GOSPODARKA NARODOWA

1
(275)
Rok LXXXV/XXVI
styczeń–luty
2015
s. 103–128

Ewa CICHOWICZ*
Agnieszka K. NOWAK**

Zarządzanie ryzykiem operacyjnym w wybranych bankach w Polsce

Streszczenie: Z uwagi na narastające znaczenie ryzyka operacyjnego w działalności instytucji sektora finansowego, coraz większa rola zaczęła być przypisywana procesowi skutecznego zarządzania tym ryzykiem. Głównym celem artykułu jest zbadanie, czy kadra zarządzająca bankiem ma świadomość istnienia ryzyka operacyjnego, a jeśli tak, to określenie jak przebiega zarządzanie nim, a w szczególności – w jaki sposób dokonywane są jego pomiar i kontrola. Umożliwić to ma (poprzedzona wstępem teoretycznym) analiza porównawcza przeprowadzona w zakresie identyfikacji ryzyka operacyjnego i systemów zarządzania tym ryzykiem w wybranych bankach komercyjnych w Polsce. Dane do analizy zostały pozyskane ze sprawozdań finansowych za 2013 r. opublikowanych przez 10 banków komercyjnych, wybranych metodą ekspercką. Na podstawie przeprowadzonego badania można stwierdzić, że we wszystkich badanych bankach dostrzegana jest ich ekspozycja na ryzyko operacyjne, przy świadomości braku możliwości jego całkowitego wyeliminowania. Zauważalne jest również to (chociaż występują pewne różnice w zakresie definicji), że banki opierają się na określeniu ryzyka operacyjnego wskazanym przez Komitet Bazylejski. Banki identyfikują także potrzebę posiadania systemów zarządzania tym ryzykiem i dostrzegają konieczność ich systematycznej poprawy, polegającej m.in. na: usprawnianiu procesu zarządzania nim, doskonaleniu metod i narzędzi monitorowania, aktualizacji bazy zdarzeń ryzyka operacyjnego, wdrożeniu systemu samooceny czy regularnej walidacji systemu i modelu wyznaczania wymogu kapitałowego.

Słowa kluczowe: ryzyko bankowe, ryzyko operacyjne w bankach, monitorowanie ryzyka operacyjnego w bankach, wskaźniki KRI, metody pomiaru ryzyka operacyjnego w bankach

Kody JEL: G21, G32

* Szkoła Główna Handlowa w Warszawie, Instytut Gospodarstwa Społecznego, e-mail: ecicho1@sgh.waw.pl

** Szkoła Główna Handlowa w Warszawie, Instytut Finansów, e-mail: anowak1@sgh.waw.pl

Artykuł nadesłany 22 maja 2014 r., zaakceptowany 7 stycznia 2015 r.

Wprowadzenie

Systematyczny wzrost ekspozycji banków na ryzyko operacyjne [Doerig, 2001; 2003, s. 7; Chernobai i inni, 2007, s. 2–4] oraz zagrożenie niewystarczającej adekwatności i skuteczności metod zarządzania nim, przyczyniły się do wejścia w życie w styczniu 2013 r. znowelizowanej Rekomendacji M Komisji Nadzoru Finansowego, dotyczącej zarządzania ryzykiem operacyjnym w bankach [DzUrz KNF, 2013, poz. 6 z dnia 27 lutego 2013 r.][1]. We wstępie Rekomendacji, Komisja podkreśliła, że analizy przykładów zdarzeń operacyjnych wskazują, iż ryzyko to, obok ryzyka kredytowego, jest najistotniejszym rodzajem ryzyka w bankach. W informacjach prezentowanych na stronie internetowej, KNF podkreśliła, że oczekuje wprowadzenia zaleceń z Rekomendacji nie później niż do 30 czerwca 2013 r. (z wyjątkiem pkt 17.3 – do 31 grudnia 2013 r.)[2].

Celem opracowania jest zbadanie, czy banki działające w Polsce mają świadomość istnienia ryzyka operacyjnego, czy je definiują i czy zbudowały systemy jego monitorowania, a także weryfikacja zgodności polityki banków z ujętymi w Rekomendacji zaleceniami oraz z dobrymi praktykami rynkowymi kluczowych elementów procesu zarządzania ryzykiem operacyjnym. W tym celu porównano sposób identyfikacji i systemy zarządzania ryzykiem operacyjnym w wybranych dziesięciu bankach komercyjnych działających w Polsce, tj.: w PKO BP S.A., Banku Pekao S.A., Banku Zachodnim WBK S.A., Alior Banku S.A., Banku BGŻ S.A., ING Banku Śląskim S.A., Banku Ochrony Środowiska S.A., Banku Millennium S.A., mBanku S.A. oraz Banku BPH S.A. Wybór banków został dokonany metodą ekspercką. Kierowano się ich zróżnicowaniem, zarówno pod względem obsługiwanych klientów (np. mBank S.A. to bank klientów korporacyjnych, a PKO BP S.A. – detalicznych), jak i struktury własności (kapitał zagraniczny oraz polski). Banki te są notowane na Giełdzie Papierów Wartościowych w Warszawie. Badanie zostało przeprowadzone na podstawie informacji prezentowanych przez te banki w sprawozdaniach finansowych (jednostkowych) za 2013 r.

Nie udało się w pełni ujednolicić prezentacji systemów zarządzania ryzykiem operacyjnym w badanych bankach. Wynika to z faktu, że informacje prezentowane w sprawozdaniach finansowych, nawet przy pewnej standaryzacji, różnią się zakresem, szczegółowością, jak i jakością. Dla zapewnienia przejrzystości prezentacji, zgodnie z Rekomendacją M oraz dobrymi praktykami rynkowymi, do analizy wybrano 10 elementów istotnych dla prawidłowo

[1] Załącznik do Uchwały Nr 8/2013 KNF z dnia 8 stycznia 2013 r. w sprawie wydania Rekomendacji M dotyczącej zarządzania ryzykiem operacyjnym w bankach.

[2] http://www.knf.gov.pl/aktualnosci/2013/Przyjecie_nowej_Rekomendacji_M.html (10.10.2014).

funkcjonującego systemu zarządzania ryzykiem operacyjnym w bankach komercyjnych.

Analiza systemów została natomiast poprzedzona podstawowymi dla tematu zagadnieniami związanymi z aspektami definicyjnymi oraz metodami kontrolowania.

Ryzyko operacyjne

Pojęcie ryzyka operacyjnego nie jest jednoznaczne, co widać już w różnorodności jego definicji formułowanych od ok. 25 lat. Termin ten pierwotnie oznaczał ryzyko, którego nie można nazwać ani ryzykiem kredytowym ani ryzykiem rynkowym. Ponieważ niniejsza definicja (skonstruowana przez zaprzeczenie) uznana została za zbyt rozległą [Hull, 2011, s. 480], dlatego jeśli jest obecnie przywoływana, to występuje razem z dodatkowymi warunkami, które wykluczają z niej m.in. ryzyko związane z wchodzeniem na nowe rynki czy ryzyko biznesowe. Z drugiej strony, spotykana w literaturze koncepcja, że ryzyko operacyjne można rozumieć jako ryzyko związane ze standardową działalnością operacyjną banku (a zatem pojęcie przeciwstawne do ryzyka strategicznego) [Holton, 2004, s. 2] wydaje się zbyt wąska. Takie założenie ogranicza przecież obszar ryzyka operacyjnego, przypisując mu charakter techniczno-organizacyjny [Zawadzka, 1996, s. 13–14].

Wobec powyższego, lepiej uzasadnione merytorycznie podejście przyjął R. Kałużny, który zdefiniował ryzyko operacyjne jako „ryzyko nie tylko związane z czynnikami wewnętrznymi (wynikającymi z operacyjnej działalności banku), ale i zewnętrznymi, takimi jak: katastrofy czy klęski żywiołowe" [Kałużny, 2004, s. 22–23]. Do komponentów ryzyka operacyjnego zaliczył zaś ryzyko:

- kadrowe, związane z zarządzaniem personelem i ładem korporacyjnym;
- technologiczne, powiązane z systemami informatycznymi i stosowanymi z bankach zabezpieczeniami;
- niewłaściwego obiegu dokumentów i informacji, wynikające ze źle zaprojektowanych procesów lub błędów pracowników;
- relacji banku z jego otoczeniem, w tym, w szczególności, w sferze zaufania publicznego i reputacji;
- zdarzeń nadzwyczajnych, takich jak: klęski żywiołowe czy ataki terrorystyczne;
- kryminalne, związane z ryzykiem przestępstwa.

Z kolei jeszcze inną koncepcję przedstawił J. Bessis, który uznał, że ryzyko operacyjne związane jest ze źle funkcjonującymi systemami informacyjnymi, systemami raportowania oraz wewnętrznymi zasadami monitorowania ryzyka, procedurami i polityką prowadzoną przez bank wobec tego ryzyka [Bessis, 2002, s. 20–21]. Dodatkowo wskazał on cztery wymiary, w których ono występuje – poziom ludzi, procesów, techniczny (modeli i narzędzi) oraz systemów IT.

Należy ponadto zauważyć, że z uwagi na fakt, iż zarządzanie ryzykiem operacyjnym stanowi ważny aspekt funkcjonowania banku, liczne definicje tego ryzyka powstają również w instytucjach finansowych. Na przykład w Bank of America ryzyko to oznacza zmienność zysków spowodowaną przez realizację operacji, procesy, ludzi, technologie, prawo, regulacje, reputację firmy i zdarzenia zewnętrzne. Dla British Bankers Association – ryzyko bezpośrednich i pośrednich strat, wynikających z niedostosowania lub zawodności wewnętrznych procesów, ludzi i systemów technicznych lub z przyczyn zewnętrznych, a dla Federal Reserve Bank of New York – ryzyko związane ze wszystkimi czynnikami ryzyka, które mają wpływ na zmienność struktury kosztów firmy, nie zaś na strukturę przychodów.

Niewątpliwie jednak najczęściej cytowaną definicją ryzyka operacyjnego jest definicja sformułowana w 2004 r. przez Komitet Bazylejski ds. Nadzoru Bankowego, według którego jest to „ryzyko straty wynikającej z niewłaściwych lub zawodnych procesów wewnętrznych, ludzi i systemów lub ze zdarzeń zewnętrznych" [*International Convergence*…, 2004, s. 137]. Uwzględnia ono ryzyko prawne, tj. związane z ponoszeniem konsekwencji naruszenia (celowo lub nieświadomie) aktów prawnych i warunków zawartych umów, natomiast tym terminem nie obejmuje się ryzyka strategicznego i ryzyka reputacji, które dotyczą poniesienia strat z tytułu utraty zaufania do banku przez potencjalnych i aktualnych klientów oraz partnerów biznesowych, spowodowanych działaniami na szkodę banku lub upadłością w całym sektorze bankowym. Według International Association of Financial Engineers, w ramach ryzyka operacyjnego należy również uwzględnić ryzyko strategiczne, reputacji, a także powiązania ryzyka operacyjnego z innymi rodzajami ryzyka (np. kredytowym i rynkowym) [Piołunowicz, 2006, s. 50]. Nieuwzględnienie w definicji ryzyka operacyjnego tych dwóch typów ryzyka, przy jednoczesnym włączeniu do niej ryzyka prawnego, spowodowane jest chęcią stworzenia minimalnych zasad, dotyczących wymogów kapitałowych, liczonych z tytułu ryzyka operacyjnego [Ślązak, 2007, s. 423].

