

POLITYKA ZARZĄDZANIA RYZYKIEM OPERACYJNYM W ŚWIETLE REKOMENDACJI M

Streszczenie

W opracowaniu poddano analizie krytycznej ogólne zapisy Rekomendacji M dotyczące zarządzania ryzykiem operacyjnym w bankach. Na ryzyko składają się cztery czynniki: błędy ludzi, systemów, procesów oraz zdarzenia zewnętrzne. W celu ukazania skutków złego zarządzania posłużono się przykładami upadków banków oraz zaprezentowano skalę oszustw wewnętrznych i zewnętrznych.

Słowa kluczowe: zarządzanie ryzykiem operacyjnym, Rekomendacja M, Bazylejski Komitet ds. Nadzoru Bankowego

Summary

Operational risk management policy in view of Recommendation M

This article aims at critical analysis of the M Recommendation which is related to the operational risk management in banks. Such risk may consist of four factors: human errors, system errors, process deficiencies as well as external influence. To exemplify the results of wrong risk management, some bank bankruptcy together with the scale of internal and external fraud have been presented.

Keywords: operational risk management, M Recommendation, Basel Committee on Banking Supervision (BCBS)

I. Ryzyko operacyjne w bankowości

W działalność banków wpisuje się wiele rodzajów ryzyk: ryzyko kredytowe (ryzyko transakcji, ryzyko koncentracji portfela), rynkowe (ryzyko stóp procentowych, walutowe, cen instrumentów kapitałowych, ryzyko cen towarów), ryzyko płynności, utraty reputacji, niewypłacalności oraz prawne [Żółtkowski, 2007: 26]. Obecność tylu rodzajów ryzyk jest spowodowana szybko zmieniającą się

¹ Doktorantka Wydziału Zarządzania i Komunikacji Społecznej UJ.

rzeczywistością, pojawianiem się nowych produktów finansowych, a co za tym idzie, wzrastającą niepewnością różnorodnych przedsięwzięć. W ostatnich kilkunastu latach wiele uwagi poświęcono zagadnieniom związanym z ryzykiem operacyjnym, mimo że nie jest ono nowym zagadnieniem. Powodem wzrostu zainteresowania banków tym rodzajem ryzyka są skutki, jakie ono z sobą niesie, co zostanie przedstawione w dalszej części niniejszego opracowania. Innymi powodami tego zainteresowania, według Joanny Krasodomskiej, są: automatyzacja technologii, rozwój e-commerce, fuzje, zróżnicowanie działalności usługowej banków, coraz częstsze stosowanie outsourcingu, które doprowadziły do powstawania strat [Krasodomska, 2008: 24].

Bazylejski Komitet ds. Nadzoru Bankowego (BCBS) jest najważniejszą instytucją, której zadaniem jest opracowywanie bankowych norm ostrożnościowych. Wspomniane regulacje nie mają mocy prawnej, ale większość państw działających na międzynarodowym rynku bankowym wdraża je do krajowych systemów bankowych. Co więcej, stopień ich wdrożenia stanowi podstawę do oceny stabilności i bezpieczeństwa funkcjonujących systemów przez Międzynarodowy Fundusz Walutowy i Bank Światowy.

Bardzo ważnym dokumentem regulującym działalność banków jest Nowa Umowa Kapitałowa inaczej nazwana Basel II. Opracowany w 1999 roku dokument został poddany konsultacjom międzynarodowym, w rezultacie czego powstało około 200 komentarzy specjalistów z dziedziny bankowości, przedstawicieli instytucji finansowych oraz osób sprawujących nadzór. Po uwzględnieniu zgłoszonych poprawek opracowano I Dokument Konsultacyjny, którego celem było wprowadzenie stabilności i bezpieczeństwa sektora bankowego. W latach 2001 i 2003 powstały kolejne dwa dokumenty konsultacyjne, ostateczna wersja Nowej Umowy Kapitałowej (NUK) powstała w 2004 roku [Krasodomska, 2008: 52]. Nowa Umowa Kapitałowa składa się z trzech filarów. W dużym uproszczeniu pierwszy filar to regulacje dotyczące minimalnych wymogów kapitałowych przewidzianych do pokrycia strat wynikających z ryzyka operacyjnego, kredytowego i rynkowego w wysokości co najmniej 8% wartości aktywów i zobowiązań pozabilansowych ważonych ryzykiem. W drugim filarze pojawiło się ważne zagadnienie, to znaczy banki powinny posiadać system pomiaru i oceny ponoszonego ryzyka, wraz z opracowanym procesem wyliczenia kapitału adekwatnego do poziomu ryzyka. Wymienione czynności podlegają weryfikacji dokonywanej przez instytucje nadzorcze [Matkowski, 2006: 69]. Jak zauważa Wiesław Thor, esencją II filaru jest optymalizacja wymogów kapitałowych przez profilowanie ryzyka i efektywne wdrażanie strategii związanych z ryzykiem, mających na celu zapewnienie wewnętrznego ładu.

W ramach drugiego filaru banki opracowują strategie i polityki zarządzania poszczególnymi ryzykami w tym również ryzykiem operacyjnym, a także procedury bezpiecznego i stabilnego zarządzania bankiem i inne dokumenty [Thor, 2008: 8–10].

