Dariusz Garczyński
Uniwersytet Ekonomiczny we Wrocławiu

IDENTYFIKACJA RYZYKA W SYSTEMACH ZARZĄDZANIA RYZYKIEM OPERACYJNYM

Wstęp

Zarządzanie ryzykiem operacyjnym w banku jest procesem ciągłym, wymagającym zastosowania wielu narzędzi na każdym etapie. Systemy zarządzania RO funkcjonują obecnie w każdym banku. Budowane, zgodnie z zaleceniami NUK, powinny uwzględniać skalę i specyfikę działania banku. Aby efektywnie zarządzać ryzykiem operacyjnym, bank powinien posiadać udokumentowany proces jego identyfikacji dla wszystkich istotnych obszarów działalności oraz wszelkich nowych produktów, procesów i systemów. Etap ten jest szczególnie istotny, gdyż pozwala na określenie profilu ryzyka banku i właściwy dobór narzędzi zarządzania tym ryzykiem.

Celem artykułu jest prezentacja założeń systemu zarządzania ryzykiem operacyjnym w banku oraz charakterystyka narzędzi do jego identyfikacji.

1. System zarządzania ryzykiem operacyjnym

Podstawowym zadaniem systemu zarządzania ryzykiem operacyjnym (SZRO) w banku jest identyfikacja, oszacowanie, redukcja i monitorowanie ryzyka operacyjnego (Garczyński 2007). Działanie systemu obejmuje również raportowanie o ryzyku operacyjnym na potrzeby zarządu oraz instytucji nadzoru. Do podstawowych elementów systemu zaliczyć można:

- strukturę organizacyjną wspomagającą proces zarządzania ryzykiem operacyjnym,
- procedury zarządzania ryzykiem operacyjnym'
- metody identyfikacji, pomiaru, monitorowania i kontroli ryzyka operacyjnego.

Prawidłowo realizowany proces zarządzania ryzykiem operacyjnym realizowany jest na każdym z poziomów zarządzania ryzykiem:

- nadzorczy – rada nadzorcza (sprawuje nadzór nad skutecznością systemu zarządzania ryzykiem operacyjnym banku);
- decyzyjny – zarząd banku (odpowiada przede wszystkim za opracowanie, wprowadzenie i aktualizację strategii, polityki oraz regulaminów i instrukcji w zakresie zarządzania ryzykiem operacyjnym);
- opiniodawczy – stanowiska/zespoły opiniotwórcze, takie jak komitet kredytowy i komitet zarządzania ryzykiem (ocenia poziom ryzyka operacyjnego w skali całego banku, rekomenduje zarządowi wartości progowe akceptowanego poziomu ryzyka operacyjnego oraz podejmowanie działań ograniczających skutki ryzyka operacyjnego, składa radzie nadzorczej i zarządowi raporty na temat poziomu ryzyka operacyjnego);
- kontrolny – Zespół Zarządzania Ryzykiem i Analiz (do zadań zespołu należy opracowanie i aktualizowanie metodyki zarządzania ryzykiem operacyjnym określonej przez system aktów normatywnych definiujących proces zarządzania ryzykiem operacyjnym oraz sposoby realizowania tego procesu; zespół inicjuje wprowadzanie oraz rozwijanie narzędzi wspomagających zarządzanie ryzykiem operacyjnym, prowadzi analizy profilu i monitorowanie poziomu ryzyka operacyjnego, opracowuje standardowe analizy i raporty dla potrzeb Komitetu Zarządzania Ryzykiem i kierownictwa jednostek i komórek organizacyjnych banku, a także sprawozdania wynikające z obowiązku informacyjnego wobec uprawnionych instytucji zewnętrznych);
- wykonawczy – pracownicy, których działalność generuje ryzyko (wszyscy pracownicy banku).

2. Narzędzia identyfikacji ryzyka operacyjnego

Do najważniejszych kwestii w obszarze zarządzania ryzykiem operacyjnym w banku należy z pewnością dobór odpowiednich metod identyfikacji, pomiaru, monitorowania i kontroli, adekwatnych do wielkości banku oraz profilu jego działalności.

Ryzyko operacyjne jest identyfikowane w ramach procesu rejestracji incydentów i zdarzeń operacyjnych w celu rozpoznawania profilu oraz monitorowania poziomu tego ryzyka. Identyfikacja ryzyka operacyjnego odbywa się również dzięki samoocenie przeprowadzanej w formie jednorazowych przeglądów ryzyka operacyjnego w celu zwiększenia świadomości ryzyka u pracowników banku. Jest to proces wewnętrzny, który można realizować poprzez system ankiet bądź identyfikację silnych i słabych stron w procesach operacyjnych. Proces rejestracji incydentów i zdarzeń operacyjnych przeprowadzany jest na każdym szczeblu struktury organizacyjnej.