Dodatkowo, w podejściu prezentowanym przez Komitet Bazylejski, zostały wyszczególnione cztery typy źródeł występowania tego ryzyka: procesy, ludzie, systemy i zdarzenia zewnętrzne (tabela 1).

Tabela 1. Kategorie zdarzeń operacyjnych (uwzględnione w definicji ryzyka operacyjnego)

Definicja		Kategoria zdarzeń operacyjnych
Ryzyko operacyjne	procesy	dokonywanie transakcji oraz zarządzanie procesami
	ludzie	oszustwo wewnętrzne zarządzanie kapitałem ludzkim i bezpieczeństwo pracy klienci, produkty i praktyka biznesowa
	systemy	zaburzenia działalności i błędy systemów
	zdarzenia zewnętrzne	utrata lub uszkodzenie aktywów fizycznych oszustwo zewnętrzne

Źródło: J. Krasodomska [2008, s. 23].

Wyróżnione zostały również poszczególne kategorie zdarzeń operacyjnych. Są to [*International Convergence*…, 2004, s. 224–225]:

1) oszustwo wewnętrzne – straty wynikające z działania przynajmniej jednego pracownika, który ma na celu świadome oszustwo, obejście przepisów, sprzeniewierzenie własności, wyłączając dyskryminację (np. kradzież, defraudacja),
2) oszustwo zewnętrzne – straty związane z działaniami osób trzecich, mające na celu zamierzone oszustwo, obejście regulacji, sprzeniewierzenie własności (np. hackerstwo, rabunek),
3) zarządzanie kadrami i bezpieczeństwo pracy – straty z tytułu wypłat odszkodowań za wypadki w miejscu pracy i dyskryminację oraz z tytułu postępowania niezgodnego z przepisami prawa pracy i BHP, a także wbrew warunkom umowy z pracownikami (np. strajki, wypadki w miejscu pracy),
4) uszkodzenie aktywów – straty będące konsekwencją zniszczenia lub utraty aktywów fizycznych z powodu klęsk żywiołowych, ataków terrorystycznych czy wandalizmu,
5) klienci, produkty i praktyka biznesowa – straty, które są rezultatem nieumyślnego (bądź wynikającego z zaniedbania) niewypełnienia obowiązków wobec klientów lub które wynikają z charakteru lub samej struktury produktu (np. agresywna sprzedaż, manipulacje rynkiem finansowym, naruszenie prywatności),
6) zaburzenia działalności i błędy systemów – straty związane z błędami i zakłóceniami pracy systemów (np. sieci, awarie systemu operacyjnego do obsługi klientów),
7) dokonywanie transakcji, dostawa i zarządzanie procesami – straty powstałe w wyniku występowania błędów w trakcie realizacji transakcji bądź zarządzania procesami (np. zagubienie dokumentacji).

Jednocześnie trzeba dodać, że pomimo powszechności stosowania definicji wprowadzonej przez Komitet, możliwe jest (pod pewnymi warunkami, tj. akceptacji przez władze nadzorcze) indywidualne określenie pojęcia ryzyka operacyjnego do celów zarządczych. Dowolność taka nie jest natomiast możliwa przy wyliczaniu wymogów kapitałowych.

Niezależnie przy tym od stosowanych definicji ryzyka operacyjnego, charakteryzuje się ono brakiem możliwości całkowitej eliminacji jego źródeł, jak i trudnościami w analizie czynników ryzyka oraz jego skutków, ustaleniu jego „właścicieli" i pomiarze. Ponadto ten rodzaj ryzyka jest specyficzny dla każdego banku – zależy od jego struktury organizacyjnej, systemu przepływu informacji, jakości i sposobu zarządzania, a jednocześnie nie jest ono podejmowane w celu osiągnięcia korzyści finansowych – jest niejako wbudowane w produkty i procesy biznesowe [Lewandowski, 2004, s. 49]. Z kolei w szacowaniu potencjalnych strat operacyjnych z jego tytułu, analizowane są przede wszystkim rozkłady częstotliwości i dotkliwości straty (najczęstszy podział opiera się na wyróżnieniu strat o dużej częstotliwości i niewielkim wpływie na wyniki oraz strat o małej częstotliwości i dużym wpływie [Gospodarowicz, 2007, s. 269–270]).

Pomiar ryzyka operacyjnego

Przyjęcie odpowiedniej definicji ryzyka operacyjnego jest ważnym elementem procesu zarządzania nim, pozwala bowiem nie tylko na jego identyfikację, ale stanowi punkt wyjścia do pomiaru, jego monitorowania i ograniczania. O ile jednak widoczne jest dążenie do ujednolicania definicji ryzyka operacyjnego i pojęć jemu pokrewnych, o tyle w przypadku kolejnych etapów zarządzania nim, można wyodrębnić różne podejścia sugerowane w literaturze przedmiotu, proponowane przez władze nadzorcze lub stosowane w praktyce.

Jeden z częściej spotykanych podziałów metod pomiaru ryzyka operacyjnego opiera się na wyborze kierunku przeprowadzanych analiz – analizie odgórnej (*top-down*) i analizie oddolnej (*bottom-up*) [Thlon, 2012, s. 72–76]. W pierwszym z podejść, punktem wyjścia są cele organizacji. Polega ono na określeniu prawdopodobieństwa i wielkości potencjalnych strat oraz identyfikacji zagrożeń, które mogą uniemożliwiać realizację celów organizacji. Z kolei drugie podejście koncentruje się na źródłach ryzyka. Źródła te odnoszą się do zależności między działaniami ludzi, technologii i procedur w organizacji, a określonymi zdarzeniami wewnętrznymi i zewnętrznymi. Instytucja zostaje podzielona według obszarów działalności, a następnie, w każdym z nich, mierzy się ryzyko, które na koniec jest sumowane dla całej instytucji.

Inna, ale równie powszechna klasyfikacja metod pomiaru ryzyka operacyjnego, różnicuje je pod względem rodzaju wykorzystywanych danych. Tu metody zostały podzielone na: jakościowe, ilościowe oraz (wyróżniane niekiedy) mieszane – ilościowo-jakościowe [Orzeł, 2005b, s. 4]. Pojęcie metod jakościowych obejmuje metody wykorzystujące oceny ekspertów, które opierają się na ich wiedzy, doświadczeniu czy intuicji. Uzyskany na ich podstawie opis lub zobrazowanie graficzne, pozwalają oszacować niezbędne parametry. Niestety w przypadku tego podejścia występuje ryzyko popełnienia błędów. Do tych metod zalicza się rozmaite techniki heurystyczne i metody opisowe oraz takie narzędzia jak: wywiady, ankiety, mapowanie ryzyka, metody samooceny (np. *Risk self-assessment*, RSA czy *Control self-assessment*, CSA).

Często stosowanymi metodami jakościowymi są techniki mapowania ryzyka i metody samooceny. Mapa ryzyka stanowi rezultat końcowy przypisania poszczególnym obszarom banku częstości i wartości zdarzeń operacyjnych, dzięki wykorzystaniu danych historycznych, skorygowanych o wyniki samooceny, kluczowych wskaźników ryzyka (*Key Risk Indicator*, KRI) lub analizy scenariuszy. Mapowanie ryzyka prowadzi do zilustrowania stopnia ekspozycji banku na ryzyko operacyjne w różnych przekrojach (produktu, procesu czy linii biznesowej). Na tej podstawie zostają wskazane obszary szczególnie obciążone ryzykiem operacyjnym, co ułatwia zdefiniowanie priorytetów, celem ograniczenia możliwości wystąpienia zdarzeń ryzyka operacyjnego. Z kolei samoocena poziomu ryzyka przeprowadzana jest na wszystkich poziomach zarządczych, a dokonują jej pracownicy danej instytucji. Zakłada się bowiem, że osoby zatrudnione w organizacji mają największą wiedzę na temat obszarów najbardziej zagrożonych ryzykiem. Samoocena jest zatem stosunkowo

prosta i charakteryzuje się dużą elastycznością, ale jest obarczona subiektywizmem, co wpływa niekorzystnie na jej wiarygodność. Metoda ta może być więc określona jako progresywna, pozwala uzyskać informacje o potencjalnych zdarzeniach operacyjnych, wykryć sytuacje awaryjne, a ponadto – usunąć niedoskonałości systemu. Dzięki niej możliwe jest też stworzenie efektywnych kanałów komunikacji pracownicy – kadra zarządzająca oraz może być ona punktem wyjścia do podjęcia działań organizacyjno-proceduralnych, mających na celu ograniczenie ryzyka. Do tych działań przede wszystkim zalicza się: szkolenia kadr, usprawnienia procesów operacyjnych, opracowanie oraz testowanie planów awaryjnych czy planów ciągłości działania (*Business Continuity Plan*, BCP).

Jako metodę mieszaną, najczęściej wskazuje się natomiast KRI [Orzeł, 2005a, s. 4]. Opiera się ona na identyfikacji obszarów szczególnie narażonych na ryzyko, a następnie na określeniu miar, które w sposób optymalny reprezentują ekspozycję na to ryzyko i spełniają dodatkowe kryteria (np. obiektywności, porównywalności, korelacji z ryzykiem). Za KRI uznaje się więc zestaw parametrów procesu biznesowego, odzwierciedlających z dużym prawdopodobieństwem zmiany profilu ryzyka operacyjnego tego procesu. Każdy wskaźnik powinien być przy tym precyzyjnie zdefiniowany oraz powinny zostać określone wobec niego poziomy ostrzegawcze i działania konieczne do podjęcia w razie ich osiągnięcia. W rezultacie, KRI stanowią jedno ze źródeł danych, umożliwiających modelowanie ryzyka operacyjnego, a ich analiza powinna pozwolić na wychwycenie potencjalnych zmian, związanych z ryzykiem operacyjnym (w perspektywie bieżącej lub przyszłej). Są one także narzędziem wczesnego ostrzegania (przed materializacją straty), a obserwacja ich wartości jest pomocna przy wskazywaniu trendów w ramach zidentyfikowanych kategorii ryzyka. Wykorzystuje się je ponadto do monitorowania zmian w zakresie ekspozycji na ryzyko. Z drugiej strony, niezwykle trudne jest stworzenie skutecznego i kompleksowego systemu KRI, a następnie utrzymywanie jego adekwatności do profilu ryzyka. Stąd musi być systematycznie przeprowadzany przegląd wykorzystywanych KRI, celem aktualizacji ich zestawu. Nie zawsze można także zdefiniować dany wskaźnik, a niektóre z nich wymagają powiązania ich z innymi kluczowymi wskaźnikami ryzyka. Oprócz tego, tak uzyskana informacja o ekspozycji oznacza jedynie potencjalne jej istnienie.

