

Dariusz Garczyński

Uniwersytet Ekonomiczny we Wrocławiu

ZARZĄDZANIE RYZYKIEM OPERACYJNYM W BANKU DETALICZNYM – UJĘCIE SYSTEMOWE

1. Wstęp

W chwili obecnej wszystkie banki działające w Polsce muszą posiadać systemy zarządzania ryzykiem operacyjnym zgodne z aktami prawnymi¹ oraz zaleceniami KNB (wyrażonymi w Rekomendacji M²). Dokumenty te są przełożeniem na grunt polskiego systemu bankowego idei Nowej Umowy Kapitałowej³ w zakresie zarządzania ryzykiem operacyjnym. Wiele banków, dostrzegając złożoność i niejednoznaczność problemu, prace nad wdrożeniem postanowień NUK rozpoczęło odpowiednio wcześniej. Przed szczególnym wyzwaniem stały się banki średnie i małe, dla których ze względu na ograniczone zasoby finansowe i ludzkie oraz brak odpowiedniej kultury zarządzania ryzykiem, implementacja NUK stanowiła poważny problem.

Celem niniejszego artykułu jest prezentacja systemu zarządzania ryzykiem operacyjnym w jednym z polskich banków. Zaprezentowane zostaną w nim doświadczenia, które autor wyniósł z uczestnictwa w procesie wdrażania takiego systemu, oraz wnioski co do konieczności dalszych prac w zakresie rozwoju takiego systemu.

2. Zalecenia NUK w zakresie systemu zarządzania ryzykiem operacyjnym

Przygotowania do wdrożenia postanowień NUK w banku obejmowały trzy podstawowe kierunki działań:

- 1) dostosowanie struktury organizacyjnej do wymagań NUK,
- 2) opracowanie wewnętrznych procedur zarządzania ryzykiem,
- 3) dostosowanie narzędzi informatycznych.

¹ Uchwały KNB nr 1/2007, 2/2007, 3/2007, 4/2007, 5/2007 i 6/2007 z 13 marca 2007 r.

² Rekomendacja M dotycząca zarządzania ryzykiem operacyjnym w bankach, KNB, Warszawa 2004.

³ The New Basel Capital Accord, BIS, czerwiec 2004.

Struktura organizacyjna

W myśl zapisów Nowej Umowy Kapitałowej bank powinien dostosować swoją organizację wewnętrzną do nowych wymagań. W uchwałach Komisji Nadzoru Bankowego wyszczególniono szereg rodzajów ryzyka (§13 uchwały 4/2007), którymi bank powinien zarządzać, co oznacza, że powinien posiadać pisemne regulacje, które zawierają procedury, metody, modele zarządzania tymi ryzykami oraz określenie zadań podmiotów zaangażowanych w proces zarządzania nimi.

Rozdzielenie funkcji zarządzania ryzykiem od działalności operacyjnej powinno nastąpić poprzez ustalenie następujących poziomów zarządzania ryzykiem:

- 1) nadzorczy – Rada Nadzorcza,
- 2) decyzyjny – Zarząd banku,
- 3) opiniodawczy – stanowiska/zespoły opiniotwórcze, takie jak Komitet Kredytowy i Komitet Zarządzania Ryzykami,
- 4) kontrolny – Zespół Zarządzania Ryzykami i Analiz; jego zadaniem jest gromadzenie, analiza i udostępnianie danych dotyczących wszystkich rodzajów ryzyka, opracowanie wewnętrznych limitów i procedur oraz stanowisko kontroli wewnętrznej i audytu, dostarczające Zarządowi i Radzie Nadzorczej informacji na temat poprawności funkcjonowania systemów zarządzania ryzykami,
- 5) wykonawczy – pracownicy, których działalność generuje ryzyko (wszyscy pracownicy banku).

