

## Proces zarządzania ryzykiem operacyjnym w banku – studium przypadku

Anna Bartoszewicz\*

**Streszczenie:** *Cel* – Celem niniejszego artykułu jest zaprezentowanie teoretycznych aspektów zarządzania ryzykiem operacyjnym w bankach oraz wskazanie praktycznego podejścia do tego zagadnienia.

*Metodologia badania* – Do realizacji przyjętego celu wykorzystano analizę literatury przedmiotu z zakresu bankowości i zarządzania ryzykiem oraz zaprezentowano studium przypadku dotyczące przebiegu procesu zarządzania ryzykiem w banku.

*Wynik* – W artykule przedstawiono zarówno aspekt teoretyczny procesu zarządzania ryzykiem operacyjnym w banku, jak również zaprezentowano praktyczne podejście do tego zagadnienia, opierając się na przebiegu ww. procesu w wybranym podmiocie badań.

*Oryginalność/Wartość* – Artykuł stanowi praktyczną prezentację procesu zarządzania ryzykiem operacyjnym.

**Słowa kluczowe:** ryzyko, zarządzanie ryzykiem, ryzyko operacyjne, bank

### Wprowadzenie

Ryzyko jest kategorią, która występuje w działalności wszystkich jednostek gospodarczych. W ogólnym ujęciu oznacza „możliwość zaistnienia zdarzenia, które będzie miało wpływ na realizację założonych celów” (*Zarządzanie ryzykiem...*: 6).

Wśród wielu instytucji działających w państwie szczególną rolę w gospodarce odgrywają banki, bowiem ich działalność ma wpływ na funkcjonowanie instytucji państwowych, podmiotów prywatnych czy też gospodarstw domowych. Ryzyko dla banku, tak jak dla innych jednostek, oznacza zagrożenie nieosiągnięciem wyznaczonych celów, co wiąże się z utratą części potencjalnych zysków, wiarygodności i płynności, a także grozi zmniejszeniem kapitału własnego. Biorąc pod uwagę korelację działalności banków z działalnością innych instytucji, konieczna wydaje się identyfikacja ryzyka i skuteczne zarządzanie nim.

Znaczący wpływ na działalność banków ma ryzyko operacyjne, które jest pojęciem niejednorodnym, związanym z wieloma czynnikami, mogącymi wywoływać poważne skutki w podmiotach, a zarządzanie nim jest złożonym procesem. Komisja Nadzoru Bankowego określiła ryzyko operacyjne jako: „ryzyko straty wynikającej z niedostosowania lub zawodności wewnętrznych procesów, ludzi i systemów technicznych lub ze zdarzeń zewnętrznych” (*Rekomendacja M...* 2004: 3).

---

\* dr Anna Bartoszewicz, adiunkt, Uniwersytet Warmińsko-Mazurski w Olsztynie, Wydział Nauk Ekonomicznych, Katedra Rachunkowości, ul. M. Oczapowskiego 4, 10-957 Olsztyn, e-mail: anna.bartoszewicz@uwm.edu.pl.

Jest to zagadnienie o stosunkowo krótkiej historii w porównaniu z ryzykiem kredytowym czy rynkowym, chociaż należy zwrócić uwagę, iż pewne ryzykowne zdarzenia operacyjne, tj. nadużycia finansowe czy błędy operacyjne, od zawsze występowały w różnych instytucjach, a szczególnie w bankach. Jednak dopiero w latach 90. ubiegłego stulecia doceniono znaczenie tej kategorii ryzyka.

Mając na uwadze wagę tych zagadnień, za główny cel artykułu przyjęto zaprezentowanie teoretycznych aspektów zarządzania ryzykiem operacyjnym w bankach oraz wskazanie praktycznego podejścia do tego zagadnienia.

## 1. Definicja i rodzaje ryzyka operacyjnego w banku

Do początku minionego dziesięciolecia ryzyko operacyjne pozostawało niedookreślone. Znane były natomiast pojęcia takie jak: ryzyko rynkowe czy kredytowe. Jednak różne wydarzenia finansowe, które miały miejsce nie tylko w Europie, spowodowały wzrost zainteresowania kategorią ryzyka operacyjnego i koniecznością jego określenia.

Definicja ryzyka operacyjnego, podana na wstępie niniejszej publikacji, została pierwotnie sformułowana przez Bazylejski Komitet Nadzoru Bankowego, a następnie zaadaptowana przez Komisję Nadzoru Bankowego w Polsce. Należy jednak podkreślić, że definicja ta nie jest jednoznaczna i bezwzględnie obowiązująca. Często banki same opracowują interpretację tego pojęcia, najlepiej pasującą do warunków i specyfiki ich jednostki.

Ze względu na złożoność pojęcia ryzyka operacyjnego nie ma jednorodnego jego podziału. Przykładowo R. Kałużny (2004: 20–22) do kategorii ryzyka operacyjnego zaliczył:

- ryzyko relacji banku ze środowiskiem zewnętrznym, związane z reputacją banku i zaufaniem publicznym,
- ryzyko kadrowe, spowodowane m.in. złym doбором, zarządzaniem oraz motywowaniem pracowników,
- ryzyko technologiczne, wynikające z operacji i rozliczeń dokonywanych przez bank oraz z błędów powstałych przy obliczeniach,
- ryzyko nieodpowiedniego obiegu dokumentacji, wiążące się z nieprawidłowo funkcjonującym systemem informacyjnym w jednostce, niewłaściwym postępowaniem kadry czy też z niebezpieczeństwem wycieku poufnych informacji na zewnątrz,
- ryzyko zdarzeń nadzwyczajnych, takich jak ataki terrorystyczne, klęski żywiołowe,
- ryzyko kryminalne, czyli zagrożenie przestępstwem generującym straty w banku.

