

**Adam Samborski**

Katedra Rachunkowości i Finansów Przedsiębiorstw  
Wyższa Szkoła Bankowa w Poznaniu

## **Zarządzanie ryzykiem w przedsiębiorstwie – uwarunkowania w kontekście zasad nadzoru korporacyjnego**

### **Wstęp**

W efekcie skandali korporacyjnych i spadku zaufania do sprawozdawczości finansowej wzrosło zainteresowanie problematyką nadzoru korporacyjnego wśród zarządów, rad nadzorczych, najwyższego kierownictwa, audytorów czy interesariuszy. Kryzys światowy unaoczniał znaczenie właściwego zarządzania ryzykiem. Wzrosła znacząco liczba firm próbujących zarządzać ryzykiem w sposób całościowy. Pojawia się więc pytanie – w jaki sposób zarządzanie ryzykiem w przedsiębiorstwie efektywnie zintegrować z systemem nadzoru korporacyjnego [Sobel 2004]. Tak sformułowany problem badawczy wyznacza kierunek prowadzonych badań, które nie ograniczają się do warstwy opisowej, diagnostycznej, lecz są próbą wyjaśnienia zachodzących zjawisk i procesów. W tym kontekście prowadzone badania służą odkrywaniu prawidłowości deterministycznych zachodzących w obrębie podejmowanej problematyki. Celem opracowania jest identyfikacja czynników warunkujących zarządzanie ryzykiem w przedsiębiorstwie, osadzonych w zasadach nadzoru korporacyjnego. W artykule ujęto stan prawny na 31 grudnia 2011 roku.

### **Ryzyko, zarządzanie ryzykiem, nadzór korporacyjny – wzajemne interakcje**

Ryzyko biznesowe oznacza niepewność, która może ograniczać zdolność osiągnięcia przez firmę wyznaczonych celów. Efekty ryzyka biznesowego mogą mieć charakter zarówno pozytywny, jak i negatywny, mogą też przyjąć postać odchylenia od oczekiwań. Ryzyko jest funkcją prawdopodobieństwa, zdarzy się lub nie [Sobel 2004]. Stąd też ryzyko zdefiniować można jako kombinację prawdopodobieństwa wystąpienia zdarzenia oraz jego skutków [Ferma 2003, s. 3].

W teorii podejmowania decyzji przez pojęcie ryzyka rozumiemy taką sytuację decyzyjną, w której z jednej strony istnieje niepewność co do przyszłych zdarzeń i kształtowania się sytuacji, z drugiej osoba podejmująca decyzję dysponuje informacjami o rozkładzie prawdopodobieństwa kształtowania się sytuacji w przyszłości [Buschgen 1997, s. 189]. We wszelkiego rodzaju przedsięwzięciach biznesowych istnieje możliwość wystąpienia zdarzeń pociągających za sobą skutki, które stanowią bądź szansę na dodatkowe korzyści, bądź też zagrożenie dla powodzenia projektu [Ferma 2003, s. 3]. Ryzyko biznesowe związane jest z celami przedsiębiorstwa, a osiągnięcie sukcesu gospodarczego warunkuje wcześniejsze podjęcie ryzyka – bez ryzyka nie ma nagrody. Z jednej strony, aby wykorzystywać możliwości strategiczne trzeba podejmować ryzyko, z drugiej jednak ryzyko zagrażające powodzeniu przedsięwzięcia musi być ograniczane [Sobel 2004].

Zarządzanie ryzykiem jest kluczowym elementem zarządzania strategicznego w każdej organizacji. Jest procesem, w którym organizacja metodycznie podchodzi do ryzyka związanego z jej działalnością [AIRMIC, ALARM, IRM 2010, s. 6]. Zarządzanie ryzykiem w sposób konsekwentny i uporządkowany pomaga kierownictwu zrozumieć i zarządzać niepewnością. Ma na celu tworzenie, ochronę i zwiększanie wartości dla akcjonariuszy poprzez zarządzanie niepewnością osiągnięcia celów organizacyjnych [Sobel 2004].

Nadzór korporacyjny jest systemem, za pośrednictwem którego korporacje są kierowane i kontrolowane [Sun, Stewart, Pollard 2011, s. 8]. System ten obejmuje zasady oraz normy odnoszące się do szeroko rozumianego zarządzania przedsiębiorstwem. Podstawowe problemy badawcze dotyczą podziału w przedsiębiorstwach uprawnień decyzyjnych i kontroli menedżerów [Samborski 2012]. Zadania stawiane przed nadzorem korporacyjnym koncentrują się na ochronie interesów udziałowców, czy też szerzej interesariuszy, minimalizacji ryzyka oraz zapewnieniu odpowiednich zwrotów z inwestycji [Aluchna 2007, s. 16–17].

