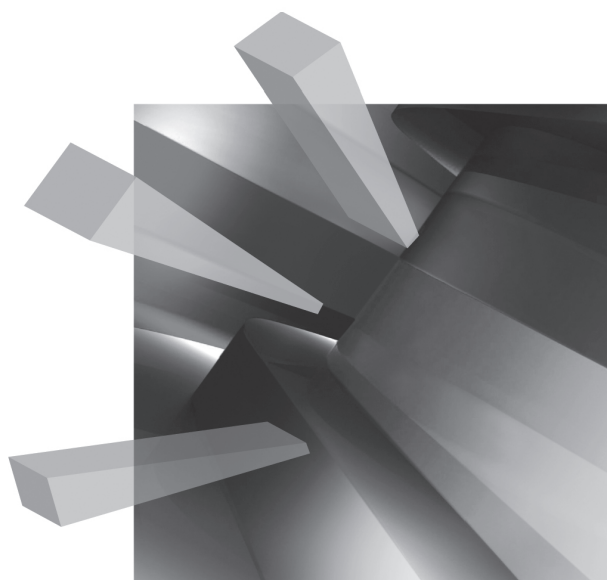


NAUKI O ZARZĄDZANIU MANAGEMENT SCIENCES

1 (22) • 2015



Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu
Wrocław 2015

Redakcja wydawnicza: Aleksandra Śliwka

Redakcja techniczna: Barbara Łopusiewicz

Korekta: Barbara Cibis

Łamanie: Beata Mazur

Projekt okładki: Beata Dębska

Informacje o naborze artykułów i zasadach recenzowania
znajdują się na stronie internetowej Wydawnictwa
www.noz.ue.wroc.pl
www.wydawnictwo.ue.wroc.pl

Publikacja udostępniona na licencji Creative Commons
Uznanie autorstwa-Użycie niekomercyjne-Bez utworów zależnych 3.0 Polska
(CC BY-NC-ND 3.0 PL)



© Copyright by Uniwersytet Ekonomiczny we Wrocławiu
Wrocław 2015

ISSN 2080-6000
e-ISSN 2449-9803

Wersja pierwotna: publikacja drukowana

Zamówienia na opublikowane prace należy składać na adres:
Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu
tel./fax 71 36 80 602; e-mail:econbook@ue.wroc.pl
www.ksiegarnia.ue.wroc.pl

Druk i oprawa: EXPOL

Spis treści

Wstęp	7
Marcin Jasiński: Metoda identyfikacji podejść do strategii.....	9
Andrzej Kozina: Ocena kompetencji negocjacyjnych (model teoretyczny i studium przypadku).....	22
Martyna Oślizło: Kampania promocyjna w kreowaniu marki kraju na przykładzie Brazylii.....	36
Sylwia Przytuła: Interakcje międzykulturowe w filii niemieckiej korporacji działającej w Polsce – studium przypadku.....	54
Anita Zbieg: Zastosowanie analizy sieci do oceny struktury organizacji i wyznaczenia kierunków jej zmian.....	71
Marta Zygier: Charakterystyka i znaczenie ryzyka operacyjnego w działalności bankowej.....	91

Summaries

Marcin Jasiński: Method of identifying approaches to strategy.....	9
Andrzej Kozina: The evaluation of negotiation competences (theoretical model and case study).....	22
Martyna Oślizło: Promotional campaign in the creation of national brand. Case study of Brazil.....	36
Sylwia Przytuła: Intercultural interactions in the German subsidiary operating in Poland. Case study.....	54
Anita Zbieg: Application of network analysis in evaluating organizational structure and determining its future shape.....	71
Marta Zygier: Overview and significance of operational risk in banking activity.....	91

Marta Zygiel

Uniwersytet Warszawski
e-mail: zygiel.marta@gmail.com

CHARAKTERYSTYKA I ZNACZENIE RYZYKA OPERACYJNEGO W DZIAŁALNOŚCI BANKOWEJ

OVERVIEW AND SIGNIFICANCE OF OPERATIONAL RISK IN BANKING ACTIVITY

DOI: 10.15611/noz.2015.1.06

JEL Classification: G21, G32.

Streszczenie: Praca ma na celu wskazanie definicji ryzyka występującego w działalności bankowej, przy szczególnym zwróceniu uwagi na pojęcie ryzyka operacyjnego. Analizie poddano podatność banków jako instytucji finansowych na wystąpienie ryzyka, szczegółowo omówiono rolę audytu wewnętrznego we wspieraniu i modyfikowaniu systemu zarządzania ryzykiem operacyjnym. Przeanalizowano działania mogące służyć eliminacji wystąpienia tego rodzaju ryzyka.

Słowa kluczowe: bank, ryzyko operacyjne, zarządzanie ryzykiem, kontrola wewnętrzna, audyt wewnętrzny, działalność bankowa.

Summary: The publication aims to identify the definition of risk existing in banking activity, with particular attention to the definition of operational risk. The article analyses the susceptibility of banks as financial institutions to the risk and discusses in detail the role of internal audit in supporting and modifying operational risk management system. It also examines activities that may be used for the elimination of such risks.

Keywords: bank, operational risk, risk management, internal control, internal audit, auditor, banking activity.

1. Wstęp

Dzięki odpowiedniemu zarządzaniu każdym rodzajem ryzyka możemy wykorzystywać szanse i minimalizować niebezpieczeństwo braku realizacji naszych celów. Zarządzanie ryzykiem w skali całego banku jest konsekwentnym i ciągłym procesem identyfikacji, oceny i kontroli potencjalnych zdarzeń, mogących wpływać na realizację celów organizacji. Dla instytucji finansowej niezbędne jest więc identyfikowanie istotnych wewnętrznie i zewnętrznie rodzajów ryzyka w sposób ciągły, aby móc reagować lub w odpowiednim czasie inicjować we właściwy sposób wszelkie