Z kolei za pomocą metod ilościowych, dochodzi do przetwarzania danych mierzalnych. Spośród wielu rodzajów tych metod można wskazać m.in.: metody oparte na modelach statystycznych (np. *Value at Risk* – VAR, *Extreme Value Theory* – EVT, scenariusze awaryjne, sieci bayesowskie). Przykładowo w metodyce opartej na VAR (*Operational VaR*, OpVAR) sporządza się bazę danych operacyjnych banku, która za pomocą metod statystycznych (zmodyfikowanych dla potrzeb oszacowania ekspozycji na ryzyko operacyjne) umożliwia oszacowanie maksymalnej hipotetycznej straty w danym okresie, przy założonym poziomie ufności i normalnych warunkach rynkowych. Z kolei szacowanie ryzyka operacyjnego na podstawie metody EVT opiera się na przyjęciu rozkładów strat, wywołanych przez ryzyko operacyjne na poziomie strat

maksymalnych, jakie może ponieść bank z tytułu danego zdarzenia. Metoda wykorzystująca scenariusze awaryjne umożliwia zaś dokonanie subiektywnej analizy wpływu hipotetycznych zdarzeń na poziom ryzyka operacyjnego, co pozwala na dostarczenie danych na temat źródeł tego ryzyka. Koncepcja sieci bayesowskich przedstawia natomiast zależności (o charakterze probabilistycznych), występujące pomiędzy zdarzeniami z wykorzystaniem rachunku prawdopodobieństwa, łącząc ilościowe dane o zaistniałych stratach z jakościowymi szacunkami ekspertów.

Za odrębną grupę metod pomiaru uznaje się metody służące do obliczania wymogu kapitałowego z tytułu ekspozycji na ryzyko operacyjne. Mowa o metodzie podstawowego wskaźnika (*Basic Indicator Approach*, BIA), metodzie standardowej (*Standarised Approach*, TSA) i alternatywnej metodzie standardowej (*Alternative Standarised Approach*, ASA) oraz metodzie pomiaru wewnętrznego (*Advanced Measurement Approach*, AMA) [Marcinkowska, 2009, s. 265–274]. W żadnej z nich nie mierzy się bezpośrednio poziomu ryzyka operacyjnego, a w zamian za to wyznaczany jest kapitał niezbędny do pokrycia strat, wynikających z tego ryzyka. Należy przy tym wspomnieć, że wybór metody uzależniony jest od spełnienia warunków wyznaczonych przez instytucję nadzorczą.

Najprostszą jest metoda BIA. W jej ramach oblicza się poziom kapitału z tytułu ryzyka operacyjnego, który powinien być utrzymywany w wysokości odpowiadającej stałemu procentowi (równemu obecnie a = 15%) średniej z trzech ostatnich, dodatnich rocznych wyników brutto. Wynik brutto jest zatem uznawany za miarę ukazującą ekspozycję na ryzyko operacyjne. Metoda TSA stanowi rozwinięcie metody podstawowej. Zgodnie z nią, wynik brutto zostaje podzielony na osiem linii biznesowych, z których każda ma zdefiniowany współczynnik b. Średni roczny dochód brutto z trzech ostatnich lat z każdego obszaru działalności mnoży się następnie przez czynnik b danego obszaru, a wysokość wymaganego kapitału stanowi sumę wszystkich tych iloczynów. Różnica pomiędzy metodą ASA a TSA polega na odmiennych podstawach wskaźnika b dla dwóch linii biznesowych (bankowości detalicznej i bankowości korporacyjnej). W metodzie alternatywnej nie jest to wynik brutto, ale wolumen kredytów i pożyczek pomnożony przez współczynnik 0,035. Obie metody są więc przykładami podejścia *top-down*.

W przypadku metody AMA (zaawansowanej metody pomiaru ryzyka operacyjnego, reprezentującej koncepcję *bottom-up*), wymóg kapitałowy porównywany jest do wielkości tego ryzyka, wyznaczonej na podstawie wewnętrznego systemu pomiaru, przy zastosowaniu kryteriów jakościowych i ilościowych. Komitet Bazylejski nie określił jednak ani metod ani zasad tego pomiaru. Mimo dowolności w zakresie modelowania ryzyka operacyjnego, często uwzględnia się trzy podejścia rozwijane przez zainteresowane tym procesem instytucje: metodę rozkładu strat (LDA), metodę scenariuszową (sbAMA) i metodę czynników ryzyka i kontroli (RDCA) – określaną wcześniej podejściem na bazie karty wyników [Matkowski, 2006, s. 144–158]. Niekiedy wymieniana jest także metoda wewnętrznych pomiarów (IMA), uznawana za najprostszą z metod

zaawansowanych, metoda pojedynczej straty (SLA) czy metoda wartości ekstremalnych (EVT) [Urbankowska-Bąk, 2012, s. 310–320]. W odróżnieniu przy tym od metod podstawowych, metoda AMA powinna opierać się na informacjach o stratach operacyjnych banku, wybranych i przeskalowanych danych zewnętrznych, kluczowych wskaźnikach ryzyka, wynikach RCSA, wynikach analizy scenariuszy oraz uwzględniać czynniki otoczenia gospodarczego i kontroli wewnętrznej, a także ewentualną redukcję wymogu kapitałowego z tytułu transferu ryzyka. Następnie na tej podstawie konstruuje się model, wskazujący wielkość kapitału potrzebnego na pokrycie strat z tytułu ryzyka operacyjnego przy zadanym poziomie ufności.

Z uwagi na fakt, że metody podstawowe zakładają pewne uogólnienia, nie jest możliwe precyzyjne wyliczenie rzeczywistej ekspozycji na ryzyko operacyjne. Lepsze wydaje się więc stosowanie bardziej kosztownych metod zaawansowanych, dzięki którym można dokonać dokładniejszego pomiaru, a dodatkowo uwzględniana jest dywersyfikacja między liniami biznesowymi i rodzajami ryzyka, co powinno pozwolić na zmniejszenie wysokości wymogów kapitałowych z tytułu ryzyka operacyjnego. Trzeba przy tym uwzględnić, że zmniejszenie poziomu kapitału przy wyborze metod zaawansowanych jest ograniczone przez nadzór[3].

Warto w tym miejscu jeszcze wspomnieć, że niejako uzupełnieniem prowadzonej polityki wobec ryzyka operacyjnego jest jego transfer. Dzieli się go na transfer działalności generującej ryzyko (*outsourcing* lub *insourcing*) oraz transfer odpowiedzialności za skutki ryzyka (polisy ubezpieczeniowe czy alternatywne techniki transferu ryzyka (*Alternative Risk Transfer*, ART)).

Systemy zarządzania ryzykiem operacyjnym w badanych bankach komercyjnych[4]

W celu usystematyzowania prezentacji systemów zarządzania ryzykiem operacyjnym w badanych bankach komercyjnych działających w Polsce, opis będzie obejmował (możliwe do wyodrębnienia na podstawie dostępnych informacji) podstawowe etapy procesu zarządzania ryzykiem operacyjnym, ujęte w Rekomendacji M[5] oraz zagadnienia z nim związane, prezentowane przez banki w sprawozdaniach finansowych (zgodnie z dobrymi praktykami rynkowymi). Będzie to łącznie 10 elementów istotnych dla procesu zarządzania

---

3 Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 575/2013 z dnia 26 czerwca 2013 r. w sprawie wymogów ostrożnościowych dla instytucji kredytowych i firm inwestycyjnych, zmieniające rozporządzenie (UE) nr 648/2012.

4 Niniejszy podrozdział został opracowany na podstawie informacji publikowanych przez badane banki w jednostkowych sprawozdaniach finansowych za 2013 r.

5 W Rekomendacji M KNF zostały wyodrębnione następujące etapy procesu zarządzania ryzykiem operacyjnym: strategia zarządzania ryzykiem operacyjnym, środowisko wewnętrzne, identyfikacja ryzyka, ocena ryzyka, przeciwdziałanie ryzyku, kontrola, monitorowanie oraz raportowanie i przejrzystość działania.

ryzykiem operacyjnym w bankach, tzn.: 1) definicja ryzyka operacyjnego i cele zarządzania (identyfikacja ryzyka), 2) strategia, 3) struktura organizacyjna zarządzania tym ryzykiem (środowisko wewnętrzne), 4) metody i narzędzia kontroli, 5) stress testy, plany awaryjne oraz BCP, 6) unikanie ryzyka (ograniczanie, transfer oraz ubezpieczenie), 7) raportowanie, 8) wyznaczanie wymogów kapitałowych, 9) zarządzanie ryzykiem w grupie kapitałowej oraz 10) informowanie o poniesionych stratach z tytułu ryzyka operacyjnego.

PKO BP S.A.[6]

Przyjęta w PKO BP S.A. definicja ryzyka jest zgodna z definicją sformułowaną przez Komitet Bazylejski. Przy czym, z ryzyka operacyjnego Bank wydziela nie tylko ryzyko biznesowe (w tym ryzyko strategiczne)[7] i ryzyko reputacji[8], ale i ryzyko prawne (braku zgodności)[9].

Podstawowym celem zarządzania jest optymalizacja efektywności operacyjnej, polegająca na obniżaniu strat operacyjnych, redukcji kosztów oraz dążeniu do zwiększania szybkości i adekwatności reakcji na zdarzenia zewnętrzne. Zasady zarządzania ryzykiem zostały dostosowane i są zgodne ze znowelizowaną Rekomendacją M.

Zarządzanie ryzykiem operacyjnym ma dwupłaszczyznowy charakter, tzn. na poziomie systemowym (realizowane przez Centralę) i bieżącym (w każdej jednostce organizacyjnej). Podstawą budowanego systemu zarządzania są gromadzone dane o zdarzeniach ryzyka operacyjnego, o charakterze wewnętrznym i zewnętrznym, zawierające informacje na temat skutków ich powstania, o otoczeniu operacyjnym oraz efektywności kontroli wewnętrznej funkcjonalnej.

Bank systematyczne dąży do ograniczenia ekspozycji na to ryzyko; w tym celu stosuje: 1) instrumenty kontrolne, 2) instrumenty zarządzania zasobami ludzkimi (dobór kadr, podnoszenie kwalifikacji, systemy motywacyjne), 3) kluczowe wskaźniki ryzyka (ang. KRI, dla których określa wartości progowe i krytyczne), 4) strategiczne limity tolerancji i limity strat na ryzyko operacyjne, 5) plany awaryjne, 6) ubezpieczenia oraz 7) outsourcing.

