PRACE NAUKOWE AKADEMII EKONOMICZNEJ WE WROCŁAWIU
Nr 1128 — 2006
Wpływ norm ostrożnościowych na ograniczanie ryzyka
w działalności banku spółdzielczego

Dariusz Garczyński
Akademia Ekonomiczna we Wrocławiu

MOŻLIWOŚCI WYKORZYSTANIA SYSTEMU ADONISRISK DO MINIMALIZACJI RYZYKA OPERACYJNEGO W BANKACH SPÓŁDZIELCZYCH

1. Wstęp

Perspektywa wprowadzenia w 2007 r. postanowień Nowej umowy kapitałowej (NUK), potwierdzonego we wrześniu 2005 r. dyrektywą Europejskiego Banku Centralnego o wymogach kapitałowych[1], sprawia, że przed bankowością spółdzielczą pojawiają się wyzwania związane z wdrażaniem nowych rozwiązań w zakresie zarządzania ryzykiem bankowym, szczególnie w obszarze ryzyka operacyjnego. Rozwój sektora bankowości spółdzielczej, sięganie po nowe sposoby świadczenia usług bankowych drogą elektroniczną, coraz śmielsze wprowadzanie nowoczesnych technologii informatycznych, także drogą outsourcingu, oraz konieczność sprostania konkurencji ze strony nie tylko banków komercyjnych, ale i SKOK-ów powoduje, że implementacja postanowień NUK staje się w chwili obecnej dla banków spółdzielczych nie tylko obowiązkiem, ale i koniecznością. Celem artykułu jest zaprezentowanie narzędzia – systemu ADONISrisk – mogącego usprawnić proces zarządzania ryzykiem operacyjnym w bankach spółdzielczych, które nie potrzebują zaawansowanych metod szacowania i sterowania tym rodzajem ryzyka.

2. Istota ryzyka operacyjnego

W rozumieniu Komitetu Bazylejskiego ryzyko operacyjne jest definiowane jako „ryzyko pośrednich lub bezpośrednich strat wynikających z nieodpowiednich lub błędnych procesów i procedur wewnętrznych, działania ludzi lub systemów, a

[1] Dyrektywa CAD 3, europa.eu.int, wrzesień 2005.

także zdarzeń zewnętrznych"[2]. Komitet podkreśla jednak, że takie określenie może być rozumiane na wiele sposobów, ponieważ instytucje finansowe, a zwłaszcza banki prowadzą różną działalność, w różnych uwarunkowaniach i w związku z tym podlegają różnym czynnikom powodującym ryzyko operacyjne[3]. Dlatego też bardzo często ryzyko operacyjne określa się jako jakiekolwiek ryzyko nie będące ryzykiem rynkowym lub kredytowym.

Na potrzeby wewnętrzne banki mogą określić własne definicje ryzyka operacyjnego, ważne jest jednak, aby uwzględniały one najważniejsze źródła strat operacyjnych. Definicje powinny brać pod uwagę także skutki wywołane przez zdarzenia związane z ryzykiem operacyjnym. Do najpoważniejszych zdarzeń operacyjnych Komitet Bazylejski zalicza:

- oszustwa wewnętrzne, występujące w przypadku błędów lub kradzieży pracowników banku,
- oszustwa zewnętrzne, np. kradzieże, fałszerstwa lub włamania hakerów komputerowych,
- organizacja miejsca pracy w zakresie m.in. zapewnienia bezpieczeństwa i norm BHP, przejawów mobbingu i dyskryminacji, właściwego wynagradzania,
- praktyki związane z zarządzaniem produktami i relacjami z klientem, np. wykorzystywanie poufnych informacji o klientach, pranie pieniędzy, sprzedaż nieautoryzowanych produktów,
- fizyczne uszkodzenia zasobów, np. powodzie, pożary, akty terroryzmu lub wandalizmu,
- błędy systemów informatycznych, np. wynikające z niewłaściwego funkcjonowania sprzętu lub oprogramowania, a także z zakłóceń transmisji telekomunikacyjnych,
- niewłaściwe zarządzanie procesami, zarówno przy pojedynczych operacjach (np. wprowadzania danych), jak i związane z relacjami z kontrahentami i dostawcami.