W ten filar wpisuje się główny dokument dotyczący zasad zarządzania ryzykiem operacyjnym, jakim jest Rekomendacja M oparta na „Zasadach Dobrej Praktyki w Zakresie Zarządzania i Nadzoru nad Ryzykiem Operacyjnym” opu-

blikowana przez BCBS w lutym 2003 roku. Bazylejski Komitet zdefiniował ryzyko operacyjne jako „ryzyko straty wynikającej z niedostosowania lub zawodności wewnętrznych procesów, ludzi i systemów technicznych lub ze zdarzeń zewnętrznych, takich jak katastrofy, kataklizmy” [Rekomendacja M..., 2004: 3]. Przytoczona definicja jest bardzo złożona i zawiera cztery podstawowe elementy: procesy, ludzie, systemy techniczne i zdarzenia zewnętrzne.

W literaturze można znaleźć wiele definicji określających w sposób bardziej precyzyjny zagadnienie ryzyka operacyjnego. W tabeli 1 przedstawiono wyniki kompilacji definicji opracowanych przez wybranych autorów.

Tabela 1

Zestawienie kategorii ryzyka operacyjnego według różnych autorów

| Rekomendacja M | D. N. Chorofas | J. Krasodomska, L. Sołtysik |
|---|--|---|
| Ryzyko 7 kategorii: – oszustwo wewnętrzne; – oszustwo zewnętrzne; – praktyka kadrowa i bezpieczeństwo pracy; – klienci, produkty i praktyka biznesowa; – uszkodzenie aktywów; – zakłócenia działalności banku i błędy systemów; – dokonywanie transakcji, dostawa i zarządzanie procesami. | – ryzyko niewłaściwego nadzoru; – ryzyko niewłaściwego zarządzania; – ryzyko braku profesjonalizmu; – ryzyko transakcyjne; – ryzyko związane z płatnościami, zawartymi umowami; – ryzyko naruszenia bezpieczeństwa; – ryzyko technologiczne. | – ryzyko kadrowe (kwalifikacje pracowników, celowe lub niezamierzone działanie na szkodę spółki, kultura organizacji, dostępność kadry); – ryzyko relacji ze środowiskiem biznesowym (relacje z klientami, akcjonariuszami, organami nadzoru); – ryzyko technologiczne (sprawność systemów IT, adekwatność wyposażenia, dostawy podstawowych usług); – ryzyko materialne i zdarzeń losowych. |
| I. Staniec, K.M. Klimczak | W. Żółtkowski | J. Bessis |
| – rodzaje ryzyka zgodne z Rekomendacją M | – ryzyko niekompetencji lub złej woli, pracowników; – wadliwe działanie systemów informatycznych; – niefunkcjonalne struktury organizacyjne; – ryzyko operacyjne obejmuje część ryzyka prawnego. | – ryzyko złego funkcjonowania systemów informatycznych, raportowania, monitorowania, polityki banku i procedur. |

Źródło: opracowanie własne na podstawie: Rekomendacja...: 3–5; Krasodomska: 18–19; Żółtkowski, 2007: 27; Staniec, 2008: 36–37.

Analizując tabelę 1, można stwierdzić, że przytoczone definicje poszczególnych autorów wpisują się w nurt definicji opracowanej przez Bazylejski Komitet ds. Nadzoru Bankowego, co w praktyce oznacza zgodność zagadnień związanych z ryzykiem operacyjnym.

Jest to bardzo ważne, ponieważ, jak zauważa Paweł Matkowski, efektywność systemu zarządzania zależy od sposobu zdefiniowania ryzyka operacyjnego. Wspomniana jednomyślność znajduje ponadto odbicie w przyjętych definicjach banków [Matkowski, 2006: 27–30].

W 2002 roku zostało przeprowadzone przez Risk Management Association badanie udziału czynników związanych z ryzykiem operacyjnym. Stwierdzono, że 64% ryzyka generują procesy, 25% ludzie, 7% zdarzenia, a najmniej, bo tylko 2% zdarzeń – systemy [Matkowski, 2006: 26; Staniec, Klimczak, 2008: 36]. Uważa się, że działaniu ludzkiemu powinna zostać przypisana większa niż 25% wartość ryzyka, ponieważ po pierwsze procedury (opracowanie i ich przestrzeganie) są wynikiem pracy ludzi, po drugie, nawet jeśli, procedury spełniają swoje zadanie, to pracownik czy też klient w każdej chwili może ulec słabości, presji czy okazji i odpowiednio dopuścić się oszustwa wewnętrznego lub zewnętrznego.