Rejestracji podlegają wszystkie zaistniałe zdarzenia operacyjne i wszystkie incydenty (na każdym szczeblu struktury organizacyjnej), przy czym rejestruje

się przede wszystkim datę wykrycia zdarzenia operacyjnego, datę, kiedy zdarzenie operacyjne faktycznie wystąpiło, charakterystykę zdarzenia (okoliczności jego powstania oraz przyczyny), działania podjęte w celu usunięcia nieprawidłowości oraz czas przestoju, rozumiany jako np. niemożność wykonywania pracy lub/oraz liczba błędnych dokumentów. Wypełnione indywidualne rejestry zdarzeń operacyjnych/incydentów podlegają okresowym przeglądom przez Zespół Zarządzania Ryzykiem oraz Controlingu i Analiz. Okresowe przeglądy ryzyka dokonywane są kwartalnie.

Jednorazowe przeglądy ryzyka operacyjnego mogą być realizowane w banku poprzez ankiety – celem ankiety jest rozpoznanie w banku zjawisk narażających go na ryzyko operacyjne. Ankieta zostaje przygotowana przez Zespół Zarządzania Ryzykiem oraz Controlingu i Analiz i może być przygotowana w dowolnym czasie.

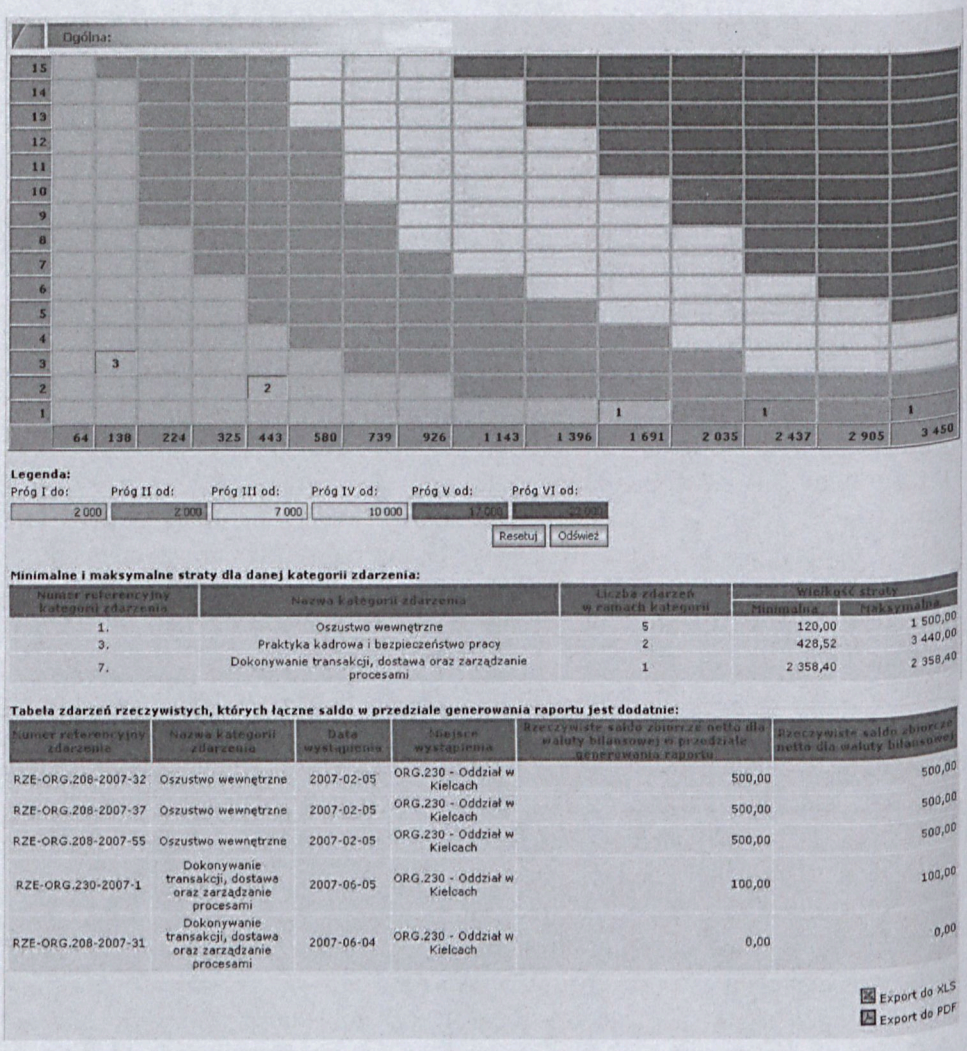
Identyfikacja ryzyka operacyjnego dokonywana jest również poprzez mapowanie ryzyka, które jest graficzną prezentacją wielkości i rozkładu ryzyka w poszczególnych procesach realizowanych przez bank. Taka prezentacja umożliwia identyfikację zagrożeń w poszczególnych procesach. Zazwyczaj mapowanie ryzyka odbywa się ze wspomaganiem odpowiedniego narzędzia informatycznego (rys. 1).

Zidentyfikowane zagrożenia z tytułu ryzyka operacyjnego są zaliczane (zgodnie z zaleceniami NUK) do jednej z siedmiu kategorii:

1) oszustwo wewnętrzne,
2) oszustwo zewnętrzne,
3) zarządzanie personelem i bezpieczeństwem pracy,
4) klienci, produkty i praktyka biznesowa,
5) uszkodzenia aktywów materialnych,
6) błędy i zakłócenia w pracy systemów,
7) transakcje, dostawy i zarządzanie aktywami.