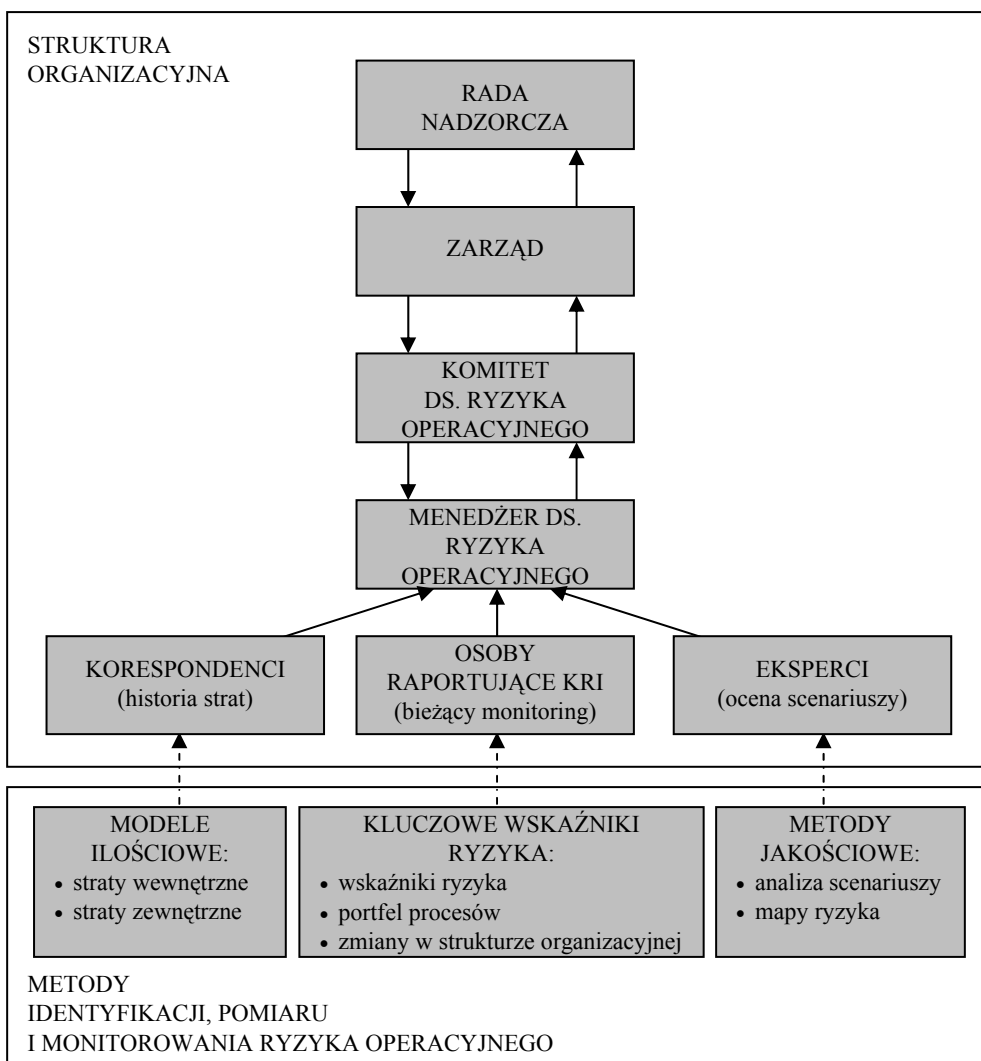
Przykładowy system zarządzania ryzykiem operacyjnym podaje Matkowski⁴, wskazując na istotność wyróżnienia w tym systemie dwóch elementów:

- stanowiska menedżera ds. ryzyka operacyjnego i Komitetu ds. Ryzyka Operacyjnego, jako podstawowych jednostek organizacyjnych, w ramach których odbywa się zarządzanie ryzykiem operacyjnym,
- źródeł danych operacyjnych (korespondenci, osoby raportujące o KRI i eksperci), stanowiących podstawę analizy ryzyka operacyjnego w banku.