2. Skutki złego zarządzania ryzykiem operacyjnym

Zanim zaczęto zwracać uwagę na kwestię systemowego zarządzania ryzykiem operacyjnym wydarzyło się wiele spektakularnych strat. Za przykład może posłużyć przypadek Barings Bank, który został założony w 1792 roku. Cieszył się on dużą popularnością wśród klientów zamożnych, a także wielkich korporacji. Nick Leeson, były pracownik banku inwestycyjnego Morgan Stanley został odelegowany do pracy w Singapurze, ponieważ z powodu toczącego się postępowania karnego nie mógł podjąć pracy w Londynie. Do jego zadań należały transakcje arbitrażowe na giełdzie w Osace i Singapurze, czyli zakup papierów na jednej giełdzie i sprzedaż na drugiej. W pewnym momencie Leeson zaczął zajmować pozycje niezabezpieczone – kupował kontrakty bez jednoczesnej sprzedaży na drugim rynku. Jego działanie przekształciło bezpieczny portfel w uzależniony od indeksu Nikkei 225. Przełożeni Leesona nie mieli o tym pojęcia. W Japonii doszło do trzęsienia ziemi i indeks zaczął drastycznie tracić na wartości. Leeson, zamiast pozbywać się niezabezpieczonych pozycji, zwiększał zaangażowanie. Jednocześnie wprowadzał do systemu fałszywe rachunki, na których wykazywał osiągnane zyski. W celu likwidacji strat stosował różne strategie, ale nie przyniosły one oczekiwanego skutku. Najstarszy bank poniósł stratę w wysokości około 1 mld funtów i w rezultacie został przejęty przez ING za symbolicznego funta.

W raporcie diagnozującym przyczyny bankructwa stwierdzono, że główne czynniki, które doprowadziły do upadku banku, to:

- straty wynikłe z nieautoryzowanych i ukrywanych transakcji przeprowadzonych przez Leesona
- słaby system kontroli, który mimo niejasności zatwierdzał legalność zysków
- naruszenie wszelkich procedur operacyjnych, na przykład bez zgody banku centralnego przekazano do singapurskiego oddziału dwukrotną war-

tość aktywów całego banku (800 mln funtów), mimo że bez uzyskanej zgody można przełać jednorazowo maksymalnie 25% wartości kapitału własnego na jedną inwestycję

- nierzetelność dokumentacji i audytów zewnętrznych [Masiukiewicz, 2009: 68–87; Efix Polska, 2008: 1–4].

Kolejnym przykładem znaczących strat dokonanych przez pracownika jest przypadek Banku Societe General; na początku 2008 roku świat obiegła elektryzująca wiadomość o oszustwie na kwotę 4,9 mld euro, którego dokonał jeden pracownik, Jecrome Kerviel. Władze banku stwierdziły, „że operacje były proste, ale posłużył się on wyrafinowanymi metodami ukrycia swoich działań, do tego stopnia, że dział audytu miał duże trudności w zrozumieniu transakcji zrealizowanych przez Jecroma” [Masiukiewicz, 2009: 93]. Podobnie jak w poprzednim przypadku naruszono wiele obowiązujących zasad. Jednym z motywów działania Kervielu była chęć udowodnienia za wszelką cenę swoich wyjątkowych uzdolnień przez stosowanie różnych skomplikowanych strategii. W 2005 roku zaczął spekulować na indeksach giełdowych, jednocześnie wprowadzając fałszywe wartości hedgingowe do systemu zarządzania ryzykiem. Jego działania przyniosły zysk o łącznej kwocie 1,4 mld euro, ale ujawnił on sumę 55 mln euro zysków, która była i tak mało prawdopodobna do osiągnięcia w najniższym co do hierarchii dziale banku, nie wzbudziła zainteresowania. Ani władze banku, ani dział kontroli nie zareagowały na informację o 74-krotnym przekroczeniu dopuszczalnych limitów, o czym sygnalizował system [Masiukiewicz, 2009: 93–99]. Kerviel bronił się, że władze banku doskonale wiedziały o całym procederze, co więcej, nawet był zachęcany przez zwiększenie pułapu spekulacyjnego. Został skazany na 5 lat więzienia i naprawienie szkody w wysokości 4,9 mld euro².

Oprócz przytoczonych przypadków w historii wystąpiło kilka innych spektakularnych strat spowodowanych przez jednego pracownika. John Rusnak naraził Allied Irish Bank na straty w wysokości 691 mln USD. W Banku of Credit and Commerce International (BCCI) zdefraudowano 10 mld dolarów z oszczędności klientów, Daiwa Bank poniósł stratę w wysokości 1 mld dolarów, Dexia Bank stracił 100 mln dolarów przez działania pracownika. Bank Credit Lyonnais stracił według różnych źródeł do 50 do 100 mld FRF (ok. 17 mld dolarów) [Krasodomska, 2008: 24–28]. Powyższe przykłady obrazują skalę zagrożenia, jakie niesie złe zarządzanie ryzykiem operacyjnym, co więcej, bardzo często przekłada się ono na zachwianie stabilności sektora bankowego i całej gospodarki. W związku z tym w skrajnych sytuacjach – zagrożenia ryzykiem upadku banku – dopuszczono możliwość udzielenia pomocy publicznej. Jak zauważa P. Masiukiewicz, za interwencjonizmem państwowym przemawiają następujące fakty:

- społeczny zasięg usług bankowych (60–90% społeczeństwa korzysta ze wspomnianych usług)
- kredytowanie rozwoju gospodarki

² Wywiad z J. Kervielem: Pauly C., <http://biznes.onet.pl/bylem-tylko-malym-trybikiem,18595,4097786,1,prasa-detaj> (dostęp: 8.01. 2011).

- przejmowanie części ryzyka od kredytobiorców
- prowadzenie rozliczeń krajowych i zagranicznych [Masiukiewicz, 2009: 15].

Istotna rola banków w gospodarce oraz spektakularne straty, które zdestabilizowały system finansowy skłoniły Bazylejski Komitet Nadzoru Bankowego do opracowania wytycznych zarządzania ryzykiem operacyjnym, które zostały zawarte w Rekomendacji M.