D. Lewandowski (2004: 48–55) wyodrębnił natomiast następujące rodzaje ryzyka operacyjnego, będące jednocześnie i jego przyczynami. Opierają się one na systematyce zdarzeń operacyjnych wymienionych w *Rekomendacji M*:

- nadużycia wewnętrzne – kradzieże dokonywane przez pracowników, fałszowanie wewnętrznej sprawozdawczości, wewnętrzne transakcje na szkodę jednostki,
- nadużycia zewnętrzne – kradzieże, napady, włamania fizyczne i komputerowe, oscylator finansowy,
- zasady zatrudniania i bezpieczeństwo pracy – np. wymagania pracowników dotyczące płacy, warunki pracy niezgodne z zasadami bhp, dyskryminacja pracowników,
- klienci, produkty, praktyki biznesowe – pranie brudnych pieniędzy, wykorzystanie poufnych danych o klientach, wykonywanie niedozwolonych operacji na rachunkach bankowych, oferowanie produktów nieposiadających autoryzacji,
- zniszczenie aktywów – akty terroryzmu, wandalizmu, działanie siły wyższej,

- brak ciągłości pracy firmy, przerwanie pracy systemów – problemy z oprogramowaniem i sprzętem, zakłócenia telekomunikacyjne,
- zarządzanie jednostką, zarządzanie procesami – niekompletna dokumentacja prawna, błędy przy wprowadzaniu danych, nieupoważniony dostęp do informacji o klientach, reklamacje, uwagi dostawców i sprzedawców.

Ponadto można wyróżnić ryzyko bankowe występujące w działalności wewnętrznej banku, związane m.in. z jakością personelu, zabezpieczeniami majątku, niezawodnością systemów i procesów, a także rodzaje ryzyka w działalności zewnętrznej, wiążące się np. z wahaniami stóp procentowych, kursów walut, pogarszaniem się wypłacalności kredytobiorców (Iwanicz-Drozdowska, Jaworski, Zawadzka 2010: 233).

Źródłem występowania ryzyka operacyjnego w banku są czynniki ryzyka, określane jako zdarzenia, które powodują wystąpienie ryzyka. *Rekomendacja M* wyróżnia cztery główne grupy czynników ryzyka operacyjnego, których syntetyczny podział zamieszczono w tabeli 1.

**Tabela 1**

Czynniki ryzyka operacyjnego

Kategoria	Podkategoria	Przykład
<b>Ludzie</b>		<ul style="list-style-type: none"> <li>– niedostępność i niskie kwalifikacje pracownice,</li> <li>– wysoka fluktuacja pracownicza,</li> <li>– godziny nadliczbowe,</li> <li>– długotrwałe niewykorzystanie urlopu wypoczynkowego,</li> <li>– absencja pracowników</li> </ul>
		– wadliwe działanie sprzętu i systemu
<b>Procesy i systemy</b>	Systemy teleinformatyczne	– nieadekwatność dokumentacji wewnętrznej,
	Dokumentacja wewnętrzna	– niewłaściwa dystrybucja dokumentacji wewnętrznej,
	Dokumentacja zewnętrzna	– błędy w dokumentacji zewnętrznej, – brak zgodności z wymogami prawnymi
	Bezpieczeństwo informacyjne	– udostępnienie informacji osobom nieuprawnionym, – brak integralności danych i systemu, – błędy przy uwierzytelnianiu użytkowników systemu
	Lokalizacja	– destabilizacja sytuacji politycznej, – różnice kulturowe, – problemy z dostępem do informacji od nadzorców z kraju macierzystego, jednostki kontroli wewnętrznej, czy audytorów zewnętrznych
<b>Zdarzenia zewnętrzne</b>	Zdarzenia przewidywalne	– fuzje, przejęcia
	Zdarzenia nieprzewidywalne	– zakłócenia dostaw energii elektrycznej, – wandalizm, wojna, kataklizmy
<b>Outsourcing</b>		<ul style="list-style-type: none"> <li>– brak kontroli nad podmiotem wykonującym zleczone czynności,</li> <li>– niezgodność zawartej umowy ze strategią banku</li> </ul>

Źródło: opracowanie własne na podstawie (*Rekomendacja M...* 2004: 6–11).

Wśród specyficznych cech ryzyka operacyjnego warto podkreślić następujące problemy (Lewandowski 2004: 48–55):

- ryzyko to nie jest podejmowane w celu osiągnięcia określonych korzyści biznesowych, lecz jest wbudowane w prowadzoną działalność,
- nie można całkowicie wyeliminować źródeł tego ryzyka,
- analiza czynników oraz konsekwencji i skutków ryzyka nie jest łatwa,
- pomiar ryzyka operacyjnego nie jest prostym zadaniem,
- trudno jednoznacznie określić właścicieli ryzyka,
- ma ono wyjątkowo heterogeniczną naturę.

## **2. Etapy procesu zarządzania ryzykiem operacyjnym**

W procesie zarządzania ryzykiem operacyjnym wyróżnia się 4 etapy (Krasodomska 2008: 34):

- 1) identyfikację ryzyka,
- 2) kwantyfikację (pomiar) i ocenę ryzyka,
- 3) monitorowanie (sterowanie) ryzyka,
- 4) kontrolę ryzyka.