---

6 http://www.pkobp.pl/media_files/f4f429ae-1140–4585-8af7-ecfc0ee^{3}d45f.pdf (14.03.2014).

7 W PKO BP S.A. ryzyko biznesowe definiowane jest jako ryzyko poniesienia strat wynikających z niekorzystnych zmian zachodzących w otoczeniu biznesowym, podjęcia niekorzystnych decyzji, nieprawidłowego wprowadzenia podjętych decyzji lub braku podjęcia odpowiednich działań, które miały być odpowiedzią na zachodzące w otoczeniu biznesowym zmiany, obejmuje ryzyko strategiczne.

8 Ryzyko reputacji to ryzyko związane z możliwością wystąpienia negatywnych odchyleń od zaplanowanego wyniku finansowego Banku w wyniki pogorszenia się wizerunku Banku.

9 Pod pojęciem braku zgodności PKO BP S.A. rozumie ryzyko poniesienia sankcji prawnych, powstania strat finansowych bądź utraty reputacji lub wiarygodności w skutek niezastosowania się PKO BP S.A., pracowników lub podmiotów działających w jego imieniu, do przepisów prawa, regulacji wewnętrznych oraz przyjętych przez bank standardów postępowania, w tym norm etycznych.

W przypadku wystąpienia zdarzenia ryzyka operacyjnego, stosowane jest jedno z trzech podejść: redukcja ryzyka (poprzez łagodzenie wpływu czynników wywołujących bądź skutków), transfer ryzyka (przeniesienie kosztów strat na podmiot zewnętrzny) lub unikanie ryzyka (wyeliminowanie czynnika ryzyka lub rezygnacja z działalności generującej ryzyko).

Bank Pekao S.A.[10]

W Banku Pekao S.A. definicja ryzyka operacyjnego jest zgodna z definicją ogłoszoną przez Komitet Bazylejski.

Celem zarządzania ryzykiem operacyjnym jest jego identyfikacja, ocena, monitorowanie, przeciwdziałanie oraz raportowanie. Badane są czynniki wewnętrzne i zewnętrzne, które mogą mieć istotny wpływ na realizację celów banku. Obowiązujący proces i zasady monitorowania są zgodne z przepisami zewnętrznymi, a także z wypracowanymi przez Grupę UniCredit standardami.

Organami odpowiedzialnymi za monitorowanie ryzyka operacyjnego są: Rada Nadzorcza (poprzez nadzór nad systemem zarządzania ryzykiem, kontrolę jego zgodności ze strategią Banku) i Zarząd Banku (opracowanie, wdrożenie i kontrola systemu zarządzania, skuteczność systemu kontroli wewnętrznej, monitorowanie procesu szacowania kapitału wewnętrznego i dokonywanie przeglądów efektywności tego procesu), Komitet Ryzyka Operacyjnego (wspieranie działań i nadzorowanie wykonania decyzji Zarządu Banku), Departament Zarządzania Ryzykiem Finansowym i Operacyjnym (monitorowanie i kontrolowanie ryzyka oraz raportowanie), Koordynatorzy ds. ryzyka operacyjnego (koordynacja zarządzania ryzykiem w pionie), a także dedykowane jednostki organizacyjne (kontrola specjalistycznych obszarów działalności Banku).

Kontrola prewencyjna ryzyka operacyjnego jest przeprowadzana na trzech poziomach zarządczych: kontrola na szczeblu działalności operacyjnej (realizowana przez wszystkich pracowników w ich zakresach odpowiedzialności), kontrola zarządzania ryzykiem (Departament Zarządzania Ryzykiem Finansowym i Operacyjnym) oraz kontrola na poziomie audytu wewnętrznego (Departament Audytu Wewnętrznego).

Do podstawowych narzędzi identyfikacji i pomiaru tego ryzyka Bank zalicza: gromadzenie danych na temat wewnętrznych i zewnętrznych zdarzeń operacyjnych, KRI, roczne limity strat i sublimity, analizę scenariuszy oraz tzw. samoocenę Pekao, natomiast do elementów przeciwdziałania ryzyku: trójstopniową kontrolę wewnętrzną, plany utrzymania ciągłości działania (*Business Continuity Planning*, BCP), plany awaryjne oraz ochronę ubezpieczeniową.

W procesie monitorowania kluczową rolę pełni informacja zarządcza, która jest przygotowywana dla: Komitetu Ryzyka Operacyjnego, Departamentu Audytu Wewnętrznego i kadry kierowniczej oraz Zarządu Banku i przedkładana

10 http://www.pekao.com.pl/informacje_dla_inwestorow/informacje_finansowe/sprawozdania_finansowe/ (21.03.2014).

Radzie Nadzorczej. Pozwala ona na ocenę profilu ryzyka, poziomu ekspozycji na ryzyko, jego ewolucji i rozłożenia geograficznego, stopnia wykorzystania rocznego limitu strat i sublimitów oraz skuteczności procesu odzyskiwania strat operacyjnych. Zawiera informacje o poziomach KRI oraz poziomie wymogu kapitałowego, a także analizę scenariuszy ryzyka operacyjnego. Raporty są opracowywane w trybie tygodniowym i miesięcznym.

Wymóg kapitałowy z tytułu ryzyka operacyjnego wyznaczany jest za pomocą metody AMA, zgodnie z modelem wewnętrznym zbudowanym przez Grupę UniCredit. Bazuje ona na danych dotyczących strat wewnętrznych, zewnętrznych i analizie scenariuszy, a także poziomach KRI. Wyznaczony całkowity wymóg kapitałowy alokowany jest na poszczególne podmioty Grupy, zgodnie z ich profilem ryzyka. Model ten jest systematycznie (tj. w okresach półrocznych) walidowany. Niezależnie od walidacji tego modelu, w Pekao S.A. (w Departamencie Zarządzania Ryzykiem Finansowym i Operacyjnym) dokonywana jest coroczna walidacja systemu zarządzania ryzykiem operacyjnym. Ma ona na celu zbadanie jego zgodności z przepisami zewnętrznymi oraz standardami Grupy. Wyniki walidacji modelu są poddawane niezależnemu przeglądowi przez Komórkę ds. Wewnętrznej Walidacji w Grupie UniCredit, a następnie – wraz z niezależnym przeglądem – są audytowane przez Departament Audytu Wewnętrznego. Wyniki walidacji przedkładane są do akceptacji Zarządowi Banku.

Bank Pekao S.A. bada i raportuje procentowy udział strat w stratach ogółem z tytułu zdarzeń operacyjnych w podziale na kategorie, zdefiniowane zgodnie z Uchwałą Nr 76/2010 KNF (z póź. zm.)[11], tj. oszustwa wewnętrzne, oszustwa zewnętrzne, zasady dotyczące zatrudnienia oraz bezpieczeństwo w miejscu pracy, klienci, produkty i praktyki operacyjne, szkody związane z aktywami rzeczowymi, zakłócenia działalności Banku i awarie systemów, wykonanie transakcji, dostawa i zarządzanie procesami operacyjnymi [DzUrz KNF, 2010, poz. 11 z dnia 9 kwietnia 2010 r. z poź. zm.].

Bank Zachodni WBK S.A.[12]

Bank Zachodni WBK S.A. (BZ WBK S.A.) stosuje definicję ryzyka operacyjnego zgodną z definicją Komitetu Bazylejskiego.

Celem zarządzania ryzykiem jest minimalizacja prawdopodobieństwa wystąpienia i/lub ograniczenie skutków niespodziewanych i niekorzystnych zdarzeń ryzyka operacyjnego. Jest ono monitorowane w ramach zintegrowanej

---

11 Analiza systemów zarządzania ryzykiem operacyjnym w poszczególnych bankach została dokonana na podstawie sprawozdań finansowych za rok 2013, kiedy to obowiązywała Uchwała Nr 76/2010 KNF z dnia 10 marca 2010 r. w sprawie zakresu i szczegółowych zasad wyznaczania wymogów kapitałowych z tytułu poszczególnych rodzajów ryzyka (DzUrz KNF, 2010, poz. 11 z dnia 9 kwietnia 2010 r. z poź. zm.). Od 1.01.2014 r. obowiązuje tzw. pakiet CRD IV/CRR. Szerzej na ten temat m.in. na oficjalnej stronie KNF: http://www.knf.gov.pl/pakiet_crd4.html (15.10.2014).

12 http://www.bzwbk.pl/_items/inwestor.bzwbk.pl/pdf/raport_roczny_bzwbk_2013.pdf (14.03.2014).

struktury zarządzania zidentyfikowanymi w Banku różnymi rodzajami ryzyka. Struktura ta obejmuje: identyfikację, pomiar, monitorowanie i kontrolę. Zasady monitorowania zostały opisane w: Strategii, Polityce i Zasadach zarządzania ryzykiem operacyjnym oraz w regulacjach wewnętrznych niższego szczebla. Standardy procesu zarządzania ryzykiem są tworzone przez powołany przez Zarząd Banku Komitet Zarządzania Ryzykiem Operacyjnym (ORMCO). Do jego zadań należą: wyznaczanie kierunków strategicznych działań, ustalanie i monitorowanie celów zarządzania tym ryzykiem, zapewnienie ciągłości biznesowej, bezpieczeństwo informacji, monitorowanie ryzyka outsourcingu i insourcingu oraz przeciwdziałanie przestępstwom. Jego posiedzenia stanowią forum do dyskusji nad problemami ryzyka operacyjnego; wyniki jego prac są raportowane Komitetowi Zarządzania Ryzykiem.

W proces monitorowania zaangażowani są pracownicy wszystkich szczebli organizacyjnych. Obejmuje on sieć elementów, ponieważ ryzyko operacyjne i jego skutki mogą być odczuwalne we wszystkich procesach biznesowych, w tym także w procesach wykonywanych przez podmioty zewnętrzne (w ramach outsourcingu lub formuły „strony trzeciej").

Do podstawowych narzędzi monitorowania Bank zalicza:

1) identyfikację i szacowanie ryzyka operacyjnego – dokonywaną w ramach samooceny; polega na oszacowaniu tego ryzyka na poziomie koherentnym i rezydualnym, pod kątem prawdopodobieństwa i konsekwencji wystąpienia potencjalnych zagrożeń oraz oceny skuteczności budowanych mechanizmów kontrolnych,
2) raportowanie i wnioskowanie – przygotowywane w cyklach miesięcznych raporty z jednostek biznesowych, których sporządzenie są podstawą zbiorczych raportów, pozwalających na określenie przyczyn, skutków, wniosków oraz działań naprawczych i prewencyjnych,
3) analizę KRI – wskaźniki tworzą mapę ryzyka operacyjnego; systematyczny ich monitoring stanowi system wczesnego ostrzegania,
4) BCP – w które wyposażone są wszystkie jednostki organizacyjne; są one systematyczne weryfikowane i testowane; Bank posiada zapasowe lokalizacje,
5) ubezpieczenie – materializacja ryzyka jest zabezpieczona za pomocą polis ubezpieczeniowych (w zakresie ryzyka finansowego, komunikacyjnego, ubezpieczenia mienia oraz odpowiedzialności cywilnej),
6) informacja zarządcza dla Komitetu Zarządzania Ryzykiem i Rady Nadzorczej – obejmuje dane dotyczące zdarzeń i strat operacyjnych, KRI i działań ograniczających to ryzyko.