3. Krytyczna analiza Rekomendacji M

Podstawą prawną Rekomendacji M jest art. 137 pkt 5 ustawy „Prawo bankowe”, w świetle którego Komisja Nadzoru Finansowego może wydawać rekomendacje dotyczące dobrych praktyk i stabilnego zarządzania bankami. Wspomniany dokument składa się zasadniczo z trzech części: wprowadzenia do zagadnienia ryzyka operacyjnego, 10 rekomendacji oraz komentarza. W tabeli 2 przedstawiono dokładne brzmienie wszystkich zaleceń.

Tabela 2

10 rekomendacji dotyczących zarządzania ryzykiem operacyjnym w bankach opracowanych przez Komisję Nadzoru Bankowego

| Rekomendacja 1 | Rekomendacja 2 |
|---|---|
| Członkowie organów banku – rady nadzorczej i zarządu banku – powinni być świadomi ważnych aspektów ryzyka operacyjnego w banku, jako odrębnego i podlegającego zarządzaniu rodzaju ryzyka i powinni znać profil ryzyka wynikającego z działalności banku. | Rada nadzorcza w ramach wypełniania swoich funkcji zatwierdza (akceptuje) opracowane przez zarząd założenia strategii prowadzenia działalności. Założenia te powinny uwzględniać występowanie ryzyka operacyjnego wynikającego z działalności banku, a w szczególności określać ogólne zasady zarządzania tym ryzykiem . Rada nadzorcza powinna dokonywać okresowej oceny realizacji przez zarząd założeń strategii (w szczególności w odniesieniu do zasad zarządzania ryzykiem operacyjnym banku). W tym celu zarząd banku powinien okresowo przedkładać radzie nadzorczej syntetyczną informację na temat skali i rodzajów ryzyka operacyjnego, na które narażony jest bank, prawdopodobieństwa jego występowania, jego skutków i metod zarządzania ryzykiem operacyjnym. |

| | |
|---|---|
| <p>Rekomendacja 3</p> <p>Zarząd banku odpowiada za opracowanie i wdrożenie strategii zarządzania ryzykiem, w tym za zorganizowanie i funkcjonowanie procesu zarządzania ryzykiem operacyjnym oraz, jeśli to konieczne – wprowadzanie niezbędnych korekt w celu usprawnienia tego procesu. Zasady i procedury zarządzania ryzykiem operacyjnym powinny obejmować pełen zakres działalności banku.</p> | <p>Rekomendacja 4</p> <p>Kontrola i ocena systemu zarządzania ryzykiem operacyjnym oraz jego regularne przeglądy powinny być dokonywane przez komórkę audytu wewnętrznego, niezależną pod względem operacyjnym i zatrudniającą kompetentny, odpowiednio wyszkolony personel. Rada nadzorcza sprawuje nadzór nad kontrolą systemu zarządzania ryzykiem operacyjnym oraz ocenia jej adekwatność i skuteczność.</p> |
| <p>Rekomendacja 5</p> <p>W banku powinny w jasny sposób zostać określone kompetencje oraz schematy podległości służbowej w obszarze zarządzania ryzykiem operacyjnym na różnych szczeblach organizacyjnych.</p> | <p>Rekomendacja 6</p> <p>W banku powinien istnieć udokumentowany proces identyfikacji i oceny zagrożeń związanych z ryzykiem operacyjnym dla wszystkich istotnych obszarów działalności banku oraz wszelkich nowych produktów, procesów i systemów. Identyfikacja i ocena ryzyka operacyjnego wynikającego z nowych produktów, zachodzących procesów i wykorzystywanych systemów powinny nastąpić przed ich wprowadzeniem w życie i zastosowaniem. Bank powinien posiadać udokumentowany proces: oceny wrażliwości banku na zidentyfikowane zagrożenia, badania ich możliwego wpływu na wynik z działalności oraz określenia możliwych zabezpieczeń.</p> |
| <p>Rekomendacja 7</p> <p>Wdrożony w banku system regularnego monitorowania zdarzeń operacyjnych powinien umożliwiać obserwację profilu ryzyka operacyjnego oraz regularne przekazywanie zarządowi informacji w tym zakresie.</p> | <p>Rekomendacja 8</p> <p>Bank powinien dokonywać okresowej weryfikacji skuteczności funkcjonowania wdrożonego systemu zarządzania ryzykiem operacyjnym oraz jego adekwatności do aktualnego profilu ryzyka banku.</p> |
| <p>Rekomendacja 9</p> <p>Bank powinien posiadać plany utrzymania ciągłości działania (w tym plany awaryjne), zapewniające nieprzerwane działanie banku na określonym poziomie, uwzględniające kategorie i czynniki ryzyka operacyjnego.</p> | <p>Rekomendacja 10</p> <p>Bank powinien ujawniać otoczeniu rynkowemu informacje umożliwiające dokonanie oceny stosunku banku do zarządzania ryzykiem operacyjnym.</p> |

Źródło: opracowanie własne na podstawie: Rekomendacja...: 12–13.