Identyfikacja ryzyka ma na celu wskazanie obszarów występowania ryzyka i ocenę stopnia zagrożenia jego wystąpieniem. Brane są tu pod uwagę wszystkie funkcjonujące w banku obszary ryzyka zagrożone czynnikami zarówno wewnętrznymi, jak i zewnętrznymi. Jednym z narzędzi służących identyfikacji ryzyka jest mapa ryzyka.

Mapa ryzyka operacyjnego dla linii biznesowej stanowi gruntowną analizę ryzyka sporządzaną przez pionierzy operacyjne. Pozwala to na identyfikację ryzyka i rozróżnienie jego typów w banku. Biorąc pod uwagę częstotliwość występowania strat i ich dotkliwość, ryzyko można zakwalifikować do jednej z czterech klas: ryzyko powtarzalne, ryzyko do pominięcia, sytuacja kryzysowa, istotne ryzyko. Na tej podstawie określa się dalsze kroki w procesie zarządzania ryzykiem operacyjnym, które zwykle polegają na hierarchizacji ważności i istotności materialnej ryzyka. Sprawia to, że zwiększa się świadomość ryzyka, które towarzyszy działalności. Ponadto wymusza odpowiedni pomiar i zarządzanie tym ryzykiem. Proces hierarchizacji pozwala także na ujawnienie braków procedur i technik w zakresie zarządzania ryzykiem operacyjnym (Lewandowski 2004: 48–55).

Drugi etap procesu zarządzania ryzykiem to pomiar i ocena zidentyfikowanego ryzyka. Często łączy się ono z pierwszym etapem w jedną całość, określaną jako analiza ryzyka. Pozwala ona na gromadzenie niezbędnych danych do dalszego zarządzania ryzykiem operacyjnym, umożliwi bowiem wspomnianą identyfikację zagrożeń wynikających z ryzyka operacyjnego, a także oszacowanie wrażliwości banku na prawdopodobieństwo ich wystąpienia. Możliwe jest oszacowanie dotkliwości strat oraz badanie związku między zagrożeniami a kapitałem banku i zabezpieczeniami pozwalającymi na redukcję tego ryzyka (por. Krasodomska 2008: 35).

Do analizy (pomiaru) ryzyka operacyjnego można wykorzystać dwa podejścia. Pierwsze to podejście dedukcyjne, które opiera się na analizie ogólnych, makroekonomicznych czynników ryzyka. W tym wypadku badane są zjawiska takie jak: zmiany regulacji ostrożnościowych, polityki fiskalnej, polityki monetarnej, rozwoju gospodarczego i popytu na poszczególne usługi bankowe. Drugim jest podejście indukcyjne, wykorzystujące analizę szczegółowych przypadków strat w określonych sferach działalności banku, które po za-

gregowaniu pozwalają określać ekspozycję na ryzyko operacyjne. Metody stosowane w tym podejściu wymagają o wiele bardziej rozbudowanych ciągów danych historycznych do budowy modeli statystyczno-ekonometrycznych niż w podejściu dedukcyjnym (Ślązak 2007: 431–432).

Trzecim etapem zarządzania ryzykiem operacyjnym jest monitorowanie, określane czasem jako sterowanie ryzykiem. Etap ten zmierza do określenia akceptowanego poziomu ryzyka, podejmowanego w przedziale wyznaczonym przez normy prawne, regulujące działalność bankową. Istnieją dwie strategie stosowane na tym etapie: aktywna i pasywna.

W ramach strategii aktywnej mogą być podejmowane takie działania jak: unikanie ryzyka, zmniejszanie wielkości ryzyka, przenoszenie ryzyka na inne podmioty czy dywersyfikacja ryzyka zwiększająca prawdopodobieństwo, że ryzyka w określonych obszarach działalności zostaną wyrównane dodatkowymi szansami w innych obszarach. Strategia pasywna natomiast oznacza traktowanie kapitału i rezerw jako swoistego „buforu” w razie wystąpienia ryzyka nierozpoznanego lub źle ocenionego (Iwanicz-Drozdowska, Jaworski, Zawadzka 2010: 239).

Monitorowanie ryzyka pozwala na ograniczenie jego wystąpienia dzięki odpowiednio wczesnemu dostreżeniu zagrożeń i modyfikacji przyjętej strategii. Powinno ono obejmować stałą analizę bieżących parametrów, norm, miar i limitów związanych z działalnością operacyjną i podejmowanie bezzwłocznych działań w razie wystąpienia strat operacyjnych. Dane uzyskane w wyniku monitoringu powinny być przedstawione w postaci raportu kierownictwu banku, osobom uczestniczącym w zarządzaniu ryzykiem operacyjnym i komórce audytu wewnętrznego (Krasodomska 2008: 37).

Ostatnim etapem procesu zarządzania ryzykiem jest kontrola, która polega na analizie i ocenie efektywności realizowanych działań. Pozwala to na doskonalenie i rozwijanie pomiaru zdarzeń ryzyka operacyjnego oraz ograniczanie jego skutków. Ważnym aspektem tego etapu jest także weryfikacja przestrzegania przepisów i procedur wewnętrznych, odnoszących się do zarządzania ryzykiem. Decydującą rolę w tym zakresie odgrywa sprawnie funkcjonujący audyt wewnętrzny (Ślązak 2007: 432–433).

Proces zarządzania ryzykiem operacyjnym powinien być wbudowany we wszystkie transakcje i czynności bankowe. Jest konieczne, by pracownicy jednostki rozumieli ideę zarządzania tym procesem i zdawali sobie sprawę z jego istotności.