niezbędne zmiany. Jednak specyfika ryzyka operacyjnego przemawia za tym, że zarządzanie tego rodzaju ryzykiem jest o wiele trudniejsze. Zatem czy banki, mając świadomość możliwości wystąpienia ryzyka operacyjnego, mogą podejmować działania służące eliminacji tego ryzyka? Mogą, jednak wiele zależy od odpowiedniego systemu informatycznego oraz kwalifikacji pracowników, w tym kadry zarządzającej. Przedmiotem badania są czynniki wywołujące ryzyko operacyjne oraz sytuacje, w których tego rodzaju ryzyko występuje w działalności bankowej. Czy możliwe jest stworzenie zamkniętego katalogu scenariuszy, których wystąpienie narazi instytucję bankową na ryzyko operacyjne oraz spisanie wszystkich działań, których zastosowanie pozwoli bankom na uniknięcie tego rodzaju ryzyka? Prowadząc obserwację oraz analizując definicje ryzyka operacyjnego, można wskazać podstawowe lub też najbardziej narażone na ryzyko obszary działalności bankowej. W niniejszym opracowaniu wymieniono obszary podatne na wystąpienie ryzyka operacyjnego, wskazano, które części działalności bankowej winny być szczególnie zabezpieczone przed tego rodzaju ryzykiem. Pokazano, iż odpowiednie zarządzanie instytucją finansową, a także zachowanie ostrożności może pozwolić nawet na uniknięcie wystąpienia ryzyka. Zarządzanie ryzykiem operacyjnym powinno więc stanowić integralny element procesu kierowania bankiem, a wszystkie banki winny zarządzać ryzykiem operacyjnym w sposób kompleksowy i adekwatny dla siebie. Ryzyko operacyjne może wywołać znaczący wpływ na działalność oraz kondycję banków, zwłaszcza że obok otoczenia oraz zdarzeń zewnętrznych jego źródłem jest organizacja bankowa sama w sobie. Stopień wrażliwości banku na ryzyko operacyjne jest zależny od wielkości zatrudnienia i złożoności struktury organizacyjnej.

2. Definicja ryzyka operacyjnego w działalności bankowej

W działalności bankowej ryzyko definiowane jest jako zagrożenie nieosiągnięcia wytyczonych przez banki celów, takich jak np. optymalizacja zysku czy zapewnienie bezpieczeństwa działania. Ryzyko bankowe jest równoznaczne z prawdopodobieństwem wystąpienia zdarzeń oddziałujących negatywnie na sytuację banku i perspektywy rozwoju.

Koncentrując się na negatywnej stronie ryzyka, należy je określać jako miarę prawdopodobieństwa wystąpienia straty, gdzie jest postrzegane jako zjawisko powodujące ujemne odchylenia od założonego celu czy planowanych wyników finansowych, a także jako sytuacja, w której występuje odchylenie negatywne od sytuacji pożądanej bądź oczekiwanej [Fabozzi 2007, s. 15-17].

Z ryzykiem związane są takie pojęcia, jak możliwość poniesienia strat czy niepewność. Niepewność dotyczy przebiegu przyszłych zdarzeń mających wpływ na funkcjonowanie banku. Poniesienie strat stanowi konsekwencję wystąpienia ryzyka [Iwanicz-Drozdowska, Nowak 2002, s. 9-10].

Ryzyko operacyjne może być definiowane na kilka sposobów. Sama kategoria tego rodzaju ryzyka została dostrzeżona niedawno i wzrastała wraz z rozwojem no-

wych technologii, jednak ze względu na to, iż jest ono związane z kadrami banku, musiało istnieć od początku bankowości.

Początkowo definicje ryzyka operacyjnego wynikały z przeciwstawienia go ryzyku strategicznemu, które pojmowane było jako ryzyko związane z długookresową działalnością banku, w szczególności było związane z kadrami kierowniczą i podejmowanymi przez nią decyzjami strategicznymi związanymi z głównymi obszarami działania banku. Ryzyko operacyjne miało zaś dotyczyć bieżącej działalności banku i związanych z nią decyzji o charakterze operacyjnym [Holton 2004]. W takim ujęciu ryzyko operacyjne ma charakter techniczno-organizacyjny, a nacisk kładzie się na jego związek z operacjami przeprowadzanymi przez bank i jego podstawową działalnością. Określenia „ryzyko operacyjne” i „ryzyko techniczno-organizacyjne” mogły być więc stosowane zamiennie [Zawadzka 1996, s. 13-14].

Ryzyko można także określać jako miarę niepewności odnoszącej się do przyszłych wyników finansowych bądź jako miarę odchylenia aktualnych wyników od oczekiwanych. Przy tym założeniu odchylenie takie może wystąpić w kierunku dodatnim (pozytywnym) i ujemnym (negatywnym). Ryzyko nie ma tu więc jasno określonego charakteru jak we wcześniejszej definicji, oznacza jedynie występowanie fluktuacji o różnym kierunku [Jorion 2003, s. 533-534].

Przy definicji ryzyka operacyjnego różnie ujmowane jest też jego źródło w stosunku do banku. Niektórzy przyjmują, iż ryzyko to wynika jedynie z czynników wewnętrznych, takich jak błędy powstałe przy dokonywaniu i rozliczaniu transakcji, które spowodowane są przez czynności wykonane przez pracowników lub urządzenia techniczne [Iwanicz-Drozdowska 2012, s. 133-134]. W takim znaczeniu ryzyko to obejmuje nie tylko zdarzenia związane z działalnością operacyjną, ale także zdarzenia związane z wyborem nieodpowiednich systemów i zabezpieczeń oraz możliwość dopuszczenia się oszustw przez pracowników.

Inni oprócz czynników natury wewnętrznej wskazują także znaczenie czynników zewnętrznych – spoza struktury banku – i zakładają, że ryzyko operacyjne jest efektem czynników zarówno endogenicznych, jak i egzogenicznych, takich jak katastrofy czy klęski naturalne [Kałużny 2004].

Najczęściej jednak stosowanym rozwiązaniem było definiowanie ryzyka operacyjnego jak każdego innego rodzaju ryzyka, które nie jest ryzykiem rynkowym ani kredytowym. Później ten typ definicji ulegał modyfikacjom i uszczegóławianiu przez enumerację czynników ryzyka. Najwcześniej zaliczono tu błędy popełnione przez ludzi i błędy techniczne. I tak dla ryzyka operacyjnego kluczowe stały się hasła: ludzie, procesy, technologia oraz zdarzenia zewnętrzne.

Obecnie organy regulujące działalność bankową uwzględniają w definicji ryzyka operacyjnego wpływ czynników zewnętrznych. Chodzi tu o oddziaływanie takich zdarzeń, jak katastrofy naturalne (np. powódź, pożar, trzęsienie ziemi), które przelożą się na funkcjonowanie banku oraz zagrożenia wynikające z przepisów prawa lub polityczne. Wszystkie te elementy są zawarte w definicji ryzyka operacyjnego sformułowanej w 2001 r. przez Bazylejski Komitet Nadzoru Bankowego, która wskazu-

je, iż ryzyko operacyjne to ryzyko poniesienia strat na skutek stosowania niewłaściwych procesów wewnętrznych lub błędów w ich realizacji, wykorzystania nieprawidłowych systemów, działań ludzkich i oddziaływania zdarzeń zewnętrznych. W mojej ocenie nie jest to jednak kompleksowa definicja, gdyż mimo iż obejmuje ryzyko prawne, pomija ryzyko utraty reputacji oraz ryzyko związane ze skutkami podjętych decyzji strategicznych.

