BANK I KREDYT *kwiecień 2004*

Ryzyko operacyjne w bankach - zarządzanie i audyt w świetle wymagań Bazylejskiego Komitetu ds. Nadzoru Bankowego

Dariusz Lewandowski

Wprowadzenie

Procesy towarzyszące deregulacji oraz globalizacji usług finansowych wraz ze wzrostem złożoności technologii informatycznych wykorzystywanych przez instytucje powodują, że działalność, a tym samym profil ryzyka instytucji stają się coraz bardziej złożone. Doświadczenia pokazują, iż konsekwencje innych rodzajów ryzyk niż kredytowe, płynności czy rynkowe dla wielu instytucji finansowych były dość poważne. Do zagadnień, które wymuszają pilną konieczność zajęcia się problematyką ryzyka operacyjnego można zaliczyć:

– coraz większe wykorzystanie zaawansowanych technologii informatycznych oraz systemów zintegrowanych w skali globalnej, wymagające wnikliwej i ciągłej kontroli ze względu na zagrożenia wystąpieniem ryzyka systemowego;

– wzrost roli i skali handlu elektronicznego (*e-commerce*) wymuszający obowiązek tworzenia zabezpieczeń przed nadużyciami o charakterze wewnętrznym oraz zewnętrznym;

– zjawiska o charakterze konsolidacyjnym, przejęcia, fuzje, wymagające dostosowania bądź stworzenia nowych zintegrowanych systemów;

– funkcjonowanie wysokokwotowych rozliczeń pomiędzy instytucjami, wysokie wartościowo transfery kwot pieniężnych, wymuszające konieczność stosowania specjalistycznych technik kontrolnych oraz tworzenie systemów zapasowych;

– konieczność wykorzystania przez banki techniki zabezpieczania przed ryzykiem (np. zabezpieczenia prawne, pochodne kredytowe, netting, sekurytyzacja aktywów) w celu optymalizacji ekspozycji na ryzyko rynkowe czy kredytowe; stosowane techniki i instrumenty otwierają z kolei ekspozycję na ryzyko, np. prawne;

– wzrasta rola *outsourcingu* oraz uczestnictwo banków w systemach rozliczeń, mogące ograniczyć ryzyko, ale także stanowiące nowe zagrożenia.

Ten szeroki zestaw czynników ryzyka z różnorodnych obszarów tematycznych został połączony i nazwany ryzykiem operacyjnym.

Definicja ryzyka operacyjnego. Obszary ryzyka operacyjnego

Definicja ryzyka operacyjnego została przedstawiona w dokumencie konsultacyjnym *Nowa Bazylejska Umowa Kapitałowa,* opracowanym w styczniu 2001 r. przez Bazylejski Komitet ds. Nadzoru Bankowego[1].

[1] W kwietniu 2003 r. Komitet Bazylejski opublikował kolejną wersję *Nowej Bazylejskiej Umowy Kapitałowej*, tzw. Trzeci Dokument Konsultacyjny. Nową Umowę Kapitałową będzie trzeba stosować w ujęciu skonsolidowanym do banków prowadzących działalność międzynarodową. Zakres stosowania w ujęciu w pełni skonsolidowanym obejmie również spółki holdingowe, będące podmiotami macierzystymi grup bankowych. Szerzej patrz: *The New Basel Capital Accord. Consultative document.* Basel Committee on Banking Supervision. April 2003.

Ryzyko operacyjne definiuje się jako „ryzyko straty wynikającej z niewłaściwych lub zawodnych procesów, ludzi i systemów lub ze zdarzeń zewnętrznych". Definicja ta obejmuje także ryzyko prawne. Ryzyko strategiczne i ryzyko reputacji nie są włączone do definicji ryzyka operacyjnego do celów minimalnego regulacyjnego wymogu kapitałowego z tytułu ryzyka operacyjnego[2]. Komitet w dalszym ciągu współpracuje z międzynarodowym środowiskiem bankowym nad tym zagadnieniem.

Szeroki charakter definicji będzie na pewno źródłem wielu wyzwań i ostateczny kształt definicji będzie zależał od specyfiki działalności danej firmy. Podstawowe znaczenie ma jednak zdefiniowanie w każdej instytucji ryzyka operacyjnego na jej własne potrzeby, jasne rozumienie przez personel całej instytucji, co się rozumie pod pojęciem ryzyka operacyjnego, zdefiniowanie czynników ryzyka. Takie podejście umożliwi efektywne zarządzania ryzykiem.

Do rodzajów ryzyka operacyjnego, które mogą wywoływać znaczne straty materialne można zaliczyć:

– **nadużycia wewnętrzne**: kradzież przez pracowników, fałszowanie sprawozdawczości wewnętrznej, transakcje wewnętrzne na szkodę instytucji,

– **nadużycia zewnętrzne**: napady, kradzieże, włamania fizyczne, włamania komputerowe, oscylator finansowy,

– **zasady zatrudniania oraz bezpieczeństwo w miejscu pracy**: roszczenia pracownicze dotyczące wynagrodzeń, warunki pracy zagrażające zdrowiu i bezpieczeństwu pracowników, dyskryminację pracowników itd.,

– **klientów, produkty oraz praktyki biznesowe:** wykorzystanie poufnych informacji o klientach, pranie pieniędzy, przeprowadzanie niedozwolonych transakcji na rachunkach bankowych, sprzedaż nieautoryzowanych produktów,

– **zniszczenie aktywów:** akty wandalizmu, terroryzmu, działania siły wyższej,

– **brak ciągłości pracy instytucji, przerwanie pracy systemów, załamanie pracy systemów:** problemy ze sprzętem, z oprogramowaniem, problemy telekomunikacyjne,

– **zarządzanie w instytucji, zarządzanie procesami:** błędy przy wprowadzaniu danych, niekompletną dokumentację prawną, nieautoryzowany dostęp do danych o klientach, reklamacje, zastrzeżenia dostawców, sprzedawców itd.

[2] Należy zwrócić uwagę, że w taki sposób zdefiniowano ryzyko operacyjne na potrzeby wyliczania przez banki minimalnych wymogów kapitałowych. Zakres definicji sformułowanej na inne potrzeby, a tym samym dla innych instytucji może się różnić.

Konieczność nowego podejścia do zarządzania ryzykiem operacyjnym

Zarządzanie pewnymi obszarami ryzyka operacyjnego w instytucjach nie jest zagadnieniem nowym. W szczególności instytucje finansowe zawsze były zainteresowane zabezpieczeniem się przed nadużyciami, przestępstwami zewnętrznymi i wewnętrznymi, redukcją błędów operacyjnych, integralnością systemów kontrolnych. Nowością w tym zakresie jest jednak zwrócenie uwagi na ważność problematyki ryzyka operacyjnego oraz wypracowanie nowoczesnych zasad całościowego procesu zarządzania ryzykiem operacyjnym, zbliżonych do zasad, technik i praktyk stosowanych w odniesieniu do ryzyka kredytowego oraz rynkowego. Wiedza i dorobek z ostatnich lat w zakresie zarządzania innymi rodzajami ryzyka powinny być wykorzystywane w celu usprawnienia zarządzania ryzykiem operacyjnym. W przeszłości banki zarządzając ryzykiem operacyjnym korzystały głównie z mechanizmów kontroli wewnętrznej stosowanych przez poszczególne komórki organizacyjne, wspomaganych przez audyt wewnętrzny. Takie podejście jest dalej ważne, ale obecnie może okazać się niewystarczające. W pewnych organizacjach pojawia się konieczność wyodrębnienia specjalnych funkcji oraz wypracowania procesowego, usystematyzowanego podejścia do zarządzania tym rodzajem ryzyka.

Konieczność nowego czy specjalnego podejścia wynika także z innych czynników, decydujących o specyfice ryzyka operacyjnego. Specyfika ta polega na tym, że :

– ryzyka operacyjnego nie podejmuje się w celu osiągnięcia określonych korzyści biznesowych; towarzyszy ono prowadzeniu działalności, jest w nią wbudowane,

– całkowita eliminacja źródeł ryzyka nie jest możliwa,

– analiza czynników ryzyka i konsekwencji oraz jego skutków nie jest prosta,

– pomiar ryzyka również nie jest zadaniem łatwym,

– trudno ustalić właścicieli ryzyka,

– ryzyko to ma wyjątkowo heterogeniczny charakter.

Na całościowej mapie wszystkich rodzajów ryzyka instytucji nie może zabraknąć ryzyka operacyjnego oraz zastosowania odpowiednich technik zarządzania.

Najlepsze praktyki dotyczące zarządzania i nadzoru nad ryzykiem operacyjnym - wytyczne Bazylejskiego Komitetu ds. Nadzoru Bankowego

Bazylejski Komitet ds. Nadzoru Bankowego opracował i opublikował w styczniu 2003 r. dokument zatytułowany *Najlepsze praktyki dotyczące zarządzania i nadzoru nad ryzykiem operacyjnym*. Określono w nim zasady dotyczące sposobu efektywnego zarządzania ryzykiem operacyjnym i nadzoru nad nim. Zasady

te powinny być wykorzystywane przez banki oraz władze nadzorcze podczas oceny adekwatności zasad i procedur zarządzania ryzykiem operacyjnym[3]. Przyjrzyjmy się tym zasadom. Zostały one opracowane i przeznaczone dla określonej grupy podmiotów, jednak zdaniem autora mogą i powinny być stosowane również przez podmioty z innych branż. Ryzyko operacyjne jest bowiem tym rodzajem ryzyka, które w odróżnieniu np. od ryzyka czysto finansowego towarzyszy wszystkim podmiotom prowadzącym działalność.

Tworzenie adekwatnego środowiska zarządzania ryzykiem

Ryzyko operacyjne jest wbudowane we wszystkie transakcje i czynności bankowe. Niezrozumienie i brak czy niewłaściwe zarządzanie nim, mogą doprowadzić do zwiększenia prawdopodobieństwa braku należytej kontroli lub braku całkowitej identyfikacji pewnych czynników ryzyka. Rada nadzorcza i zarząd odpowiadają za stworzenie właściwej kultury organizacyjnej, w ramach której problematyka efektywnego zarządzania ryzykiem operacyjnym ma priorytetowe znaczenie. Odpowiadają również za zapewnienie odpowiednich mechanizmów kontrolnych. Określenie i wprowadzenie wysokich standardów etycznego postępowania personelu całej instytucji przyczyniają się do zwiększenia efektywności zarządzania ryzykiem operacyjnym. Również rada i zarząd poprzez działania i słowa powinny promować kulturę organizacyjną.

ZASADA 1. Rada Nadzorcza powinna być świadoma najważniejszych aspektów ryzyka operacyjnego banku traktowanego jako odrębna kategoria ryzyka, którym bank powinien zarządzać. Rada powinna zatwierdzić strategię zarządzania ryzykiem operacyjnym oraz dokonywać jej okresowego przeglądu. Strategia powinna definiować, co bank rozumie przez ryzyko operacyjne, oraz powinna zawierać zasady identyfikacji, oceny, monitorowania oraz kontroli i ograniczania ryzyka.

Rada powinna - akcentując odrębność i ważność tej kategorii - wyraźnie zdefiniować swoje oczekiwania w zakresie strategii zarządzania ryzykiem operacyjnym. Powinna wskazać pożądane kierunki działań oraz zatwierdzić stworzone przez zarząd stosowne procedury i zasady polityki.

Strategia i zasady polityki powinny być oparte na właściwym zdefiniowaniu, na potrzeby instytucji, ryzyka operacyjnego. Należy się także odnieść do poziomu tolerancji i tzw. apetytu na ryzyko. Procedury zarządzania powinny wynikać z przyjętego poziomu tolerancji ryzyka. W strategii należy także wskazać priorytetowe czynności z zakresu zarządzania ryzykiem oraz zakres i sposób ewentualnego transferu ryzyka poza bank. W strategii muszą znaleźć się zapisy wskazujące na podejście banku do identyfikacji, oceny, monitorowania oraz kontroli i ograniczania ryzyka. Zarówno zakres, jak i stopień szczegółowości zapisów strategii powinny być dostosowane do profilu ryzyka instytucji.

Rada jest odpowiedzialna za utworzenie właściwej struktury zarządzania i organizacji zapewniającej realizację strategii. Ponieważ ważnym aspektem zarządzania ryzykiem jest stworzenie silnych mechanizmów i procedur kontroli wewnętrznej, istotne jest ustanowienie przez radę czytelnego zakresu odpowiedzialności, podporządkowania, podległości oraz raportowania. Dodatkowo, w celu uniknięcia konfliktu interesów, powinna być wprowadzona zasada rozdzielenia odpowiedzialności oraz raportowania. W strategii powinny być zarysowane również główne procesy, które instytucja musi wypracować w celu skutecznego zarządzania ryzykiem.

Rada powinna dokonywać regularnego przeglądu strategii pod kątem jej aktualności oraz zapewnienia, by bank właściwie zarządzał ryzykiem i uwzględniał wszystkie czynniki ryzyka, wynikające z zewnętrznych zmian rynkowych, innych czynników środowiskowych oraz towarzyszące nowym produktom, usługom, czynnościom czy systemom. W przeglądzie należy brać pod uwagę doświadczenia oraz najlepsze praktyki bankowe w tym zakresie.

ZASADA 2. Rada nadzorcza powinna zapewnić, by strategia zarządzania ryzykiem operacyjnym była przedmiotem oceny dokonywanej przez efektywny i kompleksowy audyt wewnętrzny. Audyt wewnętrzny jako niezależna funkcja nie powinien być bezpośrednio odpowiedzialny za zarządzanie ryzykiem operacyjnym.

Banki powinny mieć sprawnie funkcjonujący audyt wewnętrzny[4], który weryfikuje, czy zasady polityki i procedury operacyjne są wprowadzane i przestrzegane. Rada (bezpośrednio lub pośrednio za pośrednictwem Komitetu Audytu) powinna zadbać aby program audytu był adekwatny do profilu ryzyka w banku. Audyt powinien okresowo weryfikować i wydawać opinię na temat poprawności wdrażania wszystkich zapisów

[3] Rekomendacje opracowywane przez Komitet Bazylejski stanowią zbiór najlepszych praktyk w zakresie zarządzania poszczególnymi rodzajami ryzyka bankowego. Kierowane są do różnych banków (wielkości, charakteru działalności itp.) funkcjonujących w różnych jurysdykcjach prawnych. Tym samym nie mają one mocy obowiązującej lecz pełnią funkcję pewnych ogólnych wytycznych. Ich uniwersalny charakter oraz wysoka jakość merytoryczna sprawiają, że regulatorzy i nadzorcy bankowi w poszczególnych krajach chętnie włączają je do wytycznych dla banków.

[4] Definicja audytu wewnętrznego zatwierdzona w czerwcu 1999 r. przez Zarząd Instytutu Audytorów Wewnętrznych (The IIA' Board of Directors) brzmi następująco:
„Audyt wewnętrzny jest działalnością niezależną, obiektywnie zapewniającą i doradczą, której celem jest przysparzanie wartości i usprawnienie działalności operacyjnej organizacji. Pomaga on organizacji w osiąganiu jej celów poprzez systematyczne i zdyscyplinowane podejścia do oceny i doskonalenia skuteczności procesów zarządzania ryzykiem, kontroli i governance."

strategii zarządzania ryzykiem operacyjnym we wszystkich pionach operacyjnych banku.

Rada powinna zadbać, aby audyt wewnętrzny mimo szerokiego zaangażowania w ocenę poprawności realzacji strategii zarządzania ryzykiem operacyjnym zachowywał swoją niezależność. Niezależność będzie zagrożona, jeżeli audyt będzie bezpośrednio zaangażowany w zarządzanie ryzykiem operacyjnym. Audyt może dostarczyć dużego wsparcia osobom zarządzającym i odpowiedzialnym za ten obszar ryzyka, jednakże nie może ponosić jakiejkolwiek bezpośredniej odpowiedzialności w zarządzaniu ryzykiem[5]. Komitet Bazylejski zdaje sobie sprawę, że ze względów praktycznych audyt w pewnych - szczególnie mniejszych - bankach może na początkowym etapie uczestniczyć w opracowaniu programu zarządzania ryzykiem operacyjnym. Jednak po wprowadzeniu programu odpowiedzialność za codzienne zarządzanie musi być przypisana właściwym pionom operacyjnym.

ZASADA 3. Zarząd powinien być odpowiedzialny za realizację strategii zarządzania ryzykiem operacyjnym zatwierdzonej przez radą nadzorczą. Strategia powinna być konsekwentnie, spójnie i kompleksowo wdrażana w całym banku. Na wszystkich poziomach organizacyjnych pracownicy powinni rozumieć swoją rolę i odpowiadać za zarządzanie ryzykiem operacyjnym. Zarząd powinien odpowiadać również za opracowanie zasad polityki, procedur oraz procesów zarządzania ryzykiem operacyjnym dotyczących wszystkich produktów, obszarów działalności, procesów i systemów o materialnej istotności.

Zarząd powinien przełożyć strategię zarządzania ryzykiem operacyjnym stworzoną przez radę na konkretne zasady polityki, procesy oraz procedury operacyjne, które będą wprowadzane i weryfikowane we wszystkich pionach operacyjnych. Kierownictwo poszczególnych pionów operacyjnych odpowiada za adekwatność zasad, procedur oraz jakość kontroli w swoich jednostkach. Zarząd powinien jasno określić wymagania co do podległości, odpowiedzialności oraz trybu raportowania, jak również zadbać o istnienie w banku właściwych zasobów umożliwiających efektywne zarządzanie ryzykiem. Dodatkowo, Zarząd powinien oceniać adekwatność i skuteczność zarządzania przez kierownictwo pionów operacyjnych ryzykiem wbudowanym niejako w działania tych pionów.

Zarząd powinien zapewnić, aby poszczególne czynności bankowe były wykonywane przez wykwalifikowany personel mający odpowiednie doświadczenie, umiejętności techniczne i dostęp do technologii i zasobów. Zarząd powinien też zadbać, aby personel odpowiedzialny za monitorowanie i badanie zgodności postępowania z polityką instytucji dotyczącą zarządzania ryzykiem nie podlegał nadzorowanym pionom operacyjnym. Zarząd powinien zadbać aby zasady polityki zarządzania ryzykiem operacyjnym i wszelkie wymagania w tym zakresie były jasno komunikowane personelowi wszystkich tych pionów, których dotyczy ryzyko operacyjne.

Zarząd powinien zapewnić istnienie właściwych zasad komunikacji pomiędzy personelem odpowiedzialnym za zarządzanie ryzykiem operacyjnym i innymi rodzajami ryzyka a tymi pionami w instytucji, które odpowiadają za nabywanie usług na zewnątrz, np. zakup polis ubezpieczeniowych, czy wszelkie inne umowy *outsourcingowe*. Współpraca jest niezbędna w celu uniknięcia luk lub nakładania się pewnych zadań w całościowym programie zarządzania ryzykiem w instytucji.

Zarząd powinien prowadzić politykę w zakresie wynagrodzeń spójną z apetytem banku na ryzyko. Zasady wynagradzania, które premiują jakiekolwiek odstępstwa od zasad polityki i procedur obowiązujących w instytucji (np. przekraczanie ustanowionych limitów), negatywnie wpływają na zarządzanie ryzykiem w banku.

Należy zwrócić szczególną uwagę na jakość dokumentowania kontroli oraz praktyki w zakresie przeprowadzania transakcji. Zasady polityki, procesy i procedury odnoszące się do wykorzystywania zaawansowanych technologii, np. do obsługi transakcji wysokokwotowych, powinny być należycie dokumentowane i przydzielane właściwemu personelowi.

Zarządzanie ryzykiem: identyfikacja, ocena, monitoring oraz ograniczanie i kontrola

ZASADA 4. Banki powinny identyfikować i oceniać ryzyko operacyjne wbudowane we wszystkie produkty, czynności, procesy i systemy o materialnej istotności. Banki powinny również zapewnić, by przed podjęciem lub wprowadzeniem nowych produktów, czynności, procesów czy systemów towarzyszące im ryzyko operacyjne było przedmiotem wnikliwej analizy. W tej materii powinny istnieć stosowne procedury.

Właściwa identyfikacja ryzyka jest podstawą prawidłowego wypracowania zasad monitorowania i kontroli. Efektywna identyfikacja ryzyka wymaga rozważenia czynników wewnętrznych (struktura banku, rodzaje usług, produktów bankowych oraz czynności, jakość personelu, zmiany organizacyjne i kadrowe) oraz czynników zewnętrznych (zmiany w branży, nowe technologie), które mogą negatywnie wpływać na osiąganie celów banku.

[5] Audyt wewnętrzny jest elementem składowym procesu monitorowania systemu kontroli wewnętrznej w banku oraz wewnętrznych procedur w zakresie oceny adekwatności kapitałowej. Audyt dostarcza bowiem niezależnej oceny w zakresie adekwatności oraz zgodności z obowiązującymi przepisami. W tym sensie funkcja audytu wewnętrznego wspomaga odpowiedzialny za zarządzanie instytucją zarząd oraz radę w skutecznym podziale odpowiedzialności.

Oprócz samej identyfikacji czynników ryzyka należy szacować podatność banku na te zagrożenia. Efektywna ocena ryzyka umożliwia właściwe określenie profilu ryzyka oraz skierowanie posiadanych zasobów na obszary zagrożeń.

Spośród dostępnych narzędzi i technik identyfikacji i oceny ryzyka na uwagę zasługują:

• **Samoocena oraz samoocena w zakresie ryzyka** - ocena podatności operacji, czynności bankowych na czynniki ryzyka operacyjnego wraz z oceną zagrożeń. Jest to proces wewnętrzny w instytucji. Można go realizować poprzez system ankiet czy wewnętrznych seminariów bądź warsztatów, służących identyfikacji silnych i słabych stron w procesach.

• **Mapowanie ryzyka** - poszczególne jednostki operacyjne, funkcje organizacyjne czy procesy są nakładane na mapy ryzyka. Pomaga to identyfikować zagrożenia, słabości oraz określać priorytety działań zarządczych.

• **Wskaźniki ryzyka** - to dane statystyczne, liczbowe, finansowe odnoszące się do określonych rodzajów ryzyka. Wskaźniki muszą być wyliczane oraz cyklicznie analizowane. Mogą obejmować np. liczbę niezrealizowanych kontraktów, płatności, rotację personelu, liczbę błędów, nieprawidłowości.

• **Pomiar ryzyka operacyjnego** - pewne firmy rozpoczęły pomiar narażenia na ryzyko operacyjne stosując różne techniki. Tworzą bazy danych nt. strat historycznych. Bazy te mogą dostarczyć informacji przydatnych do usprawnienia zarządzania ryzykiem i jego kontroli w przyszłości. Dane te muszą być systematycznie rejestrowane. Powinny być opisywane wszystkie szczegóły. Cenne są też porównania z innymi instytucjami, bazami danych zewnętrznych, analizami scenariuszy.

ZASADA 5. Banki powinny regularnie monitorować profil ryzyka operacyjnego i stopień narażenia na straty o materialnej istotności. Powinien być także stworzony system regularnego raportowania zarządowi o zagrożeniach. System raportowania powinien wspierać zarządzanie ryzykiem operacyjnym.

• **Efektywny monitoring** jest ważnym elementem w zarządzaniu ryzykiem. Pozwala na szybką identyfikację słabości oraz umożliwia wprowadzenie - skutecznie i we właściwym czasie - zmian zasad polityki, procedur oraz podjęcie działań naprawczych. Dzięki temu pozwala ograniczyć częstotliwość i głębokość potencjalnych strat. Monitoring powinien obejmować analizę zdarzeń, w wyniku których doszło do strat operacyjnych oraz analizę wskaźników i sygnałów ostrzegawczych informujących o zagrożeniach wystąpieniem strat w przyszłości. Wskaźniki te powinny pomagać w prognozowaniu zagrożeń i opierać się na źródłach ryzyka operacyjnego, takich jak gwałtowny wzrost liczby operacji, wprowadzanie nowych produktów, rotacja personelu, zatrzymanie pracy systemów.

• **Częstotliwość monitoringu** powinna zależeć od ryzyka oraz charakteru i częstotliwości zmian w środowisku operacyjnym. Monitoring powinien być naturalną częścią czynności bankowych. Jego wyniki powinny być prezentowane w raportach dla zarządu i rady, wraz z przeglądami zgodności przeprowadzanymi przez audyt wewnętrzny lub pion zarządzania ryzykiem.

• **Regularne raporty dla zarządu na temat ryzyka operacyjnego powinny charakteryzować się następującymi cechami:**

– powinny być opracowywane przez właściwe piony operacyjne, departamenty, biuro ds. zarządzania ryzyka operacyjnego, audyt wewnętrzny;

– powinny zawierać wewnętrzne dane finansowe, dane operacyjne, dane weryfikujące zgodność oraz zewnętrzne dane rynkowe o wydarzeniach czy uwarunkowaniach wpływających na procesy decyzyjne;

– powinny być odpowiednio dystrybuowane do wszystkich kierujących pionami operacyjnymi, których dotyczą opisywane zagadnienia;

– powinny prezentować wszystkie obszary, na których występują problemy oraz wskazywać na konieczność natychmiastowych działań zaradczych.

Kierownictwo pionów operacyjnych w celu zapewnienia użyteczności i wiarygodności raportów powinno regularnie weryfikować terminowość, kompletność oraz adekwatność systemu raportowania oraz systemu kontroli wewnętrznej.

Właściwie funkcjonujący system raportowania powinien zapewnić otrzymywanie przez radę wystarczających zagregowanych informacji, umożliwiających zrozumienie całościowego profilu ryzyka operacyjnego instytucji i skoncentrowanie się na istotnych i strategicznych skutkach dla działalności.

ZASADA 6. Banki powinny wypracować zasady polityki, procedury i procesy w zakresie kontroli i ograniczania najbardziej istotnych rodzajów ryzyka operacyjnego. Powinny dokonywać regularnego przeglądu systemu limitów ryzyka oraz własnych strategii kontrolnych. Powinny także wykorzystywać właściwe strategie, by dostosowywać bieżący profil ryzyka operacyjnego do całkowitego profilu i skłonności do podejmowania ryzyka przez instytucję.

Czynności i mechanizmy kontrolne powinny być nakierowane na ryzyko operacyjne zidentyfikowane przez bank. W przypadku wszystkich zidentyfikowanych rodzajów ryzyka operacyjnego o materialnym znaczeniu należy zdecydować, czy zastosować określone procedury kontroli i (lub) ograniczania ryzyka, czy procedury stosowane, gdy bank świadomie decyduje się na ponoszenie ryzyka. Dla ryzyka, które nie może

być kontrolowane, bank powinien zdecydować, czy akceptuje je, ogranicza poziom działalności na pewnych zbyt ryzykownych obszarach, czy rezygnuje z danej działalności całkowicie. Bank musi mieć stosowne mechanizmy, wypracować procesy i procedury kontroli wewnętrznej oraz sprawnie funkcjonujący system zapewniający zgodność postępowania z wewnętrznymi regulacjami w zakresie zarządzania ryzykiem. Można wskazać na następujące elementy takiego systemu:

- Przeglądy postępu realizacji założonych celów dokonywane przez zarząd.
- Badanie przestrzegania mechanizmów kontrolnych opracowanych przez kierownictwo.
- Zasady polityki, procesy oraz procedury dotyczące postępowania w sytuacjach niezgodnych z obowiązującymi zasadami.
- Udokumentowane upoważnienia, zezwolenia i autoryzacje zapewniające właściwe przydzielenie odpowiedzialności na danym szczeblu kierownictwa.

Oprócz formalnych, pisemnych procedur w instytucji musi istnieć silna kultura kontroli, promująca zasady właściwego zarządzania ryzykiem. Za jej stworzenie odpowiada rada i zarząd. Efektywny system kontroli wewnętrznej powinien wymusić także właściwy podział zadań i obowiązków oraz takie przydzielenie zadań i odpowiedzialności, które nie będzie powodowało konfliktu interesów. Niewłaściwe przydzielenie zadań poszczególnym pracownikom czy zespołom może umożliwić popełnianie błędów, błędy w działaniu czy straty. Dlatego obszary potencjalnego konfliktu interesów powinny być identyfikowane, minimalizowane oraz precyzyjnie monitorowane. Do innych przykładów wewnętrznych zasad przydatnych w kontroli ryzyka operacyjnego można zaliczyć:

- praktyki uniemożliwiające ukrycie błędów,
- ciągły monitoring zgodności transakcji z limitami,
- zabezpieczenie dostępu i wykorzystywania aktywów, systemów informatycznych, zapisów księgowych,
- zapewnienie właściwych szkoleń i praktyk,
- identyfikację wszystkich nadzwyczajnych, nieoczekiwanych zysków, powstających w pionach operacyjnych, czy związanych z produktami, które nie powinny przynosić wysokich dochodów,
- regularną weryfikację i uzgodnienie transakcji i rachunków.

Konieczne jest także monitorowanie zagrożeń związanych z wprowadzaniem nowych produktów, wchodzeniem na nowe obszary, działaniem przez podmioty odległe geograficznie od siedziby centrali. W tej sytuacji należy zbadać, czy działania te zostały objęte systemem kontroli wewnętrznej i czy jest on należycie dostosowany do ryzyka.

Ważne są także monitorowanie zagrożeń typu „niskie prawdopodobieństwo, duże konsekwencje" i zabezpieczenia w postaci np. właściwych polis ubezpieczeniowych. Do takich zdarzeń można zaliczyć: błędy własne, błędy czy nadużycia partnerów zewnętrznych, fizyczną stratę papierów wartościowych, klęski żywiołowe.

Czasem przydatne jest rozważenie, czy sposoby ograniczania ryzyka - np. zakup polis ubezpieczeniowych[6], *outsourcing*, transfer ryzyka - rzeczywiście ograniczają ryzyko do pożądanego poziomu. W bankach powinny istnieć mechanizmy natychmiast identyfikujące błędy oraz korygujące je. Wymaga to dalszego inwestowania w odpowiednie technologie oraz systemy informatyczne i informacyjne. Konieczna jest także odpowiednia kontrola tych technologii.

Banki powinny wypracować politykę w zakresie *outsourcingu* oraz zasady współpracy ze wszystkimi podmiotami zewnętrznymi, z podmiotami grupy, z klientami itd. Powinny stosować właściwe techniki „*due diligence*" stron trzecich[7]. Podstawowe znaczenie ma również planowanie awaryjne.

ZASADA 7. Banki powinny mieć plany awaryjne oraz plany dotyczące ciągłości działania w sytuacjach awaryjnych w celu zapewnienia ciągłości operacyjnej oraz ograniczenia strat.

Pewne wydarzenia zewnętrzne, które są poza kontrolą banku, mogą wywrzeć negatywny wpływ na realizację części lub nawet wszystkich zobowiązań banku, w szczególności gdy uszkodzeniu czy zniszczeniu ulegnie infrastruktura fizyczna, telekomunikacyjna czy informatyczna banku. Może to spowodować poważne straty dla samego banku lub poprzez zaburzenia w systemach płatności wpłynąć na wiele podmiotów. Stąd tak dużego znaczenia nabierają plany ciągłości działania oraz wszelkie plany awaryjne. W tym celu należy identyfikować wszystkie ważne procesy biznesowe pod kątem podatności na nadużycia, uzależnienia od zewnętrznych dostawców, stron trzecich, złożoności technologii informatycznych. Analizie powinny być poddane możliwe scenariusze wydarzeń. Należy także ustalić priorytety działań w warunkach kryzysu i ocenić możliwość wykorzystania np. alternatywnych zasobów.

---

[6] Różnorodne instrumenty ubezpieczeniowe od dawna należą do ważnych narzędzi zabezpieczania przed ryzykiem operacyjnym, a tym samym zabezpieczania instytucji przed stratami. Firmy ubezpieczeniowe proponują instrumenty zabezpieczające przed stratami np. z tytułu zobowiązań wobec partnerów biznesowych powodowanych zaniedbaniami, nieuczciwością lub przestępstwami pracowników firmy, włamaniami, kradzieżami, od odpowiedzialności cywilnej. Przy transferze ryzyka operacyjnego dokonywanym poprzez zakup stosownych polis ubezpieczeniowych bank otwiera pozycję ryzyka kredytowego wystawcy polisy.

[7] W dniu 4 października 2001 r. Bazylejski Komitet ds. Nadzoru Bankowego wydał dokument *Customer due diligence for banks*. Zawiera on zalecenia dla banków oraz nadzorców bankowych na temat szeroko rozumianego procesu pogłębionej analizy klienta oraz operacji bankowych z zachowaniem zasad należytej staranności przez banki. Dokument ten zawiera minimalny zestaw standardów, które powinny posłużyć zainteresowanym stronom do rozwijania własnych praktyk w tej dziedzinie.

Rola nadzoru bankowego

ZASADA 8. Nadzorcy bankowi powinni wymagać, aby wszystkie banki, niezależnie od wielkości, miały i stosowały zasady identyfikacji, oceny, monitorowania oraz kontroli i ograniczania ryzyka operacyjnego. Zasady te powinny być częścią całościowej strategii zarządzania ryzykiem w instytucji.

Nadzorcy powinni wymagać, aby banki tworzyły strategię zarządzania ryzykiem operacyjnym opartą na wytycznych Komitetu Bazylejskiego – adekwatną do wielkości banku, skali i złożoności prowadzonej działalności, profilu ryzyka. Jeżeli rośnie poziom ryzyka operacyjnego w banku, musi on dostosowywać strategię oraz techniki zarządzania.

ZASADA 9. Nadzorcy powinni, bezpośrednio lub pośrednio, dokonywać regularnych niezależnych ocen polityki, procedur oraz praktyk dotyczących ryzyka operacyjnego. Nadzorcy powinni także zapewnić istnienie i funkcjonowanie stosownych mechanizmów, które dostarczają im wiedzy o wydarzeniach w banku.

W ramach niezależnej oceny ryzyka operacyjnego nadzorcy bankowi biorą pod uwagę:

– efektywność zarządzania ryzykiem w banku oraz całość kontroli w zakresie ryzyka operacyjnego,

– metody monitorowania ryzyka operacyjnego oraz raportowania na jego temat , włączając dane o poniesionych stratach operacyjnych oraz inne wskaźniki ryzyka,

– procedury terminowego oraz efektywnego postępowania w razie wydarzeń ryzyka oraz zagrożeń,

– procedury, mechanizmy oraz czynności kontroli wewnętrznej, przeglądy i audyty – pod kątem zapewnienia integralności całego procesu zarządzania ryzykiem operacyjnym,

– efektywność i techniki ograniczania ryzyka,

– jakość oraz kompleksowość podejścia do budowy planów naprawczych, planów awaryjnych, planów ciągłości działania,

– adekwatność kapitałową.

W przypadku banków wchodzących w skład grupy finansowej nadzór bankowy powinien również oceniać integralność i adekwatność zarządzania ryzykiem operacyjnym w ramach całej grupy. Do realizacji tego zadania niezbędne będą właściwe zasady współpracy pomiędzy nadzorcami różnych instytucji finansowych.

Rolą nadzoru powinno również być zachęcanie do ulepszania procesu zarządzania ryzykiem.

Znaczenie obowiązków sprawozdawczych

ZASADA 10. Banki powinny prezentować wystarczającą ilość informacji, które umożliwią uczestnikom rynkowym ocenę podejścia banku do zarządzania ryzykiem operacyjnym.

Prezentowanie z określoną częstotliwością aktualnych informacji przez banki wzmocni dyscyplinę rynkową, a przez to jakość zarządzania ryzykiem. Informacje mają dać właściwy obraz sytuacji banku i umożliwić inwestorom, klientom banku oraz regulatorom ocenę jakości zarządzania ryzykiem operacyjnym w instytucji.

Podsumowanie

Zdaniem autora, cenną inicjatywą Bazylejskiego Komitetu ds. Nadzoru Bankowego jest zwrócenie uwagi na zagadnienia ryzyka operacyjnego w działalności banków i określenie minimalnych wymagań w zakresie zarządzania i kontroli. Obecnie ryzyko operacyjne zaczyna być traktowane jako odrębna kategoria ryzyka. Będzie to skutkować utworzeniem i wprowadzeniem przez banki infrastruktury zarządzania i kontroli w zakresie ryzyka operacyjnego i wpisania jej w całościowy system zarządzania ryzykiem w banku. Pojawiają się propozycje definicji, narzędzi zarządzania oraz pomiaru[8]. Ryzyko operacyjne dotyczy praktycznie całego personelu danej instytucji. Trudno zarządzać tym ryzykiem w sposób zcentralizowany. Konieczne jest zarządzanie we wszystkich komórkach i pionach instytucji. Praktyka w zarządzaniu ryzykiem operacyjnym będzie zapewne zróżnicowana ze względu na silne uzależnienie od jednostki, kultury i sposobu zarządzania. Poszczególne branże i instytucje realizują odrębne zadania, jakość procesów i zarządzania procesami jest odmienna, wykorzystywane są różne systemy informatyczne; różna jest też jakość czynnika ludzkiego. W zakresie zarządzania ryzykiem operacyjnym brak jest jednolitego *benchmarku* dla wszystkich firm ze względu na specyfikę ich działalności. Nie oznacza to jednakże, iż ten rodzaj ryzyka był całkowicie pomijany. Zarządzanie nim spowoduje wzrost kosztów działania banków. Oprócz zmian organizacyjnych, kontrolnych i technologicznych pojawi się konieczność utrzymywania wymogu kapitałowego z tytułu ryzyka operacyjnego. Ten parametr przełoży się na normę adekwatności kapitałowej. Uzupełniającym instrumentem ochrony przed

[8] Patrz również: A. Wojtasik: *Wybrane metody pomiaru ryzyka operacyjnego dla instytucji finansowych działających na rynku instrumentów pochodnych.* „Bank i Kredyt" nr 1/2004.

konsekwencjami ryzyka będą różnorodne ubezpieczenia i bliższa współpraca banków z firmami ubezpieczeniowymi. Już dziś pewne banki organizują warsztaty poświęcone problematyce ryzyka operacyjnego, tworzone są komórki w instytucji do spraw zarządzania ryzykiem operacyjnym. W pionach operacyjnych powoływane są stanowiska manedżerów ds. ryzyka operacyjnego. Piony audytu wewnętrznego dedykują pewne audyty zbadaniu i ocenie tej problematyki. Organizowane są także spotkania różnych jednostek banku poświęcone tym problemom. Podejmuje się próby mapowania ryzyka oraz analizy rozkładu wartości strat operacyjnych[9] czy stosowania teorii wartości ekstremalnych, metodologii wartości zagrożonej czy analizy scenariuszy[10]. Tworzone są bazy zdarzeń ryzyka operacyjnego. Analizuje się jakość zarządzania i ryzyko procesów operacyjnych. Również polski nadzór bankowy opracował projekt rekomendacji dotyczącej zarządzania ryzykiem operacyjnym w bankach. Projekt ten jest konsultowany z bankami.

Myślę, że zestaw dobrych praktyk opublikowany przez Komitet Bazylejski będzie na wiele lat przewodnikiem po obszarach zarządzania ryzykiem operacyjnym.

[9] Autor artykułu ze względu na inną poruszaną problematykę nie poddał analizie żadnych metod pomiaru ryzyka operacyjnego. Zainteresowanych tym tematem odsyłam np. do pracy K. Jajugi: *Podstawy analizy wartości ekstremalnych na rynkach finansowych*. „Rynek Terminowy" nr 11/2001.

[10] Patrz np: P. Jorion. *Value At Risk. The New benchmark for managing financial risk*. New York. 2001 Mc Graw - Hill.