

Istniejące światowe standardy zarządzania ryzykiem mogą być bardzo dobrym punktem wyjścia do tworzenia Systemu Zarządzania Ryzykiem w danej organizacji. W celu uniknięcia bezzasadnego wyważania otwartych drzwi dużo lepiej jest zapoznać się z rozwiązaniami sugerowanymi przez podmioty, które mierzą się z ERM (Enterprise Risk Management) już od drugiej połowy poprzedniego stulecia.

Jaką metodą wybierzemy...

metodę zarządzania ryzykiem?



Marcin Okuniewski
Hestia Loss Control,
menedżer ryzyka, zajmuje się
przygotowaniem oraz wdrożeniem
systemu zarządzania ryzykiem,
absolwent Uniwersytetu Gdańskiego,
w Grupie Ergo Hestia od 2007 roku.

W trzecim numerze magazynu „Risk Focus” (czerwiec 2007) opublikowałem artykuł otwierający nowy obszar analizowanych zagadnień, związany z zarządzaniem ryzykiem. Pojęcie to rozumiane jest nie jako szacowanie i minimalizacja poszczególnych ryzyk, ale jako tworzenie kompleksowych i systemowych rozwiązań, ukierunkowanych na wykreowanie wartości dodanej poprzez dostarczenie narzędzia wspierającego proces zarządczy.

To, co nazwałem Systemem Zarządzania Ryzykiem, od lat występuje w literaturze przedmiotu pod nazwą *Enterprise Risk Management* (ERM) - czyli w wolnym tłumaczeniu *Zarządzanie Ryzykiem Korporacyjnym*. Uważam, że wiązanie ERM z korporacją jest niepotrzebnym zawężaniem pojęcia, adresującym je jedynie do przedsiębiorców. Znacznie szczęśliwszym przejściem z angielskiego *Enterprise Risk Management* (ERM) na język Mickiewicza i Słowackiego są określenia *System Zarządzania Ryzykiem* (SZR) lub *Zintegrowane Zarządzanie Ryzykiem* (ZZR).



Jak to robią inni?

Nie istnieje jeden, najlepszy sposób, w jaki należy zarządzać ryzykiem. W zasadzie każda metoda jest dobra, jeżeli jest skuteczna, czyli zapewnia osiągnięcie założonych celów. Jeden z bohaterów kultowego *Rejsu* Marka Piwowskiego pyta podczas pamiętnego zebrania pasażerów i załogi: *No, świetnie, ale jaką metodą wybierzemy metodę głosowania?* Na tak postawione pytanie w kontekście zarządzania ryzykiem dużo łatwiej będzie nam odpowiedzieć, gdy poznamy trzy najbardziej popularne podejścia do problemu.



Rysunek 1



Rysunek 2



Rysunek 3

Do najbardziej popularnych, a zarazem najszerzej stosowanych standardów zarządzania ryzykiem należy zaliczyć:

- Standard Zarządzania Ryzykiem opracowany przez Federację Europejskich Stowarzyszeń Zarządzania Ryzykiem (FERMA - *Federation of European Risk Management Associations*) - Rysunek 1.
- Zarządzanie ryzykiem korporacyjnym - zintegrowana struktura ramowa przygotowana przez Komitet Organizacji Sponsorujących Komisję Tradeway (COSO II - *The Committee of Sponsoring Organizations of the Tradeway Commission*) - Rysunek 2.
- Australijskie i Nowozelandzkie standardy zarządzania ryzykiem AS/NZS 4360:2004 - Rysunek 3.

Wymienione standardy zarządzania ryzykiem nie wyczerpują oczywiście wszystkich możliwości. Obok wskazanych rozwiązań możemy spotkać także krajowe (na przykład w RPA) lub branżowe standardy, których jednak nie będę przybliżał w niniejszym artykule. W Internecie można spotkać także projekt normy ISO 31000, jako propozycji wypracowania normy zarządzania ryzykiem. Jest ona jednak bardzo zbliżona do standardu AS/NZS 4360:2004, dlatego nie będzie przedmiotem oddzielnej analizy.