Obowiązująca w Polsce rekomendacja M [Uchwała nr 8/2013 Komisji Nadzoru Finansowego z dnia 8 stycznia 2013 r] dotycząca zarządzania ryzykiem operacyjnym w bankach, definiując owo ryzyko, przyjmuje za Bazylejskim Komitetem, że ryzyko operacyjne należy rozumieć jako ryzyko straty wynikającej z niedostosowania lub zawodności wewnętrznych procesów, ludzi i systemów technicznych lub ze zdarzeń zewnętrznych.

Oznacza to, że identyfikacja ryzyka operacyjnego uwzględnia czynniki wewnętrzne i zewnętrzne, gdzie do czynników wewnętrznych zalicza się, takie jak: struktura organizacyjna firmy, specyfika działalności, użytkowane systemy informatyczne, specyfika klientów firmy, skargi od klientów, jakość kadr, zmiany organizacyjne oraz rotacja kadr, jakość, kompletność, aktualność i przestrzeganie procedur wewnętrznych. Czynniki zewnętrzne to wszystko, co wchodzi w otoczenie działania banku: uwarunkowania polityczne, prawne, demograficzne, konkurencja, postęp technologiczny, zachowania rynków finansowych, podmioty zewnętrzne, z którymi firma współpracuje – które mogą wpływać negatywnie na realizację celów firmy.

Prof. Iwanicz-Drozdowska wskazuje, iż ogólnie rzecz ujmując, ryzyko operacyjne można wiązać ze stratami innymi niż te wynikające z ryzyka kredytowego i rynkowego (awaria systemów, zła decyzja, defraudacja) [Iwanicz-Drozdowska 2012, s. 132].

Podejście do ryzyka operacyjnego przyjęte przez Komitet Bazylejski wywoływało i nadal wywołuje wiele kontrowersji. Komitet wyszedł bowiem z założenia, że amortyzacji strat z tytułu ryzyka operacyjnego służyć będzie kapitał i w związku z tym zaproponował metody obliczania wymogu kapitałowego z tytułu tego ryzyka. Wielu praktyków bankowości zwracało jednak uwagę, iż przyjęcie analogicznego podejścia, jakie zastosowano do ryzyka kredytowego i rynkowego, również dla ryzyka operacyjnego, jest błędne. Przede wszystkim wynika to z charakteru strat ryzyka operacyjnego. Z jednej strony występują bowiem zdarzenia o relatywnie niewielkich skutkach w skali całego banku, ale za to są one dość częste. Z drugiej strony bank narażony jest na olbrzymie straty powstające wskutek nieprzewidywalnych zdarzeń, które występują relatywnie rzadko.

Podsumowując, należy stwierdzić, że wszystkie przytoczone w opracowaniu próby definicji ryzyka łączy minimalny zakres. Żaden z opisów nie jest kompletny i nie zawiera pełnej definicji problemu. Wszystkie definicje odwołują się do stwierdzenia, iż ryzykiem operacyjnym jest możliwość poniesienia straty wynikająca z niewłaściwych lub wadliwych procesów, systemów, działań pracowników czy też działań zewnętrznych. Katalog tych nieadekwatnych lub zawierających błędy dzia-

łań lub systemów jest jednak otwarty. Żadna z definicji nie wylicza wszystkich możliwych sytuacji, w których pojawia się ryzyko operacyjne. Analiza problemu pozwoliła na wypracowanie jedynie kategorii właściwych dla ryzyka operacyjnego. Zatem instytucje narażone na wystąpienie ryzyka operacyjnego, prowadząc proces jego monitoringu i obserwacji, mają możliwość stworzenia pełnego zakresu dla tego pojęcia.

W porównaniu z innymi rodzajami ryzyka występującymi w działalności banków ryzyko operacyjne ma pewne charakterystyczne cechy. Przede wszystkim do tego ryzyka ma zastosowanie wymieniona negatywna koncepcja ryzyka, która zakłada, iż ryzyko wiąże się tylko z negatywnym odchyleniem od oczekiwanego wyniku i jest źródłem potencjalnych strat. Negatywny charakter ryzyka operacyjnego przejawia się tym, że podjęcie innego rodzaju ryzyka może wiązać się z wystąpieniem zysku (np. w przypadku ryzyka kredytowego), natomiast ryzyko operacyjne wiąże się tylko ze stratami, a zarządzanie nim ma na celu zmniejszenie prawdopodobieństwa ich wystąpienia lub zminimalizowanie ich negatywnych następstw. Oznacza to, iż ryzyka operacyjnego nie podejmuje się tak jak ryzyka kredytowego czy rynkowego w celu osiągnięcia korzyści – efektem jego wystąpienia może być jedynie strata.

Kolejną cechą charakterystyczną ryzyka operacyjnego jest większe prawdopodobieństwo jego wystąpienia wraz z rozbudowaniem organizacji, stosowanych systemów oraz szeroką gamą oferowanych produktów i usług. Ponadto nie jest możliwa jego całkowita eliminacja. Nie jest też prosta analiza czynników ryzyka, jego konsekwencji i skutków, a zarazem pomiar ryzyka, ponieważ znaczną część strat z tytułu ryzyka operacyjnego powoduje występowanie zdarzeń bardzo rzadkich i trudnych do przewidzenia, co utrudnia stosowanie metod statystycznych na skutek braku dostatecznych baz danych. Źródła ryzyka operacyjnego często pozostają ukryte (na przykład niezgodne z prawem działania pracowników banku) bądź są niespodziewane (jak katastrofy naturalne). Warto także zauważyć, iż ryzyko operacyjne towarzyszy każdemu rodzajowi podejmowanej przez bank działalności. Będzie więc występowało w przypadku zarówno tradycyjnej działalności kredytowo-depozytowej, jak i oferowania przez banki produktów strukturyzowanych czy instrumentów pochodnych, a także w przypadku prowadzenia działalności maklerskiej i ubezpieczeniowej.