Niestety, wielu członków zarządów, rad nadzorczych lub wyższego kierownictwa, audytorów wewnętrznych i zewnętrznych czy menedżerów ryzyka nie rozumie we właściwy sposób istoty nadzoru korporacyjnego, szczególnie w kontekście działań dnia codziennego. Bardzo często różne osoby pojmują go w zupełnie inny sposób. Ponadto, rady nadzorcze, zarządy odpowiedzialne za proces governance w przedsiębiorstwach w natłoku codziennych obowiązków muszą polegać na pomocy innych stron (menedżerów wykonawczych, audytorów) w wypełnianiu obowiązków wynikających z governance. Te jednakże rzadko angażują się w proces governance [Sobel 2004].

## Holistyczne podejście do zarządzania ryzykiem i kontroli wewnętrznej

„Powstające w ostatnich latach koncepcje zarządzania odwołują się do holistycznej wizji postrzegania problematyki przedsiębiorstw i innych organizacji. W zasadzie żadna ze znanych współczesnych koncepcji zarządzania nie mieści się w ramach tradycyjnych funkcji zarządzania. Proponowane rozwiązania wkraczają jednocześnie w pewne obszary funkcjonowania instytucji, bądź nawet we wszystkie. Konstruowane propozycje są bardziej wszechstronne, uniwersalne i kompleksowe” [Morawski 2006].

Szeroko akceptowane zintegrowane podejście do zarządzania ryzykiem i kontroli wewnętrznej zostało wypracowane na gruncie The Committee of Sponsoring Organizations of the Treadway Commission (COSO). W ujęciu COSO zarządzanie ryzykiem korporacyjnym jest procesem realizowanym przez radę dyrektorów (zarząd, rada nadzorcza), kierownictwo i inny personel przedsiębiorstwa, uwzględnionym w strategii i w całym przedsiębiorstwie, którego celem jest identyfikacja potencjalnych zdarzeń, które mogą wywrzeć wpływ na przedsiębiorstwo, utrzymywanie ryzyka w ustalonych granicach oraz rozsądne zapewnienie realizacji celów przedsiębiorstwa [COSO 2004a, s. 7; COSO 2004b, s. 2]. Kontrolę wewnętrzną natomiast definiuje się szeroko jako proces realizowany przez radę dyrektorów (zarząd, radę nadzorczą), kierownictwo i inny personel, zapewniający osiągnięcie celów w następujących obszarach: skuteczność i efektywność działań, wiarygodność sprawozdań, zgodność z obowiązującymi regulacjami prawnymi [COSO 2011, s. 3].

Kontrola wewnętrzna stanowi integralną część zarządzania ryzykiem korporacyjnym. Została ona uwzględniona w strukturze ramowej zarządzania ryzykiem korporacyjnym, tworząc silniejszą konceptualizację i narzędzie dla kierownictwa [COSO 2004a, s. 11]. W ujęciu COSO system kontroli wewnętrznej składa się z pięciu ściśle powiązanych ze sobą elementów, a mianowicie: środowiska kontroli, oceny ryzyka, czynności kontrolnych, informacji i komunikacji oraz czynności monitorujących. Środowisko kontrolne jest zbiorem norm, struktur i procesów tworzącym podstawy dla prowadzenia kontroli wewnątrz organizacji. Ocena ryzyka obejmuje proces (dynamiczny i iteracyjny) identyfikowania i oceniania ryzyka związanego z osiągnięciem celów. Na ocenę ryzyka składają się dwa powiązane ze sobą elementy. Pierwszy to oszacowanie prawdopodobieństwa wystąpienia zdarzenia. Drugi to analiza wpływu tego zdarzenia na przedsiębiorstwo. Czynności kontrolne są działaniami ustanowionymi przez politykę i procedury, ograniczającymi ryzyko osią-

gnięcia celów. Informacja jest niezbędna w wewnętrznym procesie kontroli wspierającym realizację celów. Komunikacja wewnętrzna to środek, za pomocą którego informacja rozpowszechniana jest w organizacji – w dół, w poprzek i górę hierarchii organizacyjnej. Działania monitorujące polegają na ocenie wykorzystania poszczególnych elementów kontroli wewnętrznej. Trzeba jednak w tym miejscu podkreślić, iż kontrola wewnętrzna nie jest procesem seryjnym, gdzie poszczególne części składowe systemu wchodzi kolejno po sobie. Jest procesem wielokierunkowym, iteracyjnym, w którym poszczególne elementy na siebie wzajemnie wpływają. Istnieje bezpośredni związek między celami, czyli tym co organizacja pragnie osiągnąć, a elementami kontroli wewnętrznej, czyli tym co jest konieczne do osiągnięcia celów [COSO 2011, s. 4–6]. Zgodnie z wytycznymi COSO system kontroli wewnętrznej powinien obejmować wszystkie obszary funkcjonowania przedsiębiorstwa. Każdy z nich wpływa bowiem na realizację założonych celów, wynik finansowy i ryzyko działalności. W celu zapewnienia skuteczności systemu kontrolę wewnętrzną należy powiązać z normalnymi oraz codziennymi czynnościami podejmowanymi w przedsiębiorstwie [Spiechowicz 2011, s. 58–59]. Struktura ramowa kontroli wewnętrznej w organizacji powinna w wystarczającym stopniu zapewnić dopasowanie identyfikacji, oceny i zarządzania ryzykiem w korporacji do osiągania wyznaczonych celów, kontroli działań, komunikowania i informowania członków organizacji, czy monitorowania procesów kontrolnych [Van der Elst 2010, s. 3]. Nie ma jednak jednego, uniwersalnego modelu systemu kontroli wewnętrznej. Każdy system musi zostać dostosowany do charakteru działalności organizacji, jej otoczenia, specyficznych rodzajów ryzyka, a przede wszystkim zakładanych długoterminowych i krótkoterminowych celów [Spiechowicz 2011, s. 58–59]. Odpowiedzialność za system kontroli wewnętrznej ponoszą wszyscy, szczególnie jednak rolę przypisać należy najwyższemu kierownictwu, które odpowiedzialne jest za ustanowienie i działanie systemu kontroli wewnętrznej w organizacji [COSO 2011, s. 9].