Niezmierznie ważne jest stworzenie odpowiedniej równowagi pomiędzy formalną strategią a kulturą organizacyjną banku. Z punktu widzenia ryzyka operacyjnego istotne jest zarówno komunikowanie się wewnątrz jednostki, jak i z jego otoczeniem zewnętrznym. Ponadto do ważnych elementów kultury organizacyjnej należą: przykład kierownictwa, kodeks etyczny, informowanie o celach, zrozumiałe przypisanie pracownikom określonych zasad i celów, szkolenia, określenie reguł oceny działalności, system decydowania, transfer odpowiedzialności i uprawnień na niższe szczeble (*Rekomendacja M...* 2004: 14).

### 3. Przebieg procesu zarządzania ryzykiem w banku – studium przypadku

W celu ukazania praktycznego funkcjonowania procesu zarządzania ryzykiem operacyjnym w banku przeprowadzono studium przypadku na przykładzie jednej z placówek.

Najważniejsze regulacje, dotyczące procesu zarządzania ryzykiem operacyjnym w badanej jednostce, są zawarte w: strategii zarządzania ryzykiem operacyjnym oraz instrukcji – *Zarządzanie ryzykiem operacyjnym*, która jest jej uszczegółowieniem i rozwinięciem. Re-

gulacje te są zgodne z ustaleniami Komisji Nadzoru Bankowego oraz z *Rekomendacją M. Znajomość i przestrzeganie strategii i instrukcji jest obowiązkiem wszystkich pracowników jednostki, co jest przedmiotem szczegółowych kontroli.*

Nadrzędnym celem zarządzania ryzykiem operacyjnym w podmiocie badań jest: „utrzymanie narażenia banku na ryzyko operacyjne na akceptowalnym przez zarząd i radę nadzorczą banku, bezpiecznym dla działania i rozwoju banku poziomie” (*Strategia zarządzania ryzykiem operacyjnym w podmiocie badań*).

Organizacja zarządzania ryzykiem w banku charakteryzuje się istnieniem dwóch poziomów. Pierwszy – podstawowy – obejmuje wszystkich pracowników banku. Drugi poziom, nadrzędny, jest realizowany przez zespół handlowy i obejmuje koordynację zarządzania ryzykiem operacyjnym w całej jednostce.

W podmiocie badań wyodrębniono dwa zasadnicze kierunki zarządzania ryzykiem operacyjnym. Pierwszy to działania prewencyjne, polegające na identyfikacji i monitorowaniu ryzyka prowadzonych operacji, rozpoznawaniu i zapobieganiu powstawaniu ryzyka operacyjnego w trakcie bieżącej działalności, a także na identyfikacji i ocenie ryzyka przed podjęciem decyzji związanych z wdrożeniem nowych produktów, procesów i systemów.

Drugi kierunek jest związany z osłabieniem i niwelowaniem skutków zaszłych zdarzeń operacyjnych, poprzez opracowanie procedur i sposobów reagowania pracowników banku na wypadek wystąpienia tych zdarzeń, a także poprzez przeniesienie ryzyka na inne podmioty, jeśli rozwiązanie takie jest dostępne i korzystne dla banku.

Na proces zarządzania ryzykiem operacyjnym składają się następujące cztery etapy:

Etap I: Identyfikacja i ocena ryzyka,

Etap II: Redukcja ryzyka i podejmowanie działań zabezpieczających,

Etap III: Monitorowanie i raportowanie,

Etap IV: Kontrola ryzyka operacyjnego.

W banku ryzyko jest oceniane według prawdopodobieństwa jego wystąpienia. Na tej podstawie wyróżnia się: ryzyko o małym prawdopodobieństwie wystąpienia, gdy zdarzenia danego ryzyka dotychczas nie wystąpiły i jest mało prawdopodobne, że wystąpią w najbliższej przyszłości, oraz ryzyko o średnim i dużym prawdopodobieństwie wystąpienia.

Zdarzenia ryzyka operacyjnego mogą być oceniane także z punktu widzenia strat, jakie powodują. Według tego kryterium wyróżnia się zdarzenia wywołujące potencjalne małe, o pomijalnym wpływie na wyniki banku, straty finansowe (do kwoty 10 000 zł rocznie), średnie potencjalne straty (zauważalne, ale nie krytyczne, w kwocie od 10 000 zł do 50 000 zł rocznie) oraz potencjalne duże straty finansowe, w znaczny sposób rzutujące na jego wyniki (o wysokości przekraczającej 50 000 zł w skali roku).

W praktyce stosowana jest łączna skala oceny ryzyka, określana według wzoru:

$$\text{wielkość ryzyka} = \text{prawdopodobieństwo wystąpienia ryzyka} \times \text{siła wpływu},$$

gdzie: siła wpływu – wypadkowa straty jednostkowej oraz wielkości ekspozycji narażonej na ryzyko w skali roku (np. liczba operacji, liczba klientów).

W zależności od oszacowanej wielkości ryzyka kwalifikuje się je do odpowiedniej kategorii ryzyka:

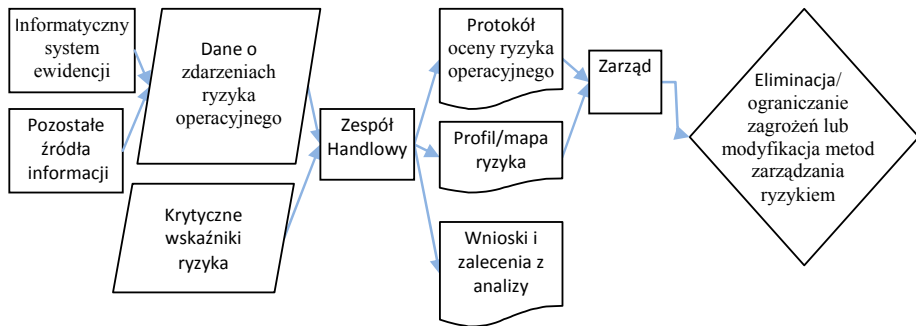
I. Ryzyko na poziomie akceptowalnym o oszacowanej wielkości w zakresie od 1 do 2,

II. Ryzyko o podwyższonym poziomie o wielkości od 3 do 4,

III. Ryzyko na wysokim poziomie – wielkość od 6 do 9.

Pierwszy etap procesu zarządzania ryzykiem w podmiocie badań polega na identyfikacji i ocenie ryzyka, która opiera się na dwóch mechanizmach: okresowych przeglądach ryzyka operacyjnego oraz jednorazowych przeglądach ryzyka, dotyczących nowych produktów, procesów i systemów.

