Pomarańczowa księga

Zarządzanie ryzykiem – zasady i koncepcje

październik 2004

MINISTERSTWO SKARBU JEJ KRÓLEWSKIEJ MOŚCI

MINISTERSTWO SKARBU JEJ KRÓLEWSKIEJ MOŚCI

Pomarańczowa księga

Zarządzanie ryzykiem – zasady i koncepcje

październik 2004

Ministerstwo Skarbu JKM – informacje kontaktowe

Z niniejszym dokumentem można zapoznać się na stronie internetowej Ministerstwa Skarbu:

www.hm-treasury.gov.uk

Więcej informacji o Ministerstwie Skarbu i jego działalności:

Correspondence and Enquiry Unit
HM Treasury
1 Horse Guards Road
London
SW1A 2HQ

Tel.: 020 7270 4558

Faks: 020 7270 4861

E-mail: ceu.enquiries@hm-treasury.gov.uk

ISBN: 1-84532-004-1

SPIS TREŚCI

		Strona
Przedmowa	Przedmowa	7
Rozdział 1	Wstęp	9
Rozdział 2	Model zarządzania ryzykiem	13
Rozdział 3	Identyfikowanie ryzyka	15
Rozdział 4	Ocena ryzyka	19
Rozdział 5	Apetyt na ryzyko	23
Rozdział 6	Postępowanie wobec ryzyka	27
Rozdział 7	Przegląd ryzyka i sprawozdawczość	31
Rozdział 8	Komunikacja i uczenie się	35
Rozdział 9	Rozszerzona działalność	37
Rozdział 10	Środowisko i kontekst ryzyka	39
Załącznik A	Przykład dokumentowania oceny ryzyka	41
Załącznik B	Ogólna pewność w zarządzaniu ryzykiem	43
Załącznik C	Wykaz aspektów monitorowania widnokręgu	47
Załącznik D	Glosariusz kluczowych terminów	49

PRZEDMOWA

W ostatnich latach wszystkie sektory gospodarki koncentrowały się na zarządzaniu ryzykiem, które uznawały za kluczowe dla pomyślnej realizacji przez organizacje wyznaczonych celów i dla jednoczesnej ochrony interesów interesariuszy. Ryzyko jest niepewnością wyniku, a dobre zarządzanie ryzykiem pozwala organizacji:

- pokładać większą ufność w osiąganie swoich zamierzonych wyników;
- skutecznie ograniczać zagrożenia do możliwych do zaakceptowania poziomów;
- podejmować świadome decyzje dotyczące możliwości rozwoju.

Dobre zarządzanie ryzykiem pozwala interesariuszom również na pokładanie większej ufności w ład korporacyjny organizacji i jej zdolność do osiągania wyników.

Na poziomie władz centralnych kilka sprawozdań, zwłaszcza sprawozdanie brytyjskiego urzędu kontroli National Audit Office z 2000 roku o wspieraniu innowacji i zarządzaniu ryzykiem w departamentach rządowych (*Supporting innovation – managing risk in government departments*) oraz sprawozdanie wydziału strategii Strategy Unit z 2002 roku na temat ulepszania zdolności rządu do radzenia sobie z ryzykiem i niepewnością (*Risk – improving government's capability to handle risk and uncertainty*), rozwinęło zagadnienie zarządzania ryzykiem i miało wpływ na opracowanie stanowisk w sprawie systemu kontroli wewnętrznej (*Statements on Internal Control*).

W 2001 roku brytyjskie Ministerstwo Skarbu wydało dokument o zarządzaniu ryzykiem (*Management of Risk – A Strategic Overview*), który szybko zyskał miano „Pomarańczowej księgi". Publikacja ta zawierała wstęp do koncepcji zarządzania ryzykiem, która okazała się bardzo popularnym źródłem do opracowywania i wdrażania procesów zarządzania ryzykiem w organizacjach rządowych. Niniejsza publikacja ma zastąpić „Pomarańczową księgę" wydaną w 2001 roku. Nadal przedstawia ona szeroko zakrojone ogólne wytyczne w odniesieniu do zasad zarządzania ryzykiem, ale została poszerzona, aby odzwierciedlić nasze doświadczenia z zakresu zarządzania ryzykiem, o które wzbogaciliśmy się wszyscy w ostatnich kilku latach. Powinna ona być czytana i wykorzystywana wraz z innymi źródłami istotnych porad, takimi jak „Zielona księga", zawierająca konkretne rady na temat „Oceny i ewaluacji w rządzie centralnym", czy też dokumentem „Zarządzanie ryzykiem", wydanym przez brytyjski Office of Government Commerce (OGC), który przedstawia bardziej szczegółowe wytyczne w kwestii praktycznego stosowania zasad i koncepcji ujętych w niniejszej publikacji, a także wytycznymi przekazanymi przez Zespół Wspierania Zarządzanie Ryzykiem w brytyjskim Ministerstwie Skarbu w ramach programu zarządzania ryzykiem „The Risk Programme". Stosowne odniesienia do dodatkowych źródeł, pozwalających na bardziej szczegółowe zgłębianie przedstawionych koncepcji, znalazły się w treści „Pomarańczowej księgi" wszędzie, gdzie było to możliwe.

Prawdopodobnie najistotniejszą zmianą od czasów wydania „Pomarańczowej księgi" w 2001 roku jest wprowadzenie we wszystkich rządowych organizacjach podstawowych procesów zarządzania ryzykiem. Oznacza to, iż głównym wyzwaniem z zakresu zarządzania ryzykiem nie jest obecnie wstępna identyfikacja i analiza ryzyka, ale raczej ciągły proces przeglądu i usprawniania zarządzania ryzykiem. Wytyczne mają na celu odzwierciedlenie tej sytuacji, zawierają one na

przykład wytyczne w kwestii takich zagadnień, jak „monitorowanie widnokręgu” (ang. *horizon scanning*), w poszukiwaniu zmian oddziałujących na profil ryzyka organizacji. Z uwagą potraktowane zostały zarówno wewnętrzne procesy zarządzania ryzykiem, jak i kwestia zarządzania ryzykiem organizacji w związku ze środowiskiem, w którym działa.

Niniejsze wytyczne mają w naszym zamierzeniu być użyteczne dla:

- osób, dla których zarządzanie ryzykiem jest czymś nowym, a także dla tych, których zadaniem jest przeprowadzanie szkoleń z zarządzania ryzykiem we własnych organizacjach – wszyscy oni uznają niniejsze wytyczne za użyteczny podstawowy dokument wprowadzający;
- osób, których dotyczy przegląd ustaleń z zakresu zarządzania ryzykiem (np. dla członków Zespołów ds. Audytu), jako wyczerpujące źródło zasad, względem których mogą być oceniane istniejące procesy zarządzania ryzykiem;
- członków wyższego kierownictwa, których przewodnictwo jest niezbędne do tworzenia kultury odpowiedniej dla efektywnego zarządzania ryzykiem;
- członków personelu operacyjnego, którzy na co dzień zarządzają ryzykiem podczas realizowania celów organizacji, i dla których niniejszy dokument będzie praktycznym wsparciem w rzeczywistym zarządzaniu ryzykiem; oraz
- osób doświadczonych w zarządzaniu ryzykiem, dla których niniejsze wytyczne zgłębiają trudniejsze koncepcje, np. apetyt na ryzyko.

Niniejsze wytyczne będą równie użyteczne dla czytelników zainteresowanych zarządzaniem ryzykiem głównie na poziomie strategicznym, programowym, jak i operacyjnym.

Mary Keegan

Dyrektor Zarządzający, Dyrektoriat Zarządzania Finansami Rządowymi

Ministerstwo Skarbu JKM

Październik 2004

1 WSTĘP

1.1 Kwestią definicji jest istnienie organizacji w określonym celu – na przykład świadczenia usług lub osiągnięcia konkretnych wyników. W sektorze prywatnym podstawowy cel istnienia organizacji jest zwykle związany ze zwiększaniem bogactwa akcjonariuszy; w sektorze rządowym cel jest zwykle związany ze świadczeniem usługi lub dostarczaniem pożytku w interesie publicznym. Niezależnie od celu istnienia danej organizacji, realizowanie jej celów szczegółowych otoczone jest aurą niepewności, która zarówno zagraża osiągnięciu powodzenia, jak i stwarza możliwości do większego nawet sukcesu.

1.2 Ryzyko definiowane jest jako taka właśnie niepewność wyniku działań lub zdarzeń, wynikająca z pojawiających się szans i zagrożeń. Ryzyko oceniane musi być w odniesieniu do kombinacji prawdopodobieństwa wystąpienia danego zdarzenia i jego oddziaływania w przypadku, jeśli rzeczywiście będzie mieć miejsce. Zarządzanie ryzykiem obejmuje identyfikowanie i ocenę ryzyka („ryzyko nieodłączne") oraz reagowanie na nie.

1.3 Środki dostępne w zarządzaniu ryzykiem stanowią zamknięty katalog, więc celem jest osiągnięcie optymalnej reakcji na ryzyko, przy hierarchizacji wynikającej z oceny ryzyka. Ryzyka nie da się uniknąć i każda organizacja powinna podejmować działania w celu zarządzania ryzykiem w sposób, jaki takie ryzyko uzasadnia, oraz prowadzący do takiego poziomu ryzyka, który jest dopuszczalny. Poziom ryzyka, który oceniany jest jako dopuszczalny i uzasadniony, nazywany jest „apetytem na ryzyko".

1.4 Reakcja na ryzyko, wywodząca się z wewnątrz organizacji, nazywana jest „kontrolą wewnętrzną" i może obejmować jedno lub więcej z następujących zachowań:

- dopuszczanie ryzyka;
- reagowanie na ryzyko w odpowiedni sposób, aby ograniczyć je do akceptowalnego poziomu lub aktywnie z niego korzystać, uznając niepewność za szansę na uzyskanie korzyści;
- przenoszenie ryzyka;
- zakończenie działalności narażającej na ryzyko.

W każdym z powyższych przypadków należy rozważyć kwestię szansy wynikającej z niepewności.

Poziom ryzyka pozostały po przeprowadzeniu kontroli wewnętrznej (ryzyko rezydualne) jest narażeniem (ang. *exposure*) w odniesieniu do danego ryzyka i powinien to być poziom możliwy do zaakceptowania i uzasadniony – powinien znajdować się w granicach apetytu na ryzyko.

1.5 Nic nie dzieje się próżni. Każda organizacja funkcjonuje w środowisku, które oddziałuje na stojące przed nią ryzyka i zapewnia kontekst dla zarządzania ryzykiem. Ponadto każda organizacja ma partnerów, od których zależy jej powodzenie w realizacji celów, niezależnie od tego, czy są to tylko dostawcy dóbr, których potrzebuje, czy też bezpośredni partnerzy w realizacji jej celów. Efektywne zarządzanie ryzykiem wymaga poświęcenia pełnej uwagi kontekstowi działania organizacji oraz priorytetom w zakresie ryzyka partnerskich organizacji.

1.6 Zarządzanie ryzykiem na poziomie strategicznym, programowym i operacyjnym musi być zintegrowane, aby poszczególne poziomy wspierały się. W ten sposób strategia zarządzania ryzykiem organizacji będzie prowadzona z góry i osadzona w zwykłych rutynowych procedurach i działaniach organizacji. Wszyscy

członkowie personelu powinni być świadomi oddziaływania ryzyka na osiąganie swoich celów oraz należy im zapewniać szkolenia wspierające ich w zarządzaniu ryzykiem.

Hierarchia ryzyka

Źródło: Strategy Unit, "Risk: improving government's capability to handle risk and uncertainty", październik 2002 r.

1.7 Zarządzający na każdym poziomie muszą zatem być wyposażeni w odpowiednie umiejętności, które umożliwią im efektywne zarządzanie ryzykiem, a organizacja jako całość potrzebuje środków, które zapewnią jej wdrażanie zarządzania ryzykiem we właściwy sposób na każdym poziomie. Każda organizacja powinna posiadać strategię zarządzania ryzykiem, zaprojektowaną w celu osiągnięcia zasad wyłożonych w niniejszej publikacji. Strategia taka powinna zostać osadzona w systemach biznesowych organizacji, m.in. w procesach kształtowania strategii i polityki, aby zapewnić, by zarządzanie ryzykiem było nieodłącznym elementem prowadzenia działalności.

1.8 Niniejszy przewodnik ma na celu przedstawienie wstępu do szeregu okoliczności, które mają wpływ na zarządzanie ryzykiem, a które mogą mieć zastosowanie na różnych poziomach, od opracowywania strategii, przez wspólną dla całej organizacji politykę dotyczącą ryzyka, aż do zarządzania poszczególnymi projektami lub operacjami. Dzieje się tak dzięki przedstawionemu w kolejnej sekcji modelowi zarządzania ryzykiem – każdy element modelu jest następnie poddany bardziej szczegółowej analizie. Przewodnik najpierw skupia uwagę na „cyklu życia" będącym podstawą modelu, a następnie przedstawia rozważania na temat szerszego spektrum zagadnień składających się na całościowe środowisko zarządzania ryzykiem. Ważne jest, iż przewodnik *nie* jest szczegółowym podręcznikiem jak zarządzać ryzykiem – jego celem jest po prostu zwrócenie uwagi na szereg zagadnień, które dotyczą zarządzania ryzykiem, oraz zaproponowanie ogólnego kierunku, który pomoże czytelnikom zastanowić się, jak postępować wobec poszczególnych zagadnień w okolicznościach specyficznych dla ich własnych organizacji.

1.9 Nie istnieje szczególny „standardowy" zestaw do zarządzania ryzykiem w organizacjach rządowych. Przewodnik ustanawia *zasady* zarządzania ryzykiem, a „Ramy oceny zarządzania ryzykiem"[1] zawierają środki do oceny *dojrzałości* zarządzania ryzykiem. Organizacje mogą wybrać przyjęcie określonych standardów (np. *Risk Management Standards* opracowane w Wielkiej Brytanii wspólnie przez

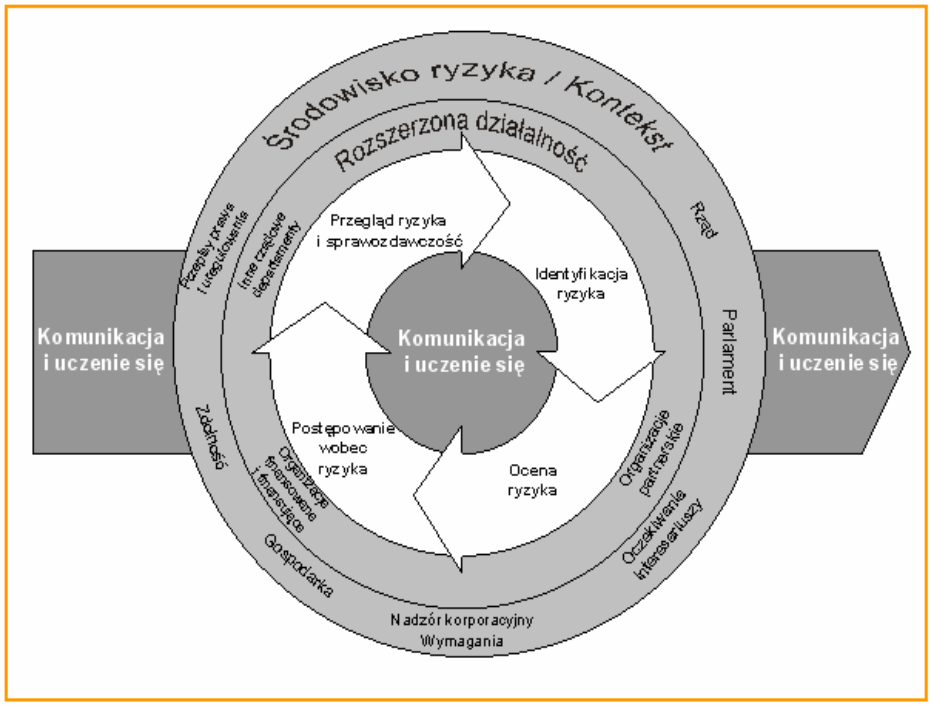
[1] „Risk Management Assessment Framework",
http://www.hm-treasury.gov.uk/media//7B1D9/risk_management_assessment_070104.pdf

IRM, ALARM i AIRMIC[1] lub standard australijski[2], CoSo[3], lub też kanadyjski standard dla sektora rządowego[4]). Ważniejsza od zachowania zgodności z jakimś szczególnym standardem jest zdolność wykazania, że ryzyko jest zarządzane w danej organizacji, w szczególnych dla niej okolicznościach, w sposób, który efektywnie wspiera realizację jej celów.

[1] http://www.airmic.com;
[2] http://www.riskmanagement.com.au/
[3] http://www.erm.coso.org/Coso/coserm.nsf/vwWebResources/PDF_Manuscript/$file/COSO_Manuscript.pdf
[4] http://www.tbs-sct.gc.ca/pubs pol/dcgpubs/Risk Management/siglist e.asp

2 MODEL ZARZĄDZANIA RYZYKIEM

Model zarządzania ryzykiem – opracowany na podstawie modelu ze sprawozdania wydziału strategii Strategy Unit z 2002 roku na temat ulepszania zdolności rządu do radzenia sobie z ryzykiem i niepewnością (*Risk – improving government's capability to handle risk and uncertainty*).



Uwagi do modelu

Zarządzanie ryzykiem nie jest procesem liniowym; jest to raczej bilansowanie wielu splecionych ze sobą elementów, które wzajemnie na siebie oddziałują, i które muszą pozostawać ze sobą w stanie równowagi, jeśli zarządzanie ryzykiem ma być efektywne. Ponadto określonym ryzykiem nie można się zajmować w odizolowaniu od innych ryzyk; zarządzanie jednym ryzykiem może wpływać na inne, możliwe do osiągnięcia są też takie działania zarządzających, które są efektywne przy równoczesnym kontrolowaniu więcej niż jednego ryzyka.

Model nie będzie pełnił żadnej funkcji w środowisku, w którym apetyt na ryzyko został określony. Koncepcja apetytu na ryzyko (jaki poziom ryzyka jest możliwy do zaakceptowania i uzasadniony) może być uznana za warstwę pokrywającą cały model.

Model tu przedstawiony, z konieczności, rozkłada na czynniki pierwsze podstawowy proces zarządzania ryzykiem na poszczególne elementy w celach ilustracyjnych, ale w rzeczywistości zlewają się one ze sobą. Ponadto konkretny etap w procesie, na którym można się znajdować dla danego ryzyka, niekoniecznie musi być ten sam dla każdego innego ryzyka.

Jak pokazano na modelu, podstawowy proces zarządzania ryzykiem nie przebiega w izolacji, ale ma miejsce w pewnym kontekście. Pokazuje także, jak konieczny jest wkład niektórych kluczowych elementów w ogół procesu, aby uzyskać pożądane produkty zarządzania ryzykiem.

3 IDENTYFIKOWANIE RYZYKA

3.1 Aby zarządzać ryzykiem organizacja musi nie tylko wiedzieć, jakie ryzyko jej zagraża, ale także musi je ocenić. Identyfikacja ryzyka jest pierwszym krokiem na drodze do stworzenia profilu ryzyka każdej organizacji. Nie ma jedynego słusznego sposobu dokumentowania profilu ryzyka organizacji, ale dokumentacja jest nieodzowna w efektywnym zarządzaniu ryzykiem.

3.2 W identyfikowaniu ryzyka można wyróżnić dwie odrębne fazy. Wyróżniamy zatem:

- wstępną identyfikację ryzyka (w przypadku organizacji, która w przeszłości nie identyfikowała ryzyka w ustrukturyzowany sposób, lub w przypadku nowej organizacji albo nowego projektu bądź działalności w danej organizacji), oraz
- ciągłą identyfikację ryzyka, która konieczna jest do identyfikacji nowego ryzyka, jakie nie występowało wcześniej, zmian w dotychczasowym ryzyku lub ryzyka, które faktycznie istniało, ale przestało być istotne dla organizacji (powinien być to rutynowy element prowadzenia działalności).

3.3 W każdym przypadku ryzyko powinno dotyczyć celów. Można dokonać oceny i hierarchizacji ryzyka tylko w odniesieniu do celów (i można tego dokonać na każdym ich poziomie, od celów indywidualnych pracowników do celów organizacji). Należy dołożyć starań w celu zidentyfikowania ryzyka ogólnego (ang. *generic risk*), które będzie miało wpływ na cele działalności, ale może nie zawsze być od razu widoczne w rozważaniach nad konkretnym celem działalności. Kiedy ryzyko zostało zidentyfikowane, może okazać się istotne w odniesieniu do więcej niż jednego celu organizacji, jego potencjalny wpływ może być różny dla różnych celów, a najlepszy sposób postępowania wobec tego ryzyka może być różny w odniesieniu do różnych celów (chociaż jest też możliwe, że jeden sposób reagowania może być odpowiedni dla ryzyka dotyczącego więcej niż jednego celu). Stwierdzając ryzyko, należy uważać, aby unikać stwierdzania oddziaływania ryzyka, które może wydawać się samym ryzykiem, a także by unikać stwierdzania ryzyka, które nie ma wpływu na cele; podobnie należy uważać, by unikać określania ryzyka sformułowaniami, które są po prostu odwrotnością celów. Stwierdzenie ryzyka powinno obejmować przyczynę oddziaływania i wpływ na cel („przyczynę i skutek"), który może się pojawić.

Cel – dojechać pociągiem z A do B na spotkanie o określonej godzinie	
Nie dojechanie z A do B na spotkanie o określonej godzinie	X Jest to po prostu odwrotność celu.
Spóźnienie się i opuszczenie spotkania.	X Jest to stwierdzenie wpływu ryzyka, a nie samego ryzyka.
W pociągu nie ma bufetu, więc zgłodnieję.	X Nie ma to wpływu na osiągnięcie celu.
Jeśli nie zdążę na pociąg, to spóźnię się i nie zdążę na spotkanie.	✓ Jest to ryzyko, które można kontrolować upewniając się, że przeznaczę dużo czasu na dotarcie do stacji.
Zła pogoda uniemożliwi odjazd pociągu, a mi dotarcie na spotkanie.	✓ Jest to ryzyko, którego nie mogę kontrolować, ale mogę stworzyć plan awaryjny.

3.4 Pojedyncze ryzyka zidentyfikowane przez organizację nie będą niezależne od siebie nawzajem; raczej będą zwykle formowały naturalne grupy. Na przykład mogą istnieć ryzyka, które można zebrać w grupę jako „zasoby", oraz inne ryzyka, które można zebrać razem jako „środowiskowe". Niektóre ryzyka będą istotne dla kilku celów organizacji. Takie grupy ryzyk będą łączyły odnośne ryzyka na poziomach strategicznym, programowym i operacyjnym (zob. 1.6). Ważne jest, by nie pomylić grupy ryzyk z samymi ryzykami. Ryzyka powinny być identyfikowane na poziomie, na którym można zidentyfikować konkretne oddziaływanie oraz konkretne działanie lub działania, które można podjąć w celu radzenia sobie z tym ryzykiem. Wszystkie ryzyka, po ich zidentyfikowaniu, powinny mieć swojego właściciela, który jest odpowiedzialny za zapewnienie, iż ryzyko jest zarządzane i monitorowane wraz z upływem czasu. Właściciel ryzyka, zgodnie z jego rozliczalnością za zarządzanie ryzykiem, powinien mieć władzę wystarczającą do zapewnienia efektywnego zarządzania ryzykiem; właściciel ryzyka nie może być osobą, która w rzeczywistości podejmuje działanie wobec ryzyka.

3.5 Konieczne jest przyjęcie właściwego podejścia lub narzędzia do identyfikacji ryzyka. Do dwóch najczęściej stosowanych podejść należą:

- zlecanie przeglądu ryzyka: tworzony jest zespół fachowców (rekrutowanych wewnętrznie, albo najmowanych spoza organizacji), których zadaniem jest przeprowadzenie analizy wszystkich operacji i działań organizacji w stosunku do jej celów oraz zidentyfikowanie związanego z tym ryzyka. Praca zespołu powinna polegać na przeprowadzaniu wywiadów z kluczowym personelem na wszystkich poziomach organizacji w celu utworzenia profilu ryzyka dla całej gamy działań (ważne jest jednak, aby zastosowanie tego podejścia nie osłabiło pojmowania przez kierownictwo liniowe swojej odpowiedzialności za zarządzanie takim ryzykiem, które jest adekwatne dla osiąganych przez nich celów);

- samoocena ryzyka: podejście, zgodnie z którym każdy poziom i część organizacji są zapraszane do przeprowadzenia przeglądu swoich działań oraz do przedstawienia swojej diagnozy związanego z tym ryzyka. Można to wykonać stosując podejście oparte na prowadzeniu dokumentacji (wyznaczając ramy diagnozy w kwestionariuszach), ale często większą skuteczność uzyskamy przyjmując podejście warsztatu kierowanego (podczas którego facylitatorzy – czyli osoby, które posiadają odpowiednie umiejętności ułatwiające przeprowadzenie całego procesu – pomagają grupom personelu zidentyfikować ryzyko oddziałujące na realizację celów). Dużą zaletą tego podejścia jest dokładniejsze określenie właściciela ryzyka, gdyż ryzyko identyfikowane jest właśnie przez samych właścicieli.

3.6 Podejścia te nie wykluczają się wzajemnie, a nawet pożądana jest kombinacja podejść w ramach procesu identyfikowania ryzyka – dzięki temu czasami ujawniane są znaczne różnice w percepcji ryzyka wewnątrz organizacji. Takie różnice w postrzeganiu ryzyka muszą zostać zniwelowane w celu osiągnięcia efektywnej integracji zarządzania ryzykiem na różnych poziomach organizacji.

3.7 Obecnie zarówno w sektorze publicznym, jak i prywatnym, coraz częściej większego znaczenia nabiera myślenie perspektywiczne i zarządzanie potencjalnym ryzykiem. Między organizacjami można zauważyć znaczne zróżnicowanie w podejściach do „monitorowania widnokręgu" z uwagi na odmienne potrzeby organizacyjne. Wykaz aspektów „monitorowania widnokręgu", udostępniony przez Civil Contingencies Secretariat przy Cabinet Office, znajduje się w Załączniku C.

3.8 Poniższa tabela pochodzi z przeprowadzonego w 2004 roku (przez Ministerstwo Skarbu) przeglądu ryzyka w głównych departamentach i zawiera zestawienie najczęściej występujących kategorii lub grup ryzyka z przykładami

charakteru źródła i skutków; tabela ta ma pomóc organizacjom sprawdzić, czy uwzględniły cały zakres potencjalnego ryzyka; tabela nie zawiera wyczerpującej listy, więc niektóre organizacje mogą zidentyfikować inne kategorie ryzyka właściwego dla swojej działalności.

KATEGORIA RYZYKA		Przykłady/zagadnienia do analizy
1. Zewnętrzne (wynikające ze środowiska zewnętrznego, nie znajduje się w całości pod kontrolą organizacji, ale można podjąć pewne działania w celu zmniejszenia tego rodzaju ryzyka) ***[Niniejsza analiza oparta jest na modelu „PESTLE" [1] – zob. „Strategy Survival Guide" na stronie www.strategy.gov.uk.]***		
1.1	**P**olityczne	Zmiana rządu, ważne decyzje polityczne (np. wprowadzenie euro); mechanizmy zmian w rządzie
1.2	**E**konomiczne	Zdolność do przyciągania i zatrzymywania personelu na rynku pracy; kursy wymiany walut wpływają na koszty transakcji międzynarodowych; wpływ gospodarki globalnej na gospodarkę brytyjską
1.3	**S**połeczno-kulturowe	Zmiany demograficzne determinują popyt na usługi; zmiana oczekiwań interesariuszy
1.4	**T**echnologiczne	Starzenie się obecnie używanych systemów; koszt zakupu najlepszej z dostępnych technologii; możliwości stwarzane przez rozwój technologiczny
1.5	**L**egislacyjne/regulacyjne	Wymogi UE/akty prawne nakładające wymagania (np. legislacja dotycząca ochrony zdrowia i bezpieczeństwa w miejscu pracy lub ochrony środowiska)
1.6	**E**kologiczne	Obiekty muszą spełniać zmieniające się normy; usuwanie śmieci i nadwyżki wyposażenia również musi spełniać zmieniające się wymogi
2. Operacyjne (związane z wykonywanymi obecnie operacjami – zarówno z realizacją zobowiązań, jak i budowaniem oraz utrzymywaniem wydajności i potencjału)		
2.1	Realizacja zobowiązań	
2.1.1	Niedostarczenie usług/produktów	Niedostarczenie usług użytkownikowi stosownie do uzgodnionych/ustalonych warunków
2.1.2	Wykonanie projektu	Niewykonanie projektu w terminie/w ramach budżetu/zgodnie ze specyfikacjami
2.2	Wydajność i potencjał	
2.2.1	Zasoby	Finansowe (niedostateczne fundusze, niewłaściwe zarządzanie budżetem, nadużycia finansowe), zasoby ludzkie (wydajność/umiejętności/ rekrutacja i zatrzymywanie personelu) Informacyjne (adekwatność podejmowanych decyzji; ochrona prywatności) Aktywa materialne (strata/uszkodzenie/kradzież)
2.2.2	Relacje	Kontrahenci (zagrożenia dla zobowiązań/przejrzystość ról) Klienci/użytkownicy usług (zadowolenie z obsługi) Rozliczalność (zwłaszcza wobec Parlamentu)
2.2.3	Operacje	Ogólna zdolność i potencjał w zakresie dostarczania usług
2.2.4	Reputacja	Zaufanie interesariuszy do organizacji
2.3	Wyniki i zdolność w zakresie zarządzania ryzykiem	
2.3.1	Nadzór	Prawidłowość i moralność/zgodność z odpowiednimi wymogami/względy etyczne
2.3.2	Monitorowanie	Niezidentyfikowanie szans i zagrożeń
2.3.3	Odporność i wytrzymałość	Możliwości systemów/dostosowanie się/systemy informatyczne odporne na negatywne wpływy i kryzysy (w tym działania wojenne i ataki terrorystyczne). Przywrócenie poprawnego działania organizacji po wystąpieniu zdarzenia kryzysowego/awaryjny plan działań
2.3.4	Bezpieczeństwo	Aktywów materialnych i informacji
3. Związane ze zmianą (ryzyko wynikające z decyzji o realizacji nowych przedsięwzięć wykraczających poza obecne zdolności)		
3.1	Cele związane z umowami w zakresie służby publicznej (PSA)	Nowe cele związane z umowami w zakresie służby publicznej podważają zdolność organizacji do realizacji zobowiązań/zdolność do wyposażenia organizacji w środki umożliwiające realizację zobowiązań
3.2	Programy zmian	Programy wprowadzające zmiany organizacyjne lub kulturowe zagrażają bieżącej zdolności do realizacji zobowiązań oraz znalezieniu możliwości zwiększenia zdolności
3.3	Nowe projekty	Podejmowanie optymalnych decyzji inwestycyjnych/hierarchizacja projektów rywalizujących o środki
3.4	Nowa polityka	Decyzje związane z nową polityką stwarzają oczekiwania tam, gdzie organizacja nie ma pewności co do zrealizowania zobowiązań

[1] Angielskie słowo *pestle* oznacza „tłuczek do moździeża" lub „ucierać, tłuc w moździeżu" [przyp. tłum.].

4 OCENA RYZYKA

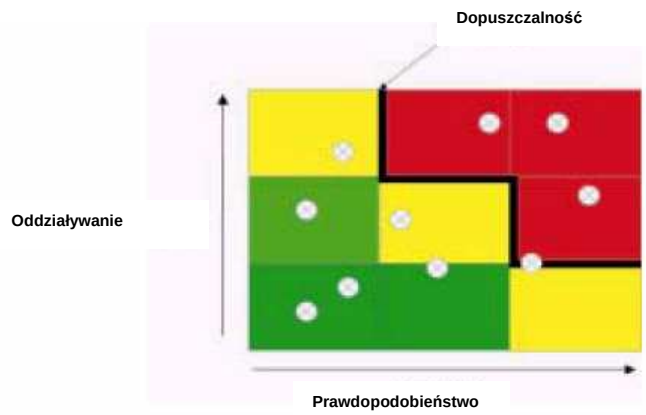
4.1 Przy ocenie ryzyka obowiązują trzy ważne zasady:

- należy zapewnić, że stosowany jest wyraźnie ustrukturyzowany proces, w którym przy ocenie każdego ryzyka uwzględniane jest zarówno prawdopodobieństwo jego wystąpienia, jak i jego oddziaływanie;
- należy dokumentować ocenę ryzyka w sposób, który ułatwia monitorowanie i identyfikację priorytetów związanych z ryzykiem;
- należy zachować wyraźne rozróżnienie między ryzykiem nieodłącznym a ryzykiem rezydualnym (zob. 1.2 oraz 1.4).

4.2 Niektóre rodzaje ryzyka poddają się analizie numerycznej – zwłaszcza ryzyko finansowe. W przypadku pozostałych rodzajów ryzyka – np. ryzyka związanego z utratą reputacji – możliwe jest zastosowanie jedynie o wiele bardziej subiektywnego osądu. Pod tym względem ocena ryzyka ma w sobie więcej ze sztuki, aniżeli z nauki. Niemniej konieczne będzie stworzenie pewnych ram oceny ryzyka. Ocena taka powinna w możliwie największym zakresie opierać się na obiektywnych i niezależnych dowodach, uwzględniać punkty widzenia wszystkich interesariuszy, których dotyczy dane ryzyko, oraz unikać pomylenia obiektywnej oceny ryzyka z osądem dotyczącym akceptowalności ryzyka.

4.3 Ocenę taką należy przeprowadzać oceniając zarówno prawdopodobieństwo wystąpienia ryzyka oraz jego oddziaływanie, jeśli takie ryzyko wystąpiło. Podział na wysokie/średnie/niskie ryzyko może okazać się wystarczający dla każdego rodzaju ryzyka i powinien być minimalnym poziomem kategoryzacji – prowadzi to do uzyskania macierzy ryzyka „3x3”. Odpowiednia może również okazać się bardziej szczegółowa skala analityczna, zwłaszcza jeśli w przypadku konkretnego ryzyka można zastosować dokładną ocenę ilościową – często używane są macierze „5x5”, gdzie oddziaływanie mierzone jest na skali „nieznaczne/małe/średnie/duże/katastrofalne”, a prawdopodobieństwo na skali „rzadkie/mało prawdopodobne/możliwe/prawdopodobne/prawie pewne”. Nie ma jedynego słusznego standardu w przypadku skali w matrycach ryzyka – organizacja powinna sama osądzić poziom szczegółowości analizy, który będzie najbardziej adekwatny dla danych okoliczności. Aby jeszcze bardziej uwydatnić znaczenie ryzyka można posłużyć się kolorem („drogowa sygnalizacja świetlna”).

Przykładowa macierz ryzyko/dopuszczalność



4.4 Kiedy ocena jest następnie porównywana z apetytem na ryzyko (zob. 4.5 poniżej), czytelny staje się zakres wymaganego działania. Ważna jest nie bezwzględna wartość ocenianego ryzyka, ale to czy ryzyko uznawane jest za *dopuszczalne*, albo, co jest równie ważne, jak daleko jest od narażenia na ryzyko do dopuszczalności.

4.5 Na poziomie organizacyjnym apetyt na ryzyko może cechować się większą złożonością (więcej informacji zob. Sekcja 5), ale na poziomie określonego ryzyka bardziej prawdopodobne jest, że poziom akceptowalnego narażenia może zostać zdefiniowany w kategoriach zarówno dopuszczalnego oddziaływania, jeśli ryzyko wystąpi, oraz dopuszczalnej częstotliwości tegoż oddziaływania. Sprzeczny z tym jest fakt, że należy porównać ryzyko rezydualne, aby zdecydować czy wymagane są dalsze działania. Dopuszczalność może być określana wartością aktywów utraconych lub zmarnowanych w przypadku negatywnego oddziaływania, postrzeganiem przez interesariuszy danego oddziaływania, zrównoważeniem kosztów kontroli i zakresu narażenia oraz zrównoważeniem potencjalnie wygenerowanych korzyści lub strat.

4.6 Analiza ryzyka często koncentruje się na ryzyku rezydualnym (tzn. ryzyku po przeprowadzeniu kontroli, które – zakładając, że kontrola jest skuteczna – będzie rzeczywistym narażeniem organizacji na ryzyko, zob. 1.4). Oczywiście ryzyko rezydualne należy często poddawać ponownej ocenie, na przykład, jeśli punkt kontrolny wymaga korekty. Ocena *przewidywanego* ryzyka rezydualnego wymagana jest do oceny proponowanych działań kontrolnych.

4.7 Należy dołożyć staranności pozyskując informacje o ryzyku *nieodłącznym*. W przeciwnym razie organizacja nie będzie wiedziała, jakie będzie jej narażenie, jeśli nie powiedzie się kontrola. Znajomość ryzyka nieodłącznego pozwala również lepiej określić, czy prowadzona jest nadmierna kontrola – jeśli ryzyko nieodłączne znajduje się w granicach apetytu na ryzyko, może nie zachodzić konieczność wydatkowania zasobów na kontrolowanie tego ryzyka. Konieczność posiadania wiedzy zarówno o ryzyku nieodłącznym, jak i rezydualnym, oznacza, że ocena ryzyka jest etapem w procesie zarządzania ryzykiem, który nie może być oddzielany od sposobu postępowania wobec ryzyka; zakres wymaganego postępowania wobec ryzyka określany jest przez ryzyko nieodłączne, a adekwatność środków stosowanych w postępowaniu wobec ryzyka można analizować dopiero po przeprowadzeniu oceny ryzyka rezydualnego.

4.8 Ocenę ryzyka należy dokumentować w taki sposób, by odnotowane zostały kolejne etapy procesu (przykład przedstawiono w Załączniku A). Dokumentowanie oceny ryzyka tworzy *profil ryzyka* dla organizacji, który:

- ułatwia identyfikację priorytetów ryzyka (w szczególności w celu zidentyfikowania najistotniejszych rodzajów ryzyka, którymi powinno się zająć kierownictwo wyższego szczebla);

- uwidacznia powody podjęcia decyzji o tym co jest, a co nie jest dopuszczalnym narażeniem na ryzyko;

- ułatwia rejestrowanie procesu decyzyjnego związanego z postępowaniem wobec ryzyka;

- umożliwia wszystkim, których dotyczy zarządzanie ryzykiem, zobaczenie całościowego profilu ryzyka oraz jak umiejscowione są w nim ich obszary obowiązków;

- ułatwia przegląd i monitorowanie ryzyka.

4.9 Po przeprowadzeniu oceny ryzyka ujawniają się priorytety ryzyka dla danej organizacji. Im mniej akceptowalne narażenie na dane ryzyko, tym wyższy priorytet powinien zostać nadany postępowaniu wobec takiego ryzyka. Ryzyka o najwyższym priorytecie (kluczowe ryzyka) powinny być regularnie brane pod uwagę na najwyższym poziomie organizacji i w związku z tym powinny być regularnie analizowane przez zarząd. Poszczególne priorytety ryzyka będą się zmieniać wraz z upływem czasu, ponieważ zajmowanie się konkretnym ryzykiem prowadzi w konsekwencji do zmiany hierarchizacji.

5 APETYT NA RYZYKO

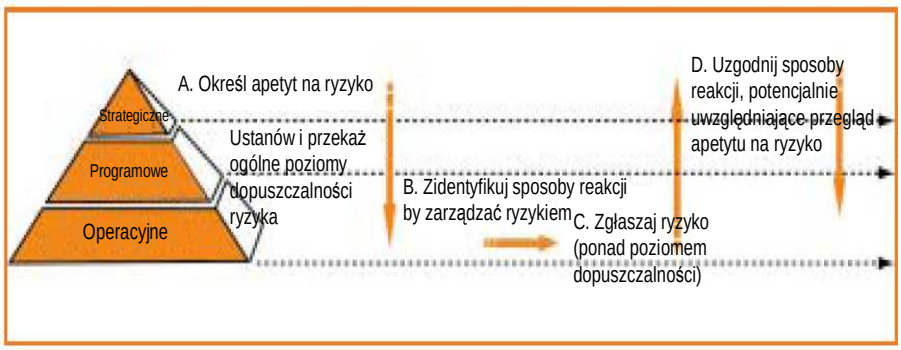
5.1 Koncepcja apetytu na ryzyko odgrywa kluczową rolę w osiąganiu efektywnego zarządzania ryzykiem i jej rozważenie jest konieczne przed zastanowieniem się, jak postępować wobec ryzyka. Koncepcję można analizować na różne sposoby, zależnie od tego, czy ryzyko (niepewność) uważana jest za zagrożenie, czy też za szansę:

- uwzględniając zagrożenia, koncepcja apetytu na ryzyko ujmuje poziom narażenia na ryzyko, który uważany jest za dopuszczalny i uzasadniony, jeśli ryzyko urzeczywistni się. W tym rozumieniu chodzi tu o porównanie kosztu (finansowego lub innego) ograniczania ryzyka z kosztem narażenia na nie w przypadku, gdyby takie narażenie stało się rzeczywistością, oraz o znalezienie możliwej do zaakceptowania równowagi;

- uwzględniając szanse, koncepcja obejmuje rozważania, na ile ktoś gotowy jest do aktywnego podjęcia ryzyka w celu uzyskania korzyści płynącej z nadarzającej się szansy. W tym rozumieniu chodzi tu o porównanie wartości (finansowej lub innej) potencjalnych korzyści ze stratami, które mogą zostać poniesione (niektóre straty mogą zostać poniesione bez uzyskania korzyści lub łącznie z nimi).

Należy zauważyć, że pewny poziom ryzyka jest nie do uniknięcia i żadna organizacja nie jest w stanie w pełni zarządzać ryzykiem, sprowadzając je do dopuszczalnego poziomu – na przykład wiele organizacji musi przyjąć do wiadomości istnienie ryzyka wynikającego z terroryzmu, którego nie są w stanie kontrolować. W takich przypadkach organizacje powinny sporządzić *plan awaryjny*.

5.2 W każdym razie apetyt na ryzyko najlepiej można wyrazić za pomocą serii limitów, stosownie zatwierdzonych przez zarządzających, które przekazują każdemu poziomowi organizacji jasne wytyczne w kwestii poziomów ryzyka, które mogą podjąć, niezależnie od tego, czy rozważają zagrożenie i koszt jego kontrolowania, czy też szansę i koszt próby jej wykorzystania. Oznacza to, że apetyt na ryzyko zostanie wyrażony przy użyciu takich samych terminów, jak te wykorzystywane przy ocenie ryzyka. Apetyt na ryzyko organizacji niekoniecznie jest stały; szczególnie zarząd będzie dysponował swobodą w zakresie różnicowania poziomu ryzyka, które gotowy jest podjąć zależnie od istniejących w danym momencie okoliczności. Poniższy model bardziej szczegółowo przedstawia te koncepcje.



5.3 Tak więc apetyt na ryzyko może podlegać dalszej analizie:

- **korporacyjny apetyt na ryzyko**: korporacyjny apetyt na ryzyko jest całkowitym poziomem ryzyka uznanym za odpowiedni i dopuszczalny dla organizacji, uzgodnionym na poziomie zarządu (litera A w modelu w podpunkcie 5.2). Może to być więcej niż jedno tylko stanowisko: na przykład OGC uwzględnia 5 kluczowych obszarów ryzyka (ryzyko polityczne/wytycznych; ryzyko personalne i systemów wewnętrznych; ryzyko dotyczące praw własności, finansów i rozliczalności, ryzyko regulacyjne; ryzyko utraty reputacji; ryzyko zewnętrzne) i wydaje oświadczenie dotyczące apetytu na ryzyko w każdym z nich. Zarząd i wyższa rangą kadra zarządzająca powinna określić dopuszczalny zakres narażenia organizacji i zidentyfikować ogólne limity dla ryzyka przekraczającego dopuszczalny poziom (lub przynajmniej dla ryzyk, które powinny zawsze być eskalowane/ poddawane zarządowi pod dyskusję i wymagają jego decyzji, jeśli wystąpią). Pracując nad tym, zarząd być może będzie chciał uwzględnić poglądy na ten temat z poszczególnych ministerstw;

- **delegowany apetyt na ryzyko**: uzgodniony korporacyjny apetyt na ryzyko może być następnie wykorzystany jako punkt wyjścia do kaskadowania poziomów dopuszczalności w dół organizacji, uzgadniając apetyt na ryzyko na jej różnych poziomach (litera B w modelu w podpunkcie 5.2). Wynikiem tego jest sytuacja, w której coś uznawanego za wysoki poziom ryzyka na jednym poziomie organizacji będzie niższym poziomem ryzyka dla wyższej rangą kadry zarządzającej. Ułatwia to zarówno proces eskalacji ryzyka, gdy przekracza ono delegowane limity i wymaga podjęcia decyzji (zob. 5.4 poniżej), jak i upoważnia personel do wprowadzania innowacji w ramach delegowanych im uprawnień;

- **projektowy apetyt na ryzyko**: projekty, które wymykają się z ram zwykłej działalności organizacji, mogą wymagać sformułowania apetytu na ryzyko na ich potrzeby. Różne rodzaje projektów mogą też wymagać różnych poziomów apetytu na ryzyko, na przykład organizacja może być gotowa do zaakceptowania wyższego poziomu ryzyka dla projektu, który miałby to pokaźnie wynagrodzić.

  - Różne rodzaje projektów to np.:

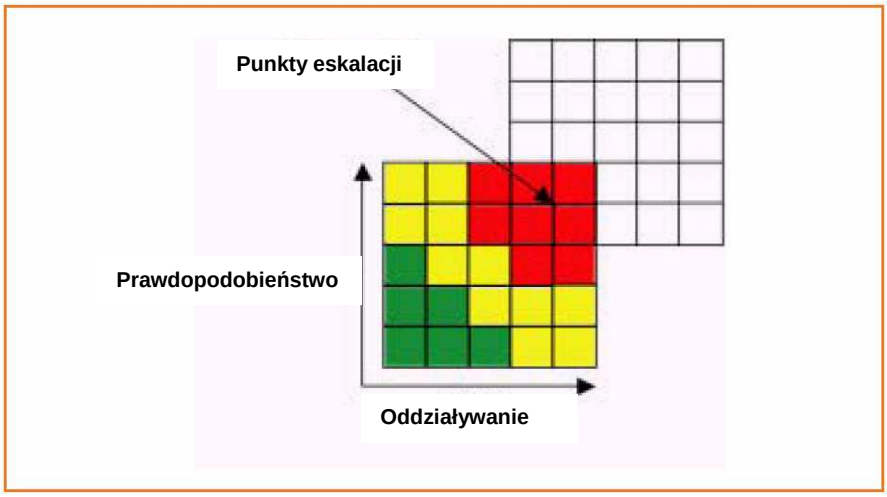
    - projekty spekulacyjne (podobne do kapitału podwyższonego ryzyka w sektorze przedsiębiorstw): z wysokim ryzykiem, ale potencjalnie dużymi korzyściami, np. projekty typu „inwestuj by uratować budżet", projekty pilotażowe. Może się zdarzyć, iż większość z takich projektów zakończy się niepomyślnie, ale pozwoli na zdobycie ważnych doświadczeń.

    - zwykłe projekty rozwojowe: np. z zakresu informatyki (IT), zamówień, budowy, itd. (w momencie wydania niniejszego dokumentu w coraz większym stopniu obejmowane przez programy Centrów Doskonałości OGC);

    - projekty krytyczne dla realizacji misji, w których organizacja musi być pewna sukcesu.

Poziom apetytu na ryzyko będzie oczywiście zróżnicowany, przy czym projekt spekulacyjny będzie gotowy do przyjęcia wyższego poziomu ryzyka niż projekt krytyczny z punktu widzenia misji.

5.4 Efektywne zarządzanie i stosowanie delegowanego apetytu na ryzyko wymaga procesów eskalacji. Możliwe jest wyznaczenie „punktów aktywacji" (ang. *trigger points*), które umożliwiają eskalację ryzyka na kolejny poziom zarządzania, ponieważ ryzyko zbliża się lub przekracza uzgodniony dla niego poziom apetytu na ryzyko (litera C w modelu w podpunkcie 5.2). Kolejny poziom w hierarchii podjąłby wtedy odpowiednie działania, które mogłyby polegać na bezpośrednim zarządzaniu ryzykiem lub na dostosowaniu poziomu ryzyka dopuszczalnego do zarządzania na niższym poziomie (litera D w modelu w podpunkcie 5.2). Często też dzieje się tak, że wyższy poziom kadry zarządzającej, zarządzający większym portfelem ryzyka, ma większe możliwości zaakceptowania wyższego ryzyka w określonym obszarze, ponieważ może zrównoważyć je niższym poziomem ryzyka w innych obszarach w swoim portfelu.



5.5 Dalsze zastosowania koncepcji apetytu na ryzyko obejmują:

- alokowanie zasobów: po wyznaczeniu apetytu na ryzyko, możliwe jest dokonanie przeglądu, czy zasoby zostały właściwie ocenione. Jeśli ryzyko nie odpowiada uzgodnionemu apetytowi na ryzyko, można skoncentrować zasoby na sprowadzeniu ryzyka do dopuszczalnego poziomu. Ryzyko znajdujące się już w obrębie uzgodnionego poziomu dopuszczalności może zostać poddane przeglądowi, aby sprawdzić, czy zasoby mogą zostać przesunięte do bardziej ryzykownych obszarów bez wywierania negatywnych konsekwencji. Urząd celny, urząd podatkowy, policja, straż – wszyscy wykorzystują alokowanie zasobów na podstawie ryzyka, aby hierarchizować przydzielanie zasobów.

- inicjowanie projektów: podejmując decyzję o inicjowaniu nowego projektu, a następnie dokonując przeglądów na poszczególnych etapach w brytyjskim OGC, apetyt na ryzyko może być wykorzystany jako wskazówka, czy projekt powinien być dalej realizowany, a także jako pomoc w identyfikowaniu i zarządzaniu ryzykiem, które może przeszkodzić w udanym zakończeniu projektu.

6 POSTĘPOWANIE WOBEC RYZYKA

6.1 Celem podejmowania działań w obliczu ryzyka jest przekształcenie niepewności w korzyść dla organizacji w drodze ograniczania zagrożeń i korzystania z szans. Każde działanie podejmowane przez organizację w ramach postępowania wobec ryzyka tworzy część większej całości zwanej „systemem kontroli wewnętrznej". Można wyróżnić pięć głównych aspektów postępowania wobec ryzyka:

DOPUSZCZANIE

Narażenie na ryzyko może być dopuszczalne bez podejmowania jakichkolwiek dalszych działań. Nawet jeśli nie jest dopuszczalne, zdolność do wywarcia wpływu na niektóre rodzaje ryzyka może być ograniczona lub też koszt podjęcia jakiegokolwiek działania może być niewspółmierny do potencjalnych korzyści, które można odnieść. W takich przypadkach odpowiedzią może być tolerowanie ryzyka istniejącego poziomu ryzyka. Taka opcja może oczywiście być uzupełniana przez plany awaryjne, mające na celu radzenie sobie z oddziaływaniem ryzyka powstałym w przypadku jego urzeczywistnienia się.

ZMNIEJSZANIE

W ten sposób postępuje się z największą liczbą ryzyk. Celem zmniejszania jest, pomimo kontynuowania w organizacji działalności powodującej powstanie ryzyka, podjęcie działania (punkt kontrolny) w celu ograniczenia ryzyka do możliwego do zaakceptowania poziomu. Takie punkty kontrolne mogą być dalej dzielone zgodnie z ich konkretnym przeznaczeniem (zob. 6.2 poniżej).

PRZENIESIENIE

Najlepszą reakcją wobec niektórych rodzajów ryzyka może być ich przeniesienie. Można to uczynić za pomocą konwencjonalnego ubezpieczenia lub płacąc stronie trzeciej za przejęcie ryzyka w inny sposób. Opcja ta jest szczególnie dobra w przypadku zmniejszania ryzyka finansowego lub ryzyka majątkowego. Przeniesienie ryzyka można rozważać albo w celu zmniejszenia narażenia organizacji, albo kiedy inna organizacja (która może być inną organizacją rządową) ma większą zdolność do efektywnego zarządzania ryzykiem. Warto odnotować, iż niektóre rodzaje ryzyka nie są (w pełni) przenoszalne – w szczególności nie jest zwykle możliwe przeniesienie ryzyka utraty reputacji, nawet jeśli świadczenie usługi jest zlecane na zewnątrz. Stosunki ze stroną trzecią, na którą przenoszone jest ryzyko, wymagają uważnego zarządzania, aby zapewnić udane przeniesienie ryzyka (zob. Sekcja 10).

ZAKOŃCZENIE

Niektóre rodzaje ryzyka można zmniejszać lub sprowadzać do akceptowalnych poziomów jedynie kończąc działalność. Należy zwrócić uwagę, iż stosowanie opcji zakończenia działalności może być poważnie ograniczone w sektorze rządowym w porównaniu do prywatnego; wiele rodzajów działalności realizowanych jest w sektorze rządowym, ponieważ związane z nimi ryzyko jest tak duże, iż nie ma innego sposobu, aby produkt lub wynik, wymagany dla dobra publicznego, został osiągnięty. Opcja ta może być szczególnie istotna w zarządzaniu projektem, jeśli staje się jasne, iż przewidywany stosunek kosztów do korzyści jest zagrożony.

KORZYSTANIE Z SZANS

Opcja ta nie jest alternatywą wobec tych wymienionych powyżej; jest to raczej opcja, która powinna być poddana rozwadze zawsze w przypadku dopuszczania ryzyka, przenoszenia go lub zmniejszania. Można wyróżnić tu dwa aspekty. Pierwszym jest stwierdzenie, czy podczas zmniejszania zagrożeń, nie pojawia się szansa wykorzystania pozytywnych oddziaływań? Na przykład, jeśli duża kwota na inwestycje kapitałowe ma być narażona na ryzyko w większym projekcie, czy stosowne systemy kontroli oceniane są wystarczająco dobrze, by uzasadnić zwiększenie przedmiotowej kwoty w celu uzyskania jeszcze większych korzyści? Drugim aspektem jest stwierdzenie, czy powstaną okoliczności, które nie generując zagrożeń, zaoferują pozytywne możliwości? Na przykład obniżenie kosztów dóbr lub usług uwalnia zasoby, które można inaczej wykorzystać.

6.2 Opcję „zmniejszania" w ramach postępowania wobec ryzyka można poddać dalszej analizie i wyróżnić cztery typy punktów kontrolnych:

ZAPOBIEGAWCZE PUNKTY KONTROLNE

Punkty te projektowane są z myślą o ograniczaniu możliwości urzeczywistnienia się niepożądanego wyniku. Im ważniejsze jest, by niepożądany wynik nie wystąpił, tym ważniejsze staje się wdrażanie stosownych zapobiegawczych punktów kontrolnych. Większość punktów kontrolnych wprowadzanych w organizacjach przynależy do tej kategorii. Przykładem zapobiegawczych punktów kontrolnych jest m.in. rozdział obowiązków, gdzie żadna osoba nie jest upoważniona do działania bez zgody innej (np. odseparowanie osoby zatwierdzająca płatność faktury od osoby zamawiającej towary zapobiega zawłaszczeniu sobie towarów przez jedną osobę na koszt publiczny) oraz ograniczenie wykonywania czynności do osób upoważnionych (np. udzielania odpowiedzi na pytania środków masowego przekazu tylko przez odpowiednio przeszkolone i uprawnione osoby zapobiega przedostawaniu się do prasy nieodpowiednich komentarzy).

KORYGUJĄCE PUNKTY KONTROLNE

Punkty te tworzone są w celu korygowania niepożądanych wyników, które stały się rzeczywistością. Zapewniają one ścieżkę częściowego powrotu do utraconych pozycji w razie poniesienia straty bądź szkody. Przykładem tego może być sformułowanie warunków umownych w sposób umożliwiający odzyskanie nadpłaty. Ubezpieczenie można również uznawać za formę korygującego punktu kontrolnego, ponieważ ułatwia odzyskanie równowagi finansowej w przypadku urzeczywistnienia się ryzyka. Tworzenie awaryjnych planów działania jest ważnym elementem korygujących punktów kontrolnych, jako że jest to środek, który pozwala organizacji planować utrzymanie ciągłości działania/powrót do równowagi po wystąpieniu zdarzeń, których kontrolować nie mogła.

NAKAZOWE PUNKTY KONTROLNE

Punkty te mają na celu zapewnić osiągnięcie konkretnego wyniku. Są one szczególnie ważne, kiedy niezwykle istotne jest, aby uniknąć wystąpienia niepożądanego zdarzenia – zwykle kojarzonego z zagrożeniem dla zdrowia i bezpieczeństwa. Przykładem tego typu punktów kontrolnych mogłoby być dodanie wymogu noszenia odzieży ochronnej w trakcie wykonywania niebezpiecznych obowiązków lub przeszkolenia personelu z zakresu koniecznych umiejętności przed pozwoleniem na pracę bez nadzoru.

WYKRYWAJĄCE PUNKTY KONTROLNE

Punkty te zaprojektowane są do identyfikowania okazji do powstania niepożądanych wyników, które już się pojawiły. Ich efekt występuje, z definicji, „po zdarzeniu", więc są odpowiednie tylko wtedy, gdy możliwe jest zaakceptowanie poniesionej straty lub szkody. Wśród przykładów wykrywających punktów kontrolnych można wymienić sprawdzenia stanów zapasów lub aktywów (które wykrywają, czy zapasy lub aktywa nie zostały wyniesione bez upoważnienia), uzgodnienie stanu kont (które może wykryć nieuprawnione transakcje), „przeglądy powdrożeniowe", które uwidaczniają płynące z projektów nauki do wykorzystania w przyszłej pracy, a także działania monitoringowe, które wykrywają wymagające reakcji zmiany.

6.3 W projektowaniu punktów kontrolnych ważne jest, by ustanowione punkty były współmierne do ryzyka. Abstrahując od najbardziej ekstremalnych niepożądanych wyników (takich jak utrata życia), zwykle wystarcza zaprojektowanie punktu kontrolnego dającego *rozsądny poziom pewności* ograniczenia prawdopodobnej straty w ramach apetytu na ryzyko organizacji. Z każdą czynnością kontrolną wiąże się koszt i ważne jest, aby czynność kontrolna oferowała odpowiedni efekt za wydane pieniądze (ang. *value for money*) w odniesieniu do ryzyka, które kontroluje. Ogólnie mówiąc, celem punktu kontrolnego jest raczej ograniczanie ryzyka aniżeli eliminowanie go.

7 PRZEGLĄD RYZYKA I SPRAWOZDAWCZOŚĆ

7.1 Zarządzanie ryzykiem musi podlegać przeglądowi i sprawozdawczości z dwóch powodów:

- aby monitorować, czy nie następują zmiany w profilu ryzyka;
- aby upewniać się, że zarządzanie ryzykiem jest efektywne oraz by zidentyfikować moment, gdy konieczne będzie dalsze działanie.

7.2 Należy ustanowić procesy przeglądu sprawdzające, czy ryzyko nadal występuje, czy pojawiło się nowe ryzyko, czy prawdopodobieństwo i oddziaływanie ryzyka zmieniło się oraz raportujące istotne zmiany, które korygują priorytety ryzyka, a także dające pewność, że kontrola jest skuteczna. Ponadto *całościowy proces zarządzania ryzykiem* powinien być poddawany regularnym przeglądom w celu uzyskania pewności, iż wciąż jest odpowiedni i efektywny. Przegląd ryzyka i przegląd procesu zarządzania ryzykiem różnią się i żaden z nich nie zastępuje drugiego. Procesy przeglądu powinny:

- zapewnić, by wszystkie aspekty procesu zarządzania ryzykiem były przedmiotem przeglądu przynajmniej raz w roku;
- zapewnić, by same ryzyko było poddawane przeglądowi odpowiednio często (przewidując przegląd ryzyka dokonywany przez samych zarządzających, jak i przegląd/audyt niezależny);
- przewidywać alarmowanie odpowiedniej rangą kadry zarządzającej o nowym ryzyku lub o zmianach w już zidentyfikowanym ryzyku, aby możliwe było podjęcie stosownego postępowania wobec ryzyka.

7.3 Dostępnych jest wiele narzędzi i technik, które są pomocne w realizacji procesu przeglądu:

- samoocena ryzyka (ang. *Risk Self Assessment*, RSA) jest techniką, do której już odnosiliśmy się przy identyfikacji ryzyka (zob. 3.5). Proces samooceny ryzyka również przyczynia się do realizacji procesu przeglądu. Sprawozdanie z wyników samooceny ryzyka uwzględniane jest w procesie w celu otrzymania profilu ryzyka obejmującego całą organizację. (Proces ten bywa nieraz nazywany samooceną ryzyka i kontroli – ang. *Control and Risk Self Assessment*, CRSA.);
- sprawozdawczość z odpowiedzialnego zarządzania (ang. *Stewardship Reporting*) wymaga składania przez wybranych członków kadry zarządzającej na różnych poziomach organizacji (zwykle przynajmniej raz w roku na koniec roku obrachunkowego, często śródokresowo co kwartał lub pół roku) sprawozdań swoim przełożonym z pracy wykonanej przez siebie na rzecz posiadania aktualnych i stosownych do okoliczności procedur związanych z ryzykiem i kontrolą w swoim obszarze odpowiedzialności. Proces ten jest kompatybilny z RSA; zarządzający mogą wykorzystać RSA jako narzędzie do zebrania informacji do sprawozdania z odpowiedzialnego zarządzania;

- Dokument „Ramy oceny zarządzania ryzykiem", wydany przez brytyjskie Ministerstwo Skarbu, dostarcza narzędzi do oceny dojrzałości zarządzania ryzykiem w organizacji. Narzędzie to jest szczególnie użyteczne w przygotowywaniu dorocznego stanowiska w sprawie systemu kontroli wewnętrznej (*Statement on Internal Control*), które jest publicznym sprawozdaniem z przeglądu systemu kontroli wewnętrznej[1].

Oprócz tych wymienionych sformalizowanych narzędzi, pracownicy, grupy robocze i zespoły powinni nieustannie pracować nad tym, poddając pod rozwagę zagadnienia związane z ryzykiem, które napotykają w wykonywanej przez siebie pracy.

7.4 Każda organizacja rządu centralnego zobowiązana jest do uwzględnienia audytu wewnętrznego. Prace wykonywane w ramach audytu wewnętrznego dają ważne, niezależne i obiektywne przesłanie na temat pewności w zakresie adekwatności zarządzania ryzykiem, kontroli i nadzoru[2]. Audyt wewnętrzny może też być wykorzystany przez zarządzających w roli specjalistycznego wewnętrznego konsultanta, który pomoże w opracowaniu dla organizacji procesu zarządzania ryzykiem strategicznym. Taki konsultant będzie miał szeroko zakrojony pogląd na cały zakres działań podejmowanych przez organizację oraz wcześniej przeprowadzoną już w pewnej formie ocenę w celu opracowania świadomego planu kontroli systemów i procesów. Ważne jest jednakże, by pamiętać, że audyt wewnętrzny nie zastąpi przyjmowania przez zarządzających odpowiedzialności za ryzyko, ani utrwalonego systemu przeglądu, realizowanego przez różnych członków personelu, którzy ponoszą odpowiedzialność za osiąganie celów organizacji (zob. więcej szczegółowych informacji o zagadnieniach związanych z audytem wewnętrznym w rządowych standardach audytu wewnętrznego *Government Internal Audit Standards*, Ministerstwo Skarbu JKM, październik 2001 r., oraz w powiązanych wytycznych dotyczących dobrych praktyk).

7.5 Wiele organizacji posiada wyspecjalizowane zespoły ds. przeglądu i pewności, które zostały powołane do konkretnych celów (np. zespoły ds. kontroli rachunków lub zespoły ds. przeglądu zgodności). Ich praca przyczynia się do uzyskiwania pewności na temat ryzyka i systemów kontroli stosowanych w organizacji. Mechanizmy odpowiedzialnego zarządzania, w których kierownicy liniowi zdają sprawozdanie z odpowiedzialnego zarządzania w swoich obszarach odpowiedzialności, również są ważne do uzyskiwania pewności, szczególnie w organizacjach ze strukturami kontroli opartymi w dużym stopniu na delegowaniu.

7.6 Poza rzadkimi wyjątkami, każda organizacja rządowa posiada Zespół ds. Audytu (ustanowiony jako zespół zarządu, najlepiej złożony z osób niepełniących funkcji kierowniczych i prowadzony przez osobę również niepełniącą funkcji kierowniczych), który ma za zadanie wspierać księgowych (ang. *Accounting Officer*) w realizacji ich obowiązków związanych z zagadnieniami dotyczącymi ryzyka, kontrolą i nadzorem oraz powiązanym z tym uzyskaniem pewności (więcej szczegółowych informacji zob. podręcznik zespołu ds. audytu *Audit Committee Handbook*, Ministerstwo Skarbu JKM, październik 2003 r.). Księgowy/zarząd powinni zwrócić się do Zespołu ds. Audytu o:

- uzyskanie pewności, że monitorowane jest ryzyko i jego zmiany;
- zebranie różnych informacji dotyczących pewności, które są dostępne na temat zarządzania ryzykiem, a następnie o sformułowanie ogólnej opinii na temat zarządzania ryzykiem;

[1] Więcej informacji zob. *Government Accounting*, rozdział 21 – www.government-accounting.gov.uk.
[2] „Definition of Internal Audit" [Definicja audytu wewnętrznego], *Government Internal Audit Standards*, Ministerstwo Skarbu JKM, październik 2001 r.

- wyrażenie opinii na temat adekwatności istniejących procesów zarządzania ryzykiem i uzyskiwania pewności.

Należy zauważyć, iż Zespół ds. Audytu nie powinien sam być właścicielem ryzyka ani nim zarządzać, ani też nie zastąpi, podobnie jak audyt wewnętrzny, właściwej roli zarządzających w zarządzaniu ryzykiem.

7.7 Niektóre organizacje mogą powoływać Zespół ds. Ryzyka. Zarząd musi zdecydować o roli, jaką takiemu zespołowi chce przeznaczyć. Jeśli Zespół ds. Ryzyka jest powołany jako zespół zarządu i jest (w dużym stopniu) złożony z osób niepełniących funkcji kierowniczych (tzn. „Zespół ds. *Pewności wobec* Ryzyka"), może on realizować funkcje opisane w podpunkcie 7.6 powyżej, które w innym przypadku zostałyby przydzielone Zespołowi ds. Audytu. Jednak jeśli Zespół ds. Ryzyka jest forum dla osób zarządzających, które w dużym stopniu odpowiadają za zarządzanie ryzykiem i są właścicielami ryzyka, i na którym to forum wymieniają doświadczenia i koordynują swoje działania na rzecz zarządzania ryzykiem (tzn. „Zespół ds. *Zarządzania* Ryzykiem", który realizuje powinność osób zarządzających do zapewnienia efektywnego zarządzania ryzykiem), w takim przypadku Zespół ds. Audytu powinien zachować swoją niezależną rolę uzyskiwania pewności, która została dla niego przewidziana. Ta druga możliwość nie wyklucza wkładu w rozważania czynione przez Zespół ds. Ryzyka ze strony osób niezajmujących kierowniczych stanowisk.

7.8 Załącznik B przedstawia założenia i kluczowe elementy procesu uzyskiwania i informowania o ogólnej pewności w zarządzaniu ryzykiem oraz zawiera omówienie procesów uzyskiwania pewności.

8 KOMUNIKACJA I UCZENIE SIĘ

8.1 Komunikacja i uczenie się nie są odrębnym etapem w zarządzaniu ryzykiem; są raczej czymś, co przenika cały ten proces. Istnieje wiele aspektów komunikacji i uczenia się wartych uwagi.

8.2 Identyfikacja nowych ryzyk lub zmian w ryzyku jest sama w sobie uzależniona od komunikacji. „Monitorowanie widnokręgu" (zob. 3.7 i Załącznik C) w szczególności zależy od utrzymania dobrej sieci komunikacyjnej z odpowiednimi kontaktami i źródłami informacji w celu ułatwienia identyfikacji zmian, które wpływają na profil ryzyka organizacji. Zakres jest dość szeroki: od informacji o bezpieczeństwie narodowym, które mogłyby wpłynąć na strategiczne planowanie organizacji rządowych, poprzez wywiad gospodarczy nakierowany na rentowność organizacji partnerskich lub głównych kontrahentów, po informacje na temat planów, jakie posiada jedna organizacja rządowa, a które mogą wpływać na żądania stawiane innej organizacji rządowej.

8.3 Wewnątrz organizacji ważna jest komunikacja dotycząca zagadnień związanych z ryzykiem.

- Należy dbać o to, by każdy rozumiał, w sposób odpowiedni dla pełnionej przez siebie roli, jaka jest strategia ryzyka organizacji, jakie są priorytety ryzyka oraz jak własne obowiązki w organizacji wpisują się w te ramy. Jeśli tego nie osiągniemy, nie osiągniemy również właściwego i spójnego utrwalania zarządzania ryzykiem, ani spójności w realizacji priorytetów ryzyka;

- Należy zapewnić, że wyciągnięta zostanie dająca się przekazać nauka z myślą o tych, którzy mogą z jej przekazania skorzystać. Na przykład, jeśli jedna część organizacji stanie wobec nowego ryzyka i opracuje skuteczny mechanizm jego kontroli, nauką tą należy podzielić się z tymi wszystkimi, którzy mogą również napotkać takie ryzyko.

- Należy zapewnić, by na każdym poziomie zarządzania, łącznie z zarządem, aktywnie poszukiwano i uzyskiwano należytą i regularną pewność co do zarządzania ryzykiem w swoim zakresie kontroli. Osoby takie muszą otrzymywać wystarczające informacje, które umożliwią im planowanie działań w odniesieniu do ryzyka, w przypadkach gdy ryzyko rezydualne nie jest akceptowalne, a także pewność związaną z ryzykiem uznawanym za akceptowalne pod kontrolą. Na równi z rutynową komunikacją w zakresie takich gwarancji powinien istnieć mechanizm powiadamiania o ważnych zagadnieniach związanych z ryzykiem, które nagle się wykształcają lub pojawiają.

8.4 Równie ważna jest komunikacja z organizacjami partnerskimi w zakresie zagadnień związanych z ryzykiem (zob. również Sekcja 9 – Rozszerzona działalność), zwłaszcza gdy jedna organizacja jest uzależniona od innej organizacji nie tylko w przypadku pojedynczego kontraktu, ale bezpośredniego zapewniania usług w imieniu tej organizacji. Nieporozumienia dotyczące poszczególnych priorytetów ryzyka mogą prowadzić do poważnych problemów – w szczególności do stosowania niewłaściwych poziomów kontroli w odniesieniu do konkretnych ryzyk, a sama niemożność uzyskania pewności co do wprowadzenia przez organizację partnerską odpowiedniego zarządzania ryzykiem może prowadzić do uzależnienia od podmiotu trzeciego, który może prowadzić bieżącą działalność w sposób niemożliwy do zaakceptowania.

8.5 Ważne jest komunikowanie się z interesariuszami na temat sposobu, w jaki organizacja zarządza ryzykiem, aby upewnić ich, że organizacja będzie działała zgodnie z ich oczekiwaniami oraz ukierunkować oczekiwania interesariuszy na to, co organizacja jest w stanie rzeczywiście osiągnąć. Jest to istotne szczególnie w odniesieniu do ryzyka, które wywiera wpływ na ogół społeczeństwa i kiedy ogół społeczeństwa polega na rządzie, który ma w ich imieniu przyjąć określoną postawę wobec takiego ryzyka.

9 ROZSZERZONA DZIAŁALNOŚĆ

9.1 Żadna organizacja nie stanowi całkowicie zamkniętej całości – będzie ona znajdowała się w sieci wzajemnych zależności z innymi organizacjami. Te współzależności, nazywane czasami „rozszerzoną działalnością" (ang. *extended enterprise*), będą wywierały wpływ na zarządzanie ryzykiem w organizacji, prowadząc do powstania pewnych dodatkowych ryzyk, którymi również trzeba będzie zarządzać. Względy takie powinny obejmować wpływ działalności organizacji na inne organizacje. W niniejszej sekcji przedstawiono niektóre z potencjalnych relacji rozszerzonego przedsiębiorstwa oraz ich ewentualne implikacje dla zarządzania ryzykiem.

9.2 Wiele organizacji będzie pozostawało w stosunku wzajemnej zależności z innymi organizacjami rządowymi, z którymi nie mają bezpośrednich relacji w zakresie kontroli – osiągnięcie ich celów będzie zależało od/wpływało na osiągnięcie celów przez inne organizacje. W takich okolicznościach działania jednej organizacji będą bezpośrednio oddziaływały na ryzyko stojące przed inną organizacją, stąd efektywna współpraca tych dwóch organizacji jest nieodzowna do wprowadzenia uzgodnionego podejścia do zarządzania ryzykiem, pozwalającego obydwu organizacjom osiągnąć swe cele.

9.3 Wiele organizacji rządowych utrzymuje relacje z podmiotami, wobec których przyjmuje rolę „macierzystą" lub które dla nich są organami macierzystymi. W szczególności wiele departamentów politycznych jest uzależnionych od organów wykonawczych lub pozaministerialnych instytucji publicznych (NDPB) w zakresie realizacji swojej polityki, a polityka wielu organów wykonawczych i pozaministerialnych instytucji publicznych ograniczana jest przez ich ministerstwa macierzyste. W takich okolicznościach priorytety ryzyka ministerstwa macierzystego będą oddziaływały na priorytety finansowanych przez nie organizacji, a zdobyte przez finansowane organizacje doświadczenie w zakresie zarządzania ryzykiem podczas realizacji danej polityki powinno być uwzględniane przez organizację macierzystą w dalszym rozwoju polityki. Regularne i otwarte dyskusje na temat zagadnień związanych z ryzykiem prowadzone przez organizacje macierzyste i organizacje finansowane są niezbędne do uzyskania ogólnej efektywności służby publicznej.

9.4 Prawdopodobnie wszystkie organizacje rządowe pozostają w stosunku wzajemnej zależności z kontrahentami lub innymi osobami trzecimi, choć zakres takiej współzależności może być różny. Relacje te mogą przybierać różne formy, od prostych dostaw produktów, które umożliwiają funkcjonowanie organizacji, po zapewnianie organizacji, lub w jej imieniu większych usług. W niektórych przypadkach trzeba będzie sporządzić umowę z osobą trzecią, aby celowo przenieść ryzyko, którym zarządzać będzie osoba trzecia z uwagi na posiadanie lepszych możliwości (zob. 7.1). Może to obejmować partnerstwa publiczno-prywatne lub outsourcing takich usług jak dostawa infrastruktury informatycznej dla organizacji. Szczególnym potencjalnym problemem w tym przypadku jest nadmierne uzależnienie organizacji od kontrahenta, gdy jest ona dla kontrahenta tylko pomniejszym klientem (np. niewielka pozaministerialna instytucja publiczna kupuje wspomniane oprogramowanie od dużej firmy konsultingowej w dziedzinie informatyki). Ważne jest, aby organizacje analizowały każdą ze swoich istotnych relacji z kontrahentami i osobami trzecimi oraz dbały o to, by osiągnięta została komunikacja i porozumienie w zakresie poszczególnych priorytetów ryzyka.

9.5 Niezależnie od złożoności charakteru związanych z ryzykiem relacji, jakie organizacja utrzymuje z innymi w ramach rozszerzonej działalności, każda relacja

wiąże się również z koniecznością uzyskania pewności, że ryzyko jest zarządzane w ramach tej relacji w sposób zarówno odpowiedni, jak i planowy. Uwzględnienie uzyskania takiej pewności jest integralną częścią tego typu związku.

10 ŚRODOWISKO I KONTEKST RYZYKA

10.1 Poza granicami „rozszerzonej działalności” znajdują się również inne czynniki tworzące środowisko, w którym zarządzane jest ryzyko. Czynniki te (zwykle znajdujące się w grupie ryzyka „zewnętrznego” przedstawionego w tabeli w Sekcji 3) mogą albo generować ryzyko, którego nie da się bezpośrednio kontrolować, albo mogą ograniczać sposób, w jaki organizacji wolno podejmować ryzyko lub jemu przeciwdziałać. Często jedynym rozwiązaniem, jakie organizacja może przyjąć w odniesieniu do środowiska ryzyka, jest opracowanie planów awaryjnych. Na przykład większość organizacji rządowych z siedzibą główną w centralnym Londynie nie może bezpośrednio kontrolować ryzyk, których źródłem jest międzynarodowy terroryzm, ale mogą one sporządzać plany awaryjne zapewniające ciągłość działania w razie większego ataku terrorystycznego (więcej informacji zob. www.ukresilience.info/lead.htm). Ważne jest, aby organizacja uwzględniała szersze środowisko ryzyka i starała się poznać sposób, w jaki oddziałuje ono na jej strategię zarządzania ryzykiem.

10.2 Na środowisko ryzyka mogą wywierać wpływ zwłaszcza przepisy i uregulowania. Dlatego ważne jest, aby organizacja znała wymagania stawiane jej mocą przepisów i uregulowań, które albo skłaniają organizację do wykonania pewnych działań, albo ograniczają działania, które organizacji wolno podejmować. Na przykład sposób postępowania organizacji wobec ryzyka nie dołożenia należytej staranności przez personel określony jest w prawie pracy.

10.3 Gospodarka zarówno krajowa, jak i globalna, jest kolejnym ważnym elementem składającym się na środowisko ryzyka. Choć dla większości organizacji ogólna gospodarka jest czymś danym, w istocie wpływa ona na rynki, na których muszą one funkcjonować pozyskując lub zapewniając dobra i usługi; gospodarka może w szczególności wywierać wpływ na zdolność organizacji do przyciągania i zatrzymywania personelu posiadającego umiejętności poszukiwane przez organizację.

10.4 Szczególnym aspektem środowiska ryzyka, który jest istotny dla organizacji rządowych, jest sam Rząd. W zasadzie organizacje rządowe istnieją, aby realizować politykę uzgodnioną przez Rząd i Ministerstwa. Istnieje szczególna strona zarządzania ryzykiem, która jest ważna w zapewnianiu Ministrom opartych na ryzyku rad o charakterze politycznym. Niemniej urzędnicy w organizacjach rządowych mogą otrzymywać oparte na decyzjach politycznych wytyczne, jakie ryzyko mogą, a jakiego nie mogą podejmować.

10.5 Swobodę działania każdej organizacji ograniczają również oczekiwania interesariuszy. Działania podejmowane w ramach zarządzania ryzykiem, które w teorii wydają się wartościowe i skuteczne, mogą być nieakceptowalne dla interesariuszy. W przypadku organizacji rządowych jest to szczególnie ważne, jeśli chodzi o relacje z ogółem społeczeństwa (zob. 7.5); działania, które byłyby skuteczne wobec określonego ryzyka, mogą wywoływać inne skutki, których ogół społeczeństwa nie zgadza się zaakceptować.

A PRZYKŁAD DOKUMENTOWANIA OCENY RYZYKA

CEL – Dojechać z A do B punktualnie na ważne spotkanie								
	Ocena ryzyka nieodłącznego		ISTNIEJĄCE PUNKTY KONTROLNE	Ocena ryzyka rezydualnego		PLANOWANE DZIAŁANIA	DOCELOWA DATA	WŁAŚCI-CIEL
RYZYKO	Oddzia-ływanie	Prawdopo-dobieństwo		Oddzia-ływanie	Prawdopo-dobieństwo			
Jeśli nie zdążę na pociąg, to spóźnię się na ważne spotkanie	Wysokie	Wysokie	Dojazd pociągiem wcześniejszym niż to konieczne	Wysokie	Niskie	Dalsze działania nie są planowane		Osobiście
Zła pogoda uniemożliwi odjazd pociągu	Wysokie	Niskie	Poza kontrolą	Wysokie	Niskie	Zapewnienie odpowiedniego zaplecza do konferencji telefonicznych w sytuacjach awaryjnych	Sierpień	Inni
Prace konstrukcyjne spowodują opóźnienie pociągu	Wysokie	Średnie	Sprawdzić, czy prowadzone są prace konstrukcyjne i uzgodnić ewentualne przesunięcie godziny spotkania z uczestniczącymi w nim osobami	Średnie	Niskie	Dalsze działania nie są planowane		Osobiście

B OGÓLNA PEWNOŚĆ W ZARZĄDZANIU RYZYKIEM

ZASADY UZYSKIWANIA PEWNOŚCI

1. Planowanie w celu uzyskania pewności

1.1 Strategia uzyskiwania pewności – ogólna pewność zostanie osiągnięta tylko wtedy, gdy opracowany zostanie strategiczny plan uzyskiwania pewności;

1.2 Proces uzyskiwania pewności – procesy uzyskiwania pewności powinny zostać osadzone w istniejących już procesach.

2. Wyraźne oznaczenie granic i zakresu pewności

Aby sformułować ogólną opinię, zakres procesów wymaganych do uzyskania pewności musi obejmować cały cykl życia zarządzania ryzykiem przez organizację. Nie oznacza to, że aby uzyskać pewność należy poddać przeglądowi każde ryzyko i każdy punkt kontrolny. Niemniej przegląd, który jest faktycznie przeprowadzany, musi określić:

2.1 pewność związaną ze strategią zarządzania ryzykiem – ustalić zakres, w jakim wszyscy kierownicy liniowi dokonują przeglądu ryzyka/punktów kontrolnych w granicach swojej odpowiedzialności;

2.2 pewność związaną z zarządzaniem ryzykiem/punktami kontrolnymi – obejmować wszystkie kluczowe ryzyka oraz dostateczną ilość innych ryzyk do uzyskania odpowiedniego poziomu ufności odnoszącego się do formułowanej ogólnej opinii;

2.3 pewność związaną z adekwatnością przeglądu/procesu uzyskiwania pewności – zapewniać jakość, która skutkuje wysokim poziomem ufności w procesie przeglądu.

3. Dowody

Dowody gromadzone na poparcie pewności powinny być wystarczające pod względem swojego zakresu (zob. 2.1 powyżej) oraz znaczenia (zob. 4.2 poniżej), aby potwierdzać wniosek i zostać uznanymi za:

- stosowne,
- wiarygodne,
- zrozumiałe,
- wolne od istotnych błędów,
- neutralne/bezstronne,
- takie, że inna osoba racjonalnie doszłaby do tego samego wniosku.

4. Ocena

4.1 Celem jest:

- ocena adekwatności polityki i strategii zarządzania ryzykiem w celu osiągnięcia ich celów;

- ocena adekwatności procesów zarządzania ryzykiem zaprojektowanych tak, by ograniczać ryzyko rezydualne do apetytu na ryzyko;

- identyfikacja ograniczeń w przedstawionych dowodach lub w głębi lub zakresie przeprowadzanych przeglądów;

- identyfikacja luk w kontroli i/lub nadmiernej kontroli, jak również zapewnianie możliwości ciągłego rozwoju; oraz

- wspieranie przygotowania SIC.

4.2 Aby podczas oceny dowodów sformułować ogólny osąd lub opinię, należy uwzględnić wszystkie kryteria odpowiedniości dowodów wymienione w punkcie 3. Niemniej należy pamiętać, że:

- nie wszystkie dowody mają takie samo znaczenie w uzyskiwaniu pewności. Dowody powinny być oceniane:

  - pod względem swojej niezależności – im bardziej dowód jest bezstronny, tym bardziej jest wiarygodny. Jednak wystąpienie niektórych okoliczności mogłoby wpłynąć na wiarygodność pozyskanych informacji, np. aby niezależne dowody zewnętrzne mogły zostać uznane za wiarygodne, musi być znane również ich źródło;

  - pod względem swojej stosowności – określenie ogólnej pewności wymaga zapewnienia, że dowody dotyczą tych elementów cyklu życia zarządzania ryzykiem, które są istotne. Dowody odnoszące się do poważniejszego ryzyka są w konsekwencji bardziej odpowiednie dla uzyskania ogólnej pewności.

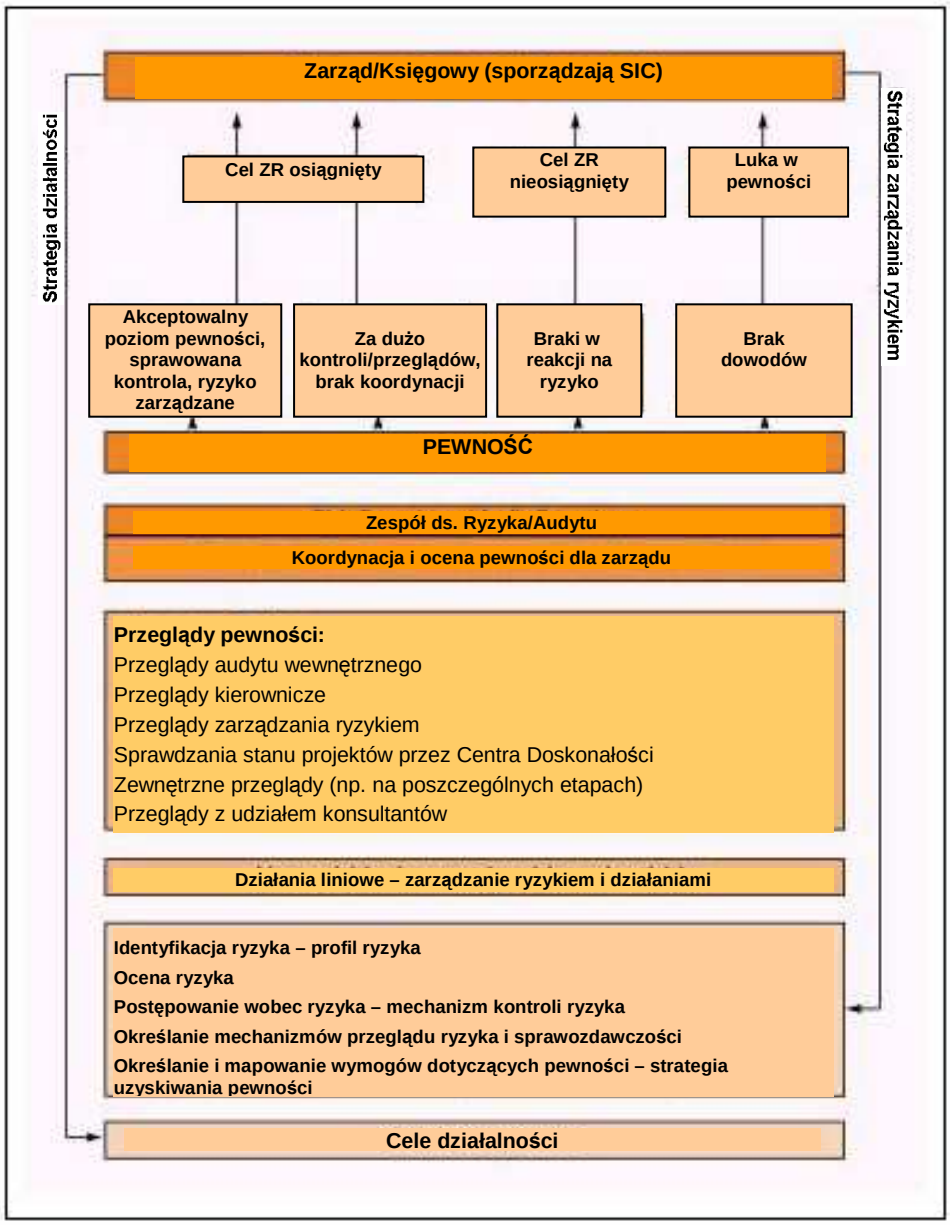
  - Dowody mogą być wadliwe pod względem zarówno ilości, jak i jakości, jeśli nie zostały spełnione kryteria odpowiedniości dowodów, a to z kolei może stanowić przeszkodę w uzyskiwaniu pewności. Na przykład mnogość dowodów nie równoważy ich niskiej jakości ani ich niewiarygodnego źródła.

5. Przeglądy i sprawozdawczość

5.1 Sprawozdania dotyczące pewności pochodzą z wielu różnych źródeł w organizacji: ze źródeł zewnętrznych, od dostawców i kontrahentów, od osób trzecich, z wewnętrznych przeglądów prowadzonych przez kierownictwo i fachowców oraz z niezależnych lub neutralnych źródeł wewnętrznych itp. Strategia uzyskiwania pewności powinna definiować etapy, na których pewność jest poddawana ocenie i przedstawiane są zarządowi sprawozdania z opiniami formułowanymi przez różne poziomy kierownictwa.

5.2 Opinie dotyczące pewności należy dokładnie przedstawiać w sprawozdaniach i tak formułować, aby wyraźnie komunikować zakres i kryteria stosowane podczas dochodzenia do takich wniosków.

OGÓLNA PEWNOŚĆ W ZARZĄDZANIU RYZYKIEM B



C WYKAZ ASPEKTÓW MONITOROWANIA WIDNOKRĘGU

Udostępniony przez Civil Contingencies Secretariat przy Cabinet Office

- **Okresowość/regularność:** monitorowanie widnokręgu może być ciągłe (w organizacji takiej jak Civil Contingencies Secretariat (CCS), nieustannie poszukującej potencjalnych wyzwań, które okażą się destrukcyjne w przyszłości) lub okresowe (np. prowadzone w odstępach tygodniowych lub rocznych)**;**

- **Skala czasowa:** decydenci mogą równie dobrze być zainteresowani rozwojem wydarzeń na przestrzeni kolejnych dwudziestu pięciu lat, natomiast monitorowanie widnokręgu, które wspiera proces decyzyjny na poziomie operacyjnym, może być ograniczone do sześciu miesięcy**;**

- **Zakres:** niektóre organizacje mogą postępować dość zachowawczo w swoich procesach identyfikacji ryzyka, jeśli dostrzegają, że główny element ryzyka pochodzi z wewnątrz organizacji; dla innych konieczne może okazać się uwzględnienie o wiele szerszego zakresu, jeśli uznają, że mogą stanąć wobec ryzyka, którego źródłem jest szersze środowisko. W zależności od charakteru działalności organizacji, ten element identyfikacji ryzyka może rozciągać się od niemal wyłącznie działalności wewnętrznej do działalności opartej na międzynarodowych sieciach informacji technicznej;

- **Szanse/zagrożenia:** czasami monitorowanie widnokręgu polega głównie na wyszukiwaniu potencjalnych problemów, ale może być również z powodzeniem wykorzystywane do monitorowania szans („ryzyko pozytywne"), bo przecież wiele problemów można przekształcić w możliwości, jeśli problemy te zostaną odpowiednio wcześnie dostrzeżone**;**

- **Rygor/strona techniczna:** monitorowanie widnokręgu zmienia się w zakresie, w jakim jest ustrukturyzowane i wspierane przez technologię. Niektóre organizacje stosują skomplikowane systemy oceny i technologie wyszukiwania informacji; z kolei inne organizacje będą polegać prawie wyłącznie na nieformalnych sieciach kontaktów i dobrym osądzie.

[Więcej informacji zob. www.ukresilience.info/home.htm]

D GLOSARIUSZ KLUCZOWYCH TERMINÓW

Pewność	Oceniona opinia, oparta na dowodach pozyskanych w czasie przeglądu, na temat nadzoru, zarządzania ryzykiem i systemu kontroli wewnętrznej w danej organizacji.
Zespół ds. Audytu	Zespół utworzony w celu wspierania księgowego (ang. *Accounting Officer*) (w pozaministerialnych instytucjach publicznych zespół zarządu powołany w celu wspierania zarządu) w zakresie monitorowania nadzoru korporacyjnego i systemów kontroli w organizacji.
Narażenie	Konsekwencje będące kombinacją oddziaływania i prawdopodobieństwa, których organizacja może doświadczyć, jeśli wystąpi określone ryzyko.
Monitorowanie widnokręgu	Systematyczne działanie mające na celu możliwie najwcześniejszą identyfikację wskaźników zapowiadających zmiany ryzyka.
Ryzyko nieodłączne	Narażenie spowodowane określonym ryzykiem przed podjęciem jakiegokolwiek działania w celu zarządzania nim.
Ryzyko rezydualne	Narażenie spowodowane określonym ryzykiem po podjęciu działania w celu zarządzania nim i przyjęciu założenia, że działanie to jest skuteczne.
Ryzyko	Niepewność wyniku działań lub zdarzeń, zarówno w przypadku pozytywnych szans, jak i negatywnych zagrożeń. Jest to kombinacja prawdopodobieństwa i oddziaływania, przy uwzględnieniu postrzeganego znaczenia.
Apetyt na ryzyko	Wielkość ryzyka, jaką organizacja gotowa jest w dowolnym czasie zaakceptować, dopuścić lub być na nią narażona.
Ocena ryzyka	Ewaluacja ryzyka w odniesieniu do jego oddziaływania, jeśli ryzyko wystąpi, oraz prawdopodobieństwa wystąpienia tegoż ryzyka.
Zespół ds. Pewności wobec Ryzyka	Zespół utworzony w celu wykonywania roli, którą w przeciwnym razie wykonywałby Zespół ds. Audytu, związanej z uzyskiwaniem pewności w zarządzaniu ryzykiem.
Zarządzanie ryzykiem	Wszystkie procesy wykorzystywane do identyfikacji, oceny i osądu ryzyka, przypisywania własności, podejmowania działań w celu zmniejszenia lub przewidzenia ryzyka oraz monitorowania i przeglądu osiąganych postępów.

Zespół ds. Zarządzania Ryzykiem	Zespół ustanowiony w celu podejmowania działań w zakresie zarządzania ryzykiem stojącym przed organizacją i wyposażony w odpowiednie uprawnienia wykonawcze.
Strategia ryzyka	Ogólne podejście organizacyjne do zarządzania ryzykiem określone przez księgowego i/lub zarząd. Strategia taka powinna być udokumentowana i łatwo dostępna dla wszystkich w organizacji.
Profil ryzyka	Podlegająca udokumentowaniu i hierarchizacji ogólna ocena zakresu określonego ryzyka stojącego przed organizacją.
System kontroli wewnętrznej	Każde działanie pochodzące z wewnątrz organizacji i podejmowane w celu zarządzania ryzykiem. Działania takie mogą być podejmowane w celu zarządzania albo oddziaływaniem ryzyka, jeśli ryzyko wystąpi, albo częstością występowania ryzyka.


ISBN 1-84532-044-1-1
9 781845 320447