

Paweł Matkowski

O POTRZEBIE ZARZĄDZANIA RYZYKIEM OPERACYJNYM W INSTYTUCJACH FINANSOWYCH

1. Wstęp

Istotą działalności wszelkich instytucji finansowych jest działalność alokacyjna i zarządzanie ryzykiem. Klienci przekazując swoje środki wyspecjalizowanym podmiotom, wierzą, że instytucje te poprzez posiadane zasoby oraz wiedzę będą w stanie lepiej nimi zarządzać niż sami klienci. Zarządzanie ryzykiem polega na [9, s. 1]:

- identyfikowaniu i definiowaniu ryzyka, na które instytucja jest narażona,
- ocenie wpływu danego ryzyka na instytucję,
- łagodzeniu ryzyka za pośrednictwem określonych procedur,
- wyodrębnieniu środków przeznaczonych na pokrycie potencjalnych strat spowodowanych zachodzeniem danego ryzyka.

Jako obiektywne kryterium oceny zarządzania środkami finansowymi coraz częściej jest stosowane podejście odnoszące osiągnięty poziom zysku do wielkości ponoszonego ryzyka (*risk-reward approach*). Wcześniej wykorzystywane miary wykorzystywały kryteria typu: suma bilansowa, przychód netto czy też całkowita kwota zgromadzona na rachunkach oszczędnościowych. Dążąc do pełnego obiektywizmu wyników, podmioty sektora finansowego powinny jednak koncentrować się na miarach odnoszących zysk do ryzyka (np. RAROC – *capital at risk*). Tego typu podejście wymaga całościowego ujmowania zagadnienia ryzyka w instytucji finansowej. Niestety w większości podmiotów nie funkcjonuje w praktyce koncepcja całościowego zarządzania ryzykiem. Stosuje się raczej podejście tradycyjne akcentujące przede wszystkim ryzyko kredytowe (ryzyko niewypłacalności kontrahenta), ryzyko rynkowe (ryzyko zmiany wartości posiadanych aktywów w wyniku zmian cen na rynku) oraz ryzyko katastrof (ryzyko wystąpienia zdarzeń najczęściej naturalnych powodujących utratę wartości bądź całkowite zniszczenie aktywów). Jako metody niwelowania powyższych rodzajów ryzyka stosuje się

przede wszystkim procedury w zakresie ustalania wiarygodności kredytowej kontrahenta, hedging (szczególnie ryzyko rynkowe, a także coraz bardziej popularne instrumenty pochodne zabezpieczające przed bankructwem kontrahenta) oraz ubezpieczenie aktywów i transakcji. Ryzyko całościowe kalkulowane na podstawie powyższej koncepcji nie uwzględnia jednak takich zdarzeń, jak np. defraudacje, błędne rozliczenia transakcji, przerwy w dostawie prądu czy nawet ataki terrorystyczne i inne. Bez wątpienia jednak takie zdarzenia mają miejsce oraz są istotnym czynnikiem ryzyka. Nieuwzględnianie tych rodzajów ryzyka powoduje bezpośrednio zawyżenie zysku na jednostkę ryzyka, błędną alokację zasobów przez klientów (przy założeniu, że nie występuje asymetria informacji), co w najgorszym wypadku może zakończyć się bankructwem instytucji finansowej i utratą części lub całości środków przez jej klientów. Konieczna wydaje się zatem zmiana koncepcji zarządzania ryzykiem w instytucjach finansowych uwzględniająca pozostałe czynniki ryzyka, które nazywane są ryzykiem operacyjnym.

2. Definicje ryzyka operacyjnego

Jedna z pierwszych definicji przyjętych przez środowisko bankowe charakteryzowała ryzyko operacyjne jako każdy rodzaj niekwantyfikowalnego ryzyka ponoszonego przez instytucję finansową (bank). Takie brzmienie było następstwem wykorzystywania modelowania ekonometrycznego do szacowania ryzyka rynkowego i kredytowego. Duże sukcesy na polu modelowania ww. rodzajów ryzyka w latach dziewięćdziesiątych, niemożność zastosowania tych samych metod do ryzyka operacyjnego, a także jego niejednorodny charakter wpłynęły na ogólny kształt definicji (inne brzmienie: każde ryzyko nie będące kredytowym lub rynkowym).

W literaturze przedmiotu można również spotkać się z definicją traktującą ryzyko operacyjne jako „ryzyko nie związane ze sposobem finansowania działalności, ale raczej ze sposobem prowadzenia działalności” [7, s. 3].

Analizując formularz rejestracyjny danych do bazy British Bankers' Association (BBA) gromadzącej obserwacje wystąpienia zdarzeń zaliczanych do klasy ryzyka operacyjnego (British Bankers Association Operational and Risk Database), znajdujemy następujące kategorie strat:

- błędne operacje zakupu/sprzedaży papierów wartościowych,
- błędy w rozliczeniach transferów pieniężnych,
- zniszczone lub skradzione aktywa rzeczowe,
- zasądzone odszkodowania,
- grzywny i kary nałożone przez organizacje członkowskie i instytucje nadzoru,
- nieodwracalne lub błędne transfery funduszy lub aktywów,
- nieprzewidziane koszty osobowe,
- szkody będące następstwem oszustw i niedbalstwa.

Bardzo istotne jest, aby zważyć, że powyższa klasyfikacja nie uwzględnia ryzyka reputacji (ryzyko poniesienia strat w wyniku utraty wiarygodności przez

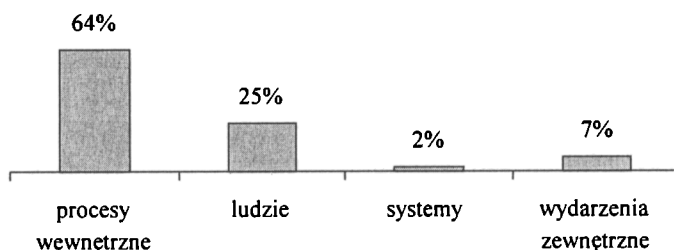
instytucję finansową) oraz ryzyka strategicznego (ryzyko związane ze zmianą strategii firmy), zawiera zaś straty będące następstwem wystąpienia ryzyka prawnego (ryzyko odszkodowań z tytułu przegranych spraw sądowych). W ten sam sposób będziemy interpretować definicję przedstawioną przez Komitet Bazylejski.