Alior Bank S.A.[13]

Przyjęta w Alior Banku S.A. definicja ryzyka operacyjnego jest zgodna z definicją sformułowaną przez Komitet Bazylejski.

13 http://www.aliorbank.pl/pl/o_banku/relacje_inwestorskie/raporty_okresowe (7.03.2014).

Celem zarządzania ryzykiem operacyjnym jest jego minimalizacja, poprzez ograniczanie możliwości wystąpienia zdarzeń i incydentów ryzyka operacyjnego, a w przypadku ich wystąpienia – ograniczenie strat. Zasady zarządzania ryzykiem operacyjnym są zgodne z przepisami zewnętrznymi.

Ogólne zasady zarządzania ryzykiem operacyjnym zatwierdza Rada Nadzorcza, za przebieg procesu zarządzania i kontroli tego ryzyka jest odpowiedzialny Zarząd Banku. Rada Nadzorcza, na podstawie okresowych raportów, ocenia poziom ryzyka i, o ile zajdzie taka potrzeba, rekomenduje działania, mające na celu ograniczenie lub zmianę profilu tego ryzyka. Zarząd Banku akceptuje zasady, system i proces zarządzania, określa podział zadań, przeprowadza kontrolę procesu, zatwierdza strukturę i poziom limitów wewnętrznych, prezentuje rynkowi zasady i podejście do ryzyka, a także dba o usprawnianie procesu zarządzania tym ryzykiem. Działania Zarządu wspierane są przez Komitet Ryzyka Operacyjnego. Do jego zadań należą: bieżące monitorowanie ryzyka i jego ocena, wydawanie decyzji, ograniczających możliwości wystąpienia zdarzeń ryzyka operacyjnego, a w przypadku ich wystąpienia – redukujących ich skutki. Komitet wskazuje obszar operacyjny o wysokim stopniu narażenia na ryzyko, Zarząd Banku podejmuje decyzję o: akceptacji ryzyka, ograniczaniu poziomu, zaprzestaniu ryzykogennej działalności bądź o ubezpieczeniu zidentyfikowanych zdarzeń ryzyka operacyjnego. Za bieżące monitorowanie odpowiedzialne jest Biuro Ryzyka Operacyjnego. Do jego zadań należy: gromadzenie informacji o zdarzeniach ryzyka operacyjnego (wewnętrznych i zewnętrznych), monitorowanie poziomu KRI, opracowywanie raportów, ocena projektowanych produktów i procesów operacyjnych (z punktu widzenia ich odporności na ryzyko operacyjne) oraz wdrażanie i doskonalenie metod monitorowania. Natomiast kontrolowanie i ograniczanie ryzyka w działalności operacyjnej należy do obowiązków wszystkich pracowników. Ich zadaniem jest podejmowanie działań, mających na celu uniknięcie i/lub ograniczenie strat operacyjnych w obszarze ich odpowiedzialności.

W celu efektywnego monitorowania ryzyka, Biuro Ryzyka Operacyjnego prowadzi ewidencję zdarzeń, incydentów i strat operacyjnych (za pomocą dedykowanego narzędzia informatycznego)[14]. Do bieżącego monitorowania profilu i poziomu ryzyka stosowane są KRI. Są one wyznaczane w cyklach miesięcznych, analizowane na posiedzeniach Komitetu Ryzyka Operacyjnego i raportowane Zarządowi Banku oraz Radzie Nadzorczej.

Bank wyznacza wymóg kapitałowy z tytułu ryzyka operacyjnego za pomocą metody standardowej.

---

14 W Alior Banku S.A. w 2013 r. zanotowano 1 144 strat operacyjnych w wysokości 4,88 mln zł (dla porównania w 2012 r. – 684 straty operacyjne, w wysokości 2,46 mln zł).

Bank Gospodarki Żywnościowej S.A.[15]

Bank Gospodarki Żywnościowej S.A. (BGŻ S.A.) przyjmuje definicję ryzyka operacyjnego zgodną z definicją Komitetu Bazylejskiego, do jego obszaru włącza ryzyko prawne (w tym – ryzyko braku zgodności).

Zasady monitorowania ryzyka zostały zbudowane zgodnie z regulacjami nadzoru finansowego. Celem zarządzania ryzykiem operacyjnym jest ograniczenie strat i kosztów powodowanych zdarzeniami ryzyka operacyjnego, przy jednoczesnym zapewnieniu najwyższej jakości usług, bezpieczeństwa oraz zgodności działania z przepisami oraz dobrą praktyką rynkową.

System zarządzania ryzykiem i jego poziom nadzoruje Zarząd Banku. W swoich działaniach jest wspierany przez Komitet Zarządzania Ryzykiem i Bilansem Banku oraz Podkomitet ds. Ryzyka Operacyjnego i Zgodności oraz Przeciwdziałania Nadużyciom. Za wdrażanie metod monitorowania ryzyka odpowiedzialny jest Departament Zarządzania Ryzkiem Operacyjnym. W jego strukturach powołane zostały Stanowiska Zarządzania Ryzkiem Operacyjnym, umiejscowione w Centrach Regionów. Pełnią one rolę koordynatorów ryzyka operacyjnego. W komórkach organizacyjnych Centrali zadania koordynatorów są powierzone wytypowanym, przeszkolonym pracownikom. Ich zadaniem jest identyfikacja i raportowanie zdarzeń ryzyka operacyjnego. Dzięki powołaniu koordynatorów na wszystkich poziomach organizacyjnych, Bank ma zapewnioną kompletność danych, co zwiększa rzetelność oceny i ułatwia podejmowanie decyzji.

Kluczowym sposobem przeciwdziałania zdarzeniom ryzyka operacyjnego jest wczesna ich identyfikacja, ocena i jasno określone zasady działań je ograniczających. Informacje o zaistniałych zdarzeniach gromadzone są w centralnej bazie danych i stanowią podstawę do opracowywania raportów dla kierownictwa Banku.

Do oceny ryzyka operacyjnego Bank wykorzystuje: KRI oraz CSA. KRI są wykorzystywane przy ocenie ryzyka dla istotnych procesów wewnętrznych, według przyjętej, trzystopniowej skali oceny. Dodatkowym źródłem informacji są wyniki kontroli funkcjonalnej, przeprowadzanej we wszystkich jednostkach organizacyjnych Banku.

Do wyznaczenia wymogu kapitałowego Bank stosuje metodę BIA. W celu oszacowania kapitału ekonomicznego, Bank zbudował zasady i model statystyczny, pozwalający na oszacowanie kapitału ekonomicznego, zgodnego z profilem jego działalności. Model ten bazuje na danych gromadzonych od ponad dziesięciu lat w dedykowanej informatycznej bazie danych o stratach z tytułu zdarzeń ryzyka operacyjnego.

15 http://media.bgz.pl/1795/pl/presskit/8225 (14.03.2014).

ING Bank Śląski S.A.[16]

ING Bank Śląski S.A. (ING S.A.), w przyjętej definicji ryzyka operacyjnego, zaliczanego do ryzyk niefinansowych, uwypukla fakt narażenia Banku na stratę materialną (bezpośrednią bądź pośrednią) oraz ryzyko utraty reputacji. Przyczynami wystąpienia tego ryzyka, tak jak w definicji Komitetu Bazylejskiego, są: procesy wewnętrzne, ludzie, systemy techniczne lub zdarzenia zewnętrzne. W ryzyku operacyjnym uwzględnia się ryzyko oszustwa, natomiast wyodrębnia ryzyko braku zgodności.

Celem zarządzania ryzykiem operacyjnym jest utrzymanie go na akceptowalnym poziomie (zgodnie z przyjętym apetytem na ryzyko), mając na uwadze bezpieczeństwo środków klientów. Apetyt na ryzyko jest określany w formie limitów kwotowych strat, które mogą powstać w wyniku materializacji ryzyka. Limity te są, w trybie kwartalnym, monitorowane i raportowane do Zarządu Banku i Rady Nadzorczej.

System zarządzania ryzykiem oraz przeciwdziałania oszustwom został opracowany zgodnie z przepisami zewnętrznymi oraz dostosowany do standardów obowiązujących w Grupie ING. System ten jest regularnie usprawniany[17].

Zasady monitorowania ryzyka operacyjnego zostały uregulowane przez Zarząd Banku, po uzyskaniu akceptacji przez Radę Nadzorczą. Został opracowany pakiet przepisów wewnętrznych: strategia zarządzania ryzykiem operacyjnym oraz przeciwdziałania oszustwom i inne regulacje, normujące zakres i obowiązki pracowników. W celu zapewnienia ciągłości procesu zarządzania ryzykiem operacyjnym, w Centrali oraz w liniach biznesowych zostały powołane Komitety Zarządzania Ryzykiem Niefinansowym. Komitety w liniach biznesowych mają charakter wspierający decyzję Komitetu w Centrali.

W ING S.A. obowiązuje trójstopniowy system ochrony przed ryzykiem, tzn.: I – w jednostkach biznesowych (identyfikujący i ograniczający ryzyko w procesach biznesowych), II – w jednostkach ryzyka i wsparcia (odpowiedzialny za organizację procesów identyfikacji, monitorowanie i kontrolę), III – w audycie wewnętrznym (pełniący rolę niezależnego kontrolera).

---

16 http://www.ingbank.pl/relacje-inwestorskie/wyniki-finansowe#tab=1 (14.03.2014).

17 Przykładowo w 2013 r. zostały m.in. zwiększone: 1) skuteczność przeciwdziałania przestępstwom związanym z transakcjami płatniczymi i kradzieżami tożsamości lub środków finansowych z użyciem elektronicznych kanałów dystrybucji, 2) badanie bezpieczeństwa systemów informatycznych, 3) mechanizmy utrzymania ciągłości kluczowych procesów (w tym procesów podlegających outsourcingowi), 4) świadomość pracowników istnienia realnego zagrożenia tym ryzykiem w celu zwiększenia efektywności przeciwdziałania zdarzeniom ryzyka operacyjnego oraz przeciwdziałania oszustwom (za pomocą szkoleń). Por. http://www.ingbank.pl/relacje-inwestorskie/wyniki-finansowe#tab=1 (14.03.2014).