Jest to także ryzyko wielowymiarowe, dotyczące różnego rodzaju działań i operacji. Obejmuje swym zakresem wiele różnych od siebie zdarzeń, jak oszustwa pracowników, łamanie obowiązujących przepisów BHP przez banki, ataki hakerów czy ataki terrorystyczne. Charakterystyczne dla ryzyka operacyjnego jest także to, iż nie kumuluje się w sektorze (rzadko występuje w kilku bankach jednocześnie), co jednak nie wyklucza, że straty z jego tytułu nie są w stanie zagrozić całemu systemowi bankowemu. Redukowanie innych rodzajów ryzyka, np. rynkowego czy kredytowego, może zwiększyć narażenie banku na ryzyko operacyjne. Dotyczy to zwłaszcza instrumentów pochodnych, w przypadku których często pracownikom banków bra-

kuje odpowiedniego doświadczenia i kwalifikacji, co zwiększa ryzyko błędu. W tym przypadku może zwiększyć się także ryzyko wystąpienia niezgodnych z prawem zachowań pracowników banku [Krasodomska 2008, s. 23-24].

Ryzyko operacyjne można więc podzielić na:

- ryzyko aktywów będących środkami trwałymi – polega na uszkodzeniu lub stracie środka trwałego mającego wpływ na funkcjonowanie instytucji;
- ryzyko technologii – ryzyko spowodowane niesprawnością systemów, złą jakością danych, błędami w oprogramowaniu;
- ryzyko kontaktów z otoczeniem – ryzyko powstające w wyniku współpracy instytucji z podmiotami w otoczeniu, np. problemy z dostawcami, odbiorcami, klientami, napady i kradzieże, relacje z akcjonariuszami, władzami, mediami;
- ryzyko personelu – cele instytucji nie są osiągane na skutek niewłaściwej polityki personalnej (dobór, kwalifikacje, etyka, cechy osobowościowe, fluktuacja).

Częścią ryzyka operacyjnego jest też ryzyko niewłaściwej struktury organizacyjnej i zasad funkcjonowania kontroli wewnętrznej i jej podporządkowanie, planowania księgowości itp., a także współdziałanie między poszczególnymi działami lub obciążenia niektórych departamentów.

Podsumowując, należy stwierdzić, że ten rodzaj ryzyka ma kilka cech, które znacząco wpływają na trudności w dokonaniu jego pomiaru:

- możliwa kumulacja ryzyka na skutek nieszczęśliwego zbiegu wydarzeń;
- nieograniczona liczba kategorii błędów;
- niska zdolność prognostyczna danych historycznych;
- niedobór informacji o stratach poniesionych przez inne instytucje;
- często subiektywny proces oceny ryzyka.

Ryzyko operacyjne nie jest jednak niczym nowym w działalności banków. Występowało zawsze, jednak wskutek zmian charakteru działalności banków i uwarunkowań rynkowych wiążących się z przemianami w sposobie prowadzenia działalności gospodarczej w ostatnich latach wzrosło jego znaczenie. Badania przeprowadzone w 1997 r. przez British Bankers Association i Coopers&Lybrand wykazały, że ryzyko operacyjne jest dla prawie 70% ankietowanych banków równie ważne, a nawet ważniejsze niż ryzyko rynkowe czy kredytowe [Krasodomska 2008].

3. Czynniki wywołujące ryzyko operacyjne

Do czynników wywołujących ryzyko operacyjne w bankach należą ludzie, procesy i systemy używane w bankach, obieg dokumentów wewnętrznych i zewnętrznych, przetwarzanie informacji, lokalizacja banku, outsourcing, jak również zdarzenia wewnętrzne – zarówno przewidywalne, jak i nieprzewidywalne. Źródłem ryzyka operacyjnego może być też strategia przedsiębiorstwa (np. innowacje produktowe).

Komitet Bazylejski zidentyfikował siedem kategorii czynników ryzyka operacyjnego. Klasyfikacja zdarzeń ryzyka operacyjnego wygląda więc następująco:

- oszustwa wewnętrzne – działania pracowników banku mające na celu zamierzone oszustwo, sprzeniewierzenie własności, obejście prawa lub polityki banku, np. oszustwo kredytowe, oszustwo czekowe, łapówkarstwo, fałszowanie sprawozdawczości wewnętrznej, celowe zniszczenie aktywów. Przykład: kradzież pracownicza, inwestycje na prywatnym koncie na podstawie poufnych informacji;
- oszustwa zewnętrzne – działania osób trzecich prowadzące do defraudacji, przywłaszczenia mienia lub omińnięcia przepisów prawa. Na przykład: kradzież, włamanie fizyczne, włamanie komputerowe – ataki hakerów;
- praktyki związane z zatrudnianiem i bezpieczeństwem w miejscu pracy, tj. tzw. polityka kadrowa i bezpieczeństwo pracy – działania niezgodne z przepisami lub zawartymi porozumieniami w kwestii zatrudniania, zdrowia i bezpieczeństwa lub inne działania skutkujące wypłatą należnego z tytułu szkód osobistych odszkodowania lub roszczeń na tle zróżnicowania i dyskryminacji. Przykładem mogą być roszczenia pracowników z tytułu wynagrodzeń, naruszenia zasad bezpieczeństwa oraz ogólna odpowiedzialność prawna, np. za klienta, który poślizgnął się i upadł, wchodząc do oddziału banku;
- praktyki związane z klientami, produktami i praktyką biznesową – niezamierzone lub wynikające z zaniedbania przypadki niespełnienia zobowiązań względem klientów banku lub stosowanie nieodpowiednich produktów lub praktyk biznesowych. Należy tu wskazać na działania prowadzące do naruszenia zaufania i wytycznych w zakresie obsługi klientów, ujawniania informacji dotyczących klientów, agresywnej strategii handlowej w celu maksymalizacji prowizji, niedozwolonych transakcji na rachunkach bankowych klientów, błędnej oceny profilu klienta, jak również wadliwie skonstruowane produkty bankowe (błędnie sporządzone wzory, umowy, regulaminy). Na przykład: sprzedaż produktów nieautoryzowanych, pranie brudnych pieniędzy;
- szkody w aktywach rzeczowych – utarta bądź zniszczenia fizyczne aktywów w efekcie działania siły wyższej – np. katastrofy naturalnej, aktów wandalizmu czy terroryzmu.
- zakłócenia działalności gospodarczej i błędy systemów – przejawiają się między innymi w nieprawidłowym działaniu sprzętu, błędach oprogramowania, problemach telekomunikacyjnych oraz z zasilaniem;
- wykonywanie transakcji, dostawa oraz zarządzanie procesami operacyjnymi – błędy w trakcie wprowadzania danych do systemu, wykonania, rozliczania i obsługi transakcji, zaniedbania w zakresie monitorowania i sprawozdawczości, nienależycie prowadzona dokumentacja dotycząca klientów banku, niewłaściwe zarządzanie rachunkami klientów, niekorzystne relacje z kontrahentami i dostawcami banku.