Procedury zarządzania ryzykiem

Określenie podstawowych, istotnych dla banku rodzajów ryzyka oraz dostosowanie struktury organizacyjnej do prawidłowego zarządzania tymi ryzykami to istotny element realizacji wymagań NUK. Działania te znajdują odzwierciedlenie w wewnętrznych, pisemnych regulacjach banku. Podstawą opracowania regulacji dostosowanych do NUK stało się przyjęcie nowej struktury organizacyjnej, zatwierdzenie Regulaminu Organizacyjnego przez Zarząd i Radę Nadzorczą oraz zatwierdzenie przez Radę Nadzorczą dokumentu o nazwie *Strategia zarządzania ryzykiem*. Kolejnym etapem powinno być zmodyfikowanie instrukcji zarządzania poszczególnymi rodzajami ryzyka.

⁴ P. Matkowski, *Zarządzanie ryzykiem operacyjnym*, Wolters Kluwer Polska, Kraków 2006, s. 170.



Rys. 1. System zarządzania ryzykiem operacyjnym

Źródło: P. Matkowski, *Zarządzanie ryzykiem operacyjnym*, Wolters Kluwer Polska, Kraków 2006, s. 170.

Informatyczne wspomaganie zarządzania ryzykiem

Spełnienie wymagań NUK wymaga również zmian w obszarze IT, które to zmiany powinny być ukierunkowane przede wszystkim na:

1) rozbudowę zasobów i funkcji systemu ewidencyjno-księgowego, eksploatowanego w banku w celu dostosowania go do zmieniających się potrzeb sprawozdawczych,

2) wdrożenie programów wspierających zarządzanie ryzykami (operacyjnym, płynności, stopy procentowej, kadrowym itp.),

3) zapewnienie bezpieczeństwa systemów informatycznych (ryzyko operacyjne, zachowanie ciągłości działania w sytuacjach kryzysowych) oraz ich zgodności z wewnętrznymi i zewnętrznymi regulacjami prawnymi (ryzyko braku zgodności).

Podstawowe zmiany w eksploatowanym systemie ewidencyjno-księgowym banku wynikają ze zmiany przepisów w zakresie:

1) sprawozdawczości obowiązkowej – zmieniony układ raportów, zawierających dane księgowe, które są przekazywane na portal SIS (System Informacji Sprawozdawczej GINB) w postaci pakietów sprawozdawczych FINREP i COREP,

2) wyliczania wymogów kapitałowych z tytułu poszczególnych rodzajów ryzyka; system powinien umożliwić podział ekspozycji kredytowych na klasy wymienione w załączniku nr 4 do uchwały nr 1/2007 KNB i automatycznie przypisać im odpowiednie wagi ryzyka,

3) technik redukcji ryzyka kredytowego – system powinien umożliwiać nadanie odpowiednich parametrów ekspozycjom kredytowym, w stosunku do których zastosowano techniki ograniczania ryzyka kredytowego i nadawać im odpowiednie wagi ryzyka,

4) ustalania i monitorowania limitów koncentracji – w oparciu o zapisy uchwały nr 5/2007 KNB; szczególnie dotyczy to koncentracji z tytułu jednego rodzaju zabezpieczenia lub dostawcy zabezpieczenia oraz koncentracji ze względu na branżę,

5) zarządzania ryzykiem ekspozycji kredytowych zabezpieczonych hipotecznie – system powinien umożliwiać ewidencję wartości zabezpieczeń nie tylko pod kątem pomniejszania podstawy tworzenia rezerw celowych, ale również pod kątem wyliczania wskaźnika LTV,

6) zapewnienia ciągłości działania – wymóg uchwały nr 4/2007 KNB.

3. System zarządzania ryzykiem operacyjnym

Strategia zarządzania ryzykiem operacyjnym w omawianym banku realizowana jest poprzez System Zarządzania Ryzykiem Operacyjnym, którego elementami są:

- struktura organizacyjna wspomagająca proces zarządzania ryzykiem operacyjnym,
- procedury zarządzania ryzykiem operacyjnym,
- metody identyfikacji, pomiaru, monitorowania i kontroli ryzyka operacyjnego.