Bank Ochrony Środowiska S.A.[18]

W Banku Ochrony Środowiska S.A. (BOŚ S.A.) przyjęta definicja ryzyka operacyjnego jest zgodna z wytycznymi Komitetu Bazylejskiego. Ryzyko to jest monitorowane z uwzględnieniem ryzyka braku zgodności.

Celem zarządzania ryzykiem jest jego ograniczenie. Monitorowane są procesy, w których ekspozycja na ryzyko jest największa oraz dąży się do skrócenia czasu reakcji i zwiększenia efektywności podejmowanych działań, ograniczających skutki zdarzeń ryzyka operacyjnego. Bank określa tolerancję na ryzyko poprzez określenie limitów na poziomie zgodnym z akceptowalnym przez Radę Nadzorczą apetytem na ryzyko.

W BOŚ S.A. stosowany jest podział na bieżące i systemowe zarządzanie ryzykiem. Bieżące polega na: 1) prewencji zdarzeń ryzyka operacyjnego, 2) podejmowaniu działań, ograniczających liczbę i skalę zdarzeń ryzyka operacyjnego, 3) likwidowaniu negatywnych skutków oraz rejestrowaniu tych zdarzeń. Systemowe – ma na celu wypracowanie przepisów wewnętrznych, procedur i rozwiązań ograniczających ryzyko. Odpowiedzialność za bieżące zarządzanie ryzykiem spoczywa na wszystkich pracownikach, w tym w szczególności na kierownictwie. Pracownicy, w toku bieżącej działalności, mają zadanie identyfikować, kwantyfikować i ograniczać ryzyko w swoich obszarach. Za budowanie systemowego zarządzania, odpowiedzialne jest Biuro Ryzyka Operacyjnego.

Podstawową metodą monitorowania jest gromadzenie informacji o istotnych zdarzeniach ryzyka w bazie danych zdarzeń ryzyka operacyjnego, za pomocą dedykowanej aplikacji informatycznej. Wśród innych narzędzi należy wymienić: kontrolę wewnętrzną, okresowe przeglądy ryzyka oparte o proces samooceny, BCP i plany awaryjne oraz testy warunków skrajnych dla wymogów kapitałowych z tytułu ryzyka operacyjnego.

Raportowanie zarządcze ma charakter bieżący (za pomocą aplikacji informatycznej, w której są odkładane dane o zdarzeniach ryzyka) i okresowy (syntetyczna informacja o profilu, poziomie ryzyka operacyjnego, której odbiorcami są: Komitet Ryzyka Operacyjnego, Zarząd Banku i Rada Nadzorcza).

Do wyznaczenia wymogu kapitałowego stosowana jest metoda standardowa.

Bank Millennium S.A.[19]

Przyjęta w Banku Millennium S.A. definicja ryzyka operacyjnego jest zgodna z definicją Komitetu Bazylejskiego. Dodatkowo, w jego ramach, wyodrębnia się ryzyko nadużyć, jako możliwość przedstawienia przez klienta nieprawdziwych bądź niepełnych informacji dotyczących danych osobowych bądź sytuacji finansowej, co może mieć bezpośredni wpływ na podjęcie niewłaściwej decyzji kredytowej lub przeprowadzenia innej transakcji. Bank podkreśla, że

18 http://www.bosbank.pl/index.php?page=3719 (14.03.2014).

19 http://www.bankmillennium.pl/pl/o-banku/relacje-inwestorskie/raporty-finansowe/ (14.03.2014).

tego ryzyka nie da się uniknąć, gdyż objawia się w każdym aspekcie działalności jego organizacji.

Zarządzanie ryzkiem dąży do systematycznego rozwój systemu i narzędzi jego monitorowania w celu dostosowania ich do najlepszych praktyk rynkowych.

W ramach zarządzania ryzykiem operacyjnym, na obowiązującą w Banku strukturę organizacyjną nałożono strukturę procesową, której bieżące zarządzanie zostało powierzone Właścicielom Procesów. Właściciele znają procesy, mogą więc najefektywniej zidentyfikować związane z nimi ryzyko i zaproponować rozwiązania celem jego uniknięcia lub ograniczenia. Właściciele raportują do Właścicieli innych jednostek uczestniczących w procesie zarządzania ryzykiem (i wzajemnie się wspierają) oraz do Komitetu Procesów i Ryzyka Operacyjnego. Zadaniem Komitetu jest zarządzanie zagrożeniami, generowanymi w więcej niż jednym procesie. Nadzór i koordynacja działań sprawowane są przez Komitet Ryzyka, Zarząd Banku oraz Radę Nadzorczą.

Do identyfikacji, badania i oceny ryzyka wykorzystywane są trzy narzędzia: zbieranie informacji o stratach, monitorowanie KRI, samoocena ryzyka operacyjnego. Są one systematycznie doskonalone. Gromadzenie informacji dotyczących zdarzeń ryzyka operacyjnego ma miejsce w dedykowanej bazie, za pomocą narzędzia informatycznego. Dane są odpowiednio klasyfikowane pod kątem kategorii ryzyka oraz procesu. Takie uporządkowanie ułatwia raportowanie oraz walidację samooceny ryzyka, a także spełnia wymogi jakościowe i ilościowe w zakresie metod zaawansowanych przy wyliczaniu wymogów kapitałowych. Wskaźniki KRI zostały opracowane przez kluczowych pracowników, dzięki czemu stanowią efektywne predyktory zbliżających się zagrożeń. Przeprowadzana okresowo samoocena ryzyka, pozwala na oszacowanie jego poziomu. W przypadku przekroczenia przyjętego dla danego procesu biznesowego poziomu tolerancji, są proponowane, a następnie wdrażane i monitorowane, działania zapobiegawcze. W ramach procesu samooceny wyznacza się i ocenia KRI, a także przeprowadza przeglądy procesów i rozwiązań w zakresie jakości obsługi klientów oraz partnerów biznesowych. Zgromadzone dane i przeprowadzone analizy stanowią element informacji zarządczej.

W celu zarządzania ryzykiem nadużyć, Bank powołał Biuro Zarządzania Ryzykiem Nadużyć, którego zadaniem jest organizacja systemu zarządzania tym ryzykiem we współpracy z innymi jednostkami organizacyjnymi.

Wymogi kapitałowe wyznaczane są za pomocą metody standardowej, adekwatnie do stopnia rozwoju systemu zarządzania tym ryzykiem oraz skali i profilu działalności Banku.

mBank S.A.[20]

Pojęcie ryzyka operacyjnego jest tożsame z definicją Komitetu Bazylejskiego, w jego ramach jest uwzględniane ryzyko prawne.

20 http://www.mbank.pl/relacje-inwestorskie/ (14.03.2014).

Organizacja systemu i procesu zarządzania ryzykiem operacyjnym jest zgodna z wymogami regulacyjnymi. Został zbudowany system umożliwiający jego monitorowanie na wszystkich poziomach organizacyjnych. Nadzór nad tym systemem sprawuje Rada Nadzorcza, wspierana przez Komisję ds. Ryzyka. Wykonawcami decyzji Rady i Komisji są: Zarząd Banku, Forum Biznesu i Ryzyka, Dyrektor Banku ds. Zarządzania Ryzykiem, Departament Zarządzania Zintegrowanym Ryzykiem i Kapitałem. Organy te są odpowiedzialne za kontrolę ryzyka, natomiast zarządzanie ma miejsce w każdej komórce organizacyjnej; jego koordynatorami są pracownicy zarządzający ryzykiem w poszczególnych obszarach biznesowych. Zarządzanie polega na identyfikowaniu ryzyka oraz podejmowaniu działań, prowadzących do jego unikania, ograniczania bądź transferu.

Bank planuje wdrożyć proces Samooceny Efektywności Zarządzania Ryzykiem, którego zadaniami będą: identyfikacja kluczowych ryzyk oraz ocena efektywności zarządzania nimi (poprzez wdrożenie mechanizmów kontrolnych i planów działań naprawczych)[21].

Bank BPH S.A.[22]

W Banku BPH S.A. obowiązuje rozszerzona definicja ryzyka operacyjnego (względem definicji Komitetu Bazylejskiego), ponieważ do tego ryzyka włączane jest ryzyko prawne oraz ryzyko reputacji (jako efekt zdarzenia operacyjnego), natomiast ryzyko strategiczne – jest analizowane odrębnie.

Celem zarządzania ryzykiem jest minimalizacja ekspozycji Banku na ryzyko, poprzez przeciwdziałanie powstaniu zdarzeń ryzyka operacyjnego oraz ograniczanie ich skutków w przypadku ich wystąpienia.

Zasady i struktura zarządzania ryzykiem zostały określone w regulacji wewnętrznej, przyjętej przez Zarząd Banku. Do zbudowanej struktury zarządzania ryzykiem zalicza się: Zarząd (odpowiedzialny za funkcjonowanie procesu zarządzania i kontroli), Komitet ds. Ryzyka Operacyjnego (podejmujący decyzje i rekomendujący działania; w jego skład wchodzą wybrani Członkowie Zarządu, przedstawiciele z Departamentu Compliance, Pionu Prawnego i Relacji Korporacyjnych oraz Departamentu Audytu Wewnętrznego), Biuro Zarządzania Ryzykiem Operacyjnym w Departamencie Ryzyka Operacyjnego i Zarządzania Nadużyciami (monitorujące ryzyko operacyjne w całym Banku oraz odpowiedzialne za rozwój i wprowadzanie metod i instrumentów kontroli ryzyka), Koordynatorzy Ryzyka Operacyjnego poszczególnych pionów/obszarów Banku (odpowiedzialni za organizację zarządzania ryzykiem w nadzorowanych obszarach, w oparciu o informacje dostarczone z nadzorowanych komórek, w szczególności przez podległych Championów Ryzyka Operacyjnego) oraz wyznaczeni przez nich Championi Ryzyka Operacyjnego

---

21 Wdrożenie tego procesu rozpoczęto w 2014 r., planowany termin zakończenia – I połowa 2015 r. Por.: http://www.mbank.pl/relacje-inwestorskie/ (8.03.2015).

22 http://www.bph.pl/pl/relacje_inwestorskie (14.03.2014).

(odpowiedzialni za wdrożenie systemu zarządzania ryzykiem w komórkach organizacyjnych, zgodnie z wytycznymi Koordynatora oraz wspieranie go w realizacji powierzonych obowiązków (w zakresie: raportowania ryzyk, zdarzeń oraz KRI)). Struktura ta obejmuje wszystkie szczeble organizacyjne Banku.

Do podstawowych narzędzi i metod pomiaru ryzyka należy zaliczyć: proces Oceny Ryzyka i Mechanizmów Kontrolnych (między-funkcyjny proces identyfikacji i oceny ryzyka oraz mechanizmów jego ograniczania), Ewidencję Danych o Stratach Operacyjnych (systematycznie gromadzone dane o stratach operacyjnych, incydentach, a także innych zdarzeniach, które nie przyniosły straty, ale zostały ocenione jako istotne; dane te są przechowywane w scentralizowanych rejestrach Banku) oraz KRI (które – z wyprzedzeniem – odzwierciedlają skalę narażenia na ryzyko oraz zmiany profilu ryzyka danego procesu oraz umożliwiają pomiar ryzyka na poziomie procesów biznesowych).