Najbardziej angielskie wśród europejskich

FERMA jest Federacją Europejskich Stowarzyszeń Zarządzania Ryzykiem, czyli instytucją, która skupia ludzi i firmy zarządzające ryzykiem na Starym Kontynencie. Od czerwca 2007 roku członkiem FERMY jest także polskie Stowarzyszenie Zarządzania Ryzykiem POLRISK. W 2002 roku FERMA opublikowała standard zarządzania ryzykiem opracowany przez trzy brytyjskie organizacje:

1. AIRIMIC (*The Association of Insurance and Risk Management*) - Stowarzyszenie Zarządzania Ryzykiem i Ubezpieczeniem;
2. ALARM (*The National Forum for Risk Management in the Public Sector*) - Narodowe Forum Zarządzania Ryzykiem w Sektorze Publicznym;
3. IRM (*The Institute of Risk Management*) - Instytut Zarządzania Ryzykiem.

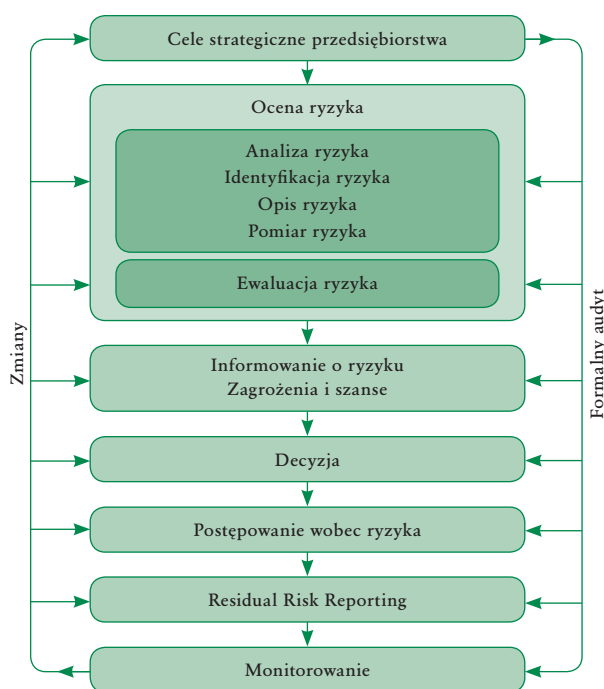
W ten sposób brytyjski standard zarządzania ryzykiem stał się standardem europejskim, a z czasem doczekał się polskiego tłumaczenia.

Lektura standardu FERMA jest bardzo przyjemna głównie ze względu na ograniczoną objętość. Standard liczy zaledwie 16 stron oraz dodatkowe odniesienia do norm i podręczników ISO/IEC. Standard wprowadza podstawowe definicje ryzyka (*kombinacja prawdopodobieństwa wystąpienia zdarzenia oraz jego skutków*) i zarządzania ryzykiem (*proces*,

w ramach którego organizacja w sposób metodyczny rozwiązuje problemy związane z ryzykiem) oraz wskazuje podstawowe czynniki ryzyka (wewnętrzne i zewnętrzne).

Kręgosłupem standardu jest ogólny opis procesu zarządzania ryzykiem, który został przedstawiony w postaci schematu (Rysunek 4). Główna oś procesu to dziesięć następujących po sobie kroków - począwszy od ustalenia celów strategicznych, poprzez działania związane z oceną ryzyka, a kończąc na reakcji na ryzyko oraz monitorowaniu. Równolegle przebiegają dwie boczne osie, które reprezentują: zmiany oraz audyt, czyli katalizatory, wpływające na proces zarządzania ryzykiem na każdym kroku.

Rysunek 4. FERMA - schemat procesu



Źródło: Standard Zarządzania Ryzykiem, FERMA 2002.

Standard FERMY przedstawia przykładowe sposoby opisywania zidentyfikowanych ryzyk oraz wprowadza trzystopniową skalę prawdopodobieństwa wystąpienia zdarzenie i jego skutków. Skutki wystąpienia traktowane są zarówno jako szansa (pozytywne skutki), jak również jako zagrożenie (negatywne skutki). W tym ujęciu ryzyko rozumiane jest zatem w pełni, a nie - jak się czasami zdarza - jedynie przez pryzmat ujemnego wpływu na organizację.