Struktura organizacyjna

Rada Nadzorcza sprawuje nadzór nad skutecznością systemu zarządzania ryzykiem operacyjnym banku. Zatwierdza dokumenty strategiczne w tym obszarze zarządzania oraz strukturę organizacyjną powołaną w celu zarządzania tym rodzajem ryzykiem.

Zarząd Banku odpowiada za opracowanie, wprowadzenie i aktualizację strategii, polityk oraz regulaminów i instrukcji w zakresie zarządzania ryzykiem operacyjnym. Wprowadza strukturę organizacyjną oraz zapewnia zasoby niezbędne do skutecznego zarządzania ryzykiem operacyjnym. Przedkłada Radzie Nadzorczej okresową informację na temat narażenia banku na ryzyko operacyjne oraz wprowadza wartości progowe akceptowanego poziomu tego ryzyka.

Komitet ds. Ryzyka Operacyjnego na podstawie wartości KRI oraz na podstawie wyników prac analitycznych prowadzonych w Zespole ds. Ryzyka Operacyjnego ocenia poziom ryzyka operacyjnego w skali całego banku. Komitet rekomenduje Zarządowi Banku wartości progowe akceptowanego poziomu ryzyka operacyjnego. Ocenia skalę zagrożenia w sytuacjach kryzysowych i rekomenduje podjęcie działań ograniczających skutki zrealizowanego ryzyka operacyjnego. Składa Radzie Nadzorczej i Zarządowi Banku raporty na temat poziomu ryzyka operacyjnego oraz informacje o najpoważniejszych zagrożeniach operacyjnych.

Do podstawowych zadań **Zespołu ds. Ryzyka Operacyjnego** należy opracowanie i aktualizowanie metodyki zarządzania ryzykiem operacyjnym określonej przez system aktów normatywnych definiujących proces zarządzania tym ryzykiem oraz sposoby jego realizowania. Pracownicy zespołu inicjują wprowadzanie oraz rozwijanie narzędzi wspomagających zarządzanie ryzykiem operacyjnym, prowadzą analizy profilu i monitorowanie poziomu ryzyka operacyjnego banku, opracowują standardowe analizy i raporty, a także sprawozdania wynikające z obowiązku informacyjnego wobec uprawnionych instytucji zewnętrznych.

Kierownictwo jednostek oraz komórek organizacyjnych banku na podstawie wyników analiz poziomu ryzyka operacyjnego zarządza ryzykiem operacyjnym podległych jednostek. Oznacza to, że kierownictwo w zakresie swoich kompetencji podejmuje działania ograniczające potencjalne zagrożenia w obszarze ryzyka operacyjnego oraz łagodzące negatywne skutki zrealizowania tego ryzyka. Kierownictwo jednostek oraz komórek organizacyjnych banku wspiera Zespół ds. Ryzyka Operacyjnego w identyfikowaniu profilu ryzyka operacyjnego banku poprzez udzielanie informacji o głównych potencjalnych zagrożeniach operacyjnych w ich obszarach odpowiedzialności. Pracownicy wszystkich jednostek i komórek organizacyjnych banku, wyznaczeni przez swoich przełożonych, zobowiązani są do przekazywania informacji o incydentach i zdarzeniach operacyjnych w trybie określonym odrębnym aktem normatywnym banku, regulującym sposób gromadzenia wymienionych danych.

Identyfikacja ryzyka operacyjnego

Ryzyko operacyjne banku jest identyfikowane poprzez rejestrację incydentów i zdarzeń operacyjnych w celu rozpoznania profilu oraz monitorowania poziomu tego ryzyka. Identyfikacja odbywa się również za pomocą samooceny w zakresie ryzyka w celu zapobiegania powstawaniu nieakceptowanego poziomu ryzyka operacyjnego w działaniach realizowanych przez bank. Identyfikacja poprzez samo-

ocenę polega na ocenie podatności operacji i czynności bankowych na czynniki ryzyka operacyjnego wraz z oceną zagrożeń. Jest to proces wewnętrzny, realizowany poprzez system ankiet bądź identyfikację silnych i słabych stron w procesach.