Na potrzeby wyznaczania wymogu kapitałowego z tytułu ryzyka operacyjnego Bank stosuje metodę standardową.

Podsumowanie

Na podstawie powyższej prezentacji systemów zarządzania ryzykiem operacyjnym w wybranych bankach komercyjnych działających w Polsce, można stwierdzić, że banki identyfikują ryzyko operacyjne i nim zarządzają. Przy czym ta identyfikacja oraz zasady zarządzania nie są w pełni porównywalne. Dalej zostanie przeprowadzona analiza definicji i systemów zarządzania ryzykiem operacyjnym w badanych tu bankach. W celu zapewnienia przejrzystości porównania, zostanie ono przeprowadzone zgodnie z konwencją przyjętą w opisach systemów zarządzania ryzykiem operacyjnym w wybranych bankach i, jak wcześniej wspominano, będzie obejmować: podstawowe etapy procesu zarządzania ryzykiem operacyjnym (ujęte w Rekomendacji M) oraz zagadnienia prezentowane przez banki w sprawozdaniach finansowych (zgodnie z dobrymi praktykami rynkowymi).

W badanych bankach ryzyko operacyjne najczęściej określane jest zgodnie z definicją Komitetu Bazylejskiego, przy czym można zauważyć zróżnicowane podejście do klasyfikowania ryzyka prawnego, reputacji i ryzyka strategicznego. Większość banków, w ramach ryzyka operacyjnego uwzględnia ryzyko prawne oraz wyłącza ryzyko reputacji i strategiczne. Dwa spośród badanych banków (BGŻ S.A. i BOŚ S.A.) do ryzyka operacyjnego zaklasyfikowały także ryzyko braku zgodności, jeden bank (Millennium S.A.) włącza ryzyko nadużyć, natomiast dwa banki (ING S.A. oraz Bank BPH S.A.) uwzględniają ryzyko reputacji, a jeden (PKO BP S.A.) – zarówno ryzyko reputacji, jak i ryzyko strategiczne.

Wszystkie banki definiowały cele zarządzania ryzykiem operacyjnym. Podstawowym zadaniem jest ograniczenie tego ryzyka poprzez minimalizację prawdopodobieństwa wystąpienia zdarzeń ryzyka operacyjnego, a w przypadku ich materializacji – ograniczenie ich negatywnych skutków (BZ WBK S.A.,

Alior Bank S.A., BGŻ S.A., BOŚ S.A., mBank S.A. i BPH S.A. oraz ING S.A.). W przypadku Millennium S.A. – celem jest rozwój systemu i narzędzi monitorowania ryzyka, w przypadku PKO BP S.A. – zwiększenie szybkości i adekwatności reakcji na zdarzenia operacyjne, natomiast w Pekao S.A. – identyfikacja, ocena, monitorowanie, przeciwdziałanie oraz raportowanie. Wśród równie ważnych celów, banki wskazują: zapewnienie bezpieczeństwa środków powierzonych przez klientów, świadczenie wysokiej jakości usług (ING S.A. i BGŻ S.A.) oraz zwiększenie efektywności tego systemu (w tym szybkości i adekwatności reakcji na zdarzenia zewnętrzne – PKO BP S.A. i BOŚ S.A.). Przy czym banki mają świadomość, że ryzyka operacyjnego nie da się uniknąć, ponieważ jest generowane we wszystkich obszarach aktywności (ING S.A.). Stąd do innych zadań budowanych systemów zaliczają: unikanie, ograniczanie bądź transfer ryzyka (mBank S.A.).

W większości banków został podkreślony fakt posiadania opracowanej i wdrożonej przez Zarząd oraz zatwierdzonej przez Radę Nadzorczą strategii ryzyka operacyjnego. Jeden bank (BPH S.A.) podał informację, że struktura zarządzania ryzykiem została zbudowana zgodnie z zatwierdzoną przez Zarząd regulacją wewnętrzną (która może być tożsama ze strategią). W przypadku pozostałych banków – można jedynie założyć, że taką strategię posiadają, gdyż informują o przyjętym i kontrolowanym poziomie akceptowanego ryzyka (BOŚ S.A.), czy posiadaniu systemu zarządzania tym ryzykiem, zgodnym z Rekomendacją M (PKO BP S.A.), przepisami zewnętrznymi (Pekao S.A., BGŻ S.A. i mBank S.A.) oraz dobrymi praktykami rynkowymi (Millennium S.A.).

Duże zróżnicowanie występuje w zbudowanych systemach zarządzania. Do organów i jednostek odpowiedzialnych za system i proces monitorowania ryzyka operacyjnego należy zaliczyć: 1) Radę Nadzorczą (określenie i zatwierdzenie strategii, ramowych zasad zarządzania ryzykiem, określenie apetytu na ryzyko), 2) Zarząd Banku (budowa i nadzór na systemem), 3) Komitety Ryzyka Operacyjnego (wsparcie merytoryczne dla Zarządu Banku), 4) Departament/Biuro Zarządzania Ryzykiem Operacyjnym (rozwój narzędzi i metod, raportowanie zarządcze), 5) Departament Audytu Wewnętrznego (niezależna kontrola) oraz 6) Koordynatorzy kontroli ryzyka operacyjnego (bieżące kontrolowanie ryzyka w działalności biznesowej, raportowanie o zdarzeniach ryzyka operacyjnego). Rola Rady, jako organu zatwierdzającego strategię i nadzorującego jej wykonanie jest podkreślona w 5 z 10 banków (Pekao S.A., Alior S.A., ING S.A., Millennium S.A. oraz mBank S.A.), rola Zarządu – jako koordynatora procesu zarządzania ryzkiem – w 6 bankach (Pekao S.A., Alior S.A., BGŻ S.A., ING S.A. oraz BPH S.A.). Siedem banków deklaruje powołanie Komitetów/Forów ryzyka operacyjnego, których zadaniem jest wspieranie decyzji i działań podejmowanych przez Zarząd (Pekao S.A., BZ WBK S.A., Alior S.A., BGŻ S.A., Millennium S.A., mBank S.A. oraz BPH S.A.). Także siedem banków informuje o utworzonych, zgodnie z rekomendacją nr 5 Rekomendacji M KNF, jednostkach (biurach czy departamentach) ds. ryzyka

operacyjnego, których zadaniem jest kontrolowanie poziomu ryzyka oraz wdrażanie i rozwój narzędzi jego monitorowania (Pekao S.A., BZ WBK S.A., Alior S.A., BOŚ S.A., Millenium S.A., mBank S.A. oraz w BPH S.A.). W sześciu bankach (PKO BP S.A., BGŻ S.A., ING S.A., BOŚ S.A., mBank S.A. oraz w BPH S.A.) struktura zarządzania tym ryzkiem jest wielopłaszczyznowa i ma miejsce nie tylko w Centrali Banku, ale również w jednostkach operacyjnych, dzięki czemu możliwe jest szybsze wykrycie zdarzeń ryzyka operacyjnego, ich raportowanie, a tym samym – eliminacja negatywnych skutków. Proces monitorowania ryzyka operacyjnego ma niekiedy miejsce na wszystkich poziomach organizacyjnych banków i są w niego zaangażowani zarówno pracownicy, jak i kadra zarządzająca (fakt ten jest podkreślony w sprawozdaniu BZ WBK S.A., Alior Bank S.A., BOŚ S.A. oraz mBank S.A.). Monitorowanie tego ryzyka jest najczęściej podzielone na: bieżące (związane z działalnością biznesową) oraz systemowe (prowadzące do zbudowania systemu, a także wypracowania przepisów wewnętrznych) – PKO BP S.A., BGŻ S.A., BOŚ S.A. i mBank S.A. W systemie zarządzania istotną rolę pełni także audyt wewnętrzny, jako niezależny organ weryfikacji podejmowanych decyzji i działań oraz wewnętrzna kontrola funkcjonalna (Pekao S.A. oraz BOŚ S.A.).

Do najważniejszych metod monitorowania ryzyka operacyjnego, stosowanych w badanych bankach, należy przede wszystkim zaliczyć: 1) ewidencję zdarzeń, incydentów i strat operacyjnych, w dedykowanych bazach danych – we wszystkich bankach (z wyjątkiem ING S.A.), 2) wskaźniki KRI – w siedmiu bankach, z wyjątkiem ING S.A., BOŚ S.A. oraz mBank S.A., 3) roczne limity strat oraz sublimity – w trzech bankach (PKO BP S.A., Pekao S.A. i ING S.A.), 4) CSA (kontrola wewnętrzna funkcjonalna, samoocena) – w pięciu bankach (Pekao S.A., BGŻ S.A., BOŚ S.A., Millennium S.A. oraz mBank S.A.).

Przeprowadzanie wymaganych przez KNF stress testów i analiz scenariuszowych deklarowały trzy banki (Pekao S.A., ING S.A. i BOŚ S.A.), natomiast posiadanie BCP i planów awaryjnych – cztery banki (Pekao S.A., BZ WBK S.A., ING S.A. i BOŚ S.A.).

W podejściu do zarządzania ryzykiem operacyjnym trzy banki (PKO S.A., BZ WBK S.A. oraz mBank S.A.) poinformowały o przyjęciu strategii: ograniczania, unikania/zaprzestania, transferu ryzyka oraz ubezpieczeniu zidentyfikowanego ryzyka.

O posiadanym systemie wewnętrznego zarządczego raportowania informuje pięć banków (Pekao S.A., BZ WBK S.A., BGŻ S.A., ING S.A. oraz BOŚ S.A.). Najczęściej wskazywanymi adresatami raportów są: Rada Nadzorcza, Zarząd oraz dedykowane Komitety ds. ryzyka operacyjnego a także audyt wewnętrzny.

Wśród metod wyznaczania wymogu kapitałowego z tytułu ryzyka operacyjnego dominowała metoda standardowa. Pięć spośród dziesięciu badanych banków w raportach finansowych opublikowało tę informację (Alior S.A., BGŻ S.A., BOŚ S.A., Millennium S.A. oraz BPH S.A.), natomiast zastosowanie metody AMA zadeklarował jeden bank (Pekao S.A.).

Ograniczona jest informacja, czy zbudowane systemy monitorowania ryzyka operacyjnego są spójne z systemami występującymi w podmiotach zależnych i powiązanych kapitałowo. Jedynie dwa banki (Pekao S.A. i ING S.A.) podkreśliły, że stworzyły systemy zgodne ze standardami obowiązującymi w ich spółkach-matkach. Natomiast brak jest informacji o spójności zasad zarządzania ryzykiem operacyjnym w spółkach im podległych.