Podobne rozróżnienie wprowadzono w Rekomendacji M, gdzie zidentyfikowano siedem głównych kategorii zdarzeń operacyjnych oraz dwadzieścia rodzajów zdarzeń w ramach tych kategorii:

- 1) oszustwo wewnętrzne:
 - a) działania nieuprawnione,
 - b) kradzież i oszustwo;
- 2) oszustwo zewnętrzne:
 - a) kradzież i oszustwo,
 - b) bezpieczeństwo systemów;
- 3) praktyka kadrowa i bezpieczeństwo pracy:
 - a) stosunki pracownicze,
 - b) bezpieczeństwo środowiska pracy,
 - c) podziały i dyskryminacja;
- 4) klienci, produkty i praktyka biznesowa:
 - a) obsługa klientów, ujawnianie informacji o klientach, zobowiązania względem klientów,
 - b) niewłaściwe praktyki biznesowe lub rynkowe,
 - c) wady produktów,
 - d) klasyfikacja klienta i ekspozycje,
 - e) usługi doradcze;
- 5) uszkodzenia aktywów:
 - a) klęski żywiołowe i inne zdarzenia;
- 6) zakłócenia działalności i błędy systemów:
 - a) systemy;
- 7) dokonywanie transakcji, dostawa oraz zarządzanie procesami:
 - a) wprowadzanie do systemu, wykonywanie, rozliczanie i obsługa transakcji,
 - b) monitorowanie i sprawozdawczość,
 - c) dokumentacja dotycząca klienta,
 - d) zarządzanie rachunkami klientów,
 - e) uczestnicy procesów niebędący klientami banku (np. izby rozliczeniowe),
 - f) sprzedawcy i dostawcy.

Oszustwo wewnętrzne jako główna kategoria zostało podzielone na dwa rodzaje zdarzeń: „działania nieuprawnione” oraz „kradzież i oszustwo”. Oszustwo wewnętrzne jest tożsame z pojęciem straty z tytułu działań mających na celu zamierzone oszustwo, sprzeniewierzenie własności lub obejście regulacji, prawa lub polityki spółki, z wyłączeniem zdarzeń z zakresu różnicowania i dyskryminacji, dotyczące co najmniej jednej osoby wewnętrznej. Pozostałe rodzaje zdarzeń dla poszczególnych kategorii zostały zdefiniowane za pomocą przykładów zdarzeń operacyjnych dla poszczególnych kategorii. Jednak w mojej ocenie taka definicja nie jest wystarczająco precyzyjna dla instrumentu podstawowego, co powoduje konieczność wykorzystania przepisów prawa powszechnie obowiązującego. Przede wszystkim zdarzenia tego typu są zdefiniowane m.in. w: *Kodeksie karnym*, *Prawie bankowym*, *Kodeksie pracy*, *Kodeksie spółek handlowych*, *Ustawie o stanie klęski żywiołowej*, *Kodeksie cywilnym*, a także we wzorach umów ubezpieczeniowych.

4. Podstawowe zasady zarządzania ryzykiem

Zdarzenia związane z ryzykiem operacyjnym mogą występować często, jednakże rzeczywisty wymiar tego ryzyka jest niezwykle trudny do określenia. Dlatego też celowe jest przygotowanie, a następnie sprawne wdrożenie procesu zarządzania w banku tym rodzajem ryzyka, polegającego na:

- identyfikacji,
- ocenie,
- zastosowaniu narzędzi redukcji ryzyka,
- monitorowaniu efektywności redukcji ryzyka,
- raportowaniu,

który to proces kontroluje rada nadzorcza, zarząd banku oraz komórki kontroli wewnętrznej, spełniając funkcję organów banku szczególnie odpowiadających za ryzyko operacyjne.

Pozwala to zbudować kompleksowy system zarządzania ryzykiem oraz identyfikację czynników ryzyka poprzez utworzenie mapy ryzyka. Mapa ryzyka to wnikliwa analiza ryzyka wykonywana przez pionierzy operacyjne. Włączenie w ten proces osób spełniających różne funkcje na różnych stanowiskach w organizacji może zaowocować identyfikacją typów i obszarów występowania ryzyka.

Należy zauważyć, że ryzyko operacyjne w ostatnich latach zyskuje na znaczeniu, a przypadki zmaterializowania się go są przyczyną znacznych strat ponoszonych przez instytucje finansowe. Dlatego też od lat 90. XX wieku bankowe i niebankowe instytucje finansowe zaczęły bacznie przyglądać się problemowi ryzyka operacyjnego, co spowodowane było znacznymi stratami spowodowanymi przez tę kategorię ryzyka. Najbardziej spektakularne straty spowodowane ryzykiem operacyjnym to przypadki oszustw lub nadużyć dokonywanych przez pracowników banków. Najczęściej opisywane w literaturze przedmiotu przypadki takich zdarzeń to [Krasodomska 2008]:

- Barings Bank, w którym w 1995 r. straty spowodowane przez niekontrolowane inwestycje w instrumenty pochodne dokonywane przez działającego w Singapurze dealera, N. Leeson, wyniosły ok. 1,4 mld USD i były przyczyną bankructwa banku,
- Daiwa Bank, w którym w 1995 r. handel obligacjami i ukrywanie strat z wykorzystaniem fałszowania dokumentów przez maklera T. Iguchi były przyczyną strat przekraczających 1 mld USD,
- Société Générale Bank, w którym w 2008 r. ujawniono straty sięgające 4,9 mln EUR, spowodowane przez skutecznie ukrywane przez Jerome'a Karviela spekulacje na rynku terminowym.