W komentarzu Komitetu Nadzoru Bankowego do Rekomendacji nr 1 i 2 pojawiło się stwierdzenie, że nieznajomość profilu ryzyka może wpływać negatywnie na jakość strategii zarządzania ryzykiem operacyjnym i w rezultacie przekłada się na wzrost tego ryzyka. Uważa się, że nieznajomość profilu ryzyka ma dużo bardziej poważne konsekwencje dla banku i zarazem jego otoczenia niż

tylko obniżenie jakości strategii. Za słuszością tego stwierdzenia przemawiają przytoczone przykłady historii upadku banków. Jak zauważa Thlon, przeinwestowanie doprowadziło do upadku Lehmans Brothers, w wyniku czego wartość notowanych firm na nowojorskiej giełdzie spadła o 400 mld dolarów (!) [Thlon, 2008]. W Rekomendacji nr 2 pojawia się stwierdzenie, że strategia powinna zawierać ogólne zasady zarządzania ryzykiem operacyjnym. Uważa się, że powinny być one precyzyjnie określone, ale przy zachowaniu równowagi, to znaczy że nie mogą one znacząco utrudniać prowadzenia działalności, aby tak się nie stało, powinny być wyznaczone ramy czy też kierunki tego zarządzania. W drugiej części Rekomendacji nr 2 Radę Nadzorczą zobowiązano do okresowej oceny realizacji strategii. Można zadać pytanie, co oznacza termin okresowa ocena. W jednym banku będzie ona dokonywana raz na dwa lata, a w innym raz na trzy miesiące. W wypadku powstania znaczącej straty operacyjnej pierwszy bank stwierdzi, że działał zgodnie z Rekomendacją M, ponieważ okresowo dokonywał oceny. W wypadku drugiego banku będzie mniejsze prawdopodobieństwo powstania strat operacyjnych. Tym bardziej zastanawia niewyznaczenie minimalnego okresu ponownej weryfikacji, skoro w komentarzu do obu rekomendacji stwierdzono, że czynniki wewnętrzne i zewnętrzne kształtujące ryzyko bardzo szybko się zmieniają. Dopiero w komentarzu do Rekomendacji nr 3 zostały zawarte bardziej szczegółowe wskazania dotyczące niezbędnych elementów strategii, takich jak: definicja ryzyka operacyjnego, profil ryzyka, zasady zarządzania i kontroli wewnętrznej [Rekomendacja..., 2004: 15–16].

W Rekomendacji nr 4 ponownie powraca problem nieścisłych wyrażań, to znaczy: regularnych przeglądów systemu zarządzania ryzykiem operacyjnym, które są dokonywane przez komórkę audytu wewnętrznego. W komentarzu do tej Rekomendacji położono nacisk na ryzyko operacyjne wynikające z nowych produktów lub wejścia na nowe rynki. Z drugiej strony nie dostrzega się znaczenia łamania procedur i sposobu ujęcia zagadnień związanych z ryzykiem w codziennej działalności, które zostaną przedstawione w dalszej części opracowania. Rekomendacje nr 5 i 6 nie budzą zastrzeżeń. W kolejnym zaleceniu nr 7 ponownie pojawia się kwestia nieprecyzyjnego słownictwa, mowa jest o regularnym monitorowaniu zasadniczych dla organizacji zdarzeń operacyjnych. Nadal jest aktualne pytanie, jak często powinien być sprawowany przegląd istotnych procesów. W komentarzu do tej Rekomendacji stwierdzono, że takie czynniki, jak poziom ryzyka operacyjnego, wrażliwość banku na to ryzyko, częstotliwość i natura zmian o charakterze operacyjnym określają częstotliwość i złożoność systemu monitorowania [Rekomendacja..., 2004: 21].

Przytoczone stwierdzenie można zinterpretować w ten sposób, że banki, które zdiagnozowały niski poziom ryzyka operacyjnego, mogą stosunkowo rzadziej monitorować to ryzyko. Tym bardziej że zdarzenia, które generują znaczące straty, stosunkowo rzadko występują w przeciwieństwie do częstych, ale małych strat. W banku, w którym nie odnotowano żadnych poważniejszych zdarzeń operacyjnych, może zostać uśpiona czujność, aż do czasu pojawienia się wydarzeń o katastrofalnych skutkach jak to się wydarzyło w przypadku Banku Lehmans Brother.

Po fali rekordowych zysków, po podniesieniu długoterminowych ratingów z A na A+, po szeregu tytułów najlepszego banku inwestycyjnego i licznych wyróżnień, w tym za system zarządzania ryzykiem, w 2008 roku następuje kryzys związany z kredytami hipotecznymi, na których rynku wspomniany bank zainwestował 60 mld dolarów. Mimo podjętych działań naprawczych i dokapitalizowaniu 158-letni bank ogłasza bankructwo [Thlon, 2008]. Regularna kontrola i monitoring wraz z rozważą w inwestowaniu być może uchroniłyby ten bank przed tak spektakularnym upadkiem.

W drugiej części Rekomendacji nr 7 pojawia się kwestia regularnego raportowania. W komentarzu występuje stwierdzenie, że częstotliwość raportowania powinna być uzależniona od skali działalności, profilu ryzyka i stopnia złożoności prowadzonej działalności. Można zadać pytanie, czy banki zatrudniające stosunkowo niewiele osób mogą rzadziej wysyłać raporty? W małych oddziałach banków dochodzi najczęściej do nadużyć; nie w centralach, chociaż i tam zdarzają się nadużycia... Zaleca się ponadto, aby bank dokonywał okresowej oceny operacji pod kątem ich funkcjonowania, dostosowania do faktycznych i potencjalnych zmian oraz zdolności ograniczania lub powstawania strat. Uważa się, że powinny zostać określone ramy czasowe tej kontroli, ponieważ to ona może być jedną z gwarancji bezpieczeństwa.