Okresowe przeglądy ryzyka są wykonywane przez zespół handlowy. Ich celem jest weryfikacja profilu ryzyka operacyjnego banku przez identyfikację i ocenę nowych rodzajów ryzyka oraz ocenę zmian w zakresie wcześniej zidentyfikowanego ryzyka. Poszczególne etapy tego procesu zilustrowano na rysunku 1.



**Rysunek 1.** Etapy przebiegu okresowego przeglądu ryzyka w banku

Źródło: opracowanie własne na podstawie instrukcji *Zarządzanie ryzykiem operacyjnym* w podmiocie badań.

Okresowa analiza ryzyka polega na ocenie zbieranych w ciągu kwartału sprawozdawczego danych dotyczących zdarzeń ryzyka operacyjnego oraz dodatkowych informacji wewnętrznych i zewnętrznych. W ramach okresowych przeglądów bada się również wpływ krytycznych wskaźników ryzyka z zachowaniem podziału na 4 kategorie: ludzie, procesy, systemy, zdarzenia zewnętrzne, co pozwala na określenie z wyprzedzeniem zmian profilu ryzyka. Przykładowe<sup>1</sup> dane w tym zakresie przedstawiono w tabeli 2.

Na podstawie przeprowadzonej analizy jest tworzony protokół oceny ryzyka operacyjnego, a także modyfikowany jest jego profil/mapa. Zespół handlowy na podstawie wyników analizy formułuje wnioski i zalecenia. Następnie, w ciągu 20 dni od zakończenia kwartału sprawozdawczego, protokół i mapa ryzyka są przekazywane zarządowi, który w razie potrzeby podejmuje decyzje mające na celu eliminację lub ograniczenie zidentyfikowanych zagrożeń lub modyfikację stosowanych metod zarządzania ryzykiem.

Poza okresowymi przeglądami w podmiocie badań są prowadzone także przeglądy jednorazowe, które mają na celu identyfikację i ocenę zagrożeń związanych z wdrożeniem nowych produktów, procesów i systemów. Ponadto mają służyć zwiększeniu świadomości występowania ryzyka wśród pracowników zaangażowanych w ich wdrożenie, a także opracowaniu działań zapobiegających bądź zmniejszających negatywne skutki wprowadzenia nowych rozwiązań. Na rysunku 2 zilustrowano etapy przeglądu jednorazowego.

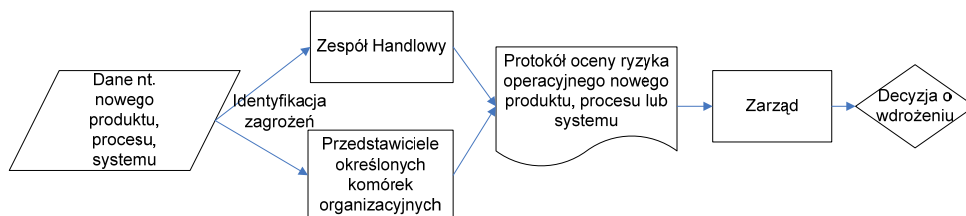
<sup>1</sup> Z uwagi na ramy objętościowe niniejszego opracowania przedstawiono jedynie przykładowe krytyczne wskaźniki ryzyka.

Tabela 2

Krytyczne wskaźniki ryzyka operacyjnego w banku

Czynniki ryzyka	Krytyczne wskaźniki ryzyka
<b>Ludzie</b>	<ul style="list-style-type: none"> <li>– liczba pracowników,</li> <li>– liczba skarg na stosunki pracownicze,</li> <li>– liczba reklamacji związanych z kulturą i jakością obsługi klientów,</li> <li>– liczba godzin nadliczbowych,</li> <li>– liczba godzin szkoleń</li> </ul>
<b>Procesy</b>	<ul style="list-style-type: none"> <li>– liczba prowadzonych rachunków,</li> <li>– liczba nowych klientów banku,</li> <li>– liczba klientów,</li> <li>– liczba rachunków,</li> <li>– liczba błędów księgowych,</li> <li>– oszustwo czekowe</li> </ul>
<b>Systemy</b>	<ul style="list-style-type: none"> <li>– wolumen transakcji,</li> <li>– liczba użytkowników systemu bankowego,</li> <li>– liczba zdefiniowanych użytkowników w poszczególnych kanałach bankowości elektronicznej,</li> <li>– liczba bankomatów i POS-ów,</li> <li>– czas niedostępności systemu transakcyjnego</li> </ul>
<b>Zdarzenia zewnętrzne</b>	<ul style="list-style-type: none"> <li>– liczba nieautoryzowanych prób dostępu do systemów bankowości elektronicznej,</li> <li>– liczba aktów wandalizmu,</li> <li>– liczba wykrytych włamań do systemu spoza banku,</li> <li>– czas niedostępności usług dostawcy zewnętrznego</li> </ul>

Źródło: opracowanie własne na podstawie instrukcji *Zarządzanie ryzykiem operacyjnym* w podmiocie badań.