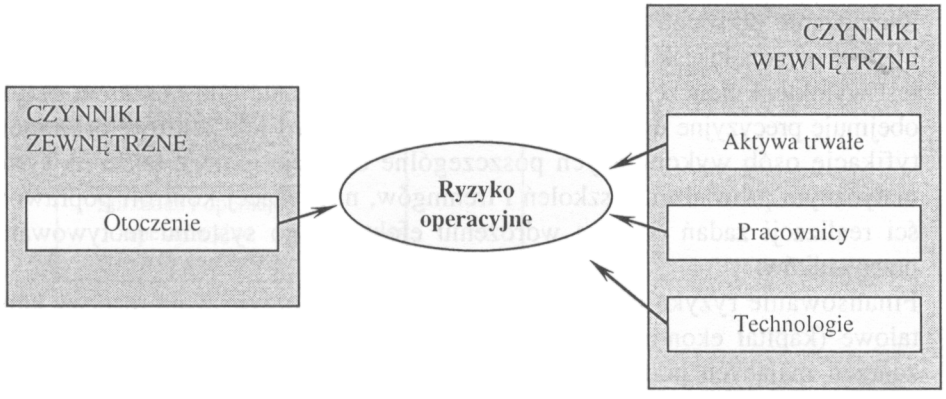
Analizując powyższe wskazówki Bazylejskiego Komitetu Nadzoru Bankowego, można zauważyć, że ryzyko operacyjne związane jest z czterema głównymi czynnikami, z których trzy mają charakter wewnętrzny, a jedno – zewnętrzny (rys. 1).

Do otoczenia banku zalicza się przede wszystkim jego klientów, a także inne instytucje finansowe i administracyjne oraz wszystkie podmioty, które swoim zachowaniem wpływają na jego działalność. Aktywa będące środkami trwałymi zapewniają sprawne działanie banku jako przedsiębiorstwa. Ryzyko operacyjne obejmuje straty wynikające z uszkodzenia lub zniszczenia tych aktywów wskutek

[2] Basel Committee on Banking Supervision, Basel II: International Convergence of Capital Measurement and Capital Standards: a Revised Framework, Basel, Jun. 2004, http://www.bis.org/publ/.

[3] Basel Committee on Banking Supervision, Sound Practices for the Management and Supervision of Operational Risk, Basel, Feb. 2003, http://www.bis.org/publ/.

klęsk żywiołowych lub działalności terrorystycznej. Wpływ nowoczesnych technologii informatycznych i telekomunikacyjnych na wielkość ryzyka operacyjnego wynika z możliwych błędów sprzętu i oprogramowania funkcjonującego w banku. Zalicza się tu przede wszystkim systemy teleinformatyczne, zapewniające właściwe gromadzenie, przetwarzanie, przesyłanie i prezentację danych związanych z prowadzeniem działalności banku. W dużym stopniu na ryzyko operacyjne wpływa czynnik ludzki, związany z pracownikami banku, ich kwalifikacjami i doświadczeniem zawodowym.



Rys. 1. Czynniki wpływające na ryzyko operacyjne

Źródło: opracowanie własne.

Zarządzanie ryzykiem operacyjnym wymaga podjęcia działań związanych z wymienionymi wyżej czynnikami. Jak podaje J. Jakóbczak [2003, s. 78], „proces zarządzania polega w pierwszej kolejności na stosowaniu różnorodnych środków mających charakter zapobiegawczy [...] w sferze organizacji pracy, technologii i zarządzania kadrami. Niecałe jednak ryzyko operacyjne da się w ten sposób wyeliminować, istnieje zatem konieczność zapewnienia środków na finansowanie strat wynikających z ryzyka operacyjnego (poprzez tworzenie rezerw albo ubezpieczenie) bądź też zlecanie działalności obarczonej ryzykiem operacyjnym na zewnątrz". Wspomniane wyżej obszary zarządzania ryzykiem mogą zostać objęte następującymi działaniami [Jakóbczak 2003, s. 79]:

- Organizacja pracy i kontrola procesów operacyjnych – obejmuje precyzyjne zdefiniowanie procedur wewnętrznych i bieżącej kontroli ich realizacji, określenie struktur organizacyjnych, zakresów kompetencji i odpowiedzialności oraz ich dostosowywanie w miarę rozwoju sytuacji, a także prowadzenie okresowych kontroli (audytu) poszczególnych obszarów funkcjonowania firmy. W tym zakresie podstawowe znaczenie ma odpowiednie dokumentowanie

prowadzonej działalności, utrzymywanie systemów zapasowych oraz przestrzeganie międzynarodowych standardów (np. ISO 17799, SSAE 1, SAS 70).