Ryzyko operacyjne nie stanowi nowego zagrożenia dla banków. Jednak do tej pory banki, funkcjonując głównie z nastawieniem na maksymalizację dochodów i osiągnięcie wyników, nie prowadziły badań czy też kontroli stosowanych procesów wewnętrznych oraz jakości działań kadry pracowniczej. Nowym aspektem w tej

dziedzinie jest natomiast podkreślenie, niedocenianej do tej pory – a mającej istotne znaczenie – konieczności opracowania metod, zasad, technik i praktyk zarządzania ryzykiem operacyjnym, analogicznych do stosowanych w przypadku ryzyka kredytowego czy rynkowego [Krasodomska 2008].

Tego typu ryzyko powinno być także traktowane jako środek do maksymalizacji dostępnych możliwości. Dzięki odpowiednim działaniom i identyfikacji ryzyka operacyjnego zmniejszeniu może ulec prawdopodobieństwo wystąpienia porażki czy też popełnienia istotnych dla funkcjonowania banku błędów. Identyfikacja ryzyka i zarządzanie nim powinno więc dotyczyć każdej osoby w organizacji i być skutecznie realizowane przez kadre zarządzającą. Wśród głównych korzyści płynących z zarządzania ryzykiem możemy wymienić:

- większe prawdopodobieństwo osiągnięcia celów organizacji;
- większy nacisk w organizacji na poprawne wykonywanie zadań;
- większy nacisk kierownictwa na sprawy faktycznie istotne;
- krótszy czas reakcji kierownictwa na sytuacje kryzysowe;
- lepsze wykorzystanie posiadanych zasobów;
- umocnienie reputacji organizacji.

5. Rola audytorów wewnętrznych we wspieraniu zarządzania ryzykiem operacyjnym

Zarówno system kontroli wewnętrznej, jak i audyt wewnętrzny są elementami składającymi się na ład korporacyjny, a więc na sposób, w jaki organizacja jest zarządzana. Oba instrumenty są niezbędne i komplementarne wobec siebie, mimo różnego katalogu zadań. Zgodnie z zaleceniami rekomendacji M banki powinny podjąć odpowiednie działania zapewniające dostarczenie zarządowi wszystkich niezbędnych informacji pozwalających na ocenę funkcjonowania adekwatnego i skutecznego systemu zarządzania ryzykiem operacyjnym. W tym celu należy opracować i wdrożyć odpowiedni system raportowania informacji, pozwalający na identyfikację, ocenę, monitorowanie i kontrolowanie ryzyka operacyjnego. Przez kontrolę wewnętrzną rozumiemy system działań podejmowanych przez kierownictwo, władze lub inne podmioty w celu poprawy zarządzania ryzykiem i zwiększenia prawdopodobieństwa zrealizowania ustalonych celów i zadań.

Do głównych zadań kontroli wewnętrznej należy sprawdzanie poprawności dokumentacji i jej zgodności z procesem zarządzania ryzykiem, właściwa organizacja komórki zarządzania ryzykiem oraz badanie zgodności procesów i pomiaru ryzyka. Ważne jest także informowanie kierownictwa o ryzyku, jakości źródeł danych, poprawności przyjętych założeń odnośnie do korelacji i zmienności, dokładności stosowanych modeli pomiaru.

Nieco inne kompetencje należą do audytu wewnętrznego. Jednostka ta prowadzi niezależną działalność doradczą, której celem jest przysporzenie wartości i uspraw-

nienie działalności operacyjnej organizacji. Audyt tworzy system niezależnego monitorowania, weryfikacji i oceny skuteczności procesów zarządzania ryzykiem, kontroli i ładu korporacyjnego.

W rekomendacji M zaleca się wyodrębnienie w strukturze organizacyjnej banku komórki ds. audytu wewnętrznego. Rola audytu wewnętrznego sprowadza się do przedstawienia niezależnej oceny i wsparcia kierownictwa w skutecznym zarządzaniu ryzykiem przez dostarczenie opinii o efektywności działań podjętych w celu ograniczenia ryzyka oraz jakości przeprowadzanych operacji bankowych. Nie oznacza to jednak, że komórka audytu wewnętrznego jest odpowiedzialna za zarządzanie ryzykiem. Należyte wywiązanie się z tego zadania leży bowiem w gestii zarządzających bankiem.

Instytut Auditorów Wewnętrznych (The Institute of Internal Auditors – IIA), tworząc mające uniwersalny charakter Międzynarodowe Standardy Profesjonalnej Praktyki Audytu Wewnętrznego (dalej: Standardy II A) [Komunikat nr 2 Ministra Finansów z dnia 17 czerwca 2013 r.], opracował najczęściej stosowaną definicję audytu wewnętrznego.

Zgodnie z nią audyt wewnętrzny jest działalnością niezależną, obiektywnie zapewniającą ocenę i doradczą, której celem jest przysporzenie wartości i usprawnienie działań organizacji. Głównym celem audytu jest pomoc organizacji w osiągnięciu jej celów poprzez systematyczne i zdyscyplinowane podejście do oceny i doskonalenia skuteczności procesów zarządzania ryzykiem, kontroli i procesów nadzoru prowadzonego przez właścicieli. Działania o charakterze zapewniającym obejmują obiektywną ocenę systemów funkcjonujących w jednostce, dokonywaną przez audytorów wewnętrznych. Audytor ma wyjątkową pozycję do wykonywania swojej pracy, opartą na przestrzeganiu najwyższych standardów obiektywizmu, niezależności wynikającej z umiejscowienia komórki audytu w strukturze organizacyjnej oraz rozległej wiedzy na temat procesów organizacyjnych, ryzyka i strategii.

Według rekomendacji H [Uchwała nr 180/2011 Komisji Nadzoru Finansowego z dnia 19 lipca 2011 r.], niezależność audytu wewnętrznego opiera się na wskazanych w uchwale KNF mechanizmach funkcjonujących w banku, zapewniających niezależność komórki audytu wewnętrznego od istotnych nacisków podczas przeprowadzania kontroli według ustalonych metod, dokonywania ocen skuteczności procedur i regulaminów oraz sporządzania raportów pokontrolnych.

Rekomendacja określa także, czym jest obiektywność audytu wewnętrznego. Wskazuje, iż należy przez nią rozumieć niezależność osądu dokonywanego przez audytorów wewnętrznych podczas przeprowadzania kontroli od czynników pozamerytorycznych. Audytorzy wewnętrzni nie mogą być stronniczy i nie mogą uzależniać swojej opinii w kwestii kontrolowanego tematu od opinii innych. Obiektywność stanowi jedno z najważniejszych kryteriów oceny jakości pracy audytora wewnętrznego. Audytorzy wewnętrzni powinni przeprowadzać kontrole w taki sposób, aby zachować poufność wyników kontroli oraz nie zgadzać się na żadne rozwiązania lub kompromisy, które mogłyby mieć negatywny wpływ na zachowanie

wysokiej jakości swojej pracy. Wyniki kontroli powinny być przedstawiane bez względu na konsekwencje, jakie mogą wywołać oraz powiązania (formalne i nieformalne), które mogą naruszać.