Jak już wspomniano, kontrola wewnętrzna stanowi integralną część zarządzania ryzykiem korporacyjnym. W ujęciu COSO struktura ramowa zarządzania ryzykiem korporacyjnym koncentruje się na osiąganiu celów przedsiębiorstwa w czterech kategoriach: strategicznej, operacyjnej, wiarygodności sprawozdawczości i zgodności z regulacjami prawnymi. Taka kategoryzacja celów umożliwia skoncentrowanie się na poszczególnych aspektach zarządzania ryzykiem. Według COSO, na zarządzanie ryzykiem korporacyjnym składa się osiem powiązanych ze sobą elementów. Wynikają one bezpośrednio ze sposobu zarządzania przedsiębiorstwem i są zintegrowane z procesem zarządzania. Elementy te to: środowisko wewnętrzne, ustalanie celów, identyfikacja zdarzeń, ocena ryzyka,

reakcja na wystąpienie ryzyka, działania kontrolne, informacja i komunikacja, monitorowanie.

Środowisko wewnętrzne to nic innego jak charakter organizacji. Stanowi podstawę postrzegania i reagowania na ryzyko przez pracowników, filozofię zarządzania ryzykiem oraz dopuszczalny poziom ryzyka, uczciwość i wartości etyczne, a także środowisko pracy. Kolejnym elementem zarządzania ryzykiem korporacyjnym jest ustalanie celów, które powinny zostać określone zanim kierownictwo przejdzie do identyfikacji potencjalnych zdarzeń wywierających wpływ na ich osiągnięcie. Procedury ustalania celów muszą korespondować z misją i wizją oraz odpowiadać poziomowi ryzyka dopuszczonego przez przedsiębiorstwo. W obszarze identyfikacji zdarzeń rozgranicza się zdarzenia na wewnętrzne i zewnętrzne, które mają wpływ na osiągnięcie celów, z rozróżnieniem ryzyka i szans. Ocena ryzyka jest podstawą decyzji o sposobie zarządzania nim, dlatego w tym celu dokonuje się jego analizy i oceny prawdopodobieństwa wystąpienia. Kierownictwo wybiera rodzaj reakcji na wystąpienie ryzyka, a następnie opracowuje zestaw działań w celu powiązania ryzyka z dopuszczalnym poziomem. Reakcja może polegać na unikaniu, akceptacji, ograniczaniu lub dzieleniu się ryzykiem. Działania kontrolne to polityka i procedury ustalone i realizowane w celu efektywnej reakcji na ryzyko. Informacje są zbierane i przekazywane w formie i ramach czasowych umożliwiających pracownikom wykonywanie swoich obowiązków. Ważna jest także w ramach organizacji skuteczna komunikacja – w dół, w poprzek i w górę hierarchii organizacyjnej. Ostatnim elementem zarządzania ryzykiem korporacyjnym jest monitorowanie procesu zarządzania. Monitorowanie realizowane jest poprzez stałe działania kierownictwa, niezależne oceny lub kombinację obu tych czynników. Tak jak w przypadku kontroli wewnętrznej, zarządzanie ryzykiem korporacyjnym nie jest procesem czysto seryjnym, w którym jeden z elementów wpływa jedynie na następny. Jest procesem wielokierunkowym, iteracyjnym, w którym prawie każdy komponent może wpływać na inny.

Trzeba w tym miejscu podkreślić, iż istnieje bezpośredni związek między tym co organizacja pragnie osiągnąć, czyli celami, a tym, co jest konieczne do osiągnięcia tych celów, czyli elementami zarządzania ryzykiem korporacyjnym. Aby elementy zarządzania ryzykiem korporacyjnym istniały i działały właściwie, nie mogą być obarczone znaczącymi słabościami, a ryzyko musi mieścić się w akceptowalnym przedziale [COSO 2004a, s. 7–11]. Odpowiedzialność za zarządzanie ryzykiem korporacyjnym w organizacji ponoszą wszyscy. Szczególną jednak rolę przypisać należy najwyższemu kierownictwu, które ponosi ostatecznie odpowiedzialność za proces zarządzania ryzykiem w przedsiębiorstwie [Rittenberg, Martens 2012, s. 21].