Rejestracja incydentów i zdarzeń operacyjnych przeprowadzana jest na każdym szczeblu struktury organizacyjnej. Do rejestrowania zdarzeń operacyjnych nie wprowadza się progu kwotowego. Rejestracji podlegają wszystkie zaistniałe zdarzenia operacyjne i wszystkie incydenty. Dokonywana jest ona zgodnie z odpowiednią instrukcją: określa się datę wykrycia zdarzenia operacyjnego, datę faktycznego wystąpienia zdarzenia operacyjnego (z opisem zdarzenia, okoliczności jego powstania oraz przyczyny), działania podjęte w celu usunięcia nieprawidłowości oraz czas przestoju, rozumiany jako np. niemożność wykonywania swojej pracy lub/ oraz ilość błędnych dokumentów.

Wypełnione indywidualne rejestry zdarzeń operacyjnych/incydentów podlegają okresowym przeglądom przez Zespół Zarządzania Ryzykami oraz Controllingu i Analiz. Okresowe przeglądy ryzyka dokonywane są kwartalnie.

Samoocena w zakresie ryzyka przeprowadzana jest w formie jednorazowych przeglądów ryzyka operacyjnego. Ma na celu zwiększenie świadomości pracowników, a także przygotowanie ich do działań zapobiegających ewentualnym negatywnym skutkom dla wyników banku, a także jego bezpieczeństwa (lub zmniejszających takie skutki).

Jednorazowe przeglądy ryzyka operacyjnego realizowane są w banku poprzez ankiety – celem ankiety jest rozpoznanie w banku zjawisk, które mogą narażać go na ryzyko operacyjne. Podsumowanie wyników ankiety zostaje przekazane Zarządowi Banku najpóźniej 30 dni po przeprowadzeniu ankiety.

Samoocena dokonywana jest również poprzez **mapowanie ryzyka**, co polega na rozpoznawaniu w procesach oraz podprocesach realizowanych przez bank przewidywanych scenariuszy zagrażających wystąpieniem straty z przyczyn operacyjnych. Jest to graficzna prezentacja wielkości i rozkładu ryzyka w poszczególnych procesach. W banku istnieje świadomość podziału działalności organizacji na podstawowe procesy operacyjne, czyli takie, których przebieg wiąże się z celami banku. Dla każdego z tych procesów określona jest jednostka organizacyjna (osoba) odpowiedzialna za przestrzeganie procedur związanych z danym procesem i ich ewentualne modyfikacje oraz za systemy teleinformatyczne biorące udział w ich realizacji. Graficzna prezentacja czynności bankowych umożliwia identyfikację potencjalnych zagrożeń w poszczególnych procesach i na określonych etapach. Narzędziem wspomagającym mapowanie ryzyka operacyjnego w banku jest odpowiedni system informatyczny. Mapa ryzyka operacyjnego umożliwia ujawnienie słabych punktów lub procesów, które generują wysokie ryzyko. Z nich bezpośrednio wynikają kluczowe wskaźniki ryzyka (KRI).

Monitorowanie ryzyka operacyjnego

Poziomy ryzyka operacyjnego są monitorowane we wszystkich obszarach działania banku – przez Zespół ds. Ryzyka Operacyjnego. W tym celu w banku wykorzystuje się odpowiednie rejestry, które zawierają informacje jakościowe lub/i ilościowe z obszarów działalności banku powiązanych z ryzykiem operacyjnym. Aktualizowane są one cyklicznie lub na bieżąco; w niektórych przypadkach przechowywane są w układzie chronologicznym.