W opisywanym standardzie znaleźć można także odniesienie do wewnętrznej legislacji w organizacji wprowadzającej system zarządzania ryzykiem. Wskazana jest konieczność stworzenia formalnych regulacji oraz określenie roli poszczególnych podmiotów zaangażowanych w proces: Zarządu, Kadry Menedżerskiej, Menedżera Ryzyka (Komitetu) oraz Audytu Wewnętrznego.

Standard FERMY jest bardzo ogólny i zarazem uniwersalny. Pokazuje w poglądowy sposób, jakie są składowe procesu zarządzania ryzykiem oraz jak wyznaczyć przykładowe punkty odniesienia dla szacowania zidentyfikowanego ryzyka. Z jednej strony ta uniwersalność pozwala na adaptację rozwiązania niemal w każdej organizacji i nie ogranicza

inwencji własnej, jednak z drugiej strony wymaga sporej wiedzy i dalszego poszukiwania szczegółowych rozwiązań dla poszczególnych problemów.

Born in the USA

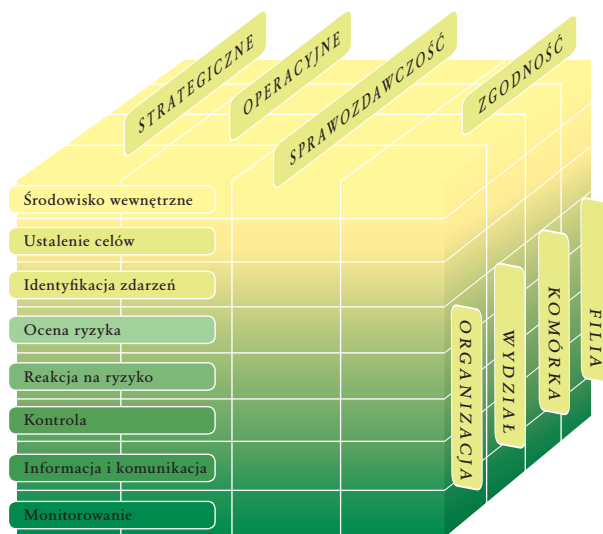
Amerykański standard zarządzania ryzykiem znany jest jako COSO II. Nazwa ta to skrótowiec literowy nazwy organizacji - *The Committee of Sponsoring Organizations of the Treadway Commission*. COSO jest organizacją prywatną, która powstała w latach osiemdziesiątych poprzedniego stulecia, aby podnieść jakość raportowania finansowego, etyki w biznesie, efektywnej kontroli wewnętrznej oraz ładu korporacyjnego.

Pierwszym standardem wydanym przez COSO w 1992 roku była Kontrola Wewnętrzna - Zintegrowana Struktura Ramowa (*Internal Control - Integrated Framework*) znane jako COSO I. Po aferze Enronu¹⁾ oraz wprowadzeniu w Stanach Zjednoczonych ustawy znanej jako SOX²⁾ wydany został w 2004 roku standard COSO II, który jest nie tyle poprawioną wersją COSO I, co jego dopełnieniem obejmującym systemowe podejście do zarządzania ryzykiem.

Standard COSO II jest bardzo obszernym i stosunkowo szczegółowym opracowaniem. Obok ponadstronicowego standardu występuje również obszerny tom technik zastosowania. Dodatkowo COSO II bezpośrednio nawiązuje do rozwiązań COSO I i koresponduje z regulacjami SOX. Jednego z pewnością nie można zarzucić autorom tego standardu - podejścia do tematu *po lebkach*. W 2007 roku ukazało się polskie tłumaczenie standardu.

Standard wprowadza własną definicję ryzyka (*możliwość, że zdarzenie będzie miało miejsce i negatywnie wpłynie na osiągnięcie celów*) i zarządzania ryzykiem (*realizowany przez zarząd, kierownictwo lub inny personel przedsiębiorstwa uwzględniony w strategii i w całym przedsiębiorstwie proces, którego celem jest identyfikacja potencjalnych zdarzeń mogących wywrzeć wpływ na przedsiębiorstwo, utrzymywanie ryzyka w granicach oraz rozsądne zapewnienie realizacji celów przedsiębiorstwa*).

Rysunek 5. COSO II - schemat procesu



Źródło: Zarządzanie ryzykiem korporacyjnym - zintegrowana struktura ramowa, COSO 2004.