- Zabezpieczenia techniczne – obejmują zarówno tradycyjne środki ochrony fizycznej, np. systemy alarmowe, jak i narzędzia kontrolne systemów informatycznych (wbudowane w ich systemy operacyjne i stosowane aplikacje), automatyczną rejestrację wszystkich niestandardowych działań personelu obsługującego system, a także szyfrowanie kanałów łączności i zbiorów przechowywanych w bazach danych oraz możliwie najdalej posuniętą automatyzację poszczególnych procesów.
- Zarządzanie personelem ma ogromne znaczenie zarówno z powodu częstych błędów personelu, jak i w związku z tym, że ok. 10% zdarzeń „operacyjnych" jest wynikiem nieuczciwości pracowników. Zarządzanie tym obszarem ryzyka obejmuje precyzyjne ustalenie zakresów upoważnień i ich kontrolę oraz identyfikację osób wykonujących poszczególne operacje, polega także na systematycznym prowadzeniu szkoleń i treningów, na bieżącej kontroli poprawności realizacji zadań oraz na wdrożeniu efektywnego systemu motywowania pracowników.
- Finansowanie ryzyka przez bank – bank może tworzyć swoje rezerwy kapitałowe (kapitał ekonomiczny) na sfinansowanie skutków nieprzewidzianych zdarzeń mających podłoże operacyjne (dotyczy to tych przypadków ryzyka operacyjnego, którym nie da się zapobiec poprzez organizację systemu kontroli z wykorzystaniem środków omówionych powyżej).

3. Metody szacowania ryzyka operacyjnego

Praktyka zarządzania ryzykiem operacyjnym wskazuje na istnienie dwóch grup metod służących do identyfikacji i oszacowania wielkości tego ryzyka. Pierwsza grupa – metody *bottom-up* – koncentrują się na źródłach powstawania ryzyka operacyjnego w poszczególnych komórkach banku, szacują jego wielkość w odniesieniu do konkretnych zdarzeń. Wielkością ryzyka operacyjnego banku jest suma tych wielkości. Przykładowe metody *bottom-up* to:

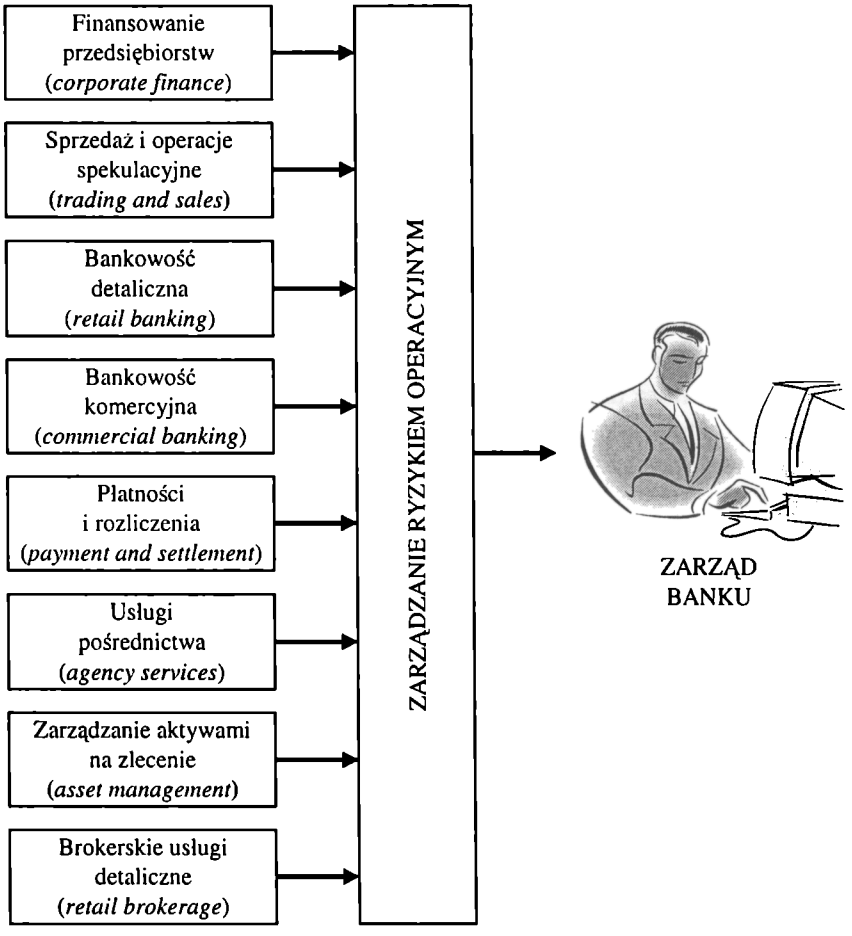
- miary statystyczne,
- analiza scenariuszy,
- metoda analizy czynników,
- model sieci bayesowskich [Lenczewski-Martins, Niedziółka 2005, s. 29].