Analizowane zagadnienie potwierdza, że banki mają problemy ze skuteczną kontrolą procesów operacyjnych. Przykładowo w jednym z banków pracownicy centrali przeprowadzili kontrolę, która nie wykazała żadnych nieprawidłowości, miesiąc później klientka złożyła reklamację, że nie zleciła likwidacji lokaty. Po ponownej kontroli okazało się, że pracownik banku zlikwidował 26 lokat, wypłacając sobie odsetki, i po kilku dniach odnawiał lokaty. Proceder trwał trzy miesiące, w trakcie których odbyła się wspomniana nieskuteczna kontrola, strata wyniosła 73 tys. zł³.

Kolejna Rekomendacja również dotyczy okresowej weryfikacji adekwatności systemu zarządzania ryzykiem operacyjnym do aktualnego profilu ryzyka banku. W komentarzu stwierdzono, że dostosowanie wspomnianego systemu zarządzania do profilu ryzyka jest ważne ze względu na jakość zarządzania. Jak wspomniano na początku, niewłaściwe zarządzanie ryzykiem operacyjnym pociąga za sobą dużo bardziej poważne konsekwencje niż obniżenie jakości. Komentarz do Rekomendacji nr 9 zawiera niepokojące stwierdzenie, że bank powinien podjąć decyzje co do traktowania poszczególnych kategorii zidentyfikowanego ryzyka operacyjnego:

- przez uruchomienie procedury kontroli i/lub ograniczania ryzyka
- przez świadomą rezygnację ze stosowania zabezpieczeń [Rekomendacja..., 2004: 24].

Przytoczony zapis jest zaskakujący z dwóch powodów. Po pierwsze, znalazł się on w przepisach, które pełnią funkcję prewencyjną, po drugie stało się to po licznych stratach, które wydarzyły się w historii bankowości, a wynikały z podejmowania nadmiernego ryzyka. Skutkiem rezygnacji ze stosowania zabezpie-

³ Badania własne przeprowadzone w latach 2005–2009 w jednej z dzielnic Krakowa.

czeń była strata Allfirst Banku wynosząca 691 mln dolarów, spowodowana tym, że John Rusnak między innymi przekonał swoich współpracowników o braku konieczności prowadzenia działań asekuracyjnych [Krasodomska, 2008: 27]. Wielu innych maklerów postępowало w podobny sposób: albo lekceważyli komunikaty systemu (Kerviel), albo samodzielnie podejmowali ryzyko przekraczające wszelkie dopuszczalne normy (Iguchi i inni). Zamiast dołożyć wszelkich starań, aby zminimalizować powstawanie zagrożeń przez odpowiednie regulacje prawne, wydaje się, że zostawiono furtkę prowadzącą do powstawania porównywalnych zagrożeń. Można rozważyć hipotetyczną sytuację, w której makler zgodnie z dobrą wolą rezygnuje z zabezpieczeń i inwestuje w nowy rynek. W wypadku powstania strat o znacznej wartości prawdopodobnie użyje argumentów, że znał wagę ryzyka operacyjnego, działał zgodnie z systemem zarządzania tym ryzykiem i podjął dozwolone przez prawo kroki – świadomie zrezygnował z zabezpieczenia, ale nie spodziewał się takich rezultatów – czyli w skrajnym przypadku, zachwiania stabilności systemu bankowego bankowego.

4. Oszustwa wewnętrzne

Wielkie oszustwa nie są domeną jedynie zagranicznych banków, zdarzają się również na rodzimym rynku. Na podstawie przytoczonych poniżej przykładów można dojść do wniosku, że Rekomendacja M mało efektywnie spełnia funkcję prewencyjną. Pierwszy przykład oszustwa wewnętrznego dotyczy dwóch pracowników banku, które wyłudziły łącznie 100 kredytów na kwotę 2 mln zł. Proceder trwał od 2004 do 2009 roku. Jedną z kobiet miała stosunkowo długi staż pracy, bo od 1991 roku, i była uważana za dobrą pracownicę aż do maja 2009 roku, kiedy to do banku zgłosił się prawnik jednego z klientów, który rzekomo wziął kredyt. Kobieta przyznała się do wykorzystania danych klientów, ich podpisów oraz posłużenia się sfałszowanymi zaświadczeniami o zatrudnieniu. Pojawia się pytanie, jak to możliwe, żeby przez sześć lat skutecznie ukrywać cały proceder przy obowiązującej od pięciu lat Rekomendacji M. Przełożeni pracownicy tłumaczyli, że akceptowali wnioski, ale nie musieli przy tym widzieć kredytobiorców [Kołakowska, 2010]. Inny przypadek tym razem 24-letniego pracownika banku, który próbował wyłudzić kwotę 2 mln zł. W tym celu otworzył konta w trzech różnych bankach, i mając dostęp do danych klientów i wzorów ich podpisów, przelewał środki pieniężne na przygotowane konta. Na trop wpadła policja. Można postawić następujące pytanie: w jaki sposób funkcjonował system zarządzania ryzykiem operacyjnym, kontroli i zarządzania podstawowymi procesami, skoro ważnym elementem w tym zagadnieniu są oszustwa wewnętrzne i zewnętrzne? Te same pytania przychodzą na myśl po przeczytaniu artykułu, w którym opisano kobietę skazaną za kradzież kwoty 1 mln zł z kont zamożnych klientów. Motywem sprzecznego z prawem działania była chęć otwarcia własnego baru. Przytoczone przypadki w niewielkim stopniu ilustrują skalę oszustw wewnętrznych. Wystarczy uważnie śledzić prasę, aby co pewien czas