**Rysunek 2.** Przebieg przeglądu jednorazowego ryzyka operacyjnego w banku

Źródło: opracowanie własne na podstawie instrukcji *Zarządzanie ryzykiem operacyjnym* w podmiocie badań.

W przeglądach jednorazowych uczestniczy zespół handlowy i przedstawiciele komórek zaangażowanych we wdrożenie lub będących przyszłymi użytkownikami nowego produktu, procesu lub systemu. W pierwszym etapie uczestnicy przeglądu identyfikują i oceniają możliwości wystąpienia zagrożeń. Na tej podstawie jest spisywany protokół oceny ryzyka operacyjnego nowego produktu, procesu lub systemu.

W protokole, oprócz identyfikacji potencjalnych zagrożeń, jest określone prawdopodobieństwo ich wystąpienia, ich wpływ na działanie banku, a także sformułowane są odpowiednie wnioski i zalecenia. Przygotowany protokół jest przekazywany do akceptacji zarządu, który na jego podstawie decyduje o wdrożeniu nowego produktu, systemu lub procesu.



Uczestnicy przeglądu jednorazowego identyfikują i oceniają możliwość wystąpienia zagrożeń związanych z nowym produktem, procesem lub systemem, wykorzystując do tego metodę ekspercką. Przykładowe rodzaje zagrożeń przedstawiono w tabeli 3.

**Tabela 3**

Rodzaje zagrożeń oceniane w przeglądzie jednorazowym

Kategoria	Rodzaj zagrożenia
<b>Ludzie</b>	<ul style="list-style-type: none"> <li>– brak potrzebnych do wdrożenia pracowników,</li> <li>– brak potrzebnych kwalifikacji osób zaangażowanych we wdrożenie,</li> <li>– możliwość negatywnego wpływu nowych czynników wynagradzania na efektywność pracy,</li> <li>– możliwości pogorszenia stosunków między pracownikami</li> </ul>
<b>Istotność i złożoność procesu lub systemu</b>	<ul style="list-style-type: none"> <li>– duża ilość obszarów banku obejmowanych procesem lub systemem,</li> <li>– możliwość wystąpienia strat finansowych w razie niepowodzenia,</li> <li>– możliwość niutrzymania odpowiedniej kontroli nad procesem lub systemem</li> </ul>
<b>Systemy teleinformatyczne</b>	<ul style="list-style-type: none"> <li>– brak odpowiedniego stopnia przygotowania do realizacji nowego produktu, procesu, systemu ze strony systemu informatycznego,</li> <li>– możliwość naruszenia bezpieczeństwa informatycznego i informacyjnego</li> </ul>
<b>Dokumentacja wewnętrzna</b>	<ul style="list-style-type: none"> <li>– brak dostosowania odpowiednich regulacji wewnętrznych,</li> <li>– konieczność zachowania wysokiej jakości dokumentacji,</li> <li>– potrzeba wysokiej dostępności i zachowania aktualności dokumentacji,</li> <li>– brak znajomości odpowiedniej dokumentacji wśród pracowników</li> </ul>
<b>Dokumentacja zewnętrzna</b>	<ul style="list-style-type: none"> <li>– sposób publikowania dokumentacji – formy, miejsc, terminów,</li> <li>– jednakowe zrozumienie przez strony definicji oraz wyrażen w umowach,</li> <li>– wynikające z potrzeby akceptacji dokumentów, np. uzyskania podpisu klienta lub potwierdzenia transakcji przez kontrahenta</li> </ul>
<b>Zdarzenia zewnętrzne</b>	<ul style="list-style-type: none"> <li>– negatywny wpływ sytuacji podmiotów zewnętrznych i podwykonawców na realizowany produkt, proces, system,</li> <li>– potencjalne przyszłe zmiany prawne,</li> <li>– możliwość wystąpienia awarii zewnętrznej, aktu wandalizmu, katastrofy</li> </ul>

Źródło: opracowanie własne na podstawie instrukcji *Zarządzanie ryzykiem operacyjnym* w podmiocie badań.

Redukcja ryzyka oraz podejmowanie działań zabezpieczających są drugim etapem procesu zarządzania ryzykiem operacyjnym w badanej jednostce. Podstawowymi działaniami, będącymi jednocześnie metodami redukcji ryzyka na poziomie akceptowalnym, są:

- kontrola wewnętrzna funkcjonalna,
- stosowanie odpowiednich procedur dokonywania operacji, a także limitów w zakresie podejmowania decyzji, w celu ograniczenia strat mogących powstać w wyniku błędów popełnionych przez człowieka,
- szkolenia pracowników, warunkujące prawidłowe wykonywanie operacji, uświadomienie istnienia ryzyka operacyjnego i sposobów ograniczania jego wpływu,
- przekazywanie informacji na temat istotnych zdarzeń ryzyka operacyjnego na bieżąco, w celu zapobiegania rozprzestrzenianiu się ryzyka i ograniczenia jego wpływu,
- nieustanne monitorowanie zdarzeń ryzyka operacyjnego, gromadzenie informacji dotyczących ryzyka i ich okresowa analiza,
- okresowe raportowanie na temat poziomu ryzyka i obszarów szczególnie narażonych na ryzyko.