Załącznik 1 niniejszego artykułu przedstawia klasyfikację strat operacyjnych według Risk Management Group (grupa robocza w strukturach Komitetu Bazylejskiego) opracowaną na podstawie propozycji BBA.

Pierwsza pełna definicja ryzyka operacyjnego została zaprezentowana w opracowaniu *Operational Risk: The Next Frontier* stworzonym wspólnie przez British Bankers' Association (BBA), The International Swaps and Derivatives Association (ISDA), Risk Management Association (RMA) i Pricewaterhouse Coopers w roku 1999. Ryzyko operacyjne zostało zdefiniowane jako „ryzyko strat pieniężnych wynikających z niewłaściwych lub błędnych procesów wewnętrznych, z winy ludzi bądź systemów lub spowodowanych wydarzeniami zewnętrznymi”. Warto zwrócić uwagę, że ryzyko wydarzeń zewnętrznych ma bardziej systemowy charakter w porównaniu z ryzykiem wydarzeń wewnątrz firmy, które zależy od rodzaju prowadzonej działalności. Powyższa definicja znalazła się również w propozycji Nowej umowy kapitałowej (uwzględnienie ryzyka operacyjnego w pierwszym filarze dotyczącym minimalnych wymagań kapitałowych) i po wielu dyskusjach prowadzonych pod kuratelą Komitetu Bazylejskiego została przyjęta przez środowisko. Aktualnie najściślej definiuje ryzyko operacyjne. Należy zaznaczyć, że definicja powyższa uwzględnia ryzyko prawne i nie uwzględnia ryzyka reputacji oraz strategicznego.

Analizując powyższe warto zwrócić uwagę na cztery czynniki ryzyka, a są to:

- ludzie,
- procesy,
- systemy,
- zdarzenia zewnętrzne.



Rys. 1. Udział poszczególnych czynników w całkowitym poziomie ryzyka operacyjnego

Źródło: strona internetowa RMA [14].

Rysunek 1 przedstawia wyniki badań sektora bankowego przeprowadzonych przez Risk Management Association (w listopadzie 2002 r.) w zakresie ryzyka operacyjnego. Poniżej zaobserwować można udział poszczególnych czynników w całkowitym poziomie ryzyka operacyjnego w instytucjach finansowych.

Niezbędne wydaje się scharakteryzowanie poszczególnych czynników określających, na czym polega zagrożenie, którego nośnikami są:

1. **Ludzie.** W tej grupie znajdują się straty spowodowane umyślnym przekroczeniem przepisów przez aktualnych i byłych pracowników. W niektórych przypadkach straty mogą być spowodowane przez osoby, które zamierzano zatrudnić, ale w efekcie nie doszło do zawarcia umowy. W tej kategorii szczególną uwagę należy zwrócić na wszelkie działania mające na celu świadome oszustwo. Ich celem jest przede wszystkim osiągnięcie korzyści materialnych, ale również prestiżu (bądź lęk przed utratą określonej pozycji społecznej). Jak pokazują badania, czynnikiem motywującym może być również „zastrzyk adrenaliny” [2, s. 7].

2. **Procesy.** Zaliczyć tu należy straty będące następstwem błędów w funkcjonujących procedurach lub braku procedur w ogóle (procedura jest błędnie zaprojektowana lub błędnie wykonywana). Powodem takiej sytuacji może być niezrozumienie procesów w instytucji finansowej lub ich znaczne skomplikowanie. Straty w tej kategorii mogą być następstwem błędów ludzkich, chociaż są nieumyślne.

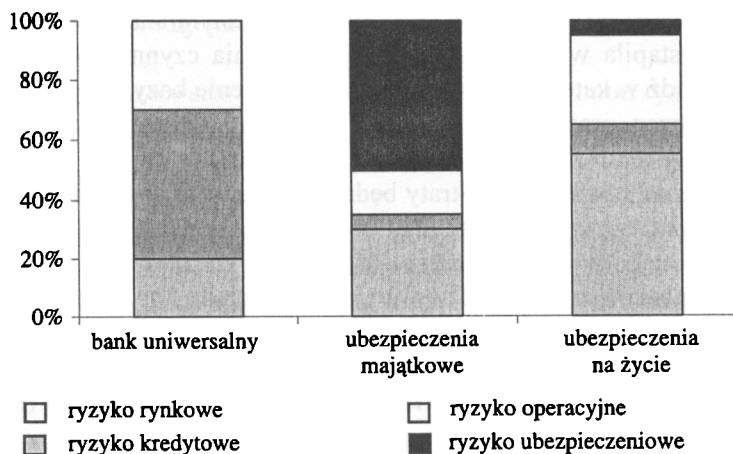
3. **Systemy.** Straty spowodowane przez awarie istniejących systemów lub technologii. Straty w tej kategorii są nieumyślne. Jeśli strata spowodowana awarią systemów wystąpiła w wyniku umyślnego działania czynnika ludzkiego, należy umieścić ją bądź w kategorii „Ludzie” (np. zniszczenie bazy danych po dokonaniu defraudacji przez pracownika) bądź w kategorii „Zdarzenia zewnętrzne” (np. włamanie do systemu z zamiarem zniszczenia danych).

4. **Zdarzenia zewnętrzne.** Straty będące efektem działania sił naturalnych lub wywołane przez człowieka, bądź jako bezpośredni rezultat działania strony trzeciej. Do tej kategorii zaliczyć można wszelkiego rodzaju katastrofy (powódzie, huragany, trzęsienia ziemi, przerwy w dostawie prądu (np. przerwa w dostawie prądu w dniach 14-15.08.2003 r., która dotknęła wschodnie wybrzeże USA i Kanady – straty z tego tytułu wycenia się na 6 mld USD [4]), niedostępność budynków dla pracowników itd.), zewnętrzne działania przestępcze (różnego typu działania terrorystyczne, włączając w to podkładanie bomb (patrz: sierpniowe (2003) doniesienia o podłożeniu 2 bomb w siedzibie firmy Charles Schwab prowadzącej działalność maklerską za pośrednictwem Internetu), pranie brudnych pieniędzy, oszustwa zewnętrzne, straty będące wynikiem niepokojów społecznych, ataki na strony internetowe korporacji w celu wprowadzenia w błąd użytkowników i odniesienia z tego tytułu korzyści materialnej (np. sierpniowa (2003) próba włączenia się oszustów na stronę internetową Citibanku), straty spowodowane korzystaniem z usług zewnętrznych i dostawców (niezapewnienie przez dostawcę określonej jakości, bankructwo firmy outsourcingowej itd.).

Szczegółowa klasyfikacja strat zaproponowana przez Komitet Bazylejski znajduje się w załączniku 1.

3. Dlaczego należy zarządzać ryzykiem operacyjnym

Konieczność zarządzania ryzykiem operacyjnym wynika bezpośrednio z istotności strat powodowanych tym ryzykiem dla instytucji finansowych. Rysunek 2 przedstawia schematycznie wielkość ekspozycji na ryzyko operacyjne w trzech różnych rodzajach działalności finansowej: dużych bankach uniwersalnych (przewaga ryzyka kredytowego), w ubezpieczeniach majątkowych (przewaga ryzyka ubezpieczeniowego w następstwie małej przewidywalności wystąpienia szkód) i ubezpieczeniach na życie (w związku z długim horyzontem inwestycyjnym przewaga ryzyka rynkowego). Jednak w każdym z tych rodzajów biznesu w ramach sektora finansowego widać znaczny udział ryzyka operacyjnego. Przyjmuje się, że w przypadku instytucji finansowej ryzyko operacyjne odpowiedzialne jest za 35% zmienności w zakresie osiąganych wyników finansowych (ryzyko kredytowe – 50%, ryzyko rynkowe – 15%) [3, s. 10]. Nie dość, że stanowi pokaźną wartość, to, co istotne, przewyższa najczęściej ryzyko rynkowe, które postrzegane jest jako jeden z ważniejszych składników ryzyka. Utrudnione postrzeganie problemu ryzyka operacyjnego wynika przede wszystkim z jego niejednorodności.



Rys. 2. Przybliżony podział kapitału ekonomicznego dla trzech różnych sektorów finansowych
Źródło: [5, s. 18].

Ryzyko operacyjne nie jest jednolite – jest zbiorem różnych rodzajów ryzyka, z którymi instytucja finansowa styka się w trakcie prowadzonej działalności. Ta różnorodność znacznie utrudnia wprowadzenie jednej metodologii postępowania. Tym też należy tłumaczyć to, że dopiero koniec lat dziewięćdziesiątych przyniósł

zainteresowanie praktyków i naukowców tematyką OPRISK (wcześniej oba środowiska skoncentrowane były na problemie ryzyka kredytowego i rynkowego). Wydarzenia z 11 września 2001 r. zwróciły uwagę na zagrożenia, które dotąd były traktowane jako mało prawdopodobne. Jednocześnie historia burzliwego rozwoju instrumentów pochodnych w latach dziewięćdziesiątych dała wiele przykładów strat spowodowanych niedostrzeganiem zagrożeń wynikających z ekspozycji na ryzyko operacyjne (np. upadek banku Barrings w wyniku *rogue trading* N. Leeson). Pomimo stosowania najlepszych praktyk oraz solidnej lekcji historii, instytucje finansowe borykają się ciągle z problemami wynikłymi z niedoceniań ryzyka operacyjnego (Allied Irish Bank: strata 690 mln USD w następstwie *rogue trading*, bankructwo drugiej największej firmy ubezpieczeniowej w Australii – HIH Insurance, afera związana z praniem brudnych pieniędzy, na łączną sumę 10 mld USD, rosyjskich grup przestępczych w Bank of New York). Badanie na grupie 400 menedżerów z instytucji finansowych przeprowadzone przez miesięcznik „Operational Risk” we współpracy z firmą informatyczną SAS (czerwiec 2003 r.) pokazuje, że 56% firm przynajmniej raz w miesiącu notuje stratę o wartości od 10 000 do 100 000 USD, w następstwie ryzyka operacyjnego. 55% instytucji finansowych doświadcza przynajmniej raz na kwartał straty o wartości od 100 000 do 500 000 USD. To samo badanie dowodzi, że najistotniejszym czynnikiem ryzyka operacyjnego według kadry kierowniczej jest „awaria systemów informatycznych/nieodpowiedni system informacyjny (*management information system*) generujący dane na potrzeby zarządu”. Drugim co do ważności czynnikiem ryzyka według respondentów są „obawy w zakresie nowych regulacji (Nowa umowa kapitałowa i ustawodawstwo krajowe) oraz dostosowanie się do nich”. Kolejne miejsca zajmują odpowiednio „brak wewnętrznej informacji nt. ryzyka operacyjnego” oraz „utrzymanie ciągłości biznesu/usuwanie strat spowodowanych katastrofami” [8, s. 28].

Komitet Bazylejski w opracowaniu poświęconym ryzyku operacyjnemu (czerwiec 2002 r.) [1, s. 2], zwraca uwagę, że wzrost istotności ryzyka operacyjnego w całkowitym wolumenie strat jest spowodowany m.in. przez następujące procesy:

- zwiększone wykorzystanie technologii automatycznych,
- e-commerce,
- fuzje na wielką skalę,
- działalność banków jako dostawców usług o bardzo dużym wolumenie,
- wzrost wykorzystania metod łagodzenia ryzyka kredytowego i rynkowego, którego efektem może być zwiększona ekspozycja na ryzyko operacyjne,
- wzrost wykorzystania outsourcingu w instytucjach finansowych.

Risk Management Group (RMG) działająca w ramach Komitetu Bazylejskiego opublikowała w roku 2002 wyniki badania przeprowadzonego na grupie 30 banków z 11 krajów [13]. Okres badania (*Qualitative Impact Study II – QIS 2*) obejmował trzy lata. Badanie polegało na gromadzeniu danych o stratach spowodowanych ryzykiem operacyjnym. RMG gromadziło dane dla ośmiu rodzajów

działalności biznesowej prowadzonej w sektorze finansowym: finanse przedsiębiorstw (*corporate finance*), handel papierami wartościowymi (*trading & sales*), bankowość detaliczna (*retail banking*), bankowość komercyjna (*commercial banking*), płatności i rozliczenia (*payment & settlement*), usługi pośrednictwa i przechowywania (*agency services & custody*), zarządzanie aktywami (*asset management*), detaliczna działalność maklerska (*retail brokerage*). Pomimo oczywistego faktu, że okres trzyletni jest zbyt krótki, aby uchwycić występowanie zdarzeń rzadkich, stanowiących o istocie ryzyka operacyjnego, badanie to zwraca uwagę na kilka interesujących zagadnień. W badanym okresie wystąpiło 27 371 strat spowodowanych ryzykiem operacyjnym o łącznej wartości 2,6 mld euro. Najwięcej obserwacji wystąpiło w bankowości detalicznej (67% obserwacji), ich wartość łączna zaś wyniosła 39% sumy strat (największa wartość). Bankowość komercyjna dała drugi co do wielkości wynik (odpowiednio 13 i 23%). Dowodzi to, że badana próbka instytucji finansowych działa przede wszystkim w tych liniach biznesowych. Najczęściej występującymi kategoriami ryzyka operacyjnego o największej sile były: zarządzanie realizacją, przekazaniem i procesami (41,99% wszystkich obserwacji; 34,76% wartości strat) oraz oszustwo zewnętrzne (odpowiednio 36,39 i 20,32%). Rodzaje strat zamieszczono w załączniku 1. Większość zgromadzonych obserwacji charakteryzowała się niewielką wartością jednostkową – jedynie 1% wszystkich obserwacji przekraczała wartość 1 mln euro. Jednak były one odpowiedzialne za prawie 75% całkowitej wartości wszystkich strat.

Przytaczane w tym rozdziale przykłady jednoznacznie dowodzą istotności wprowadzenia zintegrowanego systemu zarządzania ryzykiem operacyjnym w instytucjach finansowych, nie tylko z chęci uniknięcia strat katastrofalnych, które mogłyby się zakończyć bankructwem przedsiębiorstwa, ale również w celu minimalizowania zmienności wyników finansowych i dostarczania wartości dla akcjonariuszy i klientów powierzających środki.

4. Zarządzanie ryzykiem operacyjnym

Ciągle nie istnieje jednorodna, spójna metodologia zarządzania ryzykiem operacyjnym w instytucjach sektora finansowego. Duże przedsiębiorstwa bankowe (działające na skalę międzynarodową) aktualnie pracują nad koncepcją zintegrowanego zarządzania ryzykiem operacyjnym. Główne elementy tej koncepcji można przedstawić w następujący sposób:

1. **Identyfikacja i ocena ryzyka.** Menedżerowie poszczególnych linii biznesowych określają główne procesy, rodzaje ryzyka związane z tymi procesami oraz luki i sposoby ich eliminowania. Ich zadaniem jest również ocena siły wpływu poszczególnych rodzajów ryzyk oraz prawdopodobieństw ich zachodzenia (najlepiej w sposób ilościowy). Pomocnym narzędziem na etapie identyfikacji i oceny jest matryca (zob. załącznik 2) pozwalająca odpowiedzieć na pytanie: jaka działalność jest narażona na poszczególne rodzaje ryzyka operacyjnego.

2. Kwantyfikacja i mierzenie ryzyka. Na tym etapie niezbędne jest stworzenie baz danych gromadzących obserwacje strat z wnętrza firmy, a także konstrukcja wskaźników i zbieranie ich obserwacji (np. przychód brutto, liczba strat w czasie itd.). Wśród strat należy wyróżnić dwie kategorie: HFLI (*high frequency low impact*) – charakteryzujące się wysoką częstotliwością, lecz o małej wartości jednostkowej (monitorowane przez wewnętrzny audyt, łatwe do uzyskania z systemów i modelowania), LFHI (*low frequency high impact*) – o małej częstotliwości, lecz o dużej sile oddziaływania (bardzo rzadkie, wręcz pojedyncze – instytucje finansowe nie posiadają wystarczającej ilości tych danych z wewnętrznych źródeł pozwalającej na modelowanie) – zob. rys. 3. Wskazuje się również na konieczność wykorzystania danych zewnętrznych (zob. baza danych British Bankers' Association gromadząca obserwacje zdarzeń zaliczanych do klasy ryzyk operacyjnych). Niezmiernie ważnymi parametrami są osiągalność i integralność danych wewnętrznych oraz istotność i skalowalność danych pochodzących z zewnętrznych baz. Wykorzystywane są również dane otrzymywane na etapie identyfikacji i oceny ryzyka.



Rys. 3. Mapa ryzyka linii biznesowej

Źródło: [6].

3. Analiza, monitorowanie i raportowanie ryzyka. Celem analizy jest integracja zarządzania ryzykiem pozwalająca na prawidłową ocenę działalności instytucji finansowej. Analiza ujawnia obszary ryzyka oraz ukryte luki. Monitorowanie ryzyka operacyjnego, głównych wskaźników ryzyka i planów działania powinno odzwierciedlać zmiany w przedsiębiorstwie oraz rozbudzać czujność. Raportowanie powinno być dostosowane do adresatów na różnych poziomach zarządzania, włączając w to zarząd najwyższego szczebla instytucji finansowej.

4. Wyznaczanie poziomu kapitału zabezpieczającego nieoczekiwane straty operacyjne. Operacyjny *capital-at-risk* powinien być wyznaczony dla każdej

z linii biznesowych. Jego zadaniem jest ochrona – pokrycie nieoczekiwanych strat, w przypadku ich wystąpienia – przy uwzględnieniu określonego horyzontu czasowego oraz poziomu ufności (np. jeden rok, 99,9% OpVAR).

5. Zarządzanie ryzykiem – sposoby zabezpieczania. Zabezpieczanie się przed ryzykiem operacyjnym może być dokonane w drodze zakupu ubezpieczenia lub praktyk mających na celu minimalizację prawdopodobieństwa wystąpienia straty, a także planów, których celem jest podtrzymanie działalności w przypadku wystąpienia zdarzeń katastrofalnych. Ubezpieczenie jest szeroko wykorzystywane przez sektor finansowy, lecz ma niestety ograniczoną rolę. Po pierwsze, spowodowane jest to tym, iż zdecydowana większość towarzystw ubezpieczeniowych w podstawowej ofercie obejmuje wyłącznie bardzo specyficzne i ograniczone kategorie ryzyk operacyjnych. Rynek ubezpieczeń jest niejednorodny, co odzwierciedla się w oferowanych produktach. Poza tym tradycyjne produkty ubezpieczeniowe nie uwzględniają wielowymiarowej natury ryzyka operacyjnego. Po drugie, wycena ryzyka nie dokonuje się jawnie, co ma znaczny wpływ na wielkość premii płaconej ubezpieczycielom przez wykupujących polisę. Po trzecie, nawet w przypadku ubezpieczenia straty wypłata odszkodowania wymaga czasu, którego ubezpieczony może nie mieć. Jednocześnie sam ubezpieczyciel w przypadku wypłaty o znacznej wartości może stać się czynnikiem ryzyka kredytowego (np. ogłosić upadłość lub wystąpić o ochronę przez wierzycielami). Jak zatem widać, w sytuacji ekstremalnej ubezpieczenie może nie zapewnić przetrwania instytucji finansowej, pomimo że bezsprzecznie może być czynnikiem ograniczającym zmienność wyników finansowych.

5. Ryzyko operacyjne w nowej umowie kapitałowej

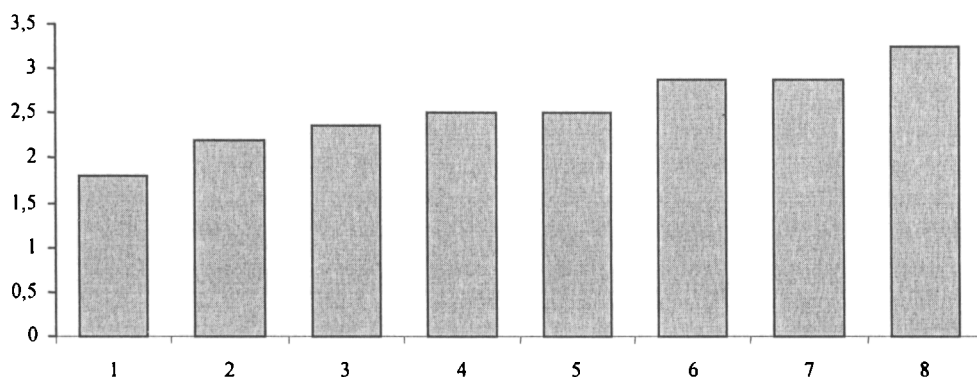
Komitety Bazylejski w 2001 r. zaproponował włączenie ryzyka operacyjnego do Nowej umowy kapitałowej, co będzie skutkowało uwzględnieniem ryzyka operacyjnego w standardach wymogów kapitałowych (środki będące zabezpieczeniem ryzyk ponoszonych przez instytucje finansowe).

Aby zachęcić podmioty zobowiązane przez regulacje do utrzymywania minimalnych poziomów kapitałowych do aktywnego zarządzania ryzykiem operacyjnym, propozycje Nowej umowy kapitałowej uwzględniają zaawansowane podejścia do zarządzania OPRISK – nie tylko określenie jednego poziomu rezerw opartego na agregacji będącym miarą aktywności dla wszystkich banków z tytułu ryzyka operacyjnego (np. przychody ogółem itd.) ale stosowanie preferencji w przypadku banków wykorzystujących zaawansowane metody szacowania i zarządzania OPRISK.

Oczywiście nadzór bankowy, podobnie jak w przypadku ryzyka rynkowego, będzie zatwierdzał system zarządzania ryzykiem, będący podstawą do ubiegania się o zmniejszenie wielkości wymogów kapitałowych.

6. Aktualny stan zarządzania ryzykiem operacyjnym w instytucjach finansowych – szanse i zagrożenia

Z badania przeprowadzonego przez *Operational Risk* i SAS [3, s. 10] wynika, że 19% spośród ankietowanych firm z sektora nie wprowadziło dotychczas żadnego programu w zakresie ryzyka operacyjnego. Z drugiej strony głównym motywatorem inicjującym wprowadzenie programu w przypadku pozostałych 81% instytucji są „propozycje Nowej umowy kapitałowej (Basel II) i ustawodawstwo krajowe”. Kolejne miejsce w hierarchii ważności zajmuje „ustalanie wewnętrznych wzorców postępowania”, następnie „obawy co do wystąpienia wewnętrznych strat operacyjnych”. Pozostałe czynniki zostały przedstawione na rys. 4.



1 – Nowa umowa kapitałowa (Basel II) i krajowe ustawodawstwo, 2 – ustalanie wewnętrznych wzorców postępowania, 3 – obawy co do wewnętrznych strat operacyjnych, 4 – inne (np. rozwój infrastruktury przeciwdziałającej praniu brudnych pieniędzy), 5 – indywidualne/wspólne inicjatywy w zakresie OPRISK/TECH., 6 – nacisk akcjonariuszy na zarządzanie i jawność, 7 – afery księgowe i reakcje regulatorów, 8 – zamachy terrorystyczne/kwestie podtrzymania ciągłości biznesu.

Rys. 4. Czynniki, które wpłynęły najbardziej na decyzję o wdrożeniu programu zarządzania OPRISK
(1 – najbardziej istotny, 4 – najmniej istotny)

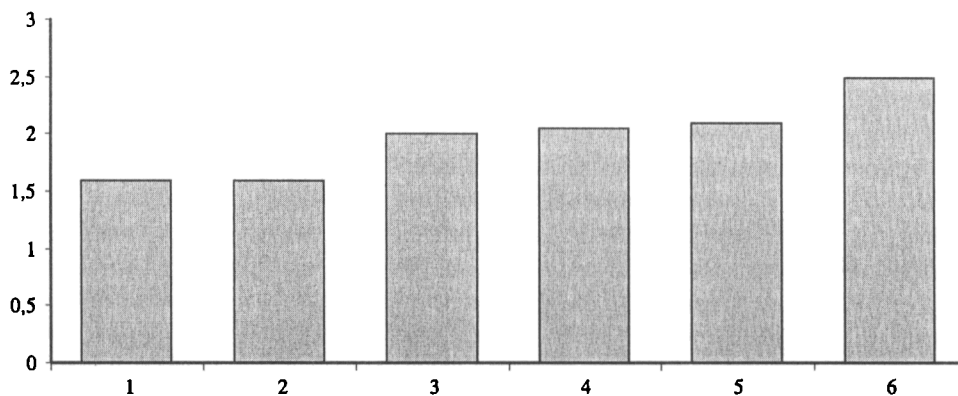
Źródło: [8, s. 28].

Znamienne jest to, że konieczność sprostania regulacjom prawnym jest czynnikiem bardziej motywującym zarządy instytucji finansowych niż świadomość ekspozycji na ryzyko strat, które może w skrajnych przypadkach spowodować bankructwo firmy.

Rysunek 5 przedstawia korzyści wynikające z pomyślnego wdrożenia zarządzania ryzykiem operacyjnym.

W zakresie zarządzania ryzykiem operacyjnym w instytucjach finansowych analizowane badanie pokazuje, że:

- 21% badanych firm posiada radę (zespół) zajmującą się ryzykiem operacyjnym, do której należą również menedżerowie zarządzający tylko i wyłącznie OPRISK na poziomie poszczególnych jednostek biznesowych,
- 19% posiada radę (zespół), do której należą menedżerowie z poziomu jednostek biznesowych, którzy zajmują się nie tylko ryzykiem operacyjnym,
- 12% badanych instytucji posiada jedynie centralną radę zajmującą się przede wszystkim dostosowaniem do międzynarodowych i krajowych regulacji,
- 14% ankietowanych nie wykształciło żadnych ciał zajmujących się ryzykiem operacyjnym.



1 – redukcja strat operacyjnych, 2 – polepszenie zarządzania biznesami i wynikami, 3 – zabezpieczenie przed utratą reputacji, 4 – ulepszenie sprawozdawczości, 5 – optymalizacja kapitału ekonomicznego, 6 – inne.

Rys. 5. Najistotniejsze korzyści wynikające z udanego wdrożenia zarządzania ryzykiem operacyjnym

(1 – najbardziej istotna, 4 – najmniej istotna)

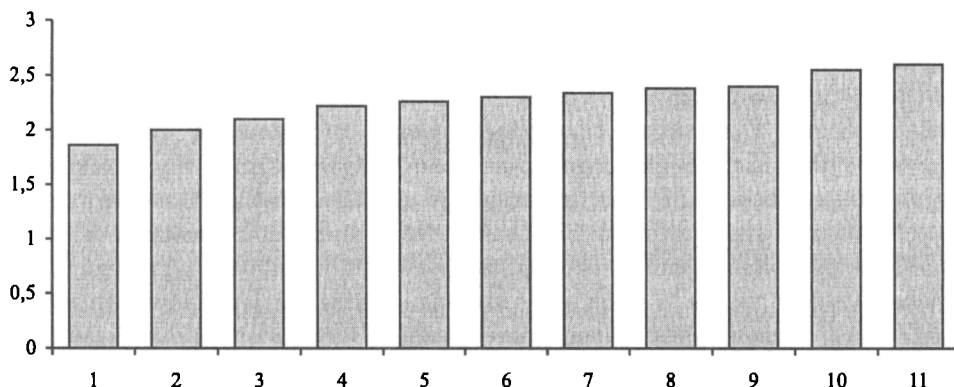
Źródło: [8, s. 28].

W przypadku 3/4 badanych instytucji zespoły dedykowane wyłącznie ryzyku operacyjnemu liczyły maksymalnie 5 osób [8, s. 28].

Powyższe dane wyraźnie pokazują, że w instytucjach finansowych zarządzanie ryzykiem operacyjnym w porównaniu z innymi ryzykami (kredytowym i rynkowym) jest ciągle niedoceniane. Należy mieć nadzieję, że regulacje prawne, szczególnie Nowa umowa kapitałowa, przyczynią się nie tylko do wprowadzenia wymogów kapitałowych w zakresie OPRISK, ale przede wszystkim zwrócą uwagę na istotność zintegrowanego zarządzania tym ryzykiem oraz umożliwi opracowanie spójnej metodologii, którą będzie można wykorzystać w praktyce. Brak całościowej koncepcji w zakresie ryzyka operacyjnego wyraźnie akcentowany jest przez środowisko. W omawianym badaniu aż 68% ankietowanych twierdzi, że budowę informatycznego systemu wspomagającego zarządzanie OPRISK w

instytucji finansowej należy przeprowadzić z wykorzystaniem wewnętrznych zasobów, z powodu braku odpowiedniej oferty ze strony integratorów (aktualna oferta rynkowa traktuje problem wycinkowo).

Hierarchię trudności związanych z zarządzaniem ryzykiem operacyjnym prezentuje rys. 6.



1 – trudności związane z modelowaniem OPRISK, 2 – trudności związane z wykorzystaniem danych historycznych, 3 – trudności związane z przenikaniem się informacji jakościowych i ilościowych, 4 – trudności z zapewnieniem jakości danych, 5 – koszt i czas wdrożenia, 6 – brak jasnych wytycznych ze strony regulatorów, 7 – trudności w ocenie/raportowanie danych OPRISK, 8 – kultura organizacyjna i obawy dotyczące OPRISK, 9 – kwestie integracji systemów, 10 – dostęp do kadry, 11 – niewystarczające zaangażowanie się zarządu.

Rys. 6. Najważniejsze przeszkody w zarządzaniu ryzykiem operacyjnym
(1 – najbardziej istotna, 4 – najmniej istotna)

Źródło: [8, s. 29].

Analizując perspektywy rozwoju zintegrowanego zarządzania ryzykiem operacyjnym, warto znów odwołać się wspomnianego badania. Jedynie 33% badanych utrzymuje, że budżet przeznaczony na zarządzanie ryzykiem operacyjnym w ich instytucji finansowej w kolejnym roku przekroczy 1 mln USD, co w zestawieniu z poziomem osiąganych strat operacyjnych jest wielkością zdecydowanie zbyt niską. Należy również zwrócić uwagę, że pozostałe 2/3 firm z sektora finansowego przeznaczą na ryzyko operacyjne mniej niż 1 mln USD, mając jednocześnie świadomość, że w tym samym badaniu 55% firm przyznaje się do odnotowywania przynajmniej jednej straty operacyjnej na kwartał o wartości z przedziału 100-500 tys. USD! W tym kontekście przewidywane nakłady na ryzyko operacyjne wydają się zdecydowanie niewystarczające.

7. Podsumowanie

Niniejsza praca, prezentując podstawowe zagadnienia związane z ryzykiem operacyjnym w instytucjach finansowych, zwraca szczególną uwagę na konieczność zintegrowanego zarządzania OPRISK przez podmioty z sektora finansowego. Jest to spowodowane procesami, które nasiliły się w ostatnich 10 latach: znacznym wzrostem operacyjnych czynników ryzyka w następstwie zwiększania skali działalności przez przedsiębiorstwa bankowe, wykorzystywaniem elektronicznych kanałów kontaktu z klientem, a także zagrożeń związanych z Internetem (wirusy, ataki DoS itd.) i ze strony międzynarodowego terroryzmu. W tym kontekście dziwne wydaje się, że głównym czynnikiem motywującym firmy z sektora do rozwijania koncepcji OPRISK są regulacje nadzoru międzynarodowego i krajowego, a nie rzeczywistość biznesowa. W tym świetle działania Komitetu Bazylejskiego włączające ryzyko operacyjne do minimalnych wymagań kapitałowych wydają się ze wszech miar słuszne. Widoczny jest jednak duży opór środowiska, szczególnie banków amerykańskich, a także azjatyckich¹, które nie garną się do poprawy bezpieczeństwa sektora kosztem zmniejszenia własnej konkurencyjności. Efektem tego procesu jest przesunięcie wejścia w życie Nowej umowy kapitałowej z 2005 na rok 2006 i głosy o braku realności terminu przed rokiem 2010. Należy mieć nadzieję, że środowisko bankowe, akceptując włączenie ryzyka operacyjnego do NUK, będzie w stanie poświęcić część zysków na rzecz ograniczenia całkowitego poziomu ryzyka sektora finansowego.

Literatura

- [1] Basel Committee on Banking Supervision, *Sound Practices for the Management and Supervision of Operational risk*, BIS, czerwiec 2002.
- [2] Brink G.J., *Operational Risk. The New Challenge for Banks*, Palgrave, New York 2002.
- [3] Cruz M., *Modeling, Measuring and Hedging Operational Risk*, John Wiley & Sons, New York, 2002.
- [4] *ERISK Weekly Review*, 16-22 August 2003. www.erisk.com.
- [5] Giese G., *Economic Capital vs. Regulatory Capital – a Market Benchmark*, „RISK” 2003 vol. 16, no. 5.
- [6] Harmantzis F., *Risky Business*, Operations Research Management Science, Institute for OR/MS, February 2003.
- [7] King J., *Operational Risk*, John Wiley & Sons, New York 2001.
- [8] Leander E., *Exclusive Surrey Snows Reality Gap*, Operational Risk, vol. 4, Issue 6, June 2003, Risk Waters Group.
- [9] Lopez J.A., *What Is Operational Risk*, „FRBSF Economic Letter”, 2002 no. 2, 25 January 2002.
- [10] Netter J., Poulsen A., *Operational Risk in Financial Service Providers and Proposed Basel Capital Accord: An Overview*, University of Georgia, Athens 2003.

¹ Bank Centralny Chin i Bank Centralny Indii zapowiedziały, że nie wdrożą postanowień Basel II i pozostaną przy „starej umowie kapitałowej”

-
- [11] *Operational Risk*, vol. 4, Issue 6, Risk Waters Group, June 2003.
[12] *RISK*, vol. 16, no 5, Risk Waters Group, May 2003.
[13] Risk Managemet Group, *The Quantitative Impact Study for Operational RISK: Overview of Individual Loss Data and Lesson Learned*, BIS, January 2002.
[14] www.rmahg.org.

THE NECCESSITY OF OPERATIONAL RISK MANAGEMENT IN FINANCIAL INSTITUTIONS

Summary

The approach of Enterprise-wide Risk Management in financial institutions requires dealing with operational risk, besides credit and market risk. The growing operational risk exposure is a result of an increased importance of internationally active banks and appearance of rare events. The surveys show that operational risk is responsible for approximately 35% earning volatility of banks. That was the main reason that regulators decided to include operational risk in New Adequacy Framework. This working paper presents a review of the literature of operational risk management.

Mgr Paweł Matkowski jest doktorantem w Katedrze Finansów Akademii Ekonomicznej we Wrocławiu.

Załącznik 1. Szczegółowa klasyfikacja strat w ryzyku operacyjnym

Typ wydarzenia (poziom 1)	Definicja 2	Kategorie (poziom 2)	Przykłady działalności (poziom 3)
1	3	4	
Oszustwa wewnętrzne	straty będące następstwem kradzieży, przywłaszczenia własności lub omijania przepisów prawa lub rozporządzeń wewnętrznych spowodowane przez osoby z wnętrza instytucji	nielegalne działania	umyślne nieodnotowywanie transakcji nielegalne transakcje oszustwa polegające na podszywaniu się pod wyższe stanowisko
		kradzieże i oszustwa	oszustwa/oszustwa kredytowe kradzież/wymuszenie/malwersacje/ rabunek przywłaszczenie aktywów niszczenie aktywów z zamiarem spowodowania strat fałszerstwo wystawianie czeków bez pokrycia przejęcie rachunku/podszywanie się pod właściciela umyślne uchylanie się od obowiązku podatkowego łapówki dokonywanie transakcji papierami wartościowymi przez osoby mające dostęp do poufnych informacji (nie na rachunek instytucji)
Oszustwa zewnętrzne	straty spowodowane przez stronę trzecią polegające na kradzieży lub przywłaszczeniu własności bądź ominięciu prawa	kradzieże i oszustwa	kradzież/rabunek fałszerstwo wystawianie czeków bez pokrycia
		bezpieczeństwo systemów	zniszczenia spowodowane włamaniami do systemów kradzież informacji
Kwestie zatrudnienia i bezpieczeństwa w miejscu pracy	straty spowodowane działaniem niezgodnym z prawem pracy i regulacjami w zakresie BHP, żądaniem odszkodowań za wypadki w miejscu pracy lub działania różnicujące/ /dyskryminacyjne	sprawy pracownicze	odszkodowania, zasiłki i przedterminowe zwolnienia działalności związków zawodowych
		bezpieczne środowisko	generalna odpowiedzialność (wypadki typu: „pośliznął się i upadł” itd.) wydarzenia naruszające zasady bezpieczeństwa i zdrowie pracowników rekompensaty dla pracowników

		różnicowanie i dyskryminacja	wszystkie rodzaje dyskryminacji w miejscu pracy
Kwestie związane z klientami, produktami i działalnością	straty spowodowane nieumyślnie lub w wyniku zaniedbań w zakresie sprostania zobowiązaniom w stosunku do określonych klientów lub wynikiem z natury bądź konstrukcji produktu	odpowiedniość, ujawnianie, powiernictwo	naruszenie powiernictwa/przekroczenie wytycznych odpowiedniość/ujawnianie naruszenie prywatności agresywna sprzedaż prowadzenie fałszywych transakcji w celu wywołania wrażeń wzmożonego handlu nieodpowiednie wykorzystanie poufnych danych
		niewłaściwe praktyki i biznesowe lub rynkowe	antytrust niewłaściwe praktyki rynkowe i w zakresie dokonywanych transakcji manipulacja rynkiem dokonywanie transakcji papierami wartościowymi przez osoby mające dostęp do poufnych informacji (na rachunek instytucji) nielicencjonowana działalność pranie brudnych pieniędzy
		wady produktów	defekty produktów błędy modeli
		selekcja, patronat, ekspozycja	przekroczenie limitów ekspozycji klienta
		działalność doradcza	spory w temacie wyników działalności doradczej
Uszkodzenia aktywów rzeczowych	straty wynikłe z uszkodzenia bądź zniszczenia aktywów rzeczowych będące wynikiem katastrof naturalnych i innych wydarzeń	katastrofy i inne wydarzenia	katastrofy naturalne straty spowodowane przez ludzi spoza instytucji (terroryzm, wandalizm)
Zakłócenia działalności i zakłócenia systemów	straty w następstwie zakłócenia działalności i uszkodzenia systemów	systemy	hardware software telekomunikacja zakłócenia i przerwy w dostawie mediów

1	2	3	4
Zarządzanie realizacją, przekazaniem i procesami	straty w wyniku błędnego przeprowadzenia transakcji, błąd błędnego zarządzania procesem oraz będące następstwem relacji ze wszystkimi podmiotami uczestniczącymi w transakcji i dostawcami	transakcja (pozyskanie, przeprowadzenie, obsługa)	błędna komunikacja błędy danych (wprowadzanie, obsługa, ładowanie) przekroczony termin lub odpowiedzialność złe funkcjonowanie modelu/systemu błąd księgowy/przyjęcie błędnej jednostki niepoprawne funkcjonowanie innych procesów/zadań błędne dostarczenie niepoprawne zarządzanie zabezpieczeniem obsługa danych wyjściowych
		monitorowanie i raportowanie	niepełnienie obowiązku raportowania nieprawidłowe raporty (wystąpiła strata)
		pozyskanie klienta i dokumentacja	zagubienie dokumentacji klienta (pozwolen, zrzeczeń) zgubienie części lub całości dokumentacji prawnej
		zarządzanie rachunkiem klienta	nieautoryzowany dostęp do rachunku klienta strata w wyniku błędnego zapisu na koncie klienta utrata części lub całości aktywów klienta w wyniku zaniedbania
		strony transakcji	spory ze stronami transakcji nie będącymi klientami
		kontrahenci i dostawcy	outsourcing spory z dostawcami

Źródło: opracowano na podstawie: Basel Committee on Banking Supervision, *Working Paper on the Regulatory Treatment of Operational Risk*, BIS, wrzesień 2001.

Załącznik 2. Matryca linii biznesowych i rodzajów strat w ryzyku operacyjnym

Jednostki biznesowe	Linie biznesowe	Oszustwa wewnętrzne	Oszustwa zewnętrzne	Kwestie zatrudnienia i bezpieczeństwa w miejscu pracy	Kwestie związane z klientami, produktami i działalnością	Uszkodzenia aktywów rzeczowych	Zakłócenia działalności i zakłócenia systemów	Zarządzanie realizacją, przekazywaniem i procesami
Bankowość inwestycyjna	finanse przedsiębiorstw*							
	handel papierami wartościowymi							
	bankowość detaliczna							
	bankowość komercyjna							
	płatności i rozliczenia							
Inne	usługi pośrednictwa i przechowywania							
	zarządzanie aktywami							
	detaliczna działalność maklerska							

* Z uwzględnieniem finansów samorządowych i publicznych (municipal & government finance) oraz bankowości kupieckiej (merchant banking).

Źródło: opracowano na podstawie: Basel Committee on Banking Supervision, *Working Paper on the Regulatory Treatment of Operational Risk*, BIS, wrzesień 2001.