znaleźć podobne tytuły: *Ukradli bankowi 8,5 mln zł. Pomógł doradca VIP, CBA zatrzymało bankowców za oszustwa i fałszerstwa* (kwota 7 mln zł), *Pracownik banku okradal klientów* [Kobiąłka, 2010; Kołakowska, 2010; „Gazeta Wyborcza” – Stołeczna, 2008; „Gazeta Wyborcza” – Bydgoszcz, 2008]. Na marginesie należy dodać, że wszystkie przytoczone informacje pojawiały się w prasie na przestrzeni 2007–2010 roku, czyli w czasie obowiązywania wytycznych Komitetu Bazylejskiego.

Należy zadać pytanie, jak się mają ogólne zapisy Rekomendacji M (świadomość rady nadzorczej i zarządu o wadze ryzyka operacyjnego, ogólne zasady formułowania strategii, okresowa weryfikacja systemu zarządzania ryzykiem operacyjnym, regularna sprawozdawczość) do wyżej wymienionych przykładów oszustw wewnętrznych.

Istnieje rozdzwięk pomiędzy przytoczonymi zapisami a praktyką – oprócz oszustw popełnionych przez pracowników istnieją sprzeczne z prawem działania klientów.

5. Skala oszustw zewnętrznych

Jednym z powodów wybrania do badań zagadnienia oszustw zewnętrznych był między innymi związek z ryzykiem operacyjnym. Analizie zostały poddane sprawy karne jednej z dzielnic Krakowa za okres 2005–2009. Akta spraw karnych wybrano na podstawie zbieżności artykułów kodeksu karnego z czynnikami definiującymi ryzyko operacyjne – w szczególności oszustw dokonanych przez pracowników i klientów. Wybrano następujące artykuły kodeksu karnego:

- Art. 286 §1 KK (oszustwo);
- Art. 297§1 KK (oszustwo kredytowe);
- Art. 284§2 KK (przywłaszczenie);
- Art. 270§1 KK (fałszerstwo).

W wyniku przeprowadzonej analizy uzyskano następujące wyniki:

- 1) 284 postępowania karne odbyły się w jednej z dzielnic Krakowa z powodu oszustw dokonanych w bankach w latach 2005–2009, co stanowi 77% wszystkich spraw z czterech rodzajów instytucji – banku, przedsiębiorstwa, instytucji finansowej, instytucji pożyczkowej.
- 2) Udzielono kredytów na podstawie bardzo słabej weryfikacji na kwotę 3 146 688 zł.
- 3) Zdemaskowano próby wyłudzeń kredytów na kwotę 1 409 699 zł⁴.

Powodem tak dużej skali zjawiska oszustw dokonanych przez pracowników i klientów jest przede wszystkim zaniedbanie obowiązujących procedur oraz kontroli wewnętrznej. Duża wina leży po stronie pracowników, którzy bardzo powierzchownie, a czasem w ogóle nie przeprowadzają weryfikacji klientów. Można odnieść wrażenie, że kierownictwo nie sprawdza zrealizowanych opera-

⁴ Badania własne.

cji, ponieważ w trakcie działań windykacyjnych okazuje się, że dana osoba nie jest pracownikiem firmy z przedstawionego zaświadczenia, mimo udzielonego kredytu i pierwszej, pozytywnej, weryfikacji.

6. Wnioski

- **Zapisy Rekomendacji M są zbyt ogólne**, w szczególności gdy dotyczą ogólnych zasad zarządzania ryzykiem operacyjnym, okresowej kontroli, regularnej sprawozdawczości, oceny systemu. Co więcej, w komentarzu znajduje się sugestia na temat podjęcia ryzyka przez świadomą rezygnację z zabezpieczeń w określonych przypadkach.
- **Zbyt mało uwagi poświęcono procesom kontroli, weryfikacji i odpowiedzialności** – gruntowna kontrola zaczyna się dopiero po wystąpieniu nieprawidłowości, tak jak to zdarzyło się w przypadku kobiet, które wylądowały kredyty o wartości 2 mln zł; po wykryciu nieprawidłowości sprawą zajął się departament audytu i departament bezpieczeństwa banku.
- **Problemy z podejściem do tematu zarządzania ryzykiem** – z jednej strony mamy do czynienia z oszustwami, czyli celowym obejściem przepisów prawa, z drugiej strony z ryzykiem kredytowym, które jest definiowane jako strata wynikająca z niewywiązania się klienta z jego zobowiązań wobec banku. Rekomendacja M podkreśla celowość zamiaru dokonania oszustwa, a jednocześnie wadliwa weryfikacja i zarządzanie ryzykiem kredytowym banku nie wychwytuje tych zamiarów, ponieważ zakłada rzetelną spłatę. Osoba dopuszczająca się oszustwa z góry wie, że nie da rady spłacić zobowiązania, ponieważ gdyby to było możliwe, starałaby się o kredyt, posiadając prawdziwe dokumenty.
- **Działalność banków** – przypatrując się temu zagadnieniu, można odnieść wrażenie, że banki całkowicie lekceważą zagrożenie z tytułu oszustw. Jeden z banków kusi promocją – ofertą kredytu na kwotę 20 000 zł bez zaświadczeń, na podstawie dowodu osobistego i oświadczenia o zatrudnieniu. Istnieje różnica pomiędzy zaświadczeniem, na którym figuruje pieczętka firmy z adresem, numerem telefonu, podpisem osoby upoważnionej a oświadczeniem ustnym. W przypadku spraw karnych z elementem fałszerstwa bada się różnice między pieczętką oryginalną a podrobioną.