Metody z grupy *top-down* poddają analizie czynniki makroekonomiczne, wpływające na bank jako całość, określając prawdopodobieństwo wystąpienia zdarzenia, które generuje określony rodzaj ryzyka operacyjnego. Idea metod z grupy *top-down* opiera się na założeniu, że ryzyko operacyjne jest większe w obszarach, gdzie występuje więcej zasobów narażonych na ryzyko. Do tej grupy należą m.in.:

- podejście wskaźnikowe,
- podejście wykorzystujące modele CAPM,
- metoda zmienności [Lenczewski-Martins, Niedziółka 2005, s. 29].

Wymienione wyżej metody mają charakter ilościowy. Ich szerszy opis podaje J. Orzeł [2005a, s. 8], wskazując na ich istotność z punktu widzenia zarządzania ryzykiem operacyjnym. Ich rolę podkreśla także Bazylejski Komitet Nadzoru Bankowego, zalecając stosowanie w praktyce bankowej następujących metod:

- metody wskaźnika podstawowego (Basic Indicator Approach),
- metody standardowej (Standardised Approach),
- metody zaawansowanej oceny (Advanced Measurement Approach).



Rys. 2. Linie biznesowe na potrzeby zarządzania ryzykiem operacyjnym

Źródło: opracowanie własne.

Na potrzeby metody standardowej i metody zaawansowanej oceny Komitet Bazylejski wyróżnia w banku osiem linii biznesowych (rys. 2), dla których indywidualnie szacuje się poziom ryzyka operacyjnego, a ryzyko operacyjne całego banku jest sumą poszczególnych wielkości ryzyka. Najdokładniejszą, ale najtrudniejszą w stosowaniu jest metoda zaawansowanej oceny. Dzięki uwzględnieniu kryteriów nie tylko ilościowych, ale także jakościowych najpełniej ujmuje ona istotę ryzyka operacyjnego. Do analizy wewnętrznej niezbędne jest wykorzystanie własnych lub zewnętrznych baz danych do określania prawdopodobieństwa wystąpienia straty i jej wielkości. Zachodnie banki dysponują odpowiednimi bazami wewnętrznymi, tworzone są także bazy zewnętrzne (np. baza Opvantage, stworzona i utrzymywana przez FitchRisk [Lenczewski-Martins, Niedziółka 2005, s. 38]). W warunkach polskich proces tworzenia tych baz w większości banków rozpoczął się 2-3 lata temu. Inicjatywa wspólnej bazy danych zgłoszona przez ZBP nie spotkała się z szerszym odzewem.

Inną grupę metod szacowania ryzyka operacyjnego stanowią metody jakościowe, przede wszystkim metody oparte na heurystyce (takie jak grupowa ocena ekspertów lub systemy ekspertowe) oraz na prawdopodobieństwie subiektywnym [Orzeł 2005b, s. 4]. Metody te służą do szacowania potencjalnych strat związanych z wystąpieniem zagrożeń w obszarze ryzyka operacyjnego oraz do szacowania prawdopodobieństwa wystąpienia tych zagrożeń. Stosowane są one stosunkowo często, ponieważ metody ilościowe są zazwyczaj skomplikowane i wymagają dużej ilości danych. W chwili obecnej banki nie posiadają jeszcze wystarczająco dużych baz danych, które dodatkowo muszą być odpowiednio skonstruowane. Podstawową wadą metod jakościowych jest konieczność zatrudnienia w procesie analizy ryzyka operacyjnego ekspertów, posiadających wysokiej jakości wiedzę na temat zarządzania ryzykiem. Gdy bank nie dysponuje takimi ekspertami, metody jakościowe są dla niego praktycznie bezużyteczne.

4. System ADONISrisk

Stosowanie metod ilościowych w warunkach polskich jest stosunkowo trudne. Brak odpowiednio przygotowanych danych (na potrzeby m.in. metod proponowanych przez Komitet Bazylejski) oraz trudności w implementacji zaawansowanych narzędzi statystycznych (poprzez np. brak odpowiedniej kadry bankowej) powodują, że wprowadzanie bardziej zaawansowanych metod (takich jak AMA) może zostać zarzucone na rzecz metod prostszych, ale mniej dokładnych. Szczególne wyzwanie stoi przed bankami średnimi i małymi, które nie dysponują odpowiednimi środkami na pozyskanie narzędzi zarządzania ryzykiem operacyjnym – przede wszystkim wysoko kwalifikowanej kadry i sprzętu informatycznego.