Rekomendacja H wskazuje także na audytora jako podmiot działający w ramach jednostki audytu wewnętrznego wykonujący w banku czynności kontrolne, posiadający kwalifikacje, doświadczenie i umiejętności w zakresie badania ryzyka występującego w działalności banku oraz postępujący zgodnie z przyjętymi w banku standardami praktyki zawodowej oraz zasadami etyki audytora wewnętrznego.

Celem działalności audytu wewnętrznego jest cykliczny przegląd i ocena wszelkich obszarów działalności i wszelkich rodzajów ryzyka występujących w firmie, które mają w racjonalny sposób zapewnić osiągnięcie celów biznesowych, takich jak wiarygodność i spójność informacji finansowych i operacyjnych, skuteczność i efektywność działań operacyjnych, ochrona aktywów czy zgodność z prawem, przepisami i umowami. Do szerokiego katalogu usług audytorów można także zaliczyć usługi doradcze wykonywane w ramach swoich rutynowych działań lub w odpowiedzi na wnioski kierownictwa.

Według Standardów II A, potencjalne kategorie mogą obejmować:

- formalne zadania doradcze – zaplanowane i przedstawione w formie pisemnej umowy,
- nieformalne zadania doradcze – rutynowe działania, takie jak uczestnictwo w stałych komitetach, projektach,
- specjalne zadania doradcze – na przykład uczestnictwo w zespole przeprowadzającym fuzję lub przejęcie albo w zespole prowadzącym przekształcenie systemu zarządzania,
- zadania doradcze w sytuacjach wyjątkowych,
- uczestnictwo w zespole ustanowionym dla celów wznowienia i kontynuowania działań operacyjnych po wystąpieniu katastrofy lub innym nadzwyczajnym wydarzeniu gospodarczym.

Audytorzy winni więc koncentrować swoją pracę na weryfikacji ryzyka operacyjnego i biznesowego bieżącej i strategicznej działalności, wykonując czynności zarówno w centrali banku, jak i w jednostkach terenowych czy oddziałach.

W swojej pracy są zobowiązani do dokonywania prawidłowej oceny adekwatności, skuteczności oraz efektywności i jakości systemu kontroli wewnętrznej banku, co oznacza prezentowanie w raporcie pokontrolnym zbadanych zdarzeń, które wymagają podjęcia działań naprawczych, unikanie niedomówień i nieścisłości, zapewnienie wiarygodności komórki audytu wewnętrznego.

Audytorzy wewnętrzni, wspomagając kadre kierowniczą wyższego szczebla, poprzez ocenę skuteczności procesów zarządzania ryzykiem dają racjonalne zapewnienie, że system kontroli wewnętrznej funkcjonuje w sposób efektywny. Mogą również wspierać kadre zarządzającą w kreowaniu procesów zarządzania ryzykiem, mogą także odegrać aktywną rolę w tworzeniu polityki i kultury sprzyjającej wdrażaniu systemów zarządzania ryzykiem, które są ochroną przed zdarzeniami nega-

tywnie wpływającymi na stabilność finansową oraz jednego z najcenniejszych zasobów banku, jakim jest reputacja. Audytor może również wspierać menedżera ryzyka poprzez zapewnienie, że procesy zarządzania ryzykiem mają odpowiedni poziom akceptacji ze strony całej struktury organizacji, a w szczególności kierownictwa wyższego szczebla.

Podsumowując, należy stwierdzić, że obok tradycyjnych funkcji, audyt wewnętrzny ma spełniać wiele nowych funkcji, takich jak:

- przegląd całościowych systemów zarządzania ryzykiem,
- integracja miar zarządzania ryzykiem z codziennym zarządzaniem ryzykiem,
- zatwierdzanie każdej zmiany w procesie zarządzania ryzykiem,
- sprawdzanie dokładności i kompletności danych służących do zarządzania ryzykiem,
- sprawdzanie spójności, terminowości i rzetelności źródeł danych wykorzystywanych w modelach wewnętrznych oraz dokładności i poprawności danych dotyczących samych modeli.

6. Zakończenie

W ostatnich latach nastąpiły zmiany charakteru działalności banków i warunków rynkowych, które wymusiły pilną konieczność zwrócenia uwagi na ryzyko operacyjne. J.E. Stiglitz, laureat Nagrody Nobla w dziedzinie ekonomii, zauważa, że: „powab łatwych zysków generowanych przez koszty transakcyjne odciągnął wiele dużych banków od wypełniania ich zasadniczych funkcji. System bankowy w Stanach Zjednoczonych i w wielu innych państwach przestał koncentrować się na kredytach dla małych i średnich firm, które w każdej gospodarce są podstawą tworzenia miejsc pracy, a zamiast tego skupił się na promowaniu sekurytyzacji” [Stiglitz 2010].

Przyglądając się działalności bankowej, można z łatwością zauważyć, iż podatność banków jako instytucji finansowych na wystąpienie ryzyka operacyjnego jest wysoka. Głównym problemem ryzyka operacyjnego jest to, że jego źródłem jest organizacja sama w sobie. Dlatego też zgodnie z Rekomendacją M bank powinien posiadać strukturę, procesy i zasoby odpowiednie do skali i złożoności prowadzonej działalności, pozwalające na sprawne zarządzanie ryzykiem operacyjnym. Każdy bank powinien wypracowywać własne mechanizmy monitorowania ryzyka operacyjnego, zwracając przede wszystkim uwagę na: rodzaj i istotność błędów, rodzaje, stopień skomplikowania i wartość zawieranych oraz planowanych transakcji, wahania osiągniętych i przewidywanych zysków, posiadany system teleinformatyczny, poziom kwalifikacji pracowników oraz zmiany kadrowe i organizacyjne. Dostosowanie systemu zarządzania i monitorowania do profilu ryzyka ma istotne znaczenie dla jakości zarządzania tym ryzykiem. Należy mieć na uwadze, że efektywna identyfikacja ryzyka operacyjnego stanowi podstawę do poprawnej jego oceny. Rekomendacja M wskazuje na konieczność wyodrębnienia w strukturze organizacyjnej banku komórki ds. audytu wewnętrznego, posiadającej odpowiednie doświadczenie