W wypadku identyfikacji zdarzeń mogących istotnie wpłynąć na wyniki banku lub jego bezpieczeństwo, a także w odniesieniu do obszarów kluczowych z punktu widzenia ryzyka,

podejmowane są natomiast dodatkowe działania zapobiegawcze. Czynności te są również wykorzystywane jako metody redukcji ryzyka o podwyższonym poziomie. Należą do nich:

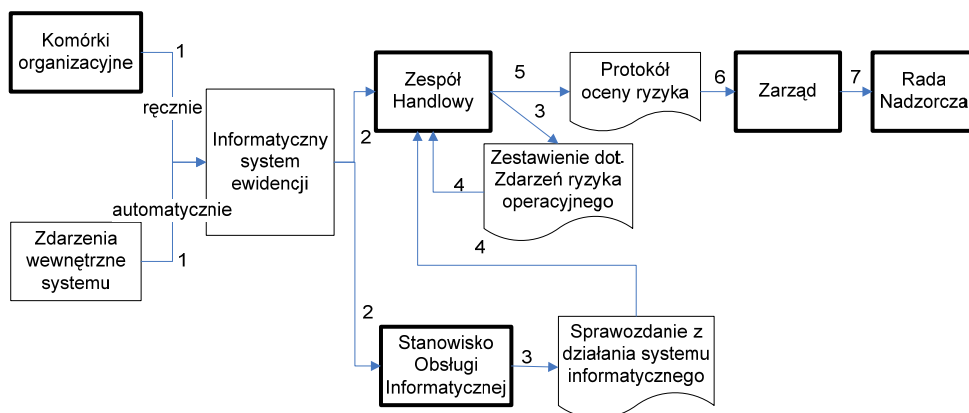
- opracowanie i wdrożenie odpowiednich planów awaryjnych lub planów utrzymania ciągłości działania,
- automatyzacja wykonywanych czynności, służąca zapobieganiu lub wychwytywaniu zdarzeń ryzyka,
- ubezpieczenia mienia w wyspecjalizowanych firmach,
- tworzenie rezerw na poczet ewentualnych strat,
- zlecenie wykonywania działań wyspecjalizowanemu podmiotowi,
- dokonywanie zapisów w umowach z dostawcami lub partnerami, ograniczających ryzyko i dających bankowi możliwość uzyskania odszkodowania w przypadku niewywiązania się z umowy przez drugą stronę,
- zwiększenie zakresu i częstotliwości kontroli lub monitorowania danego obszaru.

W razie wysokiego poziomu ryzyka należy niezwłocznie podjąć dodatkową ochronę, obejmującą działania rekomendowane dla ryzyka o podwyższonym poziomie, lub też podjąć działania zmierzające do rezygnacji z procesu lub zasobu, z którym wiąże się to ryzyko. W wypadku wystąpienia ryzyka operacyjnego należy je zgłosić przełożonemu, który odpowiada za podjęcie działań zapobiegających powiększaniu się strat i likwidujących przyczyny zdarzeń. Ponadto oszacowuje on wielkość straty i nadzoruje zarejestrowanie zdarzenia przez pracownika, który zgłosił zdarzenie. Jeżeli jest ono istotne, osoba dokonująca rejestracji musi o zaistniałym fakcie powiadomić także członka zarządu, który z kolei powiadamia prezesa i sporządza notatkę służbową na temat tego zdarzenia. Prezes banku zwołuje posiedzenie zarządu, na którym przeprowadza się analizę przyczyn zdarzenia, a także opracowuje wnioski i zalecenia mające na celu uniknięcie podobnych zdarzeń w przyszłości.

Kolejnym krokiem w procesie zarządzania ryzykiem operacyjnym w jednostce jest monitorowanie i raportowanie. Wystąpienie bowiem jakiegokolwiek ryzyka operacyjnego wymaga monitoringu przez wyznaczoną komórkę organizacyjną. Zebrane w ten sposób dane służą do cyklicznej analizy i identyfikacji zagrożeń. Na potrzeby monitorowania ryzyka operacyjnego w banku wyróżniono dwie kategorie zdarzeń. Pierwszą z nich są „zdarzenia istotne”, które prowadzą do wystąpienia szacunkowej straty finansowej na poziomie co najmniej 10 000 zł lub do przerwy w obsłudze klientów przez co najmniej 8 godzin. Zdarzenia takie będą przedmiotem wnikliwej analizy zarządu. Wszystkie inne zdarzenia występujące w działalności banku i mające wpływ na możliwość wystąpienia ryzyka w jednostce zalicza się do drugiej kategorii o nazwie „pozostałe zdarzenia”.

Poza cyklicznym raportowaniem występuje także okresowe ryzyko raportowania operacyjnego, które przebiega w porządku zaprezentowanym na rysunku 3. Wyznaczone stanowiska komórek organizacyjnych wprowadzają informacje o wystąpieniu określonych zdarzeń do systemu informatycznego, zaś zdarzenia wewnętrzne systemu są ewidencjonowane automatycznie. Na podstawie informacji wprowadzonych do systemu pracownik zespołu handlowego generuje zestawienie dotyczące zjawisk ryzyka operacyjnego, a informatyk sporządza sprawozdanie z działania systemu informatycznego w terminie 5 dni od zakończenia każdego kwartału sprawozdawczego. Zestawienie i sprawozdanie są następnie przetwarzane przez pracownika zespołu handlowego i po uzupełnieniu o inne istotne informacje umożliwiają dokonanie przez niego oceny wykonania limitów, opracowanie wniosków i zaleceń oraz aktualizację profilu ryzyka operacyjnego. W ten sposób powstaje protokół oceny ryzyka, który w terminie 20 dni od zakończenia kwartału sprawozdawczego jest

przekazywany zarządowi, który na tej podstawie przedkłada radzie nadzorczej, w okresach kwartalnych, syntetyczną informację o skali i rodzajach ryzyka operacyjnego, na które jest narażony bank, a także na temat prawdopodobieństwa i spodziewanych skutków wystąpienia ryzyka operacyjnego oraz metod zarządzania nim.