## Nadzór korporacyjny, zarządzanie ryzykiem, kontrole wewnętrzne w uregulowaniach prawnych

### Perspektywa europejska

Przez długi okres Unia Europejska (UE) koncentrowała się wyłącznie na korporacyjnych zasadach ujawniania informacji, rzetelności sprawozdawczości zewnętrznej oraz strukturze ramowej kontroli wewnętrznej. W ostatnim czasie UE stała się jednak bardzo aktywna w takich obszarach, jak: prawo spółek, rachunkowość czy prawo audytu. Powołano Grupę Ekspertów ds. Prawa Spółek (The High Level Group of Company Law Experts), która w sprawozdaniu za 2002 rok zaleciła, aby przedsiębiorstwa ujawniały informacje na temat systemów zarządzania ryzykiem (lub ich braku) w rocznych sprawozdaniach dotyczących nadzoru korporacyjnego. Zgodnie z rekomendacjami Grupy, to na radzie dyrektorów (zarząd, rada nadzorcza) powinien spoczywać obowiązek stworzenia takiego systemu, a komitet audytu musi odgrywać kluczową rolę w monitorowaniu procedur kontroli wewnętrznej i systemu zarządzania ryzykiem. W komunikacie z 2003 roku Grupa wezwała do modernizacji prawa spółek i wzmocnienia nadzoru korporacyjnego w UE. Komisja Europejska (KE) poparła propozycje Grupy. KE podkreśliła znaczenie informacji zawartych w rocznych sprawozdaniach z nadzoru korporacyjnego, obejmujących m.in. sposób zorganizowania systemu kontroli wewnętrznej. Ponadto, rozwinięto branżowe wymagania dotyczące kontroli wewnętrznej i zgodności (np. z regulacjami prawnymi) np. w przemyśle energetycznym czy sektorze finansowym [Van der Elst, van Daelen 2009, s. 28].

Trzeba jednak w tym miejscu podkreślić, iż wiele wysiłków KE ukierunkowanych na harmonizację dużej części prawa spółek, papierów wartościowych, rachunkowości napotkało wiele przeszkód i opóźnień spowodowanych sprzeciwem państw członkowskich UE. W pierwszych latach nowego stulecia UE wydała trzy dyrektywy i jedną rekomendację z zakresu prawa papierów wartościowych, prawa spółek, a także kilka branżowych zaleceń dotyczących bezpośrednio zarządzania ryzykiem i systemów kontroli wewnętrznej w ramach korporacji. Dyrektywy te, rekomendacje i kilka branżowych działań zostaną omówione poniżej [Van der Elst, van Daelen 2009, s. 28–29].

Dyrektywa 2004/109/WE Parlamentu Europejskiego i Rady z dnia 15 grudnia 2004 r. w sprawie harmonizacji wymogów dotyczących przejrzystości informacji o emitentach, których papiery wartościowe dopuszczane są do obrotu na rynku regulowanym stanowi, iż w rocznym sprawozdaniu finansowym przedsiębiorstwa powinien zostać ujęty opis podstawowych rodzajów

ryzyka i niepewności (art. 4, § 2)<sup>1</sup>. Śródroczne sprawozdanie zarządu zawarte w półrocznym sprawozdaniu finansowym musi ponadto zawierać informacje o głównych zagrożeniach oraz niepewnościach związanych z pozostałymi sześcioma miesiącami roku obrotowego (art. 5, § 4) [Dyrektywa 2004/109/WE]. Wymóg ujawniania podstawowych rodzajów ryzyka i niepewności nakłada na spółki obowiązek utworzenia przynajmniej systemu wykrywania ryzyka i niepewności. Niestety dyrektywa nie określa, czym jest ryzyko i niepewność oraz jakie ryzyko i niepewności należy uznać za podstawowe. Prawdopodobnie wymóg ten odnosi się częściowo do wymagań określonych w Dyrektywie Prospektowej 2003/71/WE i Rozporządzeniu Komisji (WE) 809/2004<sup>2</sup>, które zobowiązują spółki do ujawniania w prospekcie emisyjnym czynników ryzyka [Van der Elst, van Daelen 2009, s. 29–31]. W wymienionych aktach prawnych, w dziale zatytułowanym „Czynniki ryzyka” (załączniki), spółkę zobowiązuje się do wyraźnego opisanie i wskazania czynników ryzyka, które są specyficzne dla emitenta lub dla jego branży i/lub ryzyka związanego z wyemitowanymi papierami wartościowymi istotnego dla podejmowania decyzji inwestycyjnych (mających charakter materialny). „Czynniki ryzyka” oznaczają listę rodzajów ryzyka charakterystycznych dla sytuacji emitenta lub papierów wartościowych, które są istotne przy podejmowaniu decyzji inwestycyjnych (art. 2, ust. 3) [Rozporządzenie Komisji (WE) nr 809/2004].