Tylko w przypadku dwóch banków (Alior Bank S.A. oraz Pekao S.A.), w badanych sprawozdaniach finansowych została opublikowana informacja o stratach poniesionych w 2013 r. z tytułu ryzyka operacyjnego. Informacje na temat przeprowadzenia ewentualnej weryfikacji kontrahentów banku i stworzenia listy tych kontrahentów, z którymi bank nie zamierza współpracować (również wynikające ze znowelizowanej Rekomendacji M), nie były przez badane banki publikowane.

Tabela 2. Weryfikacja 10 wyodrębnionych elementów systemów zarządzania ryzykiem operacyjnym w badanych bankach komercyjnych

Elementy oceny/ Bank	Definicja/Cel	Strategia	Struktura organizacyjna	Metody/Narzędzia	Stres test/Plany awaryjne/BCP	Przeciwdziałanie	Raportowanie	Wymogi kapitałowe	Grupa Kapitałowa	Raportowanie strat	Łącznie
PKO BP S.A.	1	1	1	1		1					5
Bank Pekao S.A.	1	1	1	1	1		1	1	1	1	9
BZ WBK S.A.	1	1	1	1	1	1	1				7
Alior Bank S.A.	1	1	1	1				1		1	6
BGŻ S.A.	1	1	1	1			1	1			6
ING BŚ S.A.	1	1	1	1	1		1		1		7
BOŚ S.A.	1	1	1	1	1		1	1			7
Bank Millennium S.A.	1	1	1	1				1			5
mBank S.A.	1	1	1	1		1		1			6
Bank BPH S.A.	1	1	1	1							4
										Dominanta	**7**
										Średnia ocena	**6,2**

Legenda: 1 – w sprawozdaniu finansowym jest ujawniona informacja o badanym elemencie systemu zarządzania ryzykiem operacyjnym.

Źródło: opracowanie własne na podstawie informacji publikowanych przez badane banki w jednostkowych sprawozdaniach finansowych za 2013 r. Źródła danych zostały zamieszczone w bibliografii.

W tabeli 2 przedstawiono syntetyczne zestawienie informacji na temat systemów zarządzania ryzykiem operacyjnym w wybranych bankach. Jego celem była ocena badanych banków pod względem posiadania bądź braku 10 wcześniej wyodrębnionych elementów, istotnych dla kompleksowego systemu zarządzania ryzykiem operacyjnym. Dokonana ocena ma charakter 0–1, tzn. – w przypadku prezentacji informacji – bank otrzymał 1 pkt i w przypadku jej braku – 0 pkt. Przy czym przyznana liczba punktów nie jest oceną samą w sobie, lecz jej celem jest tylko podsumowanie przeprowadzonych badań i weryfikacja zgodności polityki banków z ujętymi w Rekomendacji kluczowymi elementami związanymi z zarządzaniem ryzykiem.

Zgodnie z przeprowadzoną analizą widać, że banki identyfikują ryzyko operacyjne i dostrzegają potrzebę zarządzania nim, przy czym żaden z badanych tu banków nie osiągnął maksymalnej liczby punktów (tj. 10), co świadczy o konieczności doskonalenia zbudowanych systemów zarządzania tym ryzykiem (średnia ocena to 6,2 pkt, a wartość występująca najczęściej (dominanta) to 7 pkt). Ważny jest jednak fakt, iż same banki mają tego świadomość, ponieważ siedem z dziesięciu badanych banków deklaruje systematyczny rozwój tych systemów, polegający m.in. na: jego usprawnianiu (Alior Bank S.A., ING S.A. oraz Millennium Bank S.A.), doskonaleniu metod i narzędzi monitorowania (PKO BP S.A., Alior Bank S.A. i Millennium Bank S.A.), systematycznej aktualizacji bazy zdarzeń ryzyka operacyjnego (BGŻ S.A.), wdrożeniu systemu samooceny (mBank S.A.) oraz systematycznej walidacji systemu oraz modelu wyznaczania wymogu kapitałowego (Pekao S.A.).

Bibliografia

Bessis J. [2002], *Risk Management in Banking*, John Wiley&Sons, Chichester.

Chernobai A.S., Rachev S.T., Fabozzi F.J. [2007], *Operational Risk. A Guide to Basel II Capital Requirements, Models, and Analysis*, John Wiley&Sons, Hoboken.

Doerig H.-U. [2001; 2003], *Operational Risk in Financial Services an Old Challenge in a New Environment, Credit Suisse Group*, https://www.credit-suisse.com/governance/doc/operational_risk.pdf (10.03.2014).

Gospodarowicz A. [2007], *Ryzyko operacyjne w banku*, w: *Zarządzanie ryzykiem*, red. K. Jajuga, Wydawnictwo Naukowe PWN, Warszawa.

Holton G. [2004], *Defining Risk*, "Financial Analysts Journal", November–December.

Hull J.C. [2011], *Zarządzanie ryzykiem instytucji finansowych*, Wydawnictwa Profesjonalne PWN, Warszawa.

International Convergence of Capital Measurement and Capital Standards. A Revised Framework [2004], Bank for International Settlements, Basel Committee on Banking Supervision, June.

Kałużny R. [2004], *Strzegąc swego banku*, „Bank", nr 3.

Krasodomska J. [2008], *Zarządzanie ryzykiem operacyjnym w bankach*, PWE, Warszawa.

Lewandowski D. [2004], *Ryzyko operacyjne w bankach – zarządzanie i audyt w świetle wymagań Bazylejskiego Komitetu ds. Nadzoru Bankowego*, „Bank i Kredyt", nr 4.

Marcinkowska M. [2009], *Standardy kapitałowe banków. Bazylejska Nowa Umowa Kapitałowa w polskich regulacjach nadzorczych*, Regan Press, Gdańsk.

Matkowski P. [2006], *Zarządzanie ryzykiem operacyjnym*, Oficyna Ekonomiczna Wolters Kluwer, Kraków.

Orzeł J. [2005a], *Na drodze do zaawansowanych metod ilościowego pomiaru ryzyka operacyjnego – KRI*, „Bank i Kredyt", nr 6.

Orzeł J. [2005b], *Ilościowe metody pomiaru ryzyka operacyjnego*, „Bank i Kredyt", nr 7.

Piołunowicz M. [2006], *Kategoryzacja strat operacyjnych w bankowości*, „Bank i Kredyt", nr 9.

Rekomendacja M dotycząca zarządzania ryzykiem operacyjnym w bankach, załącznik do Uchwały Nr 8/2013 KNF z dnia 8 stycznia 2013 r. w sprawie wydania Rekomendacji M dotyczącej zarządzania ryzykiem operacyjnym w bankach (DzUrz KNF, 2013, poz. 6 z dnia 27 lutego 2013 r.), http://www.knf.gov.pl/Images/Rekomendacja_M_8_01_2013_uchwala_8_tcm75–33017.pdf (15.04.2014).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 575/2013 z dnia 26 czerwca 2013 r. w sprawie wymogów ostrożnościowych dla instytucji kredytowych i firm inwestycyjnych, zmieniające rozporządzenie (UE) nr 648/2012.

Ślązak E. [2007], *Ryzyko operacyjne*, w: *Współczesna bankowość*, red. M. Zaleska, Difin, Warszawa.

Thlon M. [2012], *Zarządzanie ryzykiem operacyjnym przedsiębiorstwa. Metoda szacowania ryzyka delta-EVT*, Monografie: Prace Doktorskie nr 15, Wydawnictwo Uniwersytetu Ekonomicznego w Krakowie, Kraków.

Uchwała Nr 76/2010 KNF z dnia 10 marca 2010 r. w sprawie zakresu i szczegółowych zasad wyznaczania wymogów kapitałowych z tytułu poszczególnych rodzajów ryzyka (DzUrz KNF, 2010, poz. 11 z dnia 9 kwietnia 2010 r. z poź. zm.).

Urbankowska-Bąk K. [2012], *Ryzyko operacyjne*, w: *Zarządzanie ryzykiem bankowym*, red. M. Iwanicz-Drozdowska, Wydawnictwo Poltext, Warszawa.

Zawadzka Z. [1996], *Zarządzanie ryzykiem w banku komercyjnym*, Poltext, Warszawa.

http://media.bgz.pl/1795/pl/presskit/8225 (14.03.2014).

http://www.aliorbank.pl/pl/o_banku/relacje_inwestorskie/raporty_okresowe (7.03.2014).

http://www.bankmillennium.pl/pl/o-banku/relacje-inwestorskie/raporty-finansowe/ (14.03.2014).

http://www.bosbank.pl/index.php?page=3719 (14.03.2014).

http://www.bph.pl/pl/relacje_inwestorskie (14.03.2014).

http://www.bzwbk.pl/_items/inwestor.bzwbk.pl/pdf/raport_roczny_bzwbk_2013.pdf (14.03.2014).

https://www.credit-suisse.com/governance/doc/operational_risk.pdf (1.03.2013).

http://www.ingbank.pl/relacje-inwestorskie/wyniki-finansowe#tab=1 (14.03.2014).

http://www.knf.gov.pl/index.html (7.03.2014).

http://www.knf.gov.pl/aktualnosci/2013/Przyjecie_nowej_Rekomendacji_M.html (10.10.2014).

http://www.knf.gov.pl/pakiet_crd4.html (15.10.2014).

http://www.mbank.pl/relacje-inwestorskie/ (14.03.2014).

http://www.pekao.com.pl/informacje_dla_inwestorow/informacje_finansowe/sprawozdania_finansowe/ (21.03.2014).

http://www.pkobp.pl/media_files/f4f429ae-1140–4585-8af7-ecfc0ee3d45f.pdf (14.03.2014).

OPERATIONAL RISK MANAGEMENT IN SELECTED BANKS IN POLAND

Summary

The article addresses the growing importance of operational risk and effective risk management in financial institutions. The authors aim to establish whether or not bank managers are aware of the existence of operational risk and how they manage this kind of risk. The authors conduct a comparative analysis of operational risk and risk management in 10 selected banks in Poland. Data for the analysis comes from the banks' financial statements for 2013.

On the basis of their study, the authors conclude that all the banks were aware of their exposure to operational risk, and they also realized that such risk could not be eliminated completely. Another conclusion is that banks tend to identify operational risk in line with the recommendations of the Basel Committee on Banking Supervision, the primary global standard-setter for the prudential regulation of banks.

According to Cichowicz and Nowak, banks are also aware of the urgency of risk management and recognize the need for consistent improvement of process management and monitoring methods. Moreover, banks are aware of the need to regularly update their databases of operational risk events, and they also make efforts to systematically validate their capital requirement models, the authors say.

Keywords: banking risk, operational risk, banks, risk management, Basel Committee on Banking Supervision, capital requirement

JEL classification codes: G21, G32