**Rysunek 3.** Przebieg okresowego raportowania w procesie zarządzania ryzykiem operacyjnym w banku

Źródło: opracowanie własne na podstawie instrukcji *Zarządzanie ryzykiem operacyjnym* w podmiocie badań.

W ramach etapu monitorowania i raportowania badane jest także przestrzeganie globalnego limitu strat. Jego wysokość wynosi 15% wymogu kapitałowego<sup>2</sup> na ryzyko operacyjne. Wykonanie limitu jest badane przez zespół handlowy w układzie kwartalnym.

Ostatnim etapem zarządzania ryzykiem operacyjnym w badanej jednostce jest kontrola ryzyka operacyjnego, która polega na weryfikacji poprawności i skuteczności funkcjonowania zarządzania ryzykiem operacyjnym oraz kontroli zgodności przyjętych zasad z profilem ryzyka banku. Ten etap jest przeprowadzany przez kontrolę wewnętrzną, która nie jest wyodrębniona w strukturze banku, lecz wydelegowana przez bank zrzeszający. Wyniki i wnioski z kontroli są przedstawiane prezesowi zarządu, a następnie zarządowi i radzie nadzorczej.

<sup>2</sup> Wymóg kapitałowy informuje o kwocie, jaką bank musi przeznaczyć na pokrycie potencjalnych strat z tytułu ryzyka operacyjnego. W podmiocie badań oblicza się go, stosując metodę podstawowego wyznacznika, zgodnie z poniższym wzorem:

$$K_{BIA} = \frac{\sum_{i=1}^3 GI_i}{n} \cdot \alpha,$$

gdzie:  $K_{BIA}$  – wymóg kapitałowy z tytułu ryzyka operacyjnego,  $GI$  – roczny wynik brutto w roku  $i$ , jeśli jest dodatni,  $n$  – liczba lat, w których wynik brutto był dodatni, w okresie ostatnich trzech lat,  $\alpha$  – 15%.

## Uwagi końcowe

Zarządzanie ryzykiem operacyjnym w banku jest ważną częścią działalności podstawowej, a nierzadko głównym źródłem jego zysków. Właściwie przeprowadzony proces jest czynnikiem istotnie decydującym o tym, czy dany bank odniesie sukces, czy też nie. Aby to osiągnąć, należy starannie opracować proces zarządzania ryzykiem operacyjnym, określając metody, techniki i zasady zarządzania ryzykiem.

Należy jednak podkreślić, iż nawet dokładnie przygotowany proces nie zakończy się sukcesem bez odpowiedniego nastawienia personelu banku, bowiem jakość procesu zarządzania ryzykiem operacyjnym jest zależna nie tylko od wąskiego grona kierownictwa jednostki, ale też od podejścia wszystkich pracowników do tej kategorii ryzyka. Dlatego ważne jest, aby byli oni odpowiednio motywowani i szkoleni w zakresie kategorii ryzyka, dzięki czemu zwiększy się efektywność procesu zarządzania nim, a tym samym wzrośnie wartość rynkowa banku.

## Literatura

- Iwanicz-Drozdowska M., Jaworski W.L., Zawadzka Z. (2010), *Bankowość: zagadnienia podstawowe*, Poltext, Warszawa.
- Kałużny R. (2004), *Strzegąc swego banku*, „Bank”, nr 3.
- Krasodomska J. (2008), *Zarządzanie ryzykiem operacyjnym w bankach*, Polskie Wydawnictwo Ekonomiczne, Warszawa.
- Lewandowski D. (2004), *Ryzyko operacyjne w bankach – zarządzanie i audyt w świetle wymagań Bazylejskiego Komitetu ds. Nadzoru Bankowego*, „Bank i Kredyt”, nr 4.
- Rekomendacja M dotycząca zarządzania ryzykiem operacyjnym w bankach* (2004), Komisja Nadzoru Bankowego, Warszawa.
- Ślązak E. (2007), *Ryzyko operacyjne*, w: *Współczesna bankowość*, red. M. Zaleska, Difin, Warszawa.
- Zarządzanie ryzykiem w sektorze publicznym. Podręcznik wdrożenia systemu zarządzania ryzykiem administracji publicznej w Polsce*, Ministerstwo Finansów, www.mf.gov.pl.

### OPERATIONAL RISK MANAGEMENT PROCESS IN BANK-CASE STUDY

**Abstract: Purpose** – The main aim of this article was to present theoretical aspects of operational risk management process in banks as well as showing the practical example of this issue.

**Design/Methodology/approach** – To achieve purpose of this article there was used analyze of the literature of banking area and risk management area as well as there was shown case study of risk management process.

**Findings** – This article has been devoted to issues of operational risk management process in bank, using the example of bank unit. The paper describes phases of the operational risk management process and presents methods of a risk analysis used by object of researches.

**Originality/value** – The article is a practical presentation of operational risk management process.

**Keywords:** risk, risk management, operational risk, bank

## Cytowanie

- Bartoszewicz A. (2014), *Proces zarządzania ryzykiem operacyjnym w banku – studium przypadku*, Zeszyty Naukowe Uniwersytetu Szczecińskiego nr 833, „Finanse, Rynki Finansowe, Ubezpieczenia” nr 72, Szczecin, s. 33–44, www.wneiz.pl/frfu.