Być może w rozwiązaniu problemów związanych z zarządzaniem ryzykiem operacyjnym pomocne byłoby ściśle określenie przepisów, które regulowałyby wspomniane kwestie. Analizując Nową Umowę Kapitałową, można odnieść wrażenie, że Bazylejski Komitet ds. Nadzoru Bankowego położył nacisk raczej na neutralizację skutków wystąpienia strat operacyjnych niż na prewencję. O tym świadczą zalecenia skoncentrowane na metodach wyliczenia wielkości kapitału wewnętrznego. Nie neguje się stosowania tego typu zabezpieczeń, ale w myśl przysłowia – lepiej zapobiegać, niż leczyć.

Rekomendacja M ma jednak charakter dobrych praktyk i banki mogą w różny sposób implementować zapisy, ale gdyby zostały określone minimalne wymogi, na przykład sprawdzanie adekwatności systemu, sprawozdawczości czy też innych omówionych czynności, zwiększyłaby się skuteczność funkcji prewencyjnej tych przepisów.

Literatura

- Efix Polska (2008), *Z cyklu wielkie upadki, czyli o zarządzaniu ryzykiem. Historia Barings Bank LTD*, <http://www.efixpolska.com/C/P/doc/Dokumenty/0070AkademiaEfixa.html> (dostęp: 15.02.2011).
- „Gazeta Wyborcza” – Bydgoszcz (2008), *Ukradli bankowi 8,5 mln zł* [dok. elektr.] http://szukaj.wyborcza.pl/Archiwum/1,0,5133691,20080703BY-DLO,Ukradli_bankowi_85 mln_zl.html (dostęp: 15.12.2010).
- „Gazeta Wyborcza” – Stołeczna (2008), *Nieuczciwy bankowiec chciał ukraść miliony* [dok. elektr.] <http://gospodarka.gazeta.pl/gospodarka/1,33181,5824971.html> (dostęp: 15.12.2010).
- Kobiałka M. (2010), *CBA zatrzymało bankowców. Za oszustwa i fałszerstwa*, „Gazeta Wyborcza” [dok. elektr.] http://rzeszow.gazeta.pl/rzeszow/1,34975,8585133,CBA_zatrzymalo_bankowcow__Za_oszustwa_i_falszerstwa.html#ixzz17jfpqhQn (dostęp: 15.12.2010).
- Kołąkowska A. (2010), *Pracownica wyludziła 100 kredytów za ponad 2 mln zł*, „Gazeta Wyborcza” [dok. elektr.] http://lodz.gazeta.pl/lodz/1,90280,8597391,Pracownica_wyludzila_100_kredytow_za_ponad_2 mln_zl.html#ixzz17jhhd3H (dostęp: 15.12.2010).
- Krasodomska J. (2008), *Zarządzanie ryzykiem operacyjnym w bankach*, Polskie Wydawnictwo Ekonomiczne, Warszawa.
- Masiukiewicz P. (2009), *Międzynarodowe bankructwa i afery bankowe*, SGH, Warszawa.
- Matkowski P. (2006), *Zarządzanie ryzykiem operacyjnym*, Oficyna Ekonomiczna Wolters Kluwer Polska, Kraków.
- Pauly C. (2011), *Byłem tylko małym trybikiem*, [dok. elektr.] <http://biznes.onet.pl/bylem-tylko-malym-trybikiem,18595,4097786,1,prasa-detat> (dostęp: 8.01.2011).
- Rekomendacja M dotycząca zarządzania ryzykiem operacyjnym w bankach* (2004), Komisja Nadzoru Bankowego, Warszawa.
- Staniec I., Klimczak M.K. (2008), *Ryzyko operacyjne*, [w:] I. Staniec, J. Zawila-Niedźwiecki (red.), *Zarządzaniem ryzykiem operacyjnym*, Wydawnictwo C.H. Beck, Warszawa.
- Thlon M. (2008), *Świetność i upadek. Historia banku Lehman Brothers*, „Gazeta Bankowa” nr 42 (1042).
- Thor W. (2008), *II Filar. Praktyczne aspekty wdrożenia na przykładzie BRE Banku*, [w:] „Zeszyty BRE- Bank Case”, nr 98/2008.
- Żółtkowski W. (2007), *Zarządzanie ryzykiem bankowym w praktyce: w kontekście Nowej Umowy Kapitałowej (Basel II)*, Wydawnictwo CeDeWu, Warszawa.