Rozwiązaniem dla banków małych i średnich, w tym banków spółdzielczych, mogą być narzędzia informatyczne bazujące na podejściu procesowym, takie jak

system ADONISrisk firmy BOC Information Technologies Consulting. Jest to specjalna konfiguracja systemu ADONIS[4] służąca do szacowania, oceny i dokumentowania ryzyka operacyjnego na podstawie procesów biznesowych. Rozwiązanie to bazuje na kategoriach ryzyka zgodnych z NUK, zdefiniowanych za pomocą odpowiednich typów modeli i obiektów modelowania. Modele te służą następnie jako wzór do przypisania odpowiednich przypadków ryzyka do procesów biznesowych. Analiza ryzyka operacyjnego w systemie ADONISrisk odbywa się na trzech poziomach. Poziom pierwszy, najbardziej ogólny, uwzględnia występowanie ryzyka operacyjnego w czterech obszarach – procesów, technologii, ryzyka zewnętrznego oraz personalnym. Do każdego z tych obszarów przypisano kolejne, bardziej szczegółowe obszary (np. w odniesieniu do grupy „procesy" wyróżniono kategorie: „produkt", „procedury", „outsourcing" i „sposoby postępowania"). Poziom trzeci zawiera najbardziej szczegółowe obszary występowania ryzyka operacyjnego (jak np. „niewypełnienie powierzonych obowiązków"). Po zdefiniowaniu kategorii ryzyka następuje przypisanie im krytycznych wskaźników ryzyka. Następnie dokonywana jest agregacja i analiza ryzyka z poziomu podprocesów do procesu głównego, a wyniki mogą być prezentowane w postaci graficznej.

System ADONISrisk można w dużym stopniu dopasowywać do specyfiki dowolnego obiektu gospodarczego w zakresie zarówno kategoryzacji ryzyka, jak i zasad obliczania wskaźników krytycznych ryzyka. Cecha ta pozwala na łatwe zastosowanie systemu w różnych instytucjach, także w bankach. Stanowi on alternatywę bardziej wyszukanych metod zarządzania ryzykiem operacyjnym przede wszystkim dla banków małych, które nie będą stosować zaawansowanych narzędzi zarządzania ryzykiem ze względu na możliwości i potrzeby.

Literatura

Jakóbczak J., *Współczesne tendencje w zarządzaniu ryzykiem operacyjnym*, [w:] *Inwestycje finansowe i ubezpieczenia – tendencje światowe a polski rynek*, red. K. Jajuga, W. Ronka-Chmielowiec, AE, Wrocław 2003.

Lenczewski-Martins C., Niedziółka P., *Kwantyfikacja ryzyka operacyjnego w banku oraz jego wpływ na wymóg kapitałowy*, „Bank i Kredyt" 2005 nr 5.

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

Orzeł J., *Rola metod heurystycznych, w tym grupowej oceny ekspertów, oraz prawdopodobieństwa subiektywnego w zarządzaniu ryzykiem operacyjnym*, „Bank i Kredyt" 2005b nr 5.

Źródła internetowe

Basel Committee on Banking Supervision, Basel II: International Convergence of Capital Measurement and Capital Standards: a Revised Framework, Basel, Jun. 2004, http://www.bis.org/publ/.

[4] www.boc-pl.com, grudzień 2005.

Basel Committee on Banking Supervision, Sound Practices for the Management and Supervision of Operational Risk, Basel Feb. 2003, http://www.bis.org/publ/.
Dyrektywa CAD 3, europa.eu.int, wrzesień 2005.
www.boc-pl.com, grudzień 2005 (materiały firmy BOC).

APPLICATION OF ADONISRISK SYSTEM IN OPERATIONAL RISK MINIMALIZATION IN COMMUNITY BANKS

Summary

The paper presents concepts of operational risk management under Basel II requirements and application of the system ADONISrisk for measuring and controling this kind of risk. Quantitative methods were presented with the stress on methods proposed by Basel II – BIA, SA and AMA. Due to the high needs of financial data it is not possible for small and medium banks like community banks to adopt such methods in nearest future, therefore some other solution must be applied. The workflow management system ADONIS with its component for risk management may be one of such tools.