Mamy więc do czynienia z różnicami w wymogach w opisie ryzyka w sprawozdaniu rocznym i w prospekcie emisyjnym (czynniki ryzyka). W raporcie rocznym ujmujemy podstawowe rodzaje ryzyka, podczas gdy w prospekcie ryzyko specyficzne i materialne. Ponadto, w sprawozdaniu rocznym ująć należy obok ryzyka także i niepewność. Za ryzyko podstawowe można przyjąć kategorie zdefiniowane w strukturach ramowych COSO, co do pozostałych – należy przeprowadzić szczegółowe analizy prawne [Van der Elst, van Daelen 2009, s. 29–31].

Poprawka z 2006 roku do czwartej i siódmej dyrektywy prawa spółek stanowi, iż spółka, której papiery wartościowe zostały dopuszczone do obrotu na rynku regulowanym ma obowiązek zawrzeć w sprawozdaniu z działalności oświadczenie o stosowaniu zasad nadzoru korporacyjnego (art. 1, § 7) [Dyrektywa 2006/46/WE]. Oświadczenie to ujmuje m.in. opis głównych cech stosowanych w spółce systemów kontroli wewnętrznej i zarządzania ryzykiem w odniesieniu do procesu sporządzania sprawozdań finansowych (art. 1, § 7, ust. c), a na poziomie skonsolidowanym opis głównych cech systemów kontroli wewnętrznej i zarządzania ryzykiem stosowanych przez grupę kapitałową w odniesieniu do

<sup>1</sup> Dyrektywę częściowo zmienia Dyrektywa Parlamentu Europejskiego i Rady 2010/73/UE z dnia 24 listopada 2010 r. zmieniająca Dyrektywę 2003/71/WE oraz Dyrektywę 2004/109/WE.

<sup>2</sup> Rozporządzenie Komisji (WE) 809/2004 częściowo zmienione Dyrektywą 2010/73/UE.

procesu sporządzania skonsolidowanych sprawozdań finansowych (art. 2, § 2, ust. f) [Dyrektywa 2006/46/WE].

Dyrektywa 2006/46/WE ogranicza więc raportowanie do zastosowania systemu w procesie sprawozdawczości finansowej. Ujęto w niej wymóg, aby w raportach ujmować jedynie główne cechy systemu tak, aby w wystarczającym stopniu zapewnić racjonalność procesu sprawozdawczości finansowej. Tak więc system kontroli wewnętrznej i zarządzania ryzykiem, zapewniający osiągnięcie przez spółkę wyznaczonych celów, należy opisać przy użyciu głównych cech tego systemu. Oświadczenie o stosowaniu zasad nadzoru korporacyjnego powinno zawierać przynajmniej takie elementy jak: politykę rady dyrektorów (zarządu, rady nadzorczej) w obszarze zarządzania ryzykiem i kontroli wewnętrznej ukierunkowanej na sprawozdawczość finansową, ocenę kluczowych obszarów kontroli wewnętrznej i zarządzania ryzykiem w systemie sprawozdawczości finansowej, mechanizmy systemu (np. monitoring, szkolenia), procedury komitetu audytu, ocenę audytora zewnętrznego.

Powyższe wymagania minimalne łączą dwie cechy systemu: jego strukturę i proces. Rada dyrektorów (zarząd, rada nadzorcza), komitet audytu, kierownictwo, a w szczególności wewnętrzni i zewnętrzni audytorzy są częścią systemu. Proces odnosi się do różnych kroków mających na celu zapewnienie wiarygodności sprawozdań finansowych, zidentyfikowanych w różnych strukturach ramowych, jak np. COSO [Van der Elst, van Daelen 2009, s. 32–34].

Zgodnie z Dyrektywą 2006/43/WE Parlamentu Europejskiego i Rady z dnia 17 maja 2006 r. w sprawie ustawowych badań rocznych sprawozdań finansowych i skonsolidowanych sprawozdań finansowych, każda jednostka interesu publicznego ma posiadać komitet ds. audytu. Państwo członkowskie określa, czy komitet ds. audytu powinien składać się z członków wykonawczych organu administracyjnego lub członków organu nadzorczego badanej jednostki lub członków wybranych na walnym zgromadzeniu wspólników badanej jednostki. Stanowi ponadto, iż przynajmniej jeden członek komitetu ds. audytu jest niezależny i posiada kompetencje w dziedzinie rachunkowości lub rewizji finansowej (art. 41, § 1). W punkcie 24 wstępu do Dyrektywy 2006/43/WE zapisano, iż komitety ds. audytu oraz skuteczny system kontroli wewnętrznej pomagają w minimalizacji ryzyka finansowego, operacyjnego i ryzyka niezachowania zgodności z wymogami oraz poprawiają jakość sprawozdawczości finansowej. Ponadto, biegły rewident lub firma audytorska składają sprawozdania komitetowi ds. audytu o kluczowych zagadnieniach wynikających z badania ustawowego, a w szczególności o istotnych niedociągnięciach w kontroli wewnętrznej w odniesieniu do procesu sprawozdawczości finansowej (art. 41, § 4). Należy jednak zwrócić uwagę, iż zgodnie z Dyrektywą 2006/43/WE do podstawowych zadań komitetu ds. audytu należą także, obok monitorowania procesu sprawoz-

dawczości finansowej, monitorowanie skuteczności istniejących w spółce systemów kontroli wewnętrznej, audytu wewnętrznego (w stosownych przypadkach) oraz zarządzania ryzykiem (art. 41, § 2) [Dyrektywa 2006/43/WE].