COSO II jest trójwymiarową koncepcją, schematycznie przedstawioną w postaci sześcianu (Rysunek 5). Główna płaszczyzna przedstawia sekwencję ośmiu etapów tworzących proces zarządzania ryzykiem - począwszy od analizy środowiska, poprzez ustalenie celów, analizę ryzyka aż po kontrolę i monitorowanie.

Druga płaszczyzna odzwierciedla strukturę organizacyjną przedsiębiorstwa. Zaproponowany czterostopniowy podział oczywiście może być poszerzony lub uszczuplony w zależności od rozmiarów i stopnia złożenia organizacji. Złożenie obu warstw daje obraz ryzyka w każdej jednostce i na każdym poziomie szczegółowości.

Dla uzupełnienia modelu dodana jest trzecia płaszczyzna reprezentująca cztery kategorie celów: strategiczne, operacyjne, sprawozdawczość oraz zgodność. W ten sposób domknięty jest trójwymiarowy obraz procesu zarządzania ryzykiem, który zdaje się być bardzo wnikliwy i nieco abstrakcyjny.

Standard COSO II bardzo szczegółowo opisuje poszczególne etapy pierwszej płaszczyzny (kolejne kroki). Dodatkowo w tomie *Techniki zastosowania* przedstawione są bardzo konkretne i szczegółowo dopracowane rozwiązania pokazujące co i jak mierzyć, określać i analizować. *Techniki zastosowania* wzbogacone są o wzory, krzywe i rozkłady, które mogą być wykorzystane na kolejnych etapach wdrożenia SZR. Dodatkowo opisane są kompetencje podmiotów zaangażowanych w proces oraz przykładowe wzory dokumentów i wskaźniki liczbowe.

COSO II jest zatem bardzo kompletnym i szczegółowym standardem. Silnie wiąże się on z regulacjami dotyczącymi kontroli wewnętrznej (COSO I) oraz w bezpośredni sposób koreluje z przepisami wprowadzonymi przez SOX. Można odnieść wrażenie, że standardy COSO wprowadzają dużą biurokrację i dają niewiele miejsca na swobodne interpretacje. Moim zdaniem to wrażenie jest jak najbardziej uzasadnione, jednak w pewnych okolicznościach te atrybuty nie muszą być traktowane jako mankament.

Z punktu widzenia antypodów

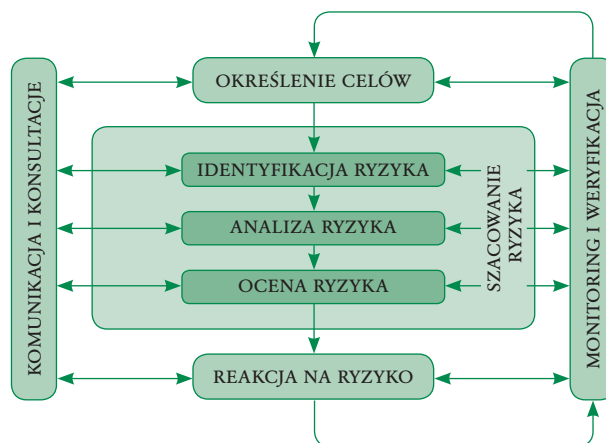
Trzecim standardem zarządzania ryzykiem, któremu chcę przyjrzeć się bliżej, jest australijsko-nowozelandzki standard AS/NZS 4360:2004. Pierwsza wersja tego standardu ukazała się w 1999 roku i miała analogiczne oznaczenie - AS/NZS 4360:1999. Po pierwszych latach stosowania standardu 4360:1999 oraz stosunkowo szerokich konsultacjach (uwzględniających zarówno przedsiębiorców, jak również przedstawicieli sektora publicznego i ośrodków akademickich i naukowych) instytucje standaryzujące z antypodów (Standards Australia oraz Standards New Zealand) wprowadziły pewne modyfikacje do standardu i opublikowały aktualnie obowiązującą wersję 4360:2004. Wersja ta nie została jak do tej pory przetłumaczona na język polski.