Kolejne podziały na podkategorie pozwalają na dokładne przypisanie zdarzenia operacyjnego do specyficznego rodzaju ryzyka, co umożliwia rozpoznanie skali zagrożenia jakie niesie.

Do pomiaru ekspozycji banku na ryzyko operacyjne stosowane są także tzw. kluczowe wskaźniki ryzyka (KRI) (Matkowski 2006). Są to statystyki i/lub miary, często finansowe, na podstawie których można określić między innymi wrażliwość banku na ryzyko, w tym ryzyko operacyjne. Wskaźniki te można wyznaczyć na podstawie danych okresowych (miesięcznych lub kwartalnych), związanych na przykład z liczbą nieudanych transakcji, wskaźnikami zmian kadrowych lub częstotliwością błędów. KRI służą przede wszystkim do monitorowania ryzyka, ale mogą też być wykorzystywane do jego pomiaru oraz jako limity ryzyka (Podręcznik 2007).



Rysunek 1. Przykładowa mapa ryzyka operacyjnego (wygenerowana w systemie Azro)
Źródło: materiały szkoleniowe firmy BSB SA.

Wartości KRI wyliczane są na podstawie danych zawartych w rejestrach (ewidencjach), mapy ryzyka lub pozyskiwanych ze źródeł zewnętrznych. Do kluczowych wskaźników ryzyka KRI można zaliczyć np. (Polityka 2009):

1) W obszarze zasobów kadrowych:
   a) fluktuację i ocenę pracowników,
   b) absencję, zwolnienia lekarskie oraz urlopy wypoczynkowe i okolicznościowe,
2) Procesów i systemów:
   a) awarie/przestoje systemów teleinformatycznych,

b) błędy księgowe – storna i korekty,
c) sprawy sądowe (odnoszące się do produktów i usług), w których stroną jest bank,
d) przeprowadzone kontrole w jednostkach/komórkach organizacyjnych banku,
e) częstotliwość archiwizacji zasobów i systemów,
f) reklamacje klientowskie – liczba i wartość roszczeń,
g) liczbę i wartość kar na rzecz klientów,

3) Zdarzeń zewnętrznych:
a) sprawy sądowe (dotyczące stosowania i interpretacji przepisów), w których stroną jest bank,
b) wandalizm i kradzieże oraz oszustwa w zakresie rozliczeń pieniężnych.

Wyznaczone wartości progowe dla kluczowych wskaźników ryzyka KRI rozpatruje się w podziale na poziomy:

- akceptowany – poziom niestanowiący zagrożenia, monitorowany,
- ostrzegawczy – poziom sygnalizujący wzrost ryzyka operacyjnego, wymagający kontrolowania i stopniowego ograniczania do poziomu akceptowanego,
- krytyczny – poziom uznany za nieakceptowany, wymagający podjęcia pilnych działań naprawczych.

Zakończenie

Banki powinny identyfikować i oceniać ryzyko operacyjne wbudowane we wszystkie produkty, czynności, procesy i systemy o materialnej wartości (Lewandowski 2004). Właściwa identyfikacja czynników ryzyka jest podstawą dalszych czynności w procesie zarządzania ryzykiem operacyjnym, pozwala na określenie profilu ryzyka banku oraz umożliwia późniejszy pomiar i skuteczne monitorowanie tego ryzyka. Nie bez znaczenia jest fakt, że proces identyfikacji ryzyka zwiększa świadomość występowania tego rodzaju ryzyka u pracowników banku, co usprawnia cały proces zarządzania.

Bibliografia

Garczyński D. (2007), *Modelowanie ryzyka operacyjnego z wykorzystaniem procesów biznesowych*, [w:] M. Marcinkowska, S. Wieteska (red.), *Harmonizacja finansów, bankowości i ubezpieczeń w skali narodowej i europejskiej*, Difin, Warszawa, s. 217-124.

Lewandowski D., (2004), *Ryzyko operacyjne w bankach – zarządzanie i audyt w świetle wymagań Bazylejskiego Komitetu ds. Nadzoru Bankowego*, Bank i Kredyt, 04, s. 48.

Matkowski P. (2006), *Zarządzanie ryzykiem operacyjnym*, Wolters Kluwer Polska, Kraków, s. 185 i in.
Podręcznik inspekcji na miejscu, Warszawa, kwiecień 2007.
Dokument *Polityka zarządzania ryzykiem operacyjnym* jednego z banków.

RISK IDENTIFICATION IN OPERATIONAL RISK MANAGEMENT SYSTEMS

Summary

Banks should identify and estimate operational risk embedded in every product, activity, process and systems of financial value. Correct risk factors identification establishes a basis for further activities in operational risk management process and makes possible subsequent risk measurement and monitoring. It's not meaningless that the risk identification process increases the risk awareness among the bank personnel what improves the whole risk management process.