i kwalifikacje do oceny i badania ryzyka występującego w działalności bankowej. Jako rolę audytorów wewnętrznych wskazuje się m.in. usługi doradcze wykonywane w ramach rutynowych działań kontroli wewnętrznej lub w odpowiedzi na wniośki kadry kierowniczej w celu zapewnienia obiektywnej oceny systemów funkcjonujących w instytucji finansowej. Podsumowując, należy stwierdzić, że banki jako instytucje finansowe są szczególnie narażone na ryzyko operacyjne. Powinny więc wdrożyć systemy bieżącego monitorowania narażenia na tego rodzaju ryzyko i powstawania strat w pionach operacyjnych. Mimo wielu opracowań oraz badań nad ryzykiem operacyjnym, a przede wszystkim czynnikami wywołującymi tego rodzaju ryzyko, nie udało się stworzyć zamkniętego katalogu zarówno sytuacji, w których możliwe jest wystąpienie ryzyka, jak i działań mających na celu zapobieganie lub usunięcie jego skutków. Rekomendacja M, zawierając definicję ryzyka operacyjnego, jednocześnie wskazuje, iż dotyczy ona jedynie minimalnego zakresu ryzyka. Sam regulator nie stworzył więc dobrych praktyk w sposób kompleksowy, pozwalając, by banki w celu zarządzania ryzykiem operacyjnym mogły stosować własną, szerszą definicję, z zastrzeżeniem, by była ona spójna z tą zawartą w Rekomendacji M. Zatem to banki jako instytucje finansowe szczególnie narażone na wystąpienie ryzyka operacyjnego winny samodzielnie dzięki monitorowaniu swojej działalności dążyć do stworzenia zamkniętego katalogu sytuacji, w których może wystąpić ryzyko operacyjne. Banki mogą także wypracować działania mające na celu uniknięcie wystąpienia ryzyka lub też stworzyć zestawienie działań służących usunięciu jego skutków. Badanie i analiza ryzyka operacyjnego winna być więc prowadzona przez instytucje i podmioty, które mają z nim do czynienia w praktyce. Wszelkie teoretyczne opracowania tego tematu mogą stanowić wskazówki dla kadry zarządzającej instytucją narażoną na tego rodzaju ryzyko, jednak nie mogą być traktowane jako kompleksowe regulacje zawierające pełny opis problemu. W mojej ocenie opracowanie metod, zasad, technik i praktyk zarządzania ryzykiem operacyjnym winno być przedmiotem wewnętrznych procedur każdej instytucji finansowej.

Literatura

- Holton G., *Defining risk*, "Financial Analysts Journal", listopad/grudzień 2004.
- Iwanicz-Drozdowska M., *Zarządzanie finansowe bankiem*, Polskie Wydawnictwo Ekonomiczne, Warszawa 2012.
- Lewandowski D., *Ryzyko operacyjne w bankach – zarządzanie i audyt w świetle wymagań Bazylejskiego Komitetu ds. Nadzoru Bankowego*, Bank i Kredyt nr 4 z kwietnia 2004.
- Krasodomska J., *Zarządzanie ryzykiem operacyjnym w bankach*, Polskie Wydawnictwo Ekonomiczne, Warszawa 2008.
- Zawadzka Z., *Zarządzanie ryzykiem w banku komercyjnym*, Poltext, Warszawa 1996.
- Kałużny R., *Strzegąc swego banku*, „Bank”, nr 3, 2004.
- Fabozzi F., *Operational Risk. A Guide to Basel II Capital Requirements, Models, and Analysis*, New York 2007.

- Iwanicz-Drozdowska M., Nowak A., *Ryzyko bankowe*, wyd. 2, Oficyna Wydawnicza SGH, Warszawa 2002.
- Rutkowska-Tomaszewska E., *Nadzór bankowy*, [w:] R. Mastalski, E. Fojcik-Mastalska, *Prawo finansowe*, Warszawa 2011.
- Jorion P., *Financial Risk Manager Handbook*, Second Edition, John Wiley&Sons, Hoboken, New Jersey 2003.
- Stiglitz J., *Freefall: Free Markets and the Sinking of the Global Economy*, Allen Lane/Penguin Books, London 2010.
- Kawulski A., *Prawo bankowe – komentarz*, LexisNexis, Warszawa 2013.
- Matkowski P., *Zarządzanie ryzykiem operacyjnym*, Oficyna Ekonomiczna, 2006.
- Jajuga K., *Zarządzanie ryzykiem*, Wydawnictwo Naukowe PWN, Warszawa 2007.
- Marcinkowska M., *Standardy kapitałowe banków*, Regan Press, Gdańsk 2009.
- Heffernan S., *Nowoczesna bankowość*, Wydawnictwo Naukowe PWN, Warszawa 2007.

Akty prawne

- Uchwała nr 180/2011 Komisji Nadzoru Finansowego z dnia 19 lipca 2011 r. w sprawie wydania Rekomendacji H dotyczącej systemu kontroli wewnętrznej w bankach. Na podstawie art. 137 pkt 5 Ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe (Dz.U. z 2002 r. nr 72, poz. 665, z późn. zm.) i art. 11 ust. 1 Ustawy z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym (Dz.U. nr 157, poz. 1119, z późn. zm.).
- Komunikat nr 2 Ministra Finansów z dnia 17 czerwca 2013 r. w sprawie standardów audytu wewnętrznego dla jednostek sektora finansów publicznych opublikowany w Dzienniku Urzędowym Ministra Finansów z dnia 24 czerwca 2013 r., poz. 15.
- Uchwała nr 8/2013 Komisji Nadzoru Finansowego z dnia 8 stycznia 2013 r. w sprawie wydania Rekomendacji M dotyczącej zarządzania ryzykiem operacyjnym w bankach.
- Generalny Inspektorat Nadzoru Bankowego. Metody proste wyliczania wymogów kapitałowych z tytułu ryzyka operacyjnego, Dokument konsultacyjny, DK/04/OPR, 2005.
- Ustawa z dnia 21.07.2006 r. o nadzorze nad rynkiem finansowym (Dz.U. nr 157, poz. 1119 z późn. zm.).

Materiały ze strony www.knf.gov.pl

- Sytuacja sektora bankowego w Polsce na dzień 31.12.2010 r. (19.02.2011).
- BION w bankach – mapa klas ryzyka i ich definicje, www.knf.gov.pl (01.02.2011 r.).