Zgodnie z zaleceniami Komisji z dnia 15 lutego 2005 r. dotyczącymi roli dyrektorów niewykonawczych lub będących członkami rady nadzorczej spółek giełdowych i komisji rady (nadzorczej) odnośnie do wewnętrznej polityki i procedur przyjętych przez spółkę, komisja audytu powinna służyć pomocą radzie (nadzorczej) przynajmniej w zakresie przeglądu, przynajmniej raz w roku, systemów kontroli wewnętrznej i zarządzania ryzykiem, pod kątem zapewnienia, że główne rodzaje ryzyka (w tym związane z przestrzeganiem obowiązujących przepisów prawa i regulacji) są prawidłowo identyfikowane, zarządzane i ujawniane. Do jej zadań należy także zapewnienie skuteczności funkcji audytu wewnętrznego, w szczególności w drodze wydania zaleceń dotyczących wyboru, powołania, ponownego powołania i odwołania szefa działu audytu wewnętrznego oraz dotyczących budżetu tego działu, a także przez monitorowanie reakcji kierownictwa na jego ustalenia i zalecenia. Kiedy w spółce nie ma funkcji audytu wewnętrznego, konieczność jej wprowadzenia powinna być przedmiotem przeglądu, przynajmniej raz w roku [Zalecenia Komisji z dnia 15 lutego 2005...].

W UE wypracowano także zasady branżowe. Dla przykładu, w branży finansowej dobrze znaną dyrektywą jest Mifid, a w branży chemicznej przedsiębiorstwa wdrażają regulacje REACH. Wiele przedsiębiorstw musi więc dostosować się nie tylko do ogólnych wytycznych dotyczących kontroli wewnętrznej, zarządzania ryzykiem, ale także do wymogów branżowych [Van der Elst, van Daelen 2009, s. 37].

## Perspektywa polska

Regulacje obowiązujące w Polsce, a dotyczące nadzoru korporacyjnego, zarządzania ryzykiem i kontroli wewnętrznych, mają charakter zarówno rekomendacji i dobrych praktyk, jak też przepisów prawa.

Dobre Praktyki Spółek Notowanych na Giełdzie Papierów Wartościowych w Warszawie (GPW) to zbiór zasad nadzoru korporacyjnego oraz reguł określających normy kształtowania relacji spółek giełdowych z ich otoczeniem rynkowym [PWC 2009]. Zgodnie z Załącznikiem do Uchwały 20/1287/2011 Rady Giełdy z dnia 19 października 2011 r. celem Dobrych Praktyk Spółek Notowanych na GPW jest umacnianie transparentności spółek giełdowych, poprawa jakości komunikacji spółek z inwestorami, wzmocnienie ochrony praw akcjonariuszy także w materiałach nieregulowanych przez prawo. Część III Załącznika stanowi, iż do obowiązków rady nadzorczej należy raz w roku sporządzać i przedstawiać

zwyczajnemu walnemu zgromadzeniu zwięzłą ocenę sytuacji spółki, z uwzględnieniem oceny systemu kontroli wewnętrznej i systemu zarządzania ryzykiem istotnym dla spółki (cz. III, pkt. 1). W Dobrych Praktykach zapisano ponadto, że przynajmniej dwóch członków rady nadzorczej powinno spełniać kryteria niezależności od spółki i podmiotów pozostających w istotnym powiązaniu ze spółką. W zakresie kryteriów niezależności członków rady nadzorczej oraz zadań i funkcjonowania komitetów działających w radzie nadzorczej powinien być stosowany odpowiednio Załącznik II i I do Zalecenia Komisji Europejskiej z dnia 15 lutego 2005 r. dotyczącego roli dyrektorów niewykonawczych lub będących członkami rady nadzorczej spółek giełdowych i komisji rady (nadzorczej) (cz. III, pkt. 6, 8).

Kodeks spółek handlowych ustanawia w spółkach akcyjnych radę nadzorczą (art. 381). Rada nadzorcza sprawuje stały nadzór nad działalnością spółki we wszystkich dziedzinach jej działalności (art. 382, § 1). Do szczególnych obowiązków rady nadzorczej należy ocena sprawozdań w zakresie ich zgodności z księgami i dokumentami, jak i ze stanem faktycznym (art. 382, § 3).

Ustawa z dnia 7 maja 2009 r. o biegłych rewidentach i ich samorządzie, podmiotach uprawnionych do badania sprawozdań finansowych oraz o nadzorze publicznym dokonuje w zakresie swojej regulacji wdrożenia postanowień dyrektywy 2006/43/WE. W myśl ustawy w jednostkach zainteresowania publicznego działa komitet audytu, którego członkowie są powoływani przez radę nadzorczą lub komisję rewizyjną spośród swoich członków (art. 86, § 1). W jednostkach zainteresowania publicznego, w których rada nadzorcza składa się z nie więcej niż 5 członków, zadania komitetu audytu mogą zostać powierzone radzie nadzorczej (art. 86, § 3). W skład komitetu audytu wchodzi co najmniej 3 członków, w tym przynajmniej jeden członek powinien spełniać warunki niezależności i posiadać kwalifikacje w dziedzinie rachunkowości lub rewizji finansowej (art. 86, § 4). Do zadań komitetu audytu należy w szczególności monitorowanie procesu sprawozdawczości finansowej oraz skuteczności systemów kontroli wewnętrznej, audytu wewnętrznego i zarządzania ryzykiem, jak również monitorowanie wykonywania czynności rewizji finansowej, a także niezależności biegłego rewidenta i podmiotu uprawnionego do badania sprawozdań finansowych (art. 86, § 7).

Ustawa z dnia 29 września 1994 r. o rachunkowości stanowi, iż przedsiębiorstwa (wymienione w UOR) wraz z rocznym sprawozdaniem finansowym sporządzają sprawozdanie z działalności jednostki gospodarczej. Sprawozdanie takie powinno obejmować istotne informacje o stanie majątkowym i sytuacji finansowej, w tym ocenę uzyskiwanych efektów oraz wskazanie czynników ryzyka i opis zagrożeń, a w szczególności informacje o stosowaniu zasad nadzoru korporacyjnego w przypadku jednostek, których papiery wartościowe zostały

dopuszczone do obrotu na jednym z rynków regulowanych Europejskiego Obszaru Gospodarczego (art. 49, § 1, § 2).

Warto w tym miejscu zwrócić jeszcze uwagę na ustawę z dnia 29 lipca 2005 r. o ofercie publicznej i warunkach wprowadzania instrumentów finansowych do zorganizowanego systemu obrotu oraz o spółkach publicznych. Zgodnie z tą ustawą dokument podsumowujący oraz podsumowanie będące częścią prospektu emisyjnego przedstawiają najważniejsze informacje i czynniki ryzyka dotyczące emitenta, podmiotu zabezpieczającego, papierów wartościowych oraz ich oferty lub dopuszczenia do obrotu na rynku regulowanym (art. 23).

Dodatkowe regulacje prawne w zakresie nadzoru, kontroli i zgodności z przepisami prawa istnieją w wybranych sektorach [PWC 2009].

## Wnioski

Przez długi okres w zarządzaniu ryzykiem zwracano uwagę na aspekty finansowe, kwestie sprawozdawczości, czy też problemy operacyjne. Obecnie jednak zarządzanie ryzykiem i kontrola wewnętrzna postrzegane są jako kluczowe elementy dobrego nadzoru korporacyjnego. Zasady nadzoru korporacyjnego wyraźnie wskazują na konieczność implementacji w poszczególnych przedsiębiorstwach systemów kontroli wewnętrznej i zarządzania ryzykiem. Rośnie presja ze strony ustawodawcy na ustanawianie systemów zarządzania ryzykiem w szczególności w odniesieniu do procesu sprawozdawczości finansowej. W efekcie problematyka ta stała się przedmiotem zainteresowania zarządów, rad nadzorczych, komitetów ds. audytu czy audytorów zewnętrznych. Kierownictwo najwyższego szczebla wzięło na siebie odpowiedzialność za określanie strategicznych kierunków oraz tworzenie warunków i struktur zapewniających skuteczne funkcjonowanie procesu zarządzania ryzykiem. Dziś zasady zarządzania ryzykiem określają w przedsiębiorstwach ogólne podejście do ryzyka, zakres tolerancji na ryzyko, metodę zarządzania ryzykiem oraz obowiązki poszczególnych osób uczestniczących w zarządzaniu ryzykiem. Kluczowymi elementami optymalnej roli kontroli wewnętrznej w zarządzaniu ryzykiem w przedsiębiorstwie stały się wymogi niezależności i obiektywizmu audytorów.

## Literatura

- AIRMIC, ALARM, IRM: *A Structured Approach To Enterprise Risk Management (ERM) And The Requirements Of ISO 31000*. AIRMIC, ALARM, IRM, London 2010.
- ALUCHNA M.: *Mechanizmy Corporate Governance w spółkach akcyjnych*. SGH, Warszawa 2007.

- BUSCHGEN H.: *Przedsiębiorstwo bankowe*. Wydawnictwo Naukowe PWN, Warszawa 1997.
- COSO: *Enterprise Risk Management – Integrated Framework*. COSO 2004b.
- COSO: *Internal Control – Integrated Framework*. COSO 2011.
- COSO: *Zarządzanie ryzykiem korporacyjnym – zintegrowana struktura ramowa*. COSO 2004a.
- Dyrektywa 2004/109/WE Parlamentu Europejskiego i Rady z dnia 15 grudnia 2004 r. w sprawie harmonizacji wymogów dotyczących przejrzystości informacji o emitentach, których papiery wartościowe dopuszczane są do obrotu na rynku regulowanym oraz zmieniająca Dyrektywę 2001/34/WE.
- Dyrektywa 2006/43/WE Parlamentu Europejskiego i Rady z dnia 17 maja 2006 r. w sprawie ustawowych badań rocznych sprawozdań finansowych i skonsolidowanych sprawozdań finansowych, zmieniająca Dyrektywy Rady 78/660/EWG i 83/349/EWG oraz uchylająca Dyrektywę Rady 84/253/EWG.
- Dyrektywa 2006/46/WE Parlamentu Europejskiego i Rady z dnia 14 czerwca 2006 r. zmieniająca Dyrektywy Rady 78/660/EWG w sprawie rocznych sprawozdań finansowych niektórych rodzajów spółek, 83/349/EWG w sprawie skonsolidowanych sprawozdań finansowych, 86/635/EWG w sprawie rocznych i skonsolidowanych sprawozdań finansowych banków i innych instytucji finansowych oraz 91/674/EWG w sprawie rocznych i skonsolidowanych sprawozdań finansowych zakładów ubezpieczeń.
- Ferma: *Standard zarządzania ryzykiem*. Ferma, Bruksela 2003.
- MORAWSKI M.: *Przedsiębiorstwo zorientowane na wiedzę*. E-mentor nr 4 (16)/2006.
- PWC: *Ład korporacyjny, zarządzanie ryzykiem i kontrole wewnętrzne*. PWC, Warszawa 2009 ([www.pwc.com/pl](http://www.pwc.com/pl)).
- RITTENBERG L., MARTENS F.: *Enterprise Risk Management – Understanding and Communicating Risk Appetite*. COSO 2012.
- Rozporządzenie Komisji (WE) nr 809/2004 z dnia 29 kwietnia 2004 r. wykonujące Dyrektywę 2003/71/WE Parlamentu Europejskiego i Rady w sprawie informacji zawartych w prospektach emisyjnych oraz formy, włączenia przez odniesienie i publikacji takich prospektów emisyjnych oraz rozpowszechniania reklam.
- SAMBORSKI A.: *Governance w przedsiębiorstwie w kontekście społecznej odpowiedzialności*. Przegląd Organizacji nr 1/2012.
- SOBEL P.: *Aligning Corporate Governance With Enterprise Risk Management: Melding Enterprise Risk Management With Governance Means Directors, Senior Management, Internal And External Auditors, And Risk Owners Must Work Interdependently*. Management Accounting Quarterly, Winter 2004.
- SPIECHOWICZ P. (red.): *Komitet audytu – pierwsze kroki. Przewodnik dla praktyków*. 4dot, 2011.
- SUN W., STEWART J., POLLARD D.: *Introduction: Rethinking Corporate Governance – Lessons From the Global Financial Crisis*, [w:] W. Sun, J. Stewart, D. Pollard, *Corporate Governance and the Global Financial Crisis. International Perspectives*. Cambridge University Press, Cambridge 2011.
- Ustawa z dnia 15 września 2000 r. Kodeks spółek handlowych (Dz.U. z 2000 r. Nr 94, poz. 1037, z późn. zm.).

- Ustawa z dnia 29 lipca 2005 r. o ofercie publicznej i warunkach wprowadzania instrumentów finansowych do zorganizowanego systemu obrotu oraz o spółkach publicznych (Dz.U. z 2009 r. Nr 185, poz. 1439, z późn. zm).
- Ustawa z dnia 29 września 1994 r. o rachunkowości (Dz.U. z 2009 r. Nr 152, z późn. zm.).
- Ustawa z dnia 7 maja 2009 r. o biegłych rewidentach i ich samorządzie, podmiotach uprawnionych do badania sprawozdań finansowych oraz o nadzorze publicznym (Dz.U. z 2009 r. Nr 77, poz. 649, z późn. zm.).
- Van der ELST CH.: *The Risks of Corporate Legal Principles of Risk Management*. ECGI Working Paper Series in Law, Working Paper No. 160/2010.
- Van der ELST CH., van DAELEN M.: *Risk Management in European and American Corporate Law*. ECGI Working Paper Series in Law, Law Working Paper No. °122/2009.
- Zalecenie Komisji 2005/162/WE z dnia 15 lutego 2005 r. dotyczące roli dyrektorów niewykonawczych lub będących członkami rady nadzorczej spółek giełdowych i komisji rady (nadzorczej).
- Załącznik do uchwały nr 20/1287/2011 Rady Giełdy z dnia 19 października 2011 r. – Dobre Praktyki Spółek Notowanych na GPW.

## **Enterprise Risk Management in the Context of the Principles of Corporate Governance**

### **Abstract**

For a long time enterprise risk management was associated with financial management, and the use of specific financial instruments such as options or swaps. Today, however, the risk analysis has been incorporated into more formal processes and structures set in the framework of internal control and risk management. As a result of corporate scandals and the loss of confidence in financial reporting there is increased interest in issues of corporate governance among the board, senior management, auditors, and stakeholders. More and more companies are trying to manage risk in a holistic manner. The question is – how to effectively integrate enterprise risk management with the system of corporate governance?