Australijski standard rozpoczyna się od słowniczka, w którym między innymi można znaleźć definicję ryzyka (*możliwość wystąpienia zdarzenia, mającego wpływ na działalność, doprowadzającego do powstania zysku lub straty, mierzonego z punktu widzenia prawdopodobieństwa oraz konsekwencji* - tłumaczenie

własne) i zarządzania ryzykiem (*kultura, proces i struktury bezpośrednio skoncentrowane na realizacji korzyści przy jednoczesnym kontrolowaniu zagrożeń* - tłumaczenie własne). Jak widać, oba pojęcia są potraktowane bardzo szeroko i uniwersalnie. Obie definicje jednoznacznie pokazują dwa oblicza ryzyka - szanse i zagrożenia; dodatkowo zarządzanie ryzykiem uwzględnia poza procesem kulturę organizacyjną oraz struktury zaangażowane w proces.

Przebieg procesu składa się z pięciu podstawowych kroków: określenie celów, identyfikacja ryzyka, analiza ryzyka, ocena ryzyka i reakcja na ryzyko. Dodatkowo wprowadzony jest szósty krok (monitorowanie i weryfikacja), który stanowi element równoległy - występuje sprzężenie zwrotne z każdym innym krokiem z procesu. Analogicznie wprowadzone zostały komunikacja i konsultacje, które występują przy każdym elemencie. Graficzny obraz procesu przedstawia schemat na Rysunku 6.

Rysunek 6. AS/NZS 4360:2004 - schemat procesu



Źródło: AS/NZS 4360:2004 (tłumaczenie własne) Standards Australia, New Zealand 2004.

AS/NZS jest ogólnym, choć bardzo konkretnym standardem i ogranicza się do 28 stron. Jako uzupełnienie i komentarz wydany został niespełna 120-stronicowy podręcznik, w którym znajdują się szczegółowe rozwinięcia poszczególnych zagadnień ze standardu. Poza doprecyzowaniem wszystkich elementów procesu zarządzania ryzykiem standard zawiera wskazówki i rady pomagające w efektywny sposób stworzyć struktury organizacyjne, określić kompetencje poszczególnych podmiotów oraz skutecznie wdrożyć SZR w organizacji.

Podręcznik do AS/NZS dostarcza wielu narzędzi, które mogą być wykorzystane przy analizie, ocenie lub reakcji na ryzyko. Są w nim zawarte tabele i wykresy, czytelnie prezentujące metodykę i możliwe podejścia. Trudne i złożone problemy zaprezentowane są w dość przejrzysty i logiczny sposób, dzięki czemu ma się wrażenie, że standard bardziej daje wskazówki niż narzuca gotowe rozwiązania.

Dopełnieniem AS/NZS 4360:2004 jest lista literatury uzupełniającej, odniesienie do komplementarnych standardów (na przykład dotyczących bezpieczeństwa informacji) oraz aktów prawnych związanych z zarządzaniem ryzykiem i pochodnych. Elastyczność standardu połączona jest z dość szczegółowym i systematycznym opisem wszystkich zmiennych, jakie należy wziąć pod uwagę podczas tworzenia SZR w dowolnej organizacji.

Czym się różnią Anglosasi?

W XIX wieku brytyjska królowa Wiktoria stworzyła imperium, nad którym nie zachodziło nigdy słońce (*The Sun never sets on the British Empire*).

Analogia do obecnej sytuacji związanej ze standardami zarządzania ryzykiem jest mocno przesadzona, jednak trzy najpopularniejsze i najbardziej kompleksowe standardy ERM pochodzą właśnie z krajów anglosaskich. Powyżej przedstawiłem ogólną charakterystykę europejskich

(brytyjskich), amerykańskich i australijskich (australijsko-nowozelandzkich) standardów, nie pozostaje mi zatem nic innego, jak tylko ich podsumowanie i zbiorcza analiza porównawcza.

Tabela 1 przedstawia wybrane atrybuty oraz ich charakterystykę w każdym z analizowanych standardów, dzięki czemu dużo łatwiej dokonać jest analizy porównawczej wszystkich trzech standardów w różnych obszarach.

Porównane zostały różne kwestie, dzięki czemu lepiej widać podobieństwa i różnice pomiędzy standardami.

Tabela 1. Porównanie standardów zarządzania ryzykiem

Atrybut	FERMA	COSO II	AS/NZS
Objętość standardu	standard - 16 stron oraz odnośniki	standard - 120 stron oraz techniki zastosowania - 110 stron	standard - 28 stron oraz podręcznik - 116 stron
Język publikacji	angielski/polski	angielski/polski	angielski
Rok publikacji	2002	2004	2004
Definicja ryzyka	kombinacja prawdopodobieństwa wystąpienia zdarzenia oraz jego skutków	możliwość, że zdarzenie będzie miało miejsce i negatywnie wpłynie na osiągnięcie celów	możliwość wystąpienia zdarzenia, mającego wpływ na działalność, doprowadzającego do powstania zysku lub straty, mierzone z punktu widzenia prawdopodobieństwa oraz konsekwencji
Definicja zarządzania ryzykiem	proces, w ramach którego organizacja w sposób metodyczny rozwiązuje problemy związane z ryzykiem	realizowany przez zarząd, kierownictwo lub inny personel przedsiębiorstwa uwzględniony w strategii i w całym przedsiębiorstwie proces, którego celem jest identyfikacja potencjalnych zdarzeń mogących wywrzeć wpływ na przedsiębiorstwo, utrzymywanie ryzyka w granicach oraz rozsądne zapewnienie realizacji celów przedsiębiorstwa	kultura, proces i struktury bezpośrednio skoncentrowane na realizacji korzyści przy jednoczesnym kontrolowaniu zagrożeń
Uniwersalność	standard możliwy do zastosowania we wszystkich organizacjach - także sektor publiczny	uniwersalny standard w szczególności dedykowany spółkom prawa USA	standard możliwy do zastosowania we wszystkich organizacjach
Poziom szczegółowości	bardzo ogólny opis poszczególnych kroków	bardzo szczegółowy opis kolejnych etapów	ogólny opis w standardzie oraz zwięzłe rozwinięcie w podręczniku
Poziom sformalizowania procesu	wskazanie podmiotów uczestniczących w procesie oraz zalecenie stworzenia ogólnych regulacji wewnętrznych	stosunkowo silne wbudowanie SZR w struktury organizacji i konieczność stworzenia rozsądnej legislacji wewnętrznej	określenie podmiotów zaangażowanych w zarządzanie ryzykiem i wskazanie formalnych dokumentów wspierających SZR
Dokumenty uzupełniające	odniesienia do norm ISO/EIC	bardzo mocno powiązany ze standardem COSO I (kontrola wewnętrzna) oraz z regulacjami SOX	sugerowane wykorzystanie dodatkowych standardów dla poszczególnych ryzyk

Źródło: Opracowanie własne

Nie ulega wątpliwości, że wszystkie trzy standardy są w pewnym sensie do siebie bardzo podobne. Zestawiając ze sobą główną oś przebiegu procesu, zauważamy jedynie kosmetyczne różnice polegające na dodaniu kolejnego kroku lub podzieleniu etapu na dwie części.

Pokazuje to, że tak naprawdę nie warto wyważać otwartych drzwi i porywać się na karkołomne próby odkrywania na nowo koła. Cały świat zarządza ryzykiem bardzo podobnie i definiuje je w zbliżony sposób.

FERMA i AS/NZS przyciągają ogólnym ujęciem problemu, natomiast COSO wraz z podręcznikiem AS/NZS dostarcza dużo więcej szczegółowych rozwiązań. COSO jest zdecydowanie najbardziej rozbudowanym standardem, który stwarza dość sztywny gorset, ale z drugiej strony postępując zgodnie z COSO, mamy mniejsze pole do popełnienia błędu niż postępując według szkicu FERMY.

COSO w przeciwieństwie do FERMY i AS/NZS koncentruje się wyłącznie na negatywnym aspekcie ryzyka, zaś FERMA jako jedyna nie wprowadza własnego słownika pojęć (opiera się na definicjach ISO/EIC). Widać więc, że różnice jak najbardziej występują, jednak nie wpływają one na przebieg głównego procesu zarządzania ryzykiem.

Wybór oręza do walki z ryzykiem

Mam cichą nadzieję, że powyższa twórczość literacka nie była zbyt ciężka w lekturze i większości czytelników udało się dotrzeć aż do tego momentu. Jak na rasowego doradcę przystało, czuję się zobowiązany do wskazania rekomendacji. Uważam, że dokonana analiza porównawcza sama w sobie jest istotną wartością dodaną, jednak niech nagrodą dla wytrwałych będzie kilka krótkich kropek nad „i” zawartych w Tabeli 2.

Tabela 2. Rekomendacja stosowania standardów

Standard	Zalecany dla...
FERMA	<p>...podmiotów, które zamierzają stworzyć własny system zarządzania ryzykiem, a standard ma być bardzo elastycznym szablonem;</p> <p>...osób, które posiadają wiedzę i doświadczenie w zarządzaniu ryzykiem, dla których standard ma być jedynie drogowskazem do uporządkowania procesu;</p>
COSO II	<p>...spółek należących do grup kapitałowych notowanych na amerykańskiej giełdzie (podlegających regulacjom SOX);</p> <p>...podmiotów o rozbudowanej strukturze organizacyjnej i dużej dyscyplinie wewnętrznej, wytrwałych we wdrażaniu dość sztywnych i konkretnych regulacji;</p>
AS/NZS 4360:2004	<p>...spółek, które zamierzają wprowadzić system zarządzania ryzykiem, a nie mają w tym zakresie doświadczenia;</p> <p>...podmiotów, które poszukują kompleksowego, a zarazem elastycznego rozwiązania, z możliwością jego modyfikacji i indywidualizacji;</p>

Źródło: Opracowanie własne

Ja już zapoznałem się ze standardami i mam swojego zdecydowanego faworyta, natomiast daleki jestem od wieszczona wyższości Świąt Bożego Narodzenia nad Świątami Wielkanocy. Jak widać z przeprowadzonej analizy, w zależności od charakteru organizacji różne standardy pozwolą na najlepsze zaspokojenie różnych potrzeb.

Pamiętać należy, że przedstawione standardy nie są sztywnymi ramami, które związują ręce menedżerom ryzyka. Są to drogowskazy i propozycje dostarczające kompleksowej odpowiedzi na pytanie, jak zarządzać ryzykiem w sposób kompleksowy.

Standardy te mogą być także wykorzystywane fragmentarycznie - nic nie stoi na przeszkodzie, aby zapoznawszy się z różnymi standardami stworzyć własny,

indywidualizowany konglomerat zawierający różne elementy z powyższych standardów i wzbogacony własnymi rozwiązaniami. Tak jak pisałem w poprzednim numerze „Risk Focusa” (Każdemu według potrzeb), zintegrowane, systemowe podejście do zarządzania ryzykiem ma być elastyczne i indywidualne.

Osobom zainteresowanym bliższym poznaniem standardów zarządzania ryzykiem życzę ciekawej lektury tychże. Jeżeli zaistnieje taka wola i potrzeba, służę dobrą radą oraz bardziej szczegółową prezentacją zagadnienia.

Marcin Okuniewski
marcin.okuniewski@bestia.pl

¹⁾ Enron - amerykańska spółka energetyczna. W latach dziewięćdziesiątych prowadziła tak zwaną „kreatywną księgowość” dzięki cichemu przyzwoleniu audytora, firmy Arthur Andersen. Wraz z ujawnieniem afery w 2001 roku spółka zbankrutowała i doprowadziła do upadku audytora. Afera ENRON-u ujawniła słabość ówczesnej kontroli wewnętrznej oraz brak precyzyjnych regulacji rachunkowych.

²⁾ Ustawa Sarbanes-Oxley, znana jako SOX, została wprowadzona w Stanach Zjednoczonych w 2002 roku w odpowiedzi na aferę ENRON-u odsłaniającą luki prawne w przepisach dotyczących rachunkowości oraz sprawozdawczości. Ustawa jest obszernym i bardzo szczegółowym aktem prawnym, który wprowadza wiele regulacji mających zapobiec możliwości prowadzenia „kreatywnej księgowości” oraz wzmacnia rolę audytu wewnętrznego. Ustawa obejmuje wszystkie spółki amerykańskiego prawa handlowego oraz wszystkie spółki z grup kapitałowych notowanych na amerykańskiej giełdzie.