Zeszyty Naukowe Uniwersytet Ekonomiczny w Krakowie

5(929)

ISSN 1898-6447
Zesz. Nauk. UEK, 2014; 5(929): 41–56
DOI: 10.15678/ZNUEK.2014.0929.0503

Michał Thlon
Katedra Teorii Ekonomii
Uniwersytet Ekonomiczny w Krakowie

Kluczowe wskaźniki ryzyka w procesie zarządzania w warunkach ryzyka operacyjnego w banku

Streszczenie

Ryzyko operacyjne definiowane jest jako możliwość poniesienia strat na skutek stosowania wadliwych systemów, niepoprawnych procedur, błędów popełnianych przez ludzi, awarii technicznych oraz zdarzeń zewnętrznych. Metody pomiaru ryzyka operacyjnego są odmienne od technik mających zastosowanie do innych rodzajów ryzyka. Specyfika ryzyka operacyjnego oraz trudny do oszacowania wpływ na poziom osiąganego dochodu znacznie komplikują pomiar jego poziomu. W związku z tym w szacowaniu poziomu ryzyka operacyjnego pojawia się tendencja do całościowego podejścia do zarządzania ryzykiem operacyjnym rozumianego jako połączenie jakościowego szacowania ryzyka, podejścia ilościowego oraz wykorzystania kluczowych wskaźników ryzyka (KRI). Głównym celem artykułu jest analiza najważniejszych aspektów związanych z wykorzystaniem KRI w procesie zarządzania ryzykiem operacyjnym. Przyjętemu celowi podporządkowana została struktura artykułu. Kolejno przeanalizowano definicję, charakterystykę, zastosowania oraz sposoby kwantyfikacji KRI.

Słowa kluczowe: ryzyko, ryzyko operacyjne, metody pomiaru ryzyka, kluczowe wskaźniki ryzyka KRI.

1. Wstęp

Zagadnienia związane z ryzykiem operacyjnym zaczęły przyciągać uwagę przedstawicieli świata finansów i ekonomii po upadku banku Barings w 1995 r. [Cruz 2002, s. 1]. Od tego czasu można zaobserwować znaczny wzrost zainteresowania tym rodzajem ryzyka.

Głównym celem publikacji jest analiza najważniejszych aspektów związanych z wykorzystaniem kluczowych wskaźników ryzyka (KRI) w procesie zarządzania ryzykiem operacyjnym. Wskaźniki te są miarą wrażliwości instytucji na zagrożenia związane z analizowanym rodzajem ryzyka [Jamson 2002, s. 4]. KRI występują w postaci statystyk odzwierciedlających dane empiryczne z poszczególnych okresów. Służą do monitorowania ekspozycji na ryzyko i – co najistotniejsze – umożliwiają podjęcie działań wyprzedzających, szczególnie chroniących przed najbardziej dotkliwymi zdarzeniami operacyjnymi.

2. Definicja ryzyka operacyjnego

Różnorodność definicji ryzyka operacyjnego jest ograniczona przez dwa skrajne ujęcia. Pierwszym z nich jest bardzo wąska definicja ryzyka operacyjnego. Zgodnie z tą koncepcją ryzyko operacyjne definiowane jest jako zaburzenia działalności operacyjnej firmy spowodowane czynnikami wewnętrznymi [Marshall 2001, s. 25]. Przeciwnym biegunem jest definicja określająca ryzyko operacyjne jako każdy rodzaj ryzyka niezaliczany do ryzyka rynkowego lub kredytowego [Goodhart 2001, s. 4]. Pierwsze z tych podejść ułatwia oszacowanie ryzyka, ale pomija ważne jego aspekty (np. związane z wpływem zdarzeń zewnętrznych). Druga – negatywna – definicja jest natomiast niejednoznaczna, co powoduje trudności w identyfikacji ryzyka. Definicja ta może być przydatna do szacowania ryzyka w kontekście alokacji kapitału [Allen i Bali 2004, s. 15].

Z uwagi na niedoskonałości skrajnych ujęć większość autorów definiuje ryzyko operacyjne w obszarze pomiędzy tymi biegunami [Marshall 2001, s. 25]. Bazylejski Komitet ds. Nadzoru Bankowego traktuje ryzyko operacyjne jako możliwość poniesienia strat na skutek stosowania niewystarczających lub wadliwych systemów, niepoprawnych procedur i metod działania, błędów popełnianych przez ludzi, awarii technicznych oraz zdarzeń zewnętrznych [Jorion 2007, s. 553]. Zgodnie z tą koncepcją wyróżnić można następujące kategorie czynników ryzyka:

– procesy – kategoria strat poniesionych w wyniku błędów w przyjętych procedurach, niedostatecznej liczby istniejących procedur lub ich braku. Straty z tej kategorii nie są skutkiem celowych działań. Mogą być następstwem ludzkich błędów lub postępowania niezgodnego z obowiązującymi procedurami;

– ludzie – źródłem tego rodzaju ryzyka są celowe lub niezamierzone działania byłych lub obecnych pracowników na szkodę pracodawcy [Bourque 2003, s. 5];

– systemy – kategoria ta odnosi się do strat poniesionych w wyniku awarii systemów telekomunikacyjnych i informatycznych, w tym także oprogramowania. Straty z tej kategorii nie są skutkiem celowych działań [Harmantzis 2004, s. 3];

– zdarzenia zewnętrzne – kategoria ta obejmuje straty zaistniałe w wyniku oddziaływania na instytucje czynników zewnętrznych.

Tabela 1 zawiera wyszczególnienie rodzajów ryzyka w kontekście przytoczonej definicji.

Tabela 1. Kategorie ryzyka operacyjnego

Rodzaje ryzyka	Definicja strat
Oszustwo wewnętrzne	spowodowane przez osoby pochodzące z danej instytucji; są one następstwem kradzieży, przywłaszczenia lub też omijania przepisów
Oszustwo zewnętrzne	wywołane przez osoby trzecie; są następstwem kradzieży, przywłaszczenia lub też omijania przepisów
Praktyka kadrowa i bezpieczeństwo pracy	spowodowane działaniami niezgodnymi z przepisami (prawem pracy, przepisami BHP), żądaniami odszkodowań za wypadki w miejscu pracy lub wszelkiego rodzaju działaniami dyskryminacyjnymi
Klienci, produkty i działalność biznesowa	spowodowane nieumyślnie lub z powodu zaniedbań w zakresie zobowiązań w stosunku do określonych klientów albo wynikłe z konstrukcji produktów
Uszkodzenia aktywów	wynikłe z uszkodzenia bądź zniszczenia aktywów rzeczowych w wyniku katastrof naturalnych lub innych wydarzeń
Zakłócenia działalności i błędy systemów	będące następstwem zakłócenia działalności i błędów systemu
Dokonywanie transakcji, dostawa oraz zarządzanie procesami	powstałe w wyniku błędnego przeprowadzenia transakcji bądź błędnego zarządzania procesem albo też będące następstwem relacji z podmiotami biorącymi udział w transakcji lub dostawcami

Źródło: opracowanie własne na podstawie [BCBS 2004, s. 224–225].

Odmienną definicję omawianego rodzaju ryzyka przedstawia J. King. Jego zdaniem ryzyko operacyjne jest zagrożeniem wystąpienia niekorzystnych odchyleń od zakładanego wyniku działalności firmy w kontekście jej działalności operacyjnej [King 2001, s. 7].

Przytoczone definicje mają charakter teoretyczny i stanowią podstawę do tworzenia indywidualnych definicji ryzyka operacyjnego dostosowanych do specyfiki działalności poszczególnych instytucji. Tabela 2 zawiera kilka wybranych definicji ryzyka operacyjnego funkcjonujących w praktyce. Przytoczone definicje zostały wybrane w ten sposób, by zaprezentować różnorodne ujęcia

ryzyka operacyjnego. Warto zwrócić uwagę na dużą różnorodność przyjętego ujęcia – część firm przyjęła wąską definicję ryzyka zgodną z zaleceniami Komitetu Bazylejskiego, inne rozszerzyły ją np. o ryzyko utraty reputacji czy franchisingowe.

Tabela 2. Definicje ryzyka operacyjnego w dużych instytucjach międzynarodowych

Instytucja	Definicje ryzyka operacyjnego
Bank of America	Potencjalne straty będące wynikiem działania ludzi, procesów, wadliwych technologii, kwestii prawnych, zdarzeń zewnętrznych, interwencji nadzoru, a także utraty reputacji
Citigroup	Ryzyko straty będącej wynikiem nieadekwatnych lub wadliwych procesów, działania ludzi, systemów oraz zdarzeń zewnętrznych. Według tej definicji do ryzyka operacyjnego zalicza się także ryzyko utraty reputacji oraz ryzyko franchisingowe
Deutsche Bank	Potencjalne straty wynikające z relacji z pracownikami, zarządzania projektami, błędów w dokumentacji i umowach z kontrahentami, awarii infrastruktury, katastrof, działalności osób trzecich i relacji z klientami. Według tej definicji ryzyko operacyjne obejmuje również ryzyko prawne i regulacyjne
Goldman Sachs	Ryzyko utraty reputacji, interwencji nadzoru lub finansowe konsekwencje nieadekwatnych lub wadliwych systemów i procesów. Straty operacyjne mogą mieć przyczynę w