Monitorowanie ryzyka operacyjnego odbywa się również za pomocą indywidualnych rejestrów zdarzeń ryzyka operacyjnego, przedstawiających istotne zdarzenia ryzyka operacyjnego. Istotnym zdarzeniem ryzyka operacyjnego dla banku jest na przykład zdarzenie, wskutek którego:

- 1) wystąpiła szacunkowa strata finansowa o określonej wartości,
- 2) nastąpiła określonej długości przerwa w obsłudze klientów placówki,
- 3) incydent wystąpił odpowiednio często w określonym przedziale czasu.

W banku zdefiniowane są **metody ograniczania ryzyka operacyjnego** oraz łągodzenia skutków zrealizowania się ryzykownych zdarzeń. Do podstawowych metod ograniczania ryzyka operacyjnego należą:

- modyfikowanie wewnętrznych aktów normatywnych w aspekcie redukcji ryzyka operacyjnego do poziomu akceptowanego,
- rozszerzone monitorowanie ryzyka operacyjnego w sytuacjach stwarzających realne zagrożenie przekroczenia wartości progowych akceptowanego poziomu ryzyka operacyjnego,
- przenoszenie odpowiedzialności (outsourcing),
- zabezpieczenia fizyczne ludzi, pomieszczeń, sprzętu, dokumentów i informacji.

Raportowanie ryzyka operacyjnego odbywa się w cyklach kwartalnych. System raportowania poziomu ryzyka operacyjnego jest udokumentowany, a definicje poszczególnych raportów obejmują następujące elementy: cel sporządzenia raportu, zakres danych, format danych, termin wykonania, nazwę odbiorcy.

4. Podsumowanie

Zaprezentowany system zarządzania ryzykiem operacyjnym powstał zgodnie z wymaganiami NUK oraz krajowego nadzoru bankowego. Pod względem formalnym jest więc skonstruowany poprawnie.

W zaleceniach Komitetu Bazylejskiego podkreśla się wagę standardów jakości w zarządzaniu ryzykiem operacyjnym. Jednakże poza ogólnymi stwierdzeniami, że system taki musi być koncepcyjnie poprawny i spójnie wdrożony, brak jest szczegółowych zaleceń co do jego budowy. Banki, tworząc swoje systemy, wybierały różne podejścia i, choć wszystkie systemy muszą być zgodne z regulacjami nadzoru bankowego, to różnią się między sobą koncepcją funkcjonowania, stosowanymi modelami, szczegółowością raportów itp. Fakt ten nasuwa dwa pytania. Po pierw-

sze, czy system zarządzania ryzykiem operacyjnym w danym banku jest adekwatny do potrzeb zarządu i rady nadzorczej i umożliwia im sprawne zarządzanie ryzykiem operacyjnym? Po drugie, czy możliwe jest porównanie systemów zarządzania ryzykiem operacyjnym w różnych bankach? Odpowiedź na te pytania wymaga zastosowania odpowiednich narzędzi oceny systemu ryzyka operacyjnego. Jednym z takich narzędzi mogą być modele dojrzałości systemów, jednakże ich zastosowanie w chwili obecnej wymaga podjęcia szeregu prac dostosowawczych.

Literatura

Matkowski P., *Zarządzanie ryzykiem operacyjnym*, Wolters Kluwer Polska, Kraków 2006.
Rekomendacja M dotycząca zarządzania ryzykiem operacyjnym w bankach, KNB, Warszawa 2004.
The New Basel Capital Accord, BIS, czerwiec 2004.
Uchwały KNB nr 1/2007, 2/2007, 3/2007, 4/2007, 5/2007 i 6/2007 z 13 marca 2007 r.

OPERATIONAL RISK MANAGEMENT IN RETAIL BANK – A SYSTEMIC FRAME

Summary

The article presents some aspects of OR management in retail banking in a systemic frame. It describes the OR management system elements and proposes the appropriate evaluation means. The requirements of Basel II are also presented as well.