, zwiększa możliwości gromadzenia, przetwarzania danych, pomagając efektywniej wykorzystywać zasoby rzeczowe, finansowe i niematerialne jednostki.

[5] Rozwój technologii obliczeniowej służy m.in. łączeniu wielu baz danych w jedną dużą i zmienną bazę danych. Rozwiązanie to może prowadzić do zdobycia nowej wiedzy w jednostce, wnosi wartość dodaną do finansów jednostki. Niedoskonałość wielu obecnych rozwiązań polega na wysokim koszcie zbierania i zapewnienia bezpieczeństwa danych, często znacznie przewyższającym wartość gromadzonych danych, m.in. ze względu na to, że gromadzi też *Dark Data* (dane nigdy nie wykorzystane do zarządzania, niepotrzebne) i *Dirty Data* (dane niekompletne, błędne, nieaktualne, zdublowane).

[6] Polega na automatycznym, cyfrowym doradztwie finansowym według reguł matematycznych lub algorytmów, wykonywanym przez oprogramowanie, bez udziału doradcy finansowego. Wykorzystywane już w planowaniu finansowym i automatycznym inwestowaniu środków. Rozwiązania będą przystosowane do prowadzenia audytu finansowego.

[7] Elementy sztucznej inteligencji stosowane są w finansowych systemach ekspertowych, np. do planowania finansowego, badania zdolności kredytowej klienta i innych. W przyszłości przewiduje się większe zastosowanie oprogramowania sztucznej inteligencji do zastępowania procesów myślowych i analitycznych w finansach.

[8] Najnowszy segment rynku finansowego opierający usługi finansowe, inwestycyjne, krypto-waluty na wykorzystaniu technologii informacyjnej i telekomunikacyjnej.

[9] Wspomaga inwestorów w technologii handlu algorytmicznego.

[10] *Blockchain* obecnie stosowana w *Bitcoinie*, jako platforma służąca do prowadzenia rejestru transakcji, płatności, zapisów księgowych. Jest zakodowana za pomocą algorytmów kryptograficznych. Stanowi publiczny i jawny rejestr, do którego dostęp może uzyskać każdy zainteresowany interesariusz. Rozwiązanie będzie wykorzystane do ściągania podatków.

wpływ zarówno na sposób prowadzenia działalności jednostki, organizację systemu kontroli wewnętrznej w środowisku informatycznym rachunkowości, jak i na wypełnianie przez rachunkowość jej funkcji, a przede wszystkim informacyjnej, kontrolnej, sprawozdawczej, analitycznej, podatkowej i dowodowej.

Bardzo szybki postęp technologiczny i organizacyjny we współczesnej rachunkowości wniesie więcej korzyści, ale również wiele dodatkowych zagrożeń dla jej zasobów informatycznych. Dlatego wykorzystanie nowych technologii cyfrowych będzie wymagało wykształcenia w tym zakresie nowych wewnętrznych zdolności oraz wiedzy eksperckiej (np. poprzez edukację i szkolenia) oraz korzystania z usług zewnętrznych specjalistów z różnych dziedzin. W dobie lawinowo rosnącej fali różnego typu zagrożeń w cyberprzestrzeni organizacyjnej, publicznej i globalnej dla rachunkowości jednostki, same najnowsze zabezpieczenia informatyczne nie będą gwarantowały jednostce skutecznej ochrony jej zasobów informatycznych (Szczepankiewicz, 2018). Z tego względu przedmiotem niniejszego opracowania jest organizacja kontroli wewnętrznej w obszarze współczesnej rachunkowości, którą prowadzi się w środowisku informatycznym. Wiedza na temat jakości kontroli wewnętrznej w środowisku informatycznym rachunkowości w polskich jednostkach stanowi nadal niewypełnioną lukę badawczą. W ostatnich dwudziestu latach w literaturze powstało wiele opracowań na temat roli i zadań kontroli w procesie zarządzania jednostką[11], ale tylko pojedyncze dotyczą problemów organizacji kontroli wewnętrznej w obszarze rachunkowości, pomimo, że rachunkowość była jednym z pierwszych obszarów, w którym formalnie rozpoczęto wdrażać i później doskonalić systemy kontroli wewnętrznej.

Przeprowadzone przez autorkę badania empiryczne w ponad 400 jednostkach pozwalają na postawienie tezy, że współczesne uwarunkowania prowadzenia rachunkowości w środowisku informatycznym powodują, że należy odejść od klasycznego postrzegania kontroli wewnętrznej, jedynie jako zespołu środków ochrony, procedur, instrukcji i działań kontrolnych, a spojrzeć na kontrolę wewnętrzną, jako system składający się kilku niezwykle ważnych, spójnych, zależnych od siebie, wzajemnie się uzupełniających komponentów, z których szczególną rolę należy przypisać procesom identyfikacji i analizy ryzyka. Szczególne uwarunkowania prowadzenia współczesnej rachunkowości wymagają opracowania nowego teoretycznego modelu oraz standardu dotyczącego kontroli wewnętrznej w obszarze rachunkowości prowadzonej w środowisku informatycznym.

Ukształtowanie sprawnego, efektywnego, skutecznego i adekwatnego systemu kontroli wewnętrznej w danej jednostce uzależnione jest od wiedzy kierownictwa nabywanej w wielu obszarach. Niezbędna jest wiedza dotycząca zarówno organizacji rachunkowości, kontroli finansowo-księgowej, kontroli wewnętrznej, audytu, jak i metod i narzędzi analizy ryzyka oraz podstaw informatyki (w tym: w zakresie identyfikacji

[11] Pojęcie „kontrola" w opracowaniach naukowych było wielokrotnie definiowane i klasyfikowane przez teoretyków z wielu dyscyplin nauk społecznych, w tym zarządzania, finansów, rachunkowości i prawa. Definicje formułowane były w wielu różnych kontekstach w zależności od charakteru, przedmiotu i zakresu prowadzonych badań. W literaturze kontrola opisywana jest bardzo wieloznacznie. Klasyfikowana jest według wielu różnych kryteriów, np. według: cech, celów, funkcji, zadań, formy, rodzajów, podmiotu, zakresu, przedmiotu, czasu realizacji, charakteru, miejsca prowadzenia, profilu, sposobów planowania. Przykładowo według kryterium podmiotowego kontrolę dzieli się na zewnętrzną i wewnętrzną.

czynników ryzyka i podatności zasobów informatycznych na to ryzyko w środowisku informatycznym). Poza znajomością regulacji, wiedza teoretyczna na temat aktualnych metod i narzędzi oraz znajomość dobrych praktyk w wyżej wymienionych obszarach, stanowi ważny czynnik doskonalenia jakości zarządzania bezpieczeństwem zasobów informatycznych w jednostkach. Niewiedza w tych dziedzinach, podobnie jak brak zainteresowania kierownictwa problemami skutecznego zapewnienia bezpieczeństwa zasobów informatycznych rachunkowości, stanowi dla jednostki zagrożenie porównywalne z brakiem zapewnienia podstawowych środków ochrony tych zasobów.

Podczas prowadzenia badań własnych autorka przyjęła również hipotezę, że polskie jednostki, które zastosowały dodatkowe, dobrowolne regulacje (standardy, rekomendacje) dotyczące kontroli wewnętrznej (finansowej, zarządczej) mają skuteczniejszy system kontroli wewnętrznej w obszarze rachunkowości prowadzonej w środowisku informatycznym. Hipoteza ta została pozytywnie zweryfikowana podczas badań empirycznych, z których wnioski zostaną przedstawione w dalszej części opracowania. Regulacje te dostarczyły interdyscyplinarnej wiedzy i pomagały kierownikom jednostek w projektowaniu, ocenie i doskonaleniu systemów kontroli wewnętrznej w środowisku informatycznym, zwiększając w znaczący sposób poziom ochrony zasobów informatycznych rachunkowości w jednostkach.

Celem artykułu jest przedstawienie, na podstawie wniosków z przeprowadzonych badań empirycznych, autorskiej propozycji założeń do rekomendacji dotyczącej kontroli wewnętrznej w rachunkowości prowadzonej w środowisku informatycznym jednostek. Na podstawie analizy aktualnych koncepcji i regulacji dotyczących kontroli wewnętrznej zaproponowano również autorski, teoretyczny model systemu kontroli wewnętrznej. Model ten może być stosowany do projektowania i doskonalenia kontroli wewnętrznej w rachunkowości w środowisku informatycznym dowolnej jednostki. Wykorzystano go do opracowania struktury proponowanej przez autorkę rekomendacji. Problemy analizowane w niniejszym opracowaniu rozpoczynają dyskusję naukową, która może prowadzić do opracowywania odpowiedniego standardu dotyczącego systemu kontroli wewnętrznej w tym obszarze.

1. Potencjał poprawy jakości zarządzania bezpieczeństwem zasobów informatycznych rachunkowości – wnioski z badań

1.1. Przegląd regulacji dotyczących kontroli wewnętrznej, zarządzania ryzykiem i zarządzania bezpieczeństwem zasobów informatycznych w Polsce

Ustawodawca od 1995 roku przepisami ustawy o rachunkowości (UoR) zobowiązał kierowników jednostek do zapewnienia wiarygodności informacji finansowej i ochrony zasobów informatycznych rachunkowości. Podczas kolejnej nowelizacji UoR w 2001 roku przepisy w tym zakresie uległy znacznemu rozszerzeniu. Po 25 latach od ich pierwszego wprowadzenia nadal ich treść jest bardzo ogólna i nie wskazuje szczegółowych rozwiązań dla jednostek. Jest to uzasadnione charakterem aktu prawnego na poziomie ustawy.

Minister finansów lub inny organ do tego uprawniony (organizacja, komitet) ma jednak prawo wydać stosowny standard, rekomendację, komunikat lub stanowisko w tym zakresie[12].

Z raportów firm specjalistycznych zajmujących się badaniem bezpieczeństwa informatycznego w podmiotach (PwC, KPMG, Ernst & Young, Deloitte, McAfee, Centrum CSIS i in.) wynika, że instytucje finansowe od kilkunastu lat są głównym celem cyberataków, na drugim miejscu miejscach znalazły się systemy informatyczne i bazy rządowe oraz w jednostkach sektora finansów publicznych, a w dalszej kolejności – bazy danych dużych korporacji i firm prywatnych (Szczepankiewicz, 2018). Zjawisko to było jednym z ważniejszych powodów ustanowienia dla sektora finansów publicznych i sektora instytucji finansowych dodatkowych regulacji dotyczących systemów kontroli wewnętrznej, zarządzania ryzykiem i zarządzania bezpieczeństwem zasobów informatycznych[13].

Już w 2003 roku dla sektora finansów publicznych minister finansów wydał w formie komunikatu pierwsze standardy kontroli finansowej (Komunikat z 30.01.2003), które zostały w niewielkim zakresie uzupełnione w 2006 roku (Komunikat z 20.06.2006). W standardach kontroli finansowej pięć z nich bezpośrednio dotyczyło kontroli wewnętrznej w środowisku informatycznym i zapewnienia bezpieczeństwa zasobów informatycznych (Standardy nr 19–23 w obszarze „Mechanizmy kontroli", dla których ustanowiono podgrupę „Mechanizmy kontroli systemów informatycznych"). W 2006 roku minister finansów zalecił jednostkom stosowanie się do standardów zarządzania zasobami informatycznymi (Cobit, 2001) oraz standardów audytu opracowanych przez Międzynarodowe Stowarzyszenie do spraw Kontroli i Audytu Systemów Informatycznych (ISACA). Następnie w grudniu 2009 roku standardy kontroli finansowej zastąpiono

[12] W 2010 r. Komitet Standardów Rachunkowości odniósł się do UoR w sprawie niektórych zasad prowadzenia ksiąg rachunkowych (Komunikat nr 10 z 18.05.2010 r.). W tym dokumencie zdefiniowano tylko wybrane pojęcia i wyjaśniono podstawowe zasady prowadzenia komputerowych ksiąg rachunkowych po nowelizacji UoR. Nie odniesiono się w nim jednak do organizacji systemu kontroli wewnętrznej w środowisku informatycznym rachunkowości, nie wskazano również metodyki identyfikacji i analizy ryzyka informatycznego ani postępowania z tym ryzykiem.

[13] Powodów ustanowienia tych regulacji w tych dwóch sektorach było znacznie więcej niż tylko zapewnienie bezpieczeństwa zasobów informatycznych w podmiotach. W sektorze finansów publicznych ustanowienie pierwszych regulacji w tym zakresie wynikało z ustaleń przedakcesyjnych z UE o nowym systemie kontroli finansów publicznych. W sektorze finansowym w celu ochrony publicznego obrotu pieniężnego i interesów klientów tych instytucji najpierw w bankach pod koniec lat 90. XX w. przyjęto pierwsze bazylejskie rekomendacje zalecane przez Generalnego Inspektora Nadzoru Bankowego (a obecnie Komisję Nadzoru Finansowego), a w pozostałych instytucjach finansowych po zmianach prawa na poziomie UE i prawa krajowego po kryzysie finansowym (2008–2010). Należy zauważyć, że specyfika działania jednostek sektora finansów publicznych i instytucji finansowych spowodowała ustanowienie określonych, formalnych wymagań dla kontroli wewnętrznej w tych jednostkach. W pozostałych jednostkach z sektora prywatnego ustawodawca nie odniósł się formalnie do kontroli wewnętrznej, pozostawiając możliwość jej indywidualnego kształtowania w danej jednostce, jako elementu systemu zarządzania właścicielskiego.

obecnie obowiązującymi standardami kontroli zarządczej (Komunikat z 16.12.2009)[14]. Mając na uwadze ugruntowaną już w tym zakresie praktykę dotyczącą zapewnienia bezpieczeństwa zasobów informatycznych poprzednie pięć standardów skupiono tylko w jednym nowym standardzie, który został poświęcony zapewnieniu mechanizmów ochrony zasobów informatycznych. Jego treść jest bardzo ogólna i nie zawiera żadnych wytycznych szczegółowych w tym zakresie. W 2012 roku minister finansów ogłosił komunikat zawierający szczegółowe wytyczne dla tego sektora w zakresie planowania i zarządzania ryzykiem (Komunikat 6.12.2012). W kolejnych latach Ministerstwo Cyfryzacji ogłosiło „Politykę ochrony cyberprzestrzeni Rzeczypospolitej Polskiej" (2013) i „Metodykę zarządzania ryzykiem cyberprzestrzeni w systemach zarządzania bezpieczeństwem informacji podmiotów rządowych" (2015). Porównanie treści standardów kontroli finansowej i zarządczej w zakresie zarządzania bezpieczeństwem zasobów informatycznych zawiera tabela 1.

Tabela 1. Treść standardów kontroli finansowej i zarządczej dotyczących zagadnień w zakresie zarządzania bezpieczeństwem zasobów informatycznych w sektorze finansów publicznych

Dokument	Numer i nazwa standardu	Treść standardu
Standardy kontroli finansowej (2003, 2006)	19. Kontrola dostępu	W jednostce funkcjonują fizyczne lub logiczne mechanizmy kontroli, które ograniczają lub wykrywają nieuprawniony dostęp do zasobów informatycznych (np. sprzętu, systemu, aplikacji, danych) mające na celu ich ochronę przed nieautoryzowanymi zmianami, utratą lub ujawnieniem
	20. Kontrola oprogramowania systemowego	Wdrożono mechanizmy kontroli, które ograniczają i monitorują dostęp do oprogramowania systemowego
	21. Kontrola tworzenia i zmian w aplikacjach	W jednostce funkcjonują mechanizmy kontroli, które zapobiegają działaniom polegającym na wprowadzaniu nieautoryzowanych aplikacji lub zmian w funkcjonujących aplikacjach i wykrywają te działania
	22. Podział obowiązków	Kluczowe obowiązki dotyczące funkcjonowania systemów informatycznych zostały rozdzielone pomiędzy różne osoby, tak aby uniemożliwić nieuprawniony dostęp do zasobów lub danych

[14] Zarówno podczas opracowywania standardów kontroli finansowej, jak i zarządczej wykorzystano strukturę komponentów kontroli wewnętrznej proponowaną w raportach COSO, o których będzie mowa w pkt. 2 tego opracowania.

ciąg dalszy tabeli 1

Dokument	Numer i nazwa standardu	Treść standardu
	23. Ciągłość działalności	Wdrożono mechanizmy, które w przypadku wystąpienia niespodziewanych zdarzeń zapewniają, że najważniejsze operacje są prowadzone bez przeszkód lub zostaną wznowione oraz, że najważniejsze dane są właściwie chronione
	24. Kontrole aplikacyjne	Poszczególne aplikacje użytkowe wyposażone są w odpowiednie mechanizmy kontroli, których celem jest zapobieganie, wykrywanie i korygowanie błędów związanych z przetwarzaniem i przepływem danych. Aplikacyjne mechanizmy kontroli funkcjonują na etapie wprowadzania i przetwarzania danych, a także generowania informacji z sytemu
Standardy kontroli zarządczej (2009)	15. Mechanizmy kontroli dotyczące systemów informatycznych	Należy określić mechanizmy służące zapewnieniu bezpieczeństwa danych i systemów informatycznych

Źródło: opracowanie własne na podstawie: Załącznik do Komunikatu z 20.06.2006; Załącznik do Komunikatu z 16.12.2009.

Poza sektorem finansów publicznych tylko dla niektórych grup instytucji finansowych opracowano regulacje dotyczące kontroli wewnętrznej, zarządzania ryzykiem i bezpieczeństwa informacji. Pierwszą grupę tych instytucji stanowiły banki, które już od 1997 roku dobrowolnie wdrażały rekomendacje Bazylejskiego Komitetu ds. Nadzoru Bankowego (BKNB) dotyczące ochrony zasobów informatycznych (Rekomendacja D), od 1999 roku dotyczące kontroli wewnętrznej (Rekomendacja H), a od 2004 roku dotyczące zarządzania ryzykiem operacyjnym (Rekomendacja M) (Szczepankiewicz, 2011b, 2011c, 2012a). Ponadto w bankach od wielu lat stosowano wytyczne pt.: „Zasady zarządzania ryzykiem w bankowości elektronicznej" (2001), „Skonsolidowane zarządzanie ryzykiem PSK" (2004). Rekomendacje[15] i wytyczne dostarczyły bankom wiedzę przydatną do projektowania i doskonalenia systemu kontroli wewnętrznej w środowisku informatycznym. Drugą grupę instytucji finansowych stanowiły zakłady

[15] Obecnie banki stosują się do: trzeciej wersji Rekomendacji D (2013) dotyczącej zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego (pierwsza wersja została ogłoszona w 1997 r., druga w 2002 r.), czwartej wersji Rekomendacji H (2017) dotyczącej kontroli wewnętrznej (pierwsza wersja została ogłoszona w 1999 r., druga w 2002 r., trzecia w 2011 r., która uwzględnia założenia z raportu COSO i COSO II), drugiej wersji Rekomendacji M (2013) dotyczącej zarządzania ryzykiem operacyjnym (pierwsza jej wersja została ogłoszona w 2004 r.).

ubezpieczeń i reasekuracji, które od 2012 roku na podstawie dyrektywy *Solvence II* i nowego prawa ubezpieczeniowego wdrażały nowe systemy zarządzania obejmujące m.in. zarządzanie ryzykiem, kontrolę wewnętrzną i audyt wewnętrzny (Kiedrowska, Szczepankiewicz, 2011; Szczepankiewicz, 2012b; *Solvency II*, 2013, Lament, 2013). Polska Izba Ubezpieczeniowa zaleciła ubezpieczycielom stosowanie Standardu nr 2.2.6 (2008) dotyczącego zarządzania ryzykiem korporacyjnym, a także opracowała wytyczne na potrzeby audytu wewnętrznego w środowisku informatycznym (Szczepankiewicz, Kiedrowska, 2011). Ostatnią grupą instytucji objętych przedmiotowymi regulacjami są towarzystwa funduszy inwestycyjnych, które od 2013 roku stosują w praktyce przepisy rozporządzenia o kontroli wewnętrznej, zarządzaniu ryzykiem i audycie wewnętrznym (Rozporządzenie z 30.04.2013; Szczepankiewicz, 2014). Natomiast dla Powszechnych Towarzystw Emerytalnych i innych instytucji finansowych nie ogłoszono dotychczas żadnych regulacji w podobnym zakresie.

Należy również podkreślić, że wiele dużych jednostek, zarówno w sektorze finansów publicznych, w sektorze finansowym, jak i w sektorze prywatnym (w szczególności korporacje), wdrożyło wytyczne i standardy ISACA, a także normy ISO dotyczące zarządzania ryzykiem informatycznym i zapewnienia bezpieczeństwa informacji, np. PN-ISO/IEC 27005:2014-01, PN-ISO/IEC 27001:2014-12 i inne.

Analizując treść wyżej wymienionych regulacji należy stwierdzić, że żadna z nich nie odnosi się bezpośrednio do organizacji kontroli wewnętrznej w obszarze rachunkowości prowadzonej w środowisku informatycznym, chociaż wiele z pojedynczych zapisów w tych regulacjach może być przydatne do rozwiązania problemów w tym obszarze.

1.2. Opis próby badawczej

Autorka od lutego 2014 roku do stycznia 2016 roku przeprowadziła pierwsze w kraju[16] badania empiryczne[17] na temat podstawowych aspektów organizacji systemów kontroli wewnętrznej w środowisku informatycznym, ze szczególnym uwzględnieniem ochrony zasobów informatycznych rachunkowości (ZIR) w jednostkach. Do przeprowadzenia badań zaaplikowano podstawowe założenia światowej koncepcji kontroli

[16] Autorka, dokonując przeglądu literatury oraz raportów na temat bezpieczeństwa informacji w polskich jednostkach, nie znalazła badań empirycznych na temat jakości systemów zapewnienia bezpieczeństwa zasobów informatycznych rachunkowości w kontekście organizacji systemów kontroli wewnętrznej w środowisku informatycznym oraz w świetle wymagań stawianych przez UoR.

[17] Badania były przeprowadzone w formie anonimowej ankiety (zbieranie wyników metodą audytoryjną i metodą CAWI) oraz w formie uzupełniających indywidualnych, ustrukturyzowanych wywiadów ukierunkowanych i eksperckich (metodą kwestionariuszową), a także metodą obserwacji uczestniczącej w wybranych jednostkach.

wewnętrznej COSO (1992, 1994, 2009) i COSO II (2004). Próbę badawczą stanowiło 415 jednostek, w tym[18]:

- 106 jednostek samorządu terytorialnego (JST), reprezentujących sektor finansów publicznych;
- 14 instytucji finansowych (IF);
- 295 firm prywatnych (FP) prowadzących rachunkowość na podstawie przepisów UoR (o różnych wielkościach, formach własności, reprezentujących różne branże), w tym 29 biur rachunkowych i firm audytorskich (zatrudniających mniej niż 20 osób).

Na potrzeby niniejszej analizy z próby badawczej reprezentującej jednostki w sektorze prywatnym usunięto odpowiedzi uzyskane z biur rachunkowych i firm audytorskich. Takie wyodrębnienie tych podmiotów autorka uznała za ważne, przyjmując hipotezę, że podmioty te najlepiej znają obowiązujące regulacje w przedmiotowym zakresie badania i prawdopodobnie restrykcyjnie przestrzegają przepisów dotyczących zapewnienia bezpieczeństwa danych finansowych swoich klientów. Wstępna analiza badań pozytywnie zweryfikowała hipotezę, dlatego w tym przypadku odpowiedzi uzyskane z tych podmiotów zawyżają wyniki badania uzyskane z małych firm w sektorze prywatnym. Z powyższych względów do niniejszej analizy przyjęto 266 z 295 ankiet z grupy jednostek reprezentujących sektor prywatny.

1.3. Metodyka i wyniki badań

Uwzględniając założenia koncepcji COSO i COSO II, prezentację wyników przeprowadzono w obszarach systemu kontroli wewnętrznej w środowisku informatycznym, które mają wpływ na właściwe zapewnienie bezpieczeństwa ZIR w badanych jednostkach. Są to następujące obszary badania:

1) kształtowanie środowiska kontroli oraz systemu informacji i komunikacji;
2) podejście do identyfikacji, analizy i postępowania z ryzykiem;
3) stosowanie mechanizmów organizacyjno-administracyjnych oraz zabezpieczeń fizyczno-technicznych i programowych.

Szczegółowe wyniki i wnioski z badań empirycznych na temat poziomu ochrony ZIR zaprezentowano w opracowaniu (Szczepankiewicz, 2018), natomiast w niniejszym artykule zostanie zweryfikowana hipoteza postawiona we wstępie, tj.: „Polskie

[18] W JST anonimowe ankiety skierowano do kierowników i pracowników wydziałów/działów finansowych oraz audytorów wewnętrznych. W pozostałych jednostkach ankiety wypełniali pracownicy działów finansowo-księgowych, pracownicy administracji oraz audytorzy wewnętrzni i zewnętrzni. W wybranych jednostkach przeprowadzono wywiady osobiste, które dotyczyły różnych aspektów stosowania określonych rozwiązań w zakresie bezpieczeństwa informatycznego.

jednostki, które przyjęły do stosowania dodatkowe regulacje (standardy, rekomendacje) dotyczące kontroli wewnętrznej mają skuteczniejszy system kontroli wewnętrznej w obszarze rachunkowości prowadzonej w środowisku informatycznym".

Wstępne wyniki badań przeprowadzonych w IF wskazywały, że łączny średni wynik oceny jakości systemu kontroli wewnętrznej w obszarze zapewnienia bezpieczeństwa zasobów informatycznych wynosi 95%, ale w poszczególnych kategoriach oceny jego komponentów wyniki zawierały się w przedziale 80–100%. Natomiast wstępne wyniki badań przeprowadzonych w JST wskazywały, że łączny średni wynik oceny jakości systemu kontroli wewnętrznej wynosi 67%, ale w poszczególnych kategoriach oceny jego komponentów wyniki zawierały się w przedziale 42–90%. W FP większość wyników była znacznie niższa niż w JST. Jedynie porównywalne wyniki do JST uzyskano w dużych FP, a w szczególności w dużych korporacjach, które stosują normy ISO dotyczące zarządzania bezpieczeństwem informacji i/lub posiadają komórki audytu wewnętrznego, które badają ten obszar zarządzania.

Ostatecznie, po wstępnym przeglądzie wyników, na potrzeby niniejszej analizy badane jednostki podzielono na dwie zasadnicze grupy. Pierwszą grupę stanowią jednostki z sektora firm prywatnych (FP), dla których podstawowe wytyczne w przedmiotowym zakresie badania określa UoR i dla jednostek tych dotychczas nie opracowano żadnych dodatkowych regulacji w przedmiotowym zakresie badania. Drugą zasadniczą grupę stanowią „jednostki odniesienia", dla których ogłoszone zostały dodatkowe regulacje w zakresie kontroli wewnętrznej, analizy ryzyka i ochrony zasobów informatycznych. Są to JST oraz IF.

W ramach firm z sektora prywatnego wyodrębniono pierwszą grupę reprezentującą małe i średnie FP i obliczono dla nich wyniki uzyskania odpowiedzi „tak" od ankietowanych według średniej ważonej. Drugą grupę reprezentują duże FP zatrudniające powyżej 100 pracowników. Taki podział na dwie podgrupy FP jest uzasadniony znacznie różniącym się podejściem do stopnia formalizowania organizacji kontroli w małych i średnich oraz dużych jednostkach[19].

Wyniki z JST oraz IF włączono do jednej grupy odniesienia, jako podmioty stosujące poza przepisami UoR dodatkowe regulacje w przedmiotowym zakresie badania. Takie połączenie odpowiedzi z JST i IF wynika z ostrożnego podejścia badawczego autorki, bowiem nie jest możliwe, ani konieczne, aby w FP systemy kontroli wewnętrznej w zakresie zapewnienia bezpieczeństwa zasobów informatycznych funkcjonowały na takim samym poziomie zaawansowania jak w IF. Następnie ustalono średnie ważone odpowiedzi „tak" ankietowanych z IF i JST. Dodatkowo ustalono również wartości

[19] Mniejsze FP charakteryzują się znacznie niższym stopniem sformalizowania organizacji i kontroli niż duże FP, które formalizują wszelkie działania na każdym poziomie organizacji w formie: pisemnych polityk, regulaminów, instrukcji, procedur, ściśle określonego podziału obowiązków, uprawnień i odpowiedzialności itp.

docelowe pokazujące wyniki uzyskane z badanych IF, bowiem można je uznać jako „wzorzec" (dobre praktyki) dla innych podmiotów, zarówno z JST, jak i FP.

W części pierwszej tabeli 2 zaprezentowano wyniki badania (odpowiedzi „tak" respondentów), a w części drugiej tabeli 2 prognozowany wzrost jakości systemu kontroli wewnętrznej w obszarze rachunkowości prowadzonej w środowisku informatycznym po wprowadzeniu standardu (wytycznych, rekomendacji lub komunikatu).

W celu ustalenia prognozowanego wzrostu jakości systemu kontroli wewnętrznej przyjęto, że zostanie on zbadany metodą potencjału wzrostu[20] na podstawie:

1) wyników uzyskanych z małych i średnich FP w odniesieniu do średniej ważonej jednostek posiadających dodatkowe regulacje (JST i IF);
2) wyników uzyskanych z małych i średnich FP w odniesieniu do wartości docelowej (wzorca – dobrych praktyk w IF);
3) wyników uzyskanych z dużych FP w odniesieniu do średniej ważonej podmiotów posiadających dodatkowe regulacje (JST i IF);
4) wyników uzyskanych w dużych FP w odniesieniu do wartości docelowej (wzorca – dobrych praktyk w IF).

Wyniki badań pozytywnie zweryfikowały postawioną we wstępnie hipotezę. Dane prezentowane w pierwszej części tabeli 2 pokazują, że zbiór regulacji wdrożonych w IF miał bardzo duży wpływ na jakość systemów kontroli wewnętrznej w środowisku informatycznym tych instytucji, bowiem jakość systemów kontroli wewnętrznej w IF ankietowani ocenili średnio na poziomie 95%. Natomiast stosowanie w sektorze finansów publicznych nawet jednego ogólnego standardu ochrony zasobów informatycznych nr 15 w ramach standardów kontroli zarządczej od 2010 roku (a wcześniej pięciu standardów kontroli finansowej od 2003 roku) w ciągu 15 lat znacznie poprawiło jakość systemów kontroli wewnętrznej w JST w stosunku do jednostek z sektora prywatnego, dla którego nie ogłoszono żadnych wytycznych ułatwiających opracowanie i wdrożenie skutecznego systemu kontroli wewnętrznej. Jakość systemów kontroli wewnętrznej w JST ankietowani ocenili średnio na poziomie 67%. Średnia ważona dla badanych JST i IF wynosiła ponad 70%. Jakość systemów kontroli wewnętrznej w małych i średnich FP ankietowani ocenili średnio na poziomie 41%, w dużych FP – 53%.

[20] Przyjęto, że wartość prognozowanego wzrostu jakości systemu kontroli wewnętrznej zostanie ustalona metodą opracowaną przez Komisję Europejską w dokumencie InCaS (2008). Przykładowy sposób obliczenia: uzyskany wynik z badań systemu kontroli wewnętrznej w FP wynosi 25%, wynik do którego jest on odniesiony (np. z JST i IF) wynosi 60%, to wartość obliczona aktualnego stanu jakości systemu kontroli wewnętrznej wynosi w FP 42% z wartości wyniku docelowego, zatem istnieje potencjał poprawy (liczony do 100% wartości odniesienia), który wynosi 58%.

Tabela 2. Prognozowany potencjał poprawy zapewnienia bezpieczeństwa ZIR w badanych jednostkach po ogłoszeniu standardu (dane w %)

Pytanie	Odpowiedzi „tak”				Prognozowany wzrost jakości systemu kontroli wewnętrznej			
	Małe i średnie FP	Duże FP	JSFP i IF posiadających dodatkowe regulacje	IF – wartość docelowa (wzorzec-dobre praktyki)	Małe i średnie FP do podmiotów posiadających dodatkowe regulacje	Małe i średnie FP do wartości docelowej (wzorca)	Duże FP do podmiotów posiadających dodatkowe regulacje	Duże FP do wartości docelowej (wzorca)
Kształtowanie środowiska kontroli oraz systemu informacji i komunikacji w obszarze zapewnienia bezpieczeństwa ZIR								
1. Czy bierze Pani/Pan udział w wystarczającym stopniu w szkoleniach, aby skutecznie realizować powierzone zadania z zakresu ochrony zasobów informatycznych?	24	40	55	94	56	74	**27**	**57**
2. Czy ma Pani/Pan bieżący dostęp do procedur/instrukcji w zakresie ochrony ZIR obowiązujących w jednostce (na przykład poprzez intranet)?	40	54	87	94	54	57	**38**	**43**
3. Czy wie Pani/Pan jak postępować w przypadku wystąpienia sytuacji nadzwyczajnej, na przykład pożaru, zalania, poważnej awarii systemu informatycznego?	82	82	84	94	2	13	**2**	**13**
4. Czy postawa osób na stanowiskach kierowniczych w Pani/Pana komórce organizacyjnej zachęca pracowników do sygnalizowania problemów i zagrożeń informatycznych przy realizacji zadań komórki organizacyjnej?	63	68	67	86	6	27	**-1**	**21**

ciąg dalszy tabeli 2

Pytanie	Odpowiedzi „tak”				Prognozowany wzrost jakości systemu kontroli wewnętrznej			
	Małe i średnie FP	**Duże FP**	**JSFP i IF posiadających dodatkowe regulacje**	**IF – wartość docelowa (wzorzec-dobre praktyki)**	**Małe i średnie FP do podmiotów posiadających dodatkowe regulacje**	**Małe i średnie FP do wartości docelowej (wzorca)**	**Duże FP do podmiotów posiadających dodatkowe regulacje**	**Duże FP do wartości docelowej (wzorca)**
5. Czy przełożeni na co dzień zwracają wystarczającą uwagę na przestrzeganie przez pracowników zasad, procedur, instrukcji itp. obowiązujących w jednostce?	41	51	58	100	29	59	**12**	**49**
Średnia dla komponentu kontroli wewnętrznej	**50**	**59**	**70**	**94**	**29**	**47**	**16**	**37**
Podejście do zarządzania ryzykiem w obszarze zapewnienia bezpieczeństwa informatycznego								
1. Czy w Pani/Pana komórce organizacyjnej systematycznie, w udokumentowany sposób identyfikuje się zagrożenia informatyczne, które mogą przeszkodzić w realizacji celów i zadań komórki organizacyjnej (na przykład poprzez sporządzanie rejestru ryzyka lub innego dokumentu zawierającego zidentyfikowane zagrożenia/ryzyka)?	17	25	52	86	67	80	**52**	**71**
2. Czy wśród zidentyfikowanych zagrożeń informatycznych wskazuje się istotne zagrożenia, które w znaczący sposób mogą przeszkodzić w realizacji celów i zadań komórki organizacyjnej? – Tylko podmioty, które odpowiadały na pytanie 1.	40	45	58	80	31	50	**22**	**44**

	Odpowiedzi „tak”				Prognozowany wzrost jakości systemu kontroli wewnętrznej			
	Małe i średnie FP	**Duże FP**	**JSFP i IF posiadających dodatkowe regulacje**	**IF – wartość docelowa (wzorzec-dobre praktyki)**	**Małe i średnie FP do podmiotów posiadających dodatkowe regulacje**	**Małe i średnie FP do wartości docelowej (wzorca)**	**Duże FP do podmiotów posiadających dodatkowe regulacje**	**Duże FP do wartości docelowej (wzorca)**
3. Czy w Pani/Pana komórce organizacyjnej podejmuje się wystarczające działania mające na celu ograniczenie zidentyfikowanych zagrożeń informatycznych, w szczególności tych istotnych? – Tylko podmioty, które odpowiadały na pytanie 1 i 2.	32	36	49	94	35	66	**27**	**62**
Średnia dla komponentu kontroli wewnętrznej (dotyczy pytania 2 i 3)	**36**	**41**	**54**	**87**	**33**	**58**	**25**	**53**
Stosowanie procedur organizacyjnych oraz zabezpieczeń technicznych i programowych w obszarze zapewnienia bezpieczeństwa informatycznego								
1. Czy w jednostce opracowano dokumenty (procedury, instrukcje, szczegółowe polityki) opisujące system bezpieczeństwa danych informatycznych?	33	61	67	100	36	57	**9**	**39**
2. Czy opracowano procedury awaryjne dla SIR?	31	41	58	86	47	64	**29**	**52**
3. Czy obowiązujące procedury/instrukcje w zakresie ochrony ZIR są aktualne, tzn. zgodne z obowiązującymi przepisami prawa i regulacjami wewnętrznymi?	38	53	81	100	53	62	**35**	**47**
4. Czy dokumenty i inne zasoby informatyczne, z których korzysta Pani/Pan w swojej pracy są odpowiednio chronione przed utratą lub zniszczeniem?	53	61	75	100	29	47	**19**	**39**

ciąg dalszy tabeli 2

Pytanie	Odpowiedzi „tak”				Prognozowany wzrost jakości systemu kontroli wewnętrznej			
	Małe i średnie FP	**Duże FP**	**JSFP i IF posiadających dodatkowe regulacje**	**IF – wartość docelowa (wzorzec-dobre praktyki)**	**Małe i średnie FP do podmiotów posiadających dodatkowe regulacje**	**Małe i średnie FP do wartości docelowej (wzorca)**	**Duże FP do podmiotów posiadających dodatkowe regulacje**	**Duże FP do wartości docelowej (wzorca)**
5. Czy w jednostce w regularnych odstępach czasu tworzy się rezerwowe kopie danych?	50	66	88	100	43	50	**25**	**34**
6. Czy rezerwowe kopie danych przechowuje się w wydzielonych i zabezpieczonych pomieszczenia dla tego celu?	35	51	76	100	53	65	**33**	**49**
7. Czy SIR wymuszają okresową zmianę hasła przez użytkownika?	51	66	85	100	40	49	**22**	**34**
8. Czy w jednostce jest procedura przydzielania użytkownikom systemów uprawnień do danych, funkcji programów i komputerów?	38	57	81	100	53	62	**30**	**43**
9. Czy organizowane są szkolenia dla nowozatrudnionych pracowników w zakresie bezpieczeństwa danych informatycznych?	28	42	48	94	42	70	**13**	**55**
10. Czy w jednostce stosuje się procedury i zabezpieczenia przed pozyskaniem danych informatycznych wobec osób i firm współpracujących, np. firm sprzątających, serwisu?	26	39	65	94	60	72	**40**	**59**
11. Czy jednostka stosuje zapasowe źródła zasilania sprzętu informatycznego?	56	69	91	100	38	44	**24**	**31**

Pytanie	Odpowiedzi „tak”				Prognozowany wzrost jakości systemu kontroli wewnętrznej			
	Małe i średnie FP	Duże FP	JSFP i IF posiadających dodatkowe regulacje	IF – wartość docelowa (wzorzec-dobre praktyki)	Małe i średnie FP do podmiotów posiadających dodatkowe regulacje	Małe i średnie FP do wartości docelowej (wzorca)	Duże FP do podmiotów posiadających dodatkowe regulacje	Duże FP do wartości docelowej (wzorca)
12. Czy w jednostce wyodrębniono specjalne strefy bezpieczeństwa, takie jak na przykład: serwerownia, archiwum przechowywania danych itp.?	31	55	73	100	58	69	**25**	**45**
13. Czy w jednostce przeprowadza się okresową weryfikację legalności oprogramowania zainstalowanego na komputerach?	39	53	67	100	42	61	**21**	**47**
Średnia dla komponentu kontroli wewnętrznej	39	55	73	98	46	59	**25**	**44**
Średnia ogółem dla systemu kontroli wewnętrznej	**41**	**53**	**70**	**95**	**42**	**57**	**24**	**44**

Źródło: opracowanie własne.

Wyniki analizy zamieszczone w prawej części tabeli 2 jednoznacznie wskazują, że istnieje wysoki potencjał poprawy jakości zarządzania bezpieczeństwem ZIR w jednostkach z sektora prywatnego, który mógłby być zrealizowany po ogłoszeniu dodatkowych regulacji w formie standardu, rekomendacji lub komunikatu dotyczącego kontroli wewnętrznej w rachunkowości prowadzonej w środowisku informatycznym.

Łączny średni potencjał poprawy jakości systemów kontroli wewnętrznej w środowisku informatycznym rachunkowości (liczony metodą do 100% wartości odniesienia tj. „wzorca" w IF) może wynosić nawet 57% dla małych i średnich firm oraz 44% dla dużych firm w sektorze prywatnym. Jednak zachowując rozsądne podejście badacza i biorąc pod uwagę jako wzorzec średnią ważoną badanych JST i IF (70%), potencjał poprawy dla małych i średnich FP wynosi co najmniej 42%, a dla dużych FP co najmniej 24%.

Wyniki badań pokazały również, że w firmach prywatnych istnieją szczególne obszary „niewiedzy", wynikające z luki metodycznej i aplikacyjnej w literaturze przedmiotu. Ich uzupełnienie przez teoretyków i odpowiednie regulacje mogą w znaczący sposób poprawić zarządzanie bezpieczeństwem zasobów informatycznych w polskich jednostkach. Takim obszarem jest na przykład podejście do identyfikacji czynników ryzyka oraz ich systematyzacja, a także sposobów postępowania z ryzykiem. W małych i średnich firmach po wprowadzeniu standardu istnieje potencjał poprawy jakości systemu kontroli wewnętrznej w obszarze identyfikacji czynników ryzyka informatycznego na poziomie 67%, a docelowo w dłuższym okresie oszacowano go na poziomie 80% (według „wzorca" IF), natomiast w dużych firmach potencjał poprawy po wdrożeniu standardu wynosi 52%, a docelowo 71%.

Ankietowanym zadano również pytanie: czy w związku z wymaganiami ustawy UoR i innymi regulacjami, a także rosnącym ryzykiem informatycznym dotyczącym jednostek, Ministerstwo Finansów lub teoretycy i specjaliści rachunkowości powinni opracować wytyczne ułatwiające samoocenę stosowanych procedur w zakresie ochrony zasobów informatycznych rachunkowości i kontroli w środowisku informatycznym rachunkowości w jednostce? Wyniki odpowiedzi uzyskane z ankiet są jednoznaczne i wskazują na bardzo duże zainteresowanie ankietowanych (średnio 87%). Oznacza to, że 336 z 396 ankietowanych (księgowych, pracowników działów finansowych, audytorów i przedstawicieli kierownictwa) jest zainteresowanych otrzymaniem wytycznych/standardu, które ułatwią ocenę stanu wypełniania obowiązków formalnych w zakresie ochrony zasobów informatycznych rachunkowości i zapewnienia skutecznej kontroli w środowisku informatycznym (zob. tab. 3).

Tabela 3. Zainteresowanie narzędziami do samooceny wypełniania obowiązków w zakresie ochrony ZIR i zapewnienia skutecznej kontroli wewnętrznej w środowisku informatycznym

Pytanie	Odpowiedzi tak (w %)						
	JST	**IF**	**BRiA**	**FP 20**	**FP 100**	**FP >100**	**Średnia**
Czy w związku z wymaganiami UoR, standardami kontroli wewnętrznej (zarządczej) i rosnącym ryzykiem informatycznym dotyczącym jednostek, Ministerstwo Finansów lub teoretycy i specjaliści rachunkowości powinni opracować szczegółowe wytyczne ułatwiające samoocenę procedur w zakresie ochrony zasobów informatycznych rachunkowości i kontroli wewnętrznej (zarządczej) w środowisku informatycznym rachunkowości w jednostce?	95	100	94	68	78	86	**87**

Źródło: opracowanie własne.

2. System kontroli wewnętrznej w jednostce według koncepcji i standardów światowych oraz model autorski kontroli wewnętrznej w jednostce

W literaturze istnieje wiele definicji kontroli. Jako funkcję zarządzania w organizacji definiowali ją znani światowi klasycy teorii organizacji i zarządzania: R.J. Mocler (1984)[21], J.A.F. Stoner i Ch. Wankel (1996), R.W. Griffin (1999), J.A.F. Stoner i in., (2001), A.P. Robbins i M. Coulter (2012). Choć definicje te nieco różnią się zakresem, to ostateczny ich kontekst jest bardzo podobny. Każda następna stanowiła pewne uzupełnienie poprzedniej, ale żadną z nich nie można uznać jako pełną. Definicje klasyków teorii i zarządzania wykorzystywano także w innych dyscyplinach nauki. Definiowali ją także teoretycy rachunkowości, np.: E. Terebucha (1976), K. Klimas (1985), K. Wierzbicki (1996), E.J. Saunders (1994, 2003), S. Kałużny (1997, 2008), K. Winiarska (2010) i inni. Każdy z tych autorów w nieco innym zakresie opisał to pojęcie, ale wszyscy podkreślili charakter funkcjonalny kontroli, jako konieczne końcowe stadium zorganizowanego działania (procesu kierowania), polegające na sprawdzaniu

[21] Definicję Moclera przytacza Stoner, Wankel (1996, s. 458).

i ocenianiu różnych obszarów działalności. W podobny sobie sposób teoretycy rachunkowości definiują cel i funkcje kontroli oraz mechanizmy kontrolne. Jako szczególną formę kontroli wewnętrznej w rachunkowości wymieniają zawsze kontrolę finansowo-księgową. W niniejszym opracowaniu pominięto prezentację powszechnie znanych definicji wyżej wymienionych autorów, a przytoczono jedynie aktualne definicje normatywne rozproszone w różnych regulacjach, bowiem to one oddają istotę aktualnego podejścia do kontroli wewnętrznej w rachunkowości. Należy przy tym wspomnieć, że na świecie głównymi inicjatorami rozwoju koncepcji kontroli wewnętrznej – były i są – organizacje zawodowe księgowych, biegłych rewidentów oraz audytorów wewnętrznych. Organizacje te ciągle doskonalą zarówno definicje, jak i samą koncepcję systemu kontroli wewnętrznej.

Dwie kluczowe definicje „kontroli wewnętrznej" oraz „systemu kontroli wewnętrznej", które stanowią fundament dla pozostałych definicji formułowanych w następnych latach przez inne organizacje zajmujące się standardami w zakresie kontroli i audytu, ogłosił w 1992 roku amerykański Komitet Sponsorujący Komisję *Treadway* (The Committee of Sponsoring Organizations of the Treadway Commission) w raporcie poświeconym kontroli wewnętrznej pod nazwą COSO[22]. Zgodnie z COSO (1992, 1994, 2009) kontrola wewnętrzna jest ciągłym procesem inicjowanym i realizowanym przez radę nadzorczą, zarząd, kierownictwo na niższych szczeblach organizacyjnych i pracowników, zaprojektowanym w celu dostarczenia kierownictwu obiektywnego zapewnienia, że możliwa jest realizacja celów jednostki w następujących obszarach:

- wydajność, efektywność i zyskowność działań operacyjnych w jednostce, w tym ochrony zasobów;
- wiarygodność sprawozdawczości finansowej i raportów wewnętrznych;
- zgodność z przepisami prawa oraz przyjętymi w jednostce regulacjami zewnętrznymi i wewnętrznymi.

System kontroli wewnętrznej według COSO składa się z 5 głównych komponentów: środowiska kontroli, oszacowania ryzyka, czynności kontrolnych, informacji i komunikacji oraz monitoringu. Należy wspomnieć, że Komisja *Treadway* w 2004 roku ogłosiła raport COSO II rozszerzający aspekty kontroli wewnętrznej w obszarze zarządzania ryzykiem. Zgodnie z COSO II (2004) system kontroli wewnętrznej powinien być zintegrowany z procesem zarządzania ryzykiem w jednostce i składać się z ośmiu głównych komponentów: środowiska wewnętrznego, ustalania celów, identyfikacji zdarzeń, oceny ryzyka, reakcji na ryzyko, działań kontrolnych, informacji i komunikowania oraz

[22] Koncepcję COSO przyjęto do stosowania w 2002 r. w sekcji 404 – *Management Assessment of Internal Controls* w *Sarbanes Oxley Act* (SOX) oraz aktach wykonawczych i innych wytycznych takich jak: *Internal Controls Over Financial Reporting* – SOX (2004), *IT Control Objectives for Sarbanes-Oxley* (2004), COBIT (2004), amerykańskich standardach rewizji finansowej AICPA, międzynarodowych standardach audytu wewnętrznego IIA, wytycznych Komisji Europejskiej, *The Revised Internal Control Standard for Effective Management* SEC (2007), polskich Standardach kontroli finansowej (2003), Standardach kontroli zarządczej (2009), Rekomendacji H, Rekomendacji M oraz wielu innych dokumentach.

monitorowania. W obu raportach COSO i COSO II zdefiniowano i szeroko opisano znaczenie poszczególnych komponentów systemu kontroli wewnętrznej.

W podobnym kontekście funkcjonalnym kontrolę wewnętrzną w 2001 roku zdefiniował Międzynarodowy Instytut Audytorów Wewnętrznych (*The Internacional Institute of Auditors – IIA*). Definicja ta znalazła się w słowniku do Międzynarodowych Standardów Profesjonalnej Praktyki Audytu Wewnętrznego. Według IIA kontrola wewnętrzna to każde działanie podejmowane przez radę nadzorczą, kierownictwo i pracowników w celu zarządzenia ryzykiem i zwiększenia prawdopodobieństwa osiągnięcia ustanowionych celów przez jednostkę. Kierownictwo planuje i organizuje wszelkie działania, aby uzyskać racjonalne zapewnienie, że ogólne i szczegółowe cele jednostki zostaną zrealizowane; kieruje także wykonaniem tych działań (Słownik w: Standardy IIA, 2016). Definicja ta od 2001 roku nie była zmieniana, pomimo czterokrotnej aktualizacji Standardów IIA. W 2016 roku IIA zdefiniowało również pojęcie „odpowiedniej kontroli", która „ma miejsce wówczas, gdy kierownictwo zaplanowało i zorganizowało kontrolę w sposób dający racjonalne zapewnienie, że organizacja skutecznie zarządza ryzykiem, a jej ogólne i szczegółowe cele zostaną sprawnie i ekonomicznie zrealizowane" (Słownik w: Standardy IIA, 2016). IIA w swoich wytycznych zaleca audytorom wewnętrznym rozpatrywanie systemu kontroli wewnętrznej zgodnie z koncepcjami COSO. W słowniku do Standardów IIA zdefiniowała tylko niektóre komponenty systemu kontroli wewnętrznej: środowisko kontroli, zarządzanie ryzykiem, procesy (zasady, procedury, mechanizmy) kontroli oraz informatyczne mechanizmy kontrolne. Jednak kontekst treści tych definicji nie odbiega w znaczący sposób od treści definicji ogłoszonych w raportach COSO i COSO II.

Międzynarodowa Organizacja Najwyższych Organów Kontroli/Audytu (International Organization of Supreme Audit Institutions – INTOSAI) w „Wytycznych w sprawie kontroli wewnętrznej w sektorze publicznym" z 2004 roku, zdefiniowała kontrolę wewnętrzną w ujęciu funkcjonalnym jako integralny proces, na który ma wpływ zarząd jednostki oraz jej pracownicy. Kontrola wewnętrzna jest procesem dynamicznym, który musi być ciągle dostosowywany do zachodzących zmian w jednostce. Kierownictwo i pracownicy wszystkich szczebli organizacyjnych powinni mieć udział w procesie kontroli poprzez odnoszenie się do ryzyk oraz dawanie rozsądnego zapewnienia o osiąganiu misji jednostki, a także realizacji przyjętych celów. Kontrola wewnętrzna powinna być zaprojektowana w taki sposób, aby odnosić się do ryzyk i dawać rozsądne zapewnienie, że wszystkie działania jednostki są skierowane na wypełnianie jej misji oraz pomagają jednostce w osiągnięciu następujących celów (Wytyczne INTOSAI, 2004):

- prowadzenie etycznej, uporządkowanej, skutecznej, gospodarczej i wydajnej działalności;
- wypełnianie obowiązków związanych z odpowiedzialnością za swoją działalność;
- zapewnienie zgodności prowadzonej działalności z prawem i przepisami;
- właściwa ochrona posiadanych zasobów przed ich niewłaściwym wykorzystaniem, utratą lub zniszczeniem.

W 2009 roku w nowej wersji Międzynarodowych Standardów Rewizji Finansowej (MSRF) również zdefiniowano kontrolę wewnętrzną oraz system kontroli wewnętrznej. Definicje te zawarto w MSRF 315. Nawiązały one już do definicji zawartych w raporcie COSO. Według MSRF 315 z 2009 roku kontrola wewnętrzna to „proces zaprojektowany, wdrożony i utrzymywany przez osoby sprawujące nadzór, kierownika jednostki i innych pracowników, mający dostarczyć wystarczającej pewności, że cele jednostki dotyczące wiarygodności sprawozdawczości finansowej, skuteczności i wydajności działalności oraz zgodności z mającymi zastosowanie przepisami prawa oraz regulacjami są osiągane". Wskazano również, że sposób zaprojektowania, wdrożenia i prowadzenia kontroli wewnętrznej może różnić się w poszczególnych jednostkach w zależności od ich wielkości i złożoności działalności. W standardzie tym określono także cel podstawowy kontroli wewnętrznej, zgodnie z którym „kontrola wewnętrzna jest projektowana, wdrażana i prowadzona, jako reakcja na zidentyfikowane ryzyka gospodarcze zagrażające osiągnięciu trzech celów jednostki, które dotyczą (punkt A51 KSRF 315): wiarygodności sprawozdawczości finansowej jednostki; efektywności i skuteczności działań jednostki; przestrzegania przepisów prawa i regulacji". Elementy kontroli wewnętrznej w MSRF 315 zostały podobnie określone jak w raporcie COSO, są nimi: środowisko kontroli; proces oceny ryzyka przez jednostkę; system informacyjny (w tym powiązane procesy gospodarcze, znaczące dla sprawozdawczości finansowej) i komunikacji; działania kontrolne (znaczące dla rewizji finansowej) oraz monitorowanie kontroli. Zostały one szczegółowo zdefiniowane w załączniku do MSRF 315. Obecnie definicje te są zawarte w Międzynarodowym Standardzie Badania (MSB) 315, który został przyjęty w 2015 roku jako Krajowy Standard Rewizji Finansowej (KSRF) 315 przez Polską Izbę Biegłych Rewidentów. Niestety, po ostatnich zmianach w MSB 315 nie uwzględniono nadal koncepcji zintegrowanego systemu kontroli wewnętrznej COSO II.

Po analizie treści definicji kontroli wewnętrznej teoretyków zarządzania i rachunkowości oraz definicji normatywnych można sprowadzić je do sformułowania autorskiej definicji oddającej pełniej istotę współczesnej kontroli wewnętrznej (funkcjonalnej) w jednostce, a mianowicie: „kontrola wewnętrzna to określony system organizacyjny (system kontroli wewnętrznej) wewnętrznie skoordynowany, mający określoną strukturę (układ elementów – komponenty), w którym poszczególne jego części składowe powinny się wzajemnie uzupełniać, tworząc logiczną całość. Jej komponenty muszą być współzależne, spójne i niesprzeczne. Muszą być powiązane ze wszystkimi obszarami funkcjonowania jednostki, jej funkcjami, procesami, systemami i celami. Kontrola wewnętrzna jest ciągłym procesem inicjowanym i realizowanym przez radę nadzorczą, zarząd, kierownictwo oraz pracowników na wszystkich szczeblach organizacyjnych zgodnie z zakresem kompetencji, uprawnień i odpowiedzialności. Stanowi ciągły, aktywny proces, będący integralnym elementem procesu kierowania, mający na celu uzyskanie przekonania kierownictwa i zainteresowanych interesariuszy, że wszystkie zasoby jednostki wykorzystywane są w sposób optymalny dla realizacji ustalonych celów. Pomaga jednostce: przystosować się do zmian w otoczeniu, radzić sobie ze złożonością organizacji, minimalizować koszty, regulować oraz korygować wszelkie czynności

i procesy zapewniając ich sprawność i skuteczność oraz efektywnie ograniczać kumulowanie się błędów. System kontroli wspomaga obserwowanie określonych zjawisk i czynników ryzyka, analizowanie ich charakteru i komunikowanie spostrzeżeń organom kierującym. Dlatego celem kontroli wewnętrznej jest systematyczne działanie na rzecz ustanowienia norm efektywności przy planowanych celach jednostki, porównania rzeczywistej efektywności z wyznaczonymi celami, ustalanie uchybień i pomiar ich znaczenia oraz podejmowanie wszelkich kroków potrzebnych do zapewnienia, by wszystkie zasoby jednostki były wykorzystywane najskuteczniej i najsprawniej do osiągnięcia ustanowionych celów, a jednostka działała zgodnie z przepisami i regulacjami wewnętrznymi, zapewniając wiarygodną sprawozdawczość wewnętrzną i zewnętrzną. Poprzez wykorzystanie zaprojektowanych informacyjnych sprzężeń zwrotnych, kontrola wewnętrzna w procesie zarządzania jednostką pełni funkcję dostosowawczą jednostki do otoczenia".

Projektując w jednostce system kontroli wewnętrznej, jako podstawowe komponenty kontroli wewnętrznej można przyjąć elementy systemu wskazane w raporcie COSO II. Można uznać, że model systemu kontroli wewnętrznej zaproponowany w raporcie COSO II z 2004 roku może być przydatny dla wielu jednostek rozpoczynających działalność, które projektują i wdrażają po raz pierwszy system kontroli wewnętrznej. Jednak dla jednostek, które prowadzą działalność i chcą doskonalić funkcjonujący już system kontroli wewnętrznej ta koncepcja nie będzie już tak przydatna. Zdaniem autorki, mając na uwadze obecne uwarunkowania funkcjonowania kontroli w jednostce należałoby znacznie zmodyfikować modelową strukturę systemu kontroli wewnętrznej proponowaną w COSO II.

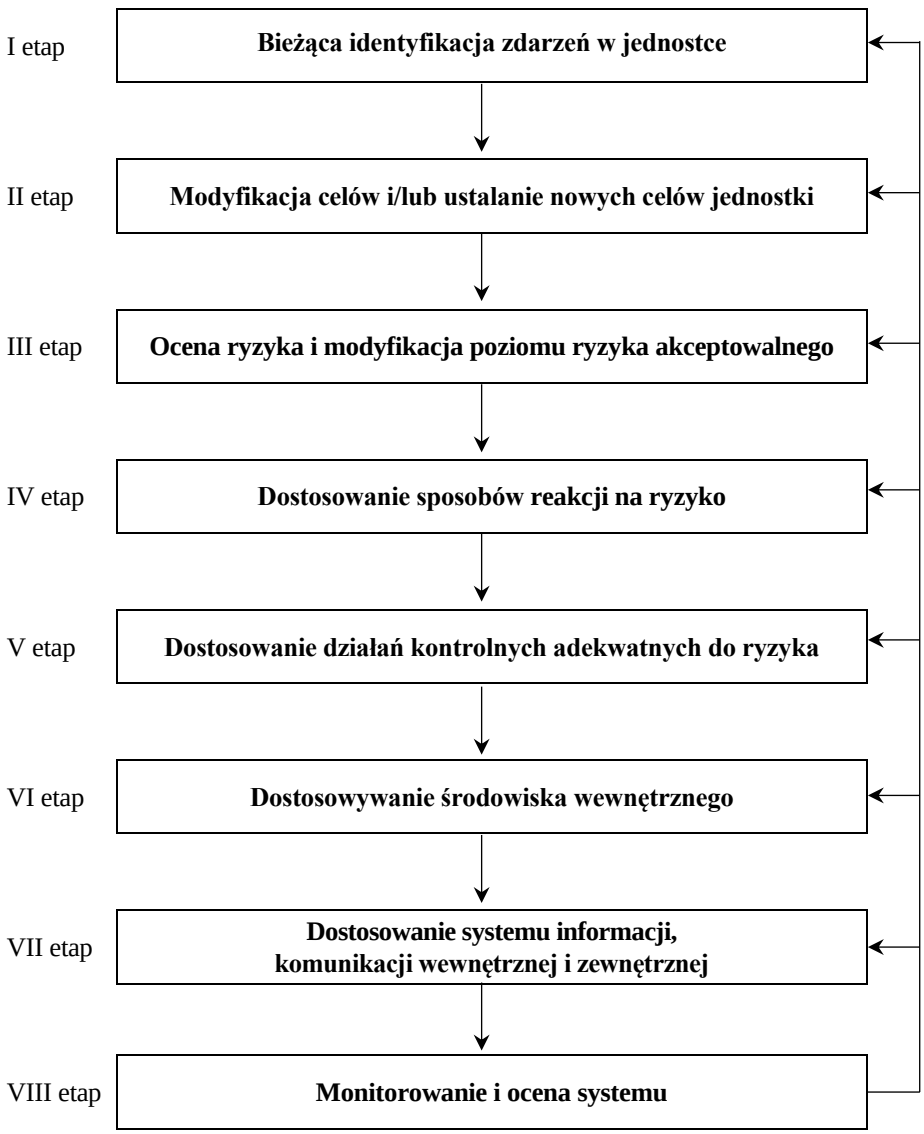
Na podstawie badań własnych i prowadzonej analizy rozwiązań w praktyce autorka proponuje teoretyczne modelowe ujęcie systemu kontroli wewnętrznej w jednostce. Autorski model systemu kontroli wewnętrznej został opracowany z wykorzystaniem ogólnej struktury komponentów tego systemu ogłoszonej w koncepcji COSO, COSO II, standardach kontroli finansowej i standardach kontroli zarządczej dla jednostek sektora finansów publicznych, Rekomendacji H i M dla banków, standardach IIA, MSB 315.

Pierwszym etapem projektowania systemu kontroli wewnętrznej, a także w późniejszym okresie jego doskonalenia, jest bieżąca identyfikacja zdarzeń w jednostce. Powinno to skutkować modyfikacją aktualnie realizowanych celów i/lub ustalaniem nowych celów oraz zadań jednostki wynikającą z bieżącej oceny ryzyka, a następnie ustaleniem lub modyfikacją poziomu ryzyka akceptowalnego, dostosowaniem sposobów reakcji na ryzyko, a następnie dostosowaniem działań kontrolnych adekwatnych do zidentyfikowanego ryzyka, którego nie można uniknąć, a którym można w określony sposób zarządzać. Kolejnymi etapami będą: dostosowywanie środowiska wewnętrznego do aktualnych warunków funkcjonowania jednostki i zidentyfikowanego ryzyka oraz dostosowanie systemu informacji, komunikacji wewnętrznej i zewnętrznej do aktualnych potrzeb organizacji. Ostatni etap to bieżące monitorowanie, samoocena, niezależna ocena okresowa systemu kontroli wewnętrznej w celu jego dalszego doskonalenia.

Niezbędne jest tutaj zapewnienie sprzężenia zwrotnego pozwalającego na ciągłe doskonalenie poszczególnych komponentów systemu, czyli działań w tym zakresie podejmowanych w jednostce.

Rysunek 1 prezentuje teoretyczne modelowe ujęcie systemu kontroli wewnętrznej we współczesnych jednostkach.

Rysunek 1. Modelowe ujęcie systemu kontroli wewnętrznej i jego doskonalenia w jednostce



Źródło: opracowanie własne.

O skuteczności i efektywności systemu kontroli wewnętrznej w jednostce zadecyduje realizacja wszelkich czynności kontrolnych realizowanych przez wszystkich członków organizacji (kontrola pionowa, kontrola pozioma, samoocena) oraz różne mechanizmy (strategie, polityki, procedury, regulaminy, instrukcje, inne działania) wpisane w funkcje poszczególnych, wzajemnie uzupełniających się komponentów tego systemu[23]. Taki system kontroli wewnętrznej poprzez określone zasady, polityki i procedury przyjęte przez kierownictwo ma za zadanie wspierać efektywne prowadzenie działalności jednostki. System ten powinien być zgodny z ogólnymi zasadami określonymi dla wypełniania funkcji kontrolnej w procesie zarządzania jednostką. Systemem tym należy objąć wszystkie obszary, systemy, procesy i funkcje działalności jednostki, w tym także rachunkowość jednostki, wspierając jej prawidłowe prowadzenie i ochronę zasobów informatycznych rachunkowości. W ujęciu przedmiotowym (funkcjonalnym) powinien on zapewniać w szczególności:

1) zgodność działania jednostki z przepisami prawa i regulacjami wewnętrznymi, w tym: z procedurami, instrukcjami, limitami, planami i innymi mechanizmami kontrolnymi;
2) wiarygodną sprawozdawczość zewnętrzną i wewnętrzną, w tym w postaci bieżących raportów zarządczych;
3) efektywne wykorzystanie zasobów, a także ich ochronę zasobów, w tym zapewnienie bezpieczeństwa zasobów informatycznych rachunkowości i informacji korporacyjnej;
4) bieżące reagowanie na różne nieprawidłowości, w tym: błędy, uchybienia wynikające z niedbalstwa, nadużycia czy oszustwa we wszystkich obszarach działalności jednostki.

Zdaniem autorki system ten powinien charakteryzować się określonymi cechami, czyli być:

1) kompleksowy, tzn. zbudowany z określonych wzajemnie uzupełniających się komponentów, które warunkują efektywność pozostałych w tym systemie, a także posiada mechanizmy kontrolne ze wszystkich wymaganych grup zabezpieczeń (fizyczne, techniczne, organizacyjno-administracyjne i programowe);
2) spójny, tzn. mechanizmy kontroli w systemie będą wzajemnie ze sobą powiązane i nie będzie w systemie luk;
3) niesprzeczny, tzn. podejmowane działania i zastosowane mechanizmy kontroli nie powodują kolizji między sobą;
4) adekwatny, tzn. zawiera określone mechanizmy kontrolne uwzględniające aktualne potrzeby jednostki i wyniki analizy ryzyka;
5) skuteczny, tzn. mechanizmy kontroli są projektowane i wdrożone w odpowiedzi na konkretne zidentyfikowane zagrożenia i czynniki ryzyka (nie są mechanizmami przypadkowymi), a także zapewniają ochronę zasobów i prawidłowe funkcjonowanie

[23] Opis takich działań charakterystycznych dla środowiska informatycznego rachunkowości zawiera np. publikacja Szczepankiewicz (2016).

jednostki (realizację celów) we wszystkich obszarach, w których zostały ustanowione; o skuteczności całego systemu zawsze decyduje najsłabsze ogniwo tego systemu;
6) efektywny, tzn. mechanizmy kontroli i inne komponenty systemu są spójne, kompleksowe i sprawnie działające, nakierowane nie tylko na jakość kontroli, ale i na redukcję lub eliminację ryzyka; mogące w efekcie zapewnić realizację celów kontroli i celów jednostki;
7) ciągle doskonalony, na podstawie wyników bieżącego monitorowania i okresowej oceny skuteczności (np. w procesie samooceny systemu przez kierownictwo i badania przez audyt wewnętrzny lub zewnętrzny).

Zaproponowany wyżej autorski model systemu kontroli wewnętrznej może być wykorzystany do opracowania i doskonalenia skutecznych, efektywnych, wydajnych i adekwatnych mechanizmów kontroli wewnętrznej w dowolnym obszarze funkcjonowania jednostki, w tym w obszarze rachunkowości prowadzonej w środowisku informatycznym.

3. Autorska koncepcja struktury rekomendacji dotyczącej kontroli wewnętrznej w obszarze zapewnienia bezpieczeństwa zasobów informatycznych rachunkowości

W celu zapewnienia skuteczności kontroli wewnętrznej w obszarze rachunkowości, zdaniem autorki, proces projektowania struktury systemu kontroli wewnętrznej należy powiązać z procesem zarządzania ryzykiem. Ryzyko powinno być na bieżąco identyfikowane w każdym z obszarów związanych z rachunkowością jednostki, w każdym procesie i podsystemie, a zwłaszcza w procesie sprawozdawczości (Szczepankiewicz, 2011a). Możliwie dokładna identyfikacja charakteru i zakresu potencjalnego ryzyka[24] umożliwia wybór i podjęcie we właściwym czasie odpowiedniej metody i narzędzi jego ograniczenia. Uzyskanie w jednostce efektywnego i adekwatnego systemu kontroli wewnętrznej wymaga oprócz posiadania i doskonalenia mechanizmów kontrolnych będących reakcją na zidentyfikowane ryzyko również kilka niezbędnych elementów organizacyjnych, które utworzą ten system. Zatem kierownictwo jednostki musi zadbać o właściwe funkcjonowanie także takich komponentów systemu kontroli wewnętrznej, jak: środowisko kontroli, system przepływu informacji i komunikacji oraz monitorowanie systemu kontroli. Szczególne znaczenie ma tutaj konstrukcja systemu kontroli wewnętrznej uwzględniająca wszystkie aspekty środowiska informatycznego, w którym prowadzona jest rachunkowość jednostki.

[24] Ryzyko operacyjne w rachunkowości prowadzonej z wykorzystaniem systemów informatycznych może być związane z czynnikami losowymi, błędami w działaniu oprogramowania stosowanego w rachunkowości, awariami sprzętu komputerowego, przypadkowymi błędami ludzkimi lub celowymi działaniami kadry kierowniczej lub personelu, które prowadzą do nadużyć finansowych.

Na podstawie postulatów wyrażonych przez ankietowanych, które prezentowano w tabeli 3 oraz przeprowadzonej analizy przepisów UoR, koncepcji systemów kontroli wewnętrznej w światowych raportach COSO i COSO II, a także standardów kontroli finansowej, standardów kontroli zarządczej, rekomendacji D, H i M, standardów audytu wewnętrznego IIA i rewizji finansowej MSB 315, w tabeli 4 zawarto autorską propozycję struktury rekomendacji dotyczącej kontroli wewnętrznej w rachunkowości w środowisku informatycznym, ze szczególnym uwzględnieniem zapewnienia bezpieczeństwa zasobów informatycznych rachunkowości.

Podstawowe komponenty systemu kontroli wewnętrznej w obszarze rachunkowości prowadzonej w środowisku informatycznym w strukturze proponowanej rekomendacji odpowiadają koncepcjom prezentowanym w wyżej wymienionych raportach i regulacjach. Zdaniem autorki, system kontroli wewnętrznej w jednostce powinien objąć wszystkie zasoby informatyczne związane zarówno z informacjami finansowymi, jak i pozafinansowymi (korporacyjnymi)[25]. Od 2017 roku wiele z informacji niefinansowych musi być ujawnianych i podlega weryfikacji przez biegłego rewidenta zgodnie z obowiązującą dyrektywą 2014/95/UE. Wiele z nich wykorzystywane jest do sporządzania zintegrowanych sprawozdań rocznych. Dlatego z punktu widzenia wypełniania obowiązków informacyjnych informacje takie muszą być tak samo chronione, jak informacje finansowe.

W obecnych uwarunkowaniach prowadzenia rachunkowości w środowisku informatycznym, pierwszym i najważniejszym komponentem warunkującym strukturę i sprawność całego systemu kontroli wewnętrznej w środowisku informatycznym powinien być obszar celów i zarządzania ryzykiem (McName, 1998; Spira, Page, 2003; Saunders 2003). Działania w tym obszarze nadadzą kierunek projektowania kolejnych komponentów systemu. Jest to podejście zgodne z zaproponowanym wyżej autorskim, teoretycznym modelem systemu kontroli wewnętrznej.

Dla każdego z pięciu o komponentów systemu zaproponowano po kilka punktów (rekomendacji szczegółowych), które kierownictwu jednostek pozwolą sprawnie zaprojektować kolejne elementy tego systemu, w taki sposób, aby zapewnić wypełnienie wymogów stawianych przez UoR w zakresie ochrony zasobów informatycznych rachunkowości. Proponowany przez autorkę układ kolejnych elementów systemu kontroli wewnętrznej pozwoli wypełnić zadania kontroli w obszarze zinformatyzowanej rachunkowości, która powinna interesariuszom dostarczać wiarygodnych informacji finansowych i niefinansowych w ciągle zmieniających się uwarunkowaniach środowiska informatycznego, skutecznie wypełniając funkcję informacyjną, kontrolną, sprawozdawczą, atestacyjną, podatkową i dowodową przez rachunkowość.

[25] Obecnie w artykułach z zakresu finansów oraz nauk o zarządzaniu dużą uwagę przywiązuje się do ochrony wszelkich baz danych zawierających informacje korporacyjne, czyli dokumenty/informacje o misji, marce, historii, działalności, badaniach, technologiach, produktach, projektach, różnych grupach interesariuszy, realizowanych umowach, danych osobowych, analizie ryzyka, strategiach, politykach, procedurach i innych dokumentach tworzonych w codziennej działalności jednostki.

Tabela 4. Proponowana struktura rekomendacji dotyczącej kontroli wewnętrznej w obszarze zapewnienia bezpieczeństwa zasobów informatycznych rachunkowości i informacji korporacyjnej

Komponent systemu	Rekomendacja
A. Cele i zarządzanie ryzykiem	1. Identyfikacja celów strategicznych i operacyjnych jednostki, w tym celów oraz zadań w zakresie bezpieczeństwa zasobów informatycznych rachunkowości i informacji korporacyjnej
	2. Wskazanie i analiza procesów jednostki obsługiwanych przez IT i rachunkowość
	3. Identyfikacja czynników ryzyka dla procesów obsługiwanych przez IT i rachunkowość
	4. Identyfikacja zasobów chronionych IT (tj. zasobów informatycznych rachunkowości i informacji korporacyjnej)
	5. Wycena wartości zasobów chronionych IT
	6. Identyfikacja zagrożeń i podatności zasobów chronionych IT
	7. Szacowanie zagrożeń i podatności zasobów chronionych IT
	8. Oszacowanie ryzyka dla zasobów chronionych IT (oszacowanie prawdopodobieństwa i skutków) oraz określenie priorytetów i materialnej istotności
	9. Identyfikacja metod i środków unikania, redukcji, dywersyfikacji lub transferu ryzyka IT oraz narzędzi kontroli wraz z oszacowaniem ich kosztów i skuteczności
	10. Określenie poziomu ryzyka IT akceptowanego przez kierownictwo
	11. Opracowanie polityki bezpieczeństwa zasobów chronionych IT i sposobów postępowania z ryzykiem IT, które zostaną wdrożone (metody i środki kontroli, redukcji lub transferu ryzyka)
B. Mechanizmy kontroli	12. Wdrożenie polityki bezpieczeństwa zasobów chronionych IT i dokumentowanie systemu kontroli wewnętrznej
	13. Wdrożenie metod i środków kontroli, redukcji lub transferu ryzyka
	14. Nadzór nad zapewnieniem ciągłości działalności
	15. Ochrona zasobów informatycznych rachunkowości
	16. Szczegółowe mechanizmy kontroli dotyczące operacji finansowych i gospodarczych w środowisku informatycznym rachunkowości
	17. Szczegółowe mechanizmy kontroli dotyczące systemu informatycznego rachunkowości, w tym: kontrola dostępu użytkowników informacji finansowej, kontrola oprogramowania systemowego, kontrola tworzenia i zmian w aplikacjach, podział uprawnień i obowiązków, ciągłość funkcjonowania aplikacji, kontrole aplikacyjne
C. Środowisko wewnętrzne systemu kontroli	18. Przestrzeganie wartości etycznych
	19. Kompetencje zawodowe i szkolenia w zakresie bezpieczeństwa IT
	20. Struktura organizacyjna i przypisanie odpowiedzialności w zakresie bezpieczeństwa zasobów IT
	21. Delegowanie uprawnień

Komponent systemu	Rekomendacja
D. Przepływ informacji oraz skuteczna komunikacja	22. Bieżąca informacja
	23. Komunikacja wewnętrzna
	24. Komunikacja zewnętrzna
E. Monitorowanie i ocena systemu kontroli	25. Monitorowanie aktualności celów oraz zadań w zakresie bezpieczeństwa zasobów IT i ocena ich realizacji
	26. Bieżące monitorowanie i kontrola skuteczności postępowania z ryzykiem IT
	27. Samoocena systemu kontroli wewnętrznej w obszarze bezpieczeństwa zasobów IT
	28. Audyt wewnętrzny lub informatyczny, w tym audyt bezpieczeństwa informacji
	29. Raportowanie wyników kierownictwu o stanie kontroli wewnętrznej w obszarze bezpieczeństwa zasobów IT
	30. Reakcja kierownictwa na naruszenie bezpieczeństwa zasobów IT

Źródło: opracowanie własne na podstawie: COSO (1994), COSO II (2004), Standardy kontroli finansowej (2003), Standardy kontroli zarządczej (2009), Rekomendacja H (2013), Standardy IIA (2016), MSB 315.

Należy podkreślić, że w UoR ustawodawca użył wiele pojęć związanych z prowadzeniem rachunkowości w środowisku informatycznym, ale nie zawarł ich definicji. Są to następujące pojęcia (sformułowania): ochrona danych; ochrona przed niedozwolonymi zmianami, nieupoważnionym rozpowszechnianiem, uszkodzeniem lub zniszczeniem; informatyczne nośniki danych; zagrożenia nośników danych; dobór stosownych środków ochrony zewnętrznej; systematyczne tworzenie rezerwowych kopii zbiorów danych; ochrona programów komputerowych, ochrona danych systemu informatycznego rachunkowości; księgi rachunkowe przy użyciu komputera; wykaz zbiorów danych tworzących księgi rachunkowe na informatycznych nośnikach danych; opis systemu przetwarzania danych; opis systemu informatycznego, zawierającego wykaz programów, procedur lub funkcji, w zależności od struktury oprogramowania, z opisem algorytmów i parametrów; programowe zasady ochrony danych, system służący ochronie danych i ich zbiorów. W dokumencie: *Stanowisko Komitetu Standardów Rachunkowości w sprawie niektórych zasad prowadzenia ksiąg rachunkowych* z 2010 roku wydanym po nowelizacji UoR z 2009 roku zostały zdefiniowane jedynie takie pojęcia jak: system komputerowy, system finansowo-księgowy.

Zdaniem autorki, w celu opracowania wewnętrznego dokumentu określającego system kontroli wewnętrznej w jednostce, a także opracowania w przyszłości przez właściwe organy rekomendacji (wytycznych, stanowiska lub standardu) w tym zakresie, można wykorzystać i/lub zmodyfikować definicje związane z systemami kontroli wewnętrznej zawarte także w dziewięciu źródłach wskazanych w tabeli 5.

Pozostałe pojęcia dotyczące technologii informacji, technologii telekomunikacyjnej, ochrony zasobów informatycznych, systemów zarządzania ryzykiem informatycznym, które warto wykorzystać na etapie opracowywania takiej regulacji, zostały zdefiniowane w kilku normach ISO dotyczących bezpieczeństwa informacji, a także wytycznych i standardach ISACA np. *Cobit*.

Tabela 5. Źródła istotnych definicji dla systemu kontroli wewnętrznej i proponowanego standardu

COSO (1992)	**COSO II (2004)**	**MSB 315 (2018)**	**Standardy IIA (2016)**	**Standardy kontroli finansowej (2003)**	**Standardy kontroli zarządczej (2009)**	**Rekomendacja D (2017)**	**Rekomendacja H (2013)**	**Rekomendacja M (2013)**
Środowisko kontroli, oszacowanie ryzyka, czynności kontrolne, informacja i komunikacja, monitoring	Środowisko wewnętrzne, ustalanie celów, identyfikacja zdarzeń, ocena ryzyka, reakcja na ryzyko, działania kontrolne, informacje i komunikowanie, monitorowanie	Środowisko kontroli, proces oceny ryzyka przez jednostkę, system informacyjny (w tym powiązane procesy gospodarcze, znaczące dla sprawozdawczości finansowej) i komunikacji, działania kontrolne (znaczące dla rewizji finansowej), monitorowanie kontroli, audyt wewnętrzny	Środowisko kontroli, ryzyko, zarządzanie ryzykiem, procesy kontroli, oszustwo, kontrola, odpowiednia kontrola, informatyczne mechanizmy kontrolne, audyt wewnętrzny	Kontrola dostępu, kontrola oprogramowania systemowego, kontrola tworzenia i zmian w aplikacjach, podział obowiązków, ciągłość działalności, kontrole aplikacyjne	Mechanizmy kontroli dotyczące systemów informatycznych	Bezpieczeństwo informacji, *Cloud Computing*, dostępność danych, incydent naruszenia bezpieczeństwa środowiska teleinformatycznego, infrastruktura teleinformatyczna, integralność danych i bezpieczeństwa środowiska teleinformatycznego, obszar technologii informacyjnej	System kontroli wewnętrznej, mechanizmy kontroli ryzyka, badanie zgodności działania z przepisami prawa i regulacjami wewnętrznymi, audyt wewnętrzny	Strategia zarządzania ryzykiem operacyjnym, środowisko wewnętrzne, identyfikacja ryzyka, ocena ryzyka, przeciwdziałanie ryzyku, kontrola, monitorowanie, raportowanie i przejrzystość działania, kluczowe procesy, krytyczne procesy, profil ryzyka operacyjnego, strategia zarządzania ryzykiem operacyjnym, system kontroli wewnętrznej, system zarządzania ryzykiem, tolerancja/apetyt na ryzyko

Źródło: opracowanie własne.

Podsumowanie

Na potrzeby niniejszego artykułu przeprowadzono analizę krajowych przepisów i regulacji w zakresie zapewnienia wiarygodności informacji finansowej i bezpieczeństwa zasobów informatycznych rachunkowości. W wyniku tej analizy można stwierdzić, że oprócz przepisów ogólnych ustanowionych w tym zakresie, które powszechnie obowiązują wszystkie jednostki, tj. UoR, w praktyce jednostek stosuje się również inne szczególne regulacje sektorowe dotyczące kontroli wewnętrznej i zapewnienia bezpieczeństwa informacji w środowisku informatycznym.

Przeprowadzone badania empiryczne wskazują, że wprowadzenie tych regulacji w badanych sektorach, choć większość z nich nie stanowiła przepisów prawa powszechnie obowiązującego, a są jedynie wytycznymi – w konsekwencji – doprowadziło do doskonalenia w tych podmiotach systemów kontroli wewnętrznej, także w obszarze zarządzania bezpieczeństwem zasobów informatycznych rachunkowości. Dodatkowe regulacje (standardy, wytyczne, rekomendacje, normy) pomogły kierownikom jednostek zarówno w projektowaniu, jak i ocenie i doskonaleniu obecnych systemów kontroli wewnętrznej w środowisku informatycznym i zwiększeniu ochrony zasobów informatycznych rachunkowości w jednostkach.

Na podstawie analizy danych z badania empirycznego wykazano, że największych pozytywnych efektów po wdrożeniu takiego standardu należy spodziewać się w jednostkach sektora prywatnego, które mają największe problemy z zapewnieniem odpowiedniego poziomu ochrony zasobów informatycznych i dla których dotychczas nie opracowano wytycznych w tym zakresie[26]. Łączny średni potencjał poprawy jakości systemów kontroli wewnętrznej w środowisku informatycznym rachunkowości (liczony metodą do 100%) może wynosić nawet 57% dla małych i średnich firm oraz 44% dla dużych firm w sektorze prywatnym. Badanie pokazało, że w firmach prywatnych istnieją szczególne obszary „niewiedzy" np. w zakresie zarządzania ryzykiem informatycznym. Wynikają one z luki metodycznej i aplikacyjnej w literaturze przedmiotu, których uzupełnienie przez teoretyków może w znaczący sposób poprawić zarządzanie bezpieczeństwem zasobów informatycznych w polskich jednostkach.

Na podstawie analizy koncepcji światowych i różnych standardów branżowych przyjętych w Polsce zaproponowano również autorski model systemu kontroli wewnętrznej, który może być wykorzystany do opracowania i doskonalenia skutecznych, efektywnych, wydajnych i adekwatnych mechanizmów kontroli wewnętrznej w dowolnym obszarze funkcjonowania jednostki, w tym w obszarze rachunkowości prowadzonej w środowisku informatycznym. Model ten posłużył także do przedstawienia autorskiej koncepcji struktury rekomendacji dotyczącej kontroli wewnętrznej w obszarze zapewnienia bezpieczeństwa zasobów informatycznych rachunkowości i informacji

[26] Jak ujawniają różne raporty w ostatnich latach, zasoby informatyczne jednostek sektora prywatnego stają się są coraz częściej przedmiotem wewnętrznych i zewnętrznych cyberataków. Dotychczas szczególną uwagę zwracano na ten problem w odniesieniu do instytucji finansowych, baz rządowych i jednostek sektora finansów publicznych.

korporacyjnej. Wskazano również 12 źródeł aktualnych pojęć i definicji, które można byłoby wykorzystać do opracowania w przyszłości takiej rekomendacji lub innych regulacji na przykład w formie standardu, stanowiska lub wytycznych. Wiele pojęć dotyczących podstawowych komponentów systemu kontroli wewnętrznej występujących w tych rozproszonych źródłach pochodzi ze światowych raportów COSO i COSO II. Jest także wiele definicji, które bez szczególnej modyfikacji treści, można włączyć do słownika pojęć tych regulacji, na przykład terminy dotyczące zagadnień z zakresu zarządzania ryzykiem i informatyki.

Zdaniem autorki, regulacje dotyczące kontroli wewnętrznej w rachunkowości w środowisku informatycznym nie muszą stanowić przepisów prawa powszechnie obowiązującego, lecz mogą mieć charakter rekomendacji (wytycznych, stanowiska lub standardu), których stosowanie zależy od decyzji kierownika danej jednostki. Propozycja takiego charakteru regulacji jest uzasadniona tym, że kontrola wewnętrzna w jednostkach sektora prywatnego stanowi element indywidualnie kształtowanego systemu zarządzania właścicielskiego. Najważniejsze wytyczne w zakresie ochrony zasobów informatycznych rachunkowości zawiera UoR, a rekomendacje w tym zakresie mogą kierownikom jednostek ułatwić wypełnianie obowiązków podstawowych wynikających z UoR i doskonalić system kontroli wewnętrznej w rachunkowości jednostki.

Badania własne autorki pokazały, że dodatkowe regulacje sektorowe w zakresie kontroli wewnętrznej w jednostkach sektora finansów publicznych i w bankach pomogłyby kierownictwom tych jednostek opracować, wdrożyć, oceniać i doskonalić procesy zarządzania bezpieczeństwem zasobów informatycznych, w tym zasobów informatycznych rachunkowości. Zatem każde opracowanie o charakterze poznawczym, empirycznym i aplikacyjnym na temat doskonalenia systemów kontroli wewnętrznej w rachunkowości prowadzonej w środowisku informatycznym może stanowić bardzo ważny wkład zarówno do dyscypliny naukowej, jak i praktyki w zakresie poprawy bezpieczeństwa zasobów informatycznych rachunkowości w jednostkach.

Literatura

Griffin R.W. (1999), *Management*, Houghton Miffilin Company, Boston–New York.

Jajuga K. (2017), *Rynki finansowe przyszłości – co może powodować rewolucja technologiczna* (wykład), 21. Konferencja WallStreet, Karpacz 2.06.2017, www. bankier.pl (dostęp 20.07.2017).

Kałużny S. (2008), *Kontrola wewnętrzna. Teoria i praktyka*, Polskie Wydawnictwo Ekonomiczne, Warszawa.

Kałużny S. (1997), *Nadzór i kontrola w przedsiębiorstwie. Kompendium wiedzy dla kontrolujących i kontrolowanych*, KWANTUM, Warszawa.

Kiedrowska M., Szczepankiewicz E.I (2011), *Internal control in the concept of integrated Enterprise Risk Management (ERM) system in insurance undertakings*, „Finanse. Rynki Finansowe. Ubezpieczenia", 38, s. 695–706.

Klimas K. (1985), *Kontrola wewnętrzna w przedsiębiorstwie*, Państwowe Wydawnictwo Ekonomiczne, Warszawa.

Lament M. (2013). *Audit as a control mechanism employed by an insurance company*, „Wiadomości Ubezpieczeniowe", 3, s. 105–199.

McNamee D. (1998), *Business Risk Assessment*, IIA, 247 Maitland Avenue, Altamonte Springs.

Mockler R.J. (1984), *The Management Control Process*, Prentice-Hall, Englewood Cliffs, N.J.
Robbins A.P., Coulter M. (2012), *Management*, Pearson, Upper Saddle River, NJ.
Saunders E.J. (1994), *Kontrola wewnętrzna w bankowości*, FRR w Polsce, Warszawa.
Saunders E.J. (2003), *Audyt i kontrola wewnętrzna w przedsiębiorstwach*, EDUCATOR, Częstochowa.
Spira L.F., Page M. (2003), *Risk management: The reinvention of internal control and the changing role of internal audit*, „Accounting, Auditing and Accountability Journal", 16 (4), s. 640–661.
Stoner J.A.F, Wankel Ch. (1996), *Kierowanie*, Wydawnictwo Naukowe PWN, Warszawa.
Stoner J.A.F., Freeman F.E., Gilbert D.R. (2001), *Kierowanie*, Polskie Wydawnictwo Ekonomiczne, Warszawa.
Szczepankiewicz E.I. (2011a), *Ewolucja światowych koncepcji kontroli wewnętrznej w systemie rachunkowości i ich wpływ na standardy audytu*, „Zeszyty Teoretyczne Rachunkowości", 64 (120), s. 101–127.
Szczepankiewicz E.I. (2011b). *The role of the audit committee, the internal auditor and the statutory auditor as the bodies supporting effective corporate governance in banks*, „Finanse, Rynki Finansowe. Ubezpieczenia", 38, s. 885–897. Available online: http://www.wneiz.pl/nauka_wneiz/frfu/38-2011/FRFU-38-885.pdf (dostęp 28.11.2017).
Szczepankiewicz E.I. (2011c). *Selected issues in effective implementation of the integrated risk management system in an organization*, „Finanse. Rynki Finansowe. Ubezpieczenia", 49, s. 153–162. http://www.wneiz.pl/nauka_wneiz/frfu/49-2011/FRFU-49-153.pdf (dostęp 28.11.2017).
Szczepankiewicz E.I. (2012a). *New Regulations and Internal Control System as Supporting Effective Corporate Governance in Commercial Banks in Poland*, [w:] *Banking and Financial Markets. After Global Crisis of the Years 2008–2010*, ed. A.P. Balcerzak, Nicolaus Copernikus University, Toruń, s. 81–102.
Szczepankiewicz E.I. (2012b). *The role and tasks of the Internal Audit and Audit Committee as bodies supporting effective Corporate Governance in Insurance Sector Institutions in Poland*, „Oeconomia Copernicana", 4, s. 23–39; http://economic-research.pl/Journals/index.php/oc/article/view/456 /420 (dostęp 28.11.2017).
Szczepankiewicz E.I. (2014). *Zasady rachunkowości, kontrola wewnętrzna i audyt w towarzystwach funduszy inwestycyjnych*, CeDeWu, Warszawa.
Szczepankiewicz E.I. (2016), *Audyt kontroli wewnętrznej rachunkowości w środowisku informatycznym*, Difin, Warszawa.
Szczepankiewicz E.I. (2017), *Kontrola zarządcza w jednostkach samorządu terytorialnego, Ocena i doskonalenie procedur kontroli zarządczej w środowisku informatycznym rachunkowości*, UE w Poznaniu &Wydawnictwo Naukowe CONTACT, Poznań.
Szczepankiewicz E.I. (2018), *Zarządzanie bezpieczeństwem zasobów informatycznych rachunkowości w polskich jednostkach – wyniki badań*, „Zeszyty Teoretyczne Rachunkowości", 97 (153), s. 115–138.
Szczepankiewicz E.I., Kiedrowska M. (2011), *Organizacja audytu wewnętrznego w zakładach ubezpieczeń w świetle Solvency II oraz standardów audytu*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu", 228, s. 454–462; http://bazekon.icm.edu.pl/ bazekon/element/bwmeta1.element.ekon-element-000171209097 (dostęp 28.11.2017).
Terebucha E. (1976), *Zasady kontroli wewnętrznej w przedsiębiorstwie. Poradnik księgowego*, Państwowe Wydawnictwo Ekonomiczne, Warszawa.
Wierzbicki K. (1996), *Kontrola wewnętrzna w podstawowych jednostkach gospodarczych*, UNIVERS, Zielona Góra.
Winiarska K. (2010), *Definicja i klasyfikacja kontroli wewnętrznej*, [w:] K. Winiarska (red.), *Kontrola wewnętrzna w jednostkach gospodarczych*, Polskie Wydawnictwo Ekonomiczne, Warszawa.

Akty prawne i inne regulacje

COBIT – Control Objectives for Information and related Technology (2004), ISACA, IT Governance Institute, *www.isaca.org*, (dostęp 12.02.2012).
COBIT 5 – Framework for the governance and management of enterprise IT (2013), ISACA, IT Governance Institute, *www.isaca.org*, (dostęp 18.04.2018).

COSO II: Enterprise Risk Management – Integrated Framework (2004), Committee of Sponsoring Organizations of the Treadeway Commision, USA, www.sox-online.com /coso__cobit. html (dostęp 10.03.2011)

COSO: Internal Control – Integrated Framework (1992, 1994), Committee of Sponsoring Organizations of the Treadeway Commision, USA, www.sox-online.com /coso_cobit. html. (dostęp 10.03.2011)

Dyrektywa Parlamentu Europejskiego i Rady 2014/95/EU z dnia 22 października 2014 r. zmieniająca dyrektywę 2013/34/UE w odniesieniu do ujawniania informacji niefinansowych i informacji dotyczących różnorodności przez niektóre duże jednostki oraz grupy *https://www.mf.gov.pl/c/document_library/get_file?uuid=457d39d0-bb29-4eae-9821-a741c4c34b07&groupId=764034*

InCaS (2008), *Intellectual Capital Statement – Made in Europe, European ICS Guideline,* European Commission.

Internal Controls Over Financial Reporting – SOX (2004), Allied Irish Banks plc.

IT Control Objectives for Sarbanes-Oxley (2004), IT Governance Institute, *www.isaca.org* (dostęp 12.02.2012).

Komunikat nr 6 Ministra Finansów z 6 grudnia 2012 r. w sprawie szczegółowych wytycznych dla sektora finansów publicznych w zakresie planowania i zarządzania ryzykiem, (Dz. Urz. Min. Fin., poz. 56).

MSB 315 – Identyfikacja i ocena ryzyk istotnego zniekształcenia dzięki zrozumieniu jednostki i jej otoczenia, Załącznik nr 1.10 do uchwały nr 2783/52/2015 Krajowej Rady Biegłych Rewidentów z dnia 10 lutego 2015 r.

Metodyka zarządzania ryzykiem cyberprzestrzeni w systemach zarządzania bezpieczeństwem informacji podmiotów rządowych (2015), Warszawa, www.mc.gov.pl (dostęp 12.12.2015).

PN-ISO/IEC 27001:2014-12. *Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania,* (2014), Polski Komitet Normalizacyjny, Warszawa.

PN-ISO/IEC 27005:2014-01. *Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji.* (2014) Polski Komitet Normalizacyjny, Warszawa.

Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej (2013), Ministerstwo Administracji i Cyfryzacji, www.mac.gov.pl (dostęp 12.02.2015).

Rekomendacja D dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach (2013), Komisja Nadzoru Finansowego, Warszawa.

Rekomendacja H dotycząca kontroli wewnętrznej w banku (2017), Komisja Nadzoru Finansowego, Warszawa.

Rekomendacja M dotycząca zarządzania ryzykiem operacyjnym w banku (2013), Komisja Nadzoru Finansowego, Warszawa.

Rozporządzenie Ministra Finansów z dnia 30 kwietnia 2013 r. w sprawie sposobu, trybu oraz warunków prowadzenia działalności przez towarzystwa funduszy inwestycyjnych (Dz.U. 2013, poz. 538).

Sarbanes Oxley Act (SOX), (2002).

Skonsolidowane Zarządzanie Ryzykiem PSK (2004), Bank Rozrachunków Międzynarodowych.

Solvency II (2013), The role of Internal Audit under Solvency II, The European Confederation of National Institutes of Internal Auditors, http://www.theiia.org/guidance/standards-and-guidance/interactiveippf/. (dostęp 12.02.2014).

Standard No. 2.2.6. on Enterprise Risk Management for Capital Adequacy and Solvency Purposes. 2008, International Association of Insurance Supervisors www.iaisweb.org. (dostęp 10.03.2011).

Standardy kontroli finansowej (2003), Załącznik do Komunikatu nr 1 Ministra Finansów z dnia z dnia 30 stycznia 2003 r. w sprawie ogłoszenia „Standardów kontroli finansowej w jednostkach sektora finansów publicznych" (Dz. Urz. Min. Fin. 2003, nr 3, poz. 13).

Standardy kontroli finansowej (2006), Załącznik do Komunikatu nr 13 Ministra Finansów z dnia 30 czerwca 2006 r. w sprawie ogłoszenia standardów kontroli finansowej w jednostkach sektora finansów publicznych (Dz. Urz. Min. Fin. 2006, nr 7, poz. 56).

Standardy kontroli zarządczej (2009), Załącznik do Komunikatu nr 23 Ministra Finansów z dnia 16 grudnia 2009 r. w sprawie standardów kontroli finansowej dla jednostek sektora finansów publicznych (Dz. Urz. Min. Fin. 2009, nr 15, poz. 84).

Stanowisko Komitetu Standardów Rachunkowości z dnia 13 kwietnia 2010 r. w sprawie niektórych zasad prowadzenia ksiąg rachunkowych (2010). Załącznik do Komunikatu nr 10 Ministra Finansów z dnia 18.05.2010 r. w sprawie ogłoszenia uchwały Komitetu Standardów Rachunkowości w sprawie przyjęcia stanowiska Komitetu w sprawie niektórych zasad prowadzenia ksiąg rachunkowych (Dz. Urz. Min. Fin. 2010, nr 6, poz. 26).

The International Standards for the Professional Practice of Internal Audit (2016), IIA. www.iia.org (dostęp 10.03.2017).

The Revised Internal Control Standard for Effective Management SEC (2007), European Commission.

Ustawa o rachunkowości z dnia 29 września 1994 r. (Dz.U. 2018, poz. 62).

Wytyczne w sprawie standardów kontroli wewnętrznej w sektorze publicznym (2004), International Organization of Supreme Audit Institutions – INTOSAI.

Zasady zarządzania ryzykiem w bankowości elektronicznej (2001), Bank Rozrachunków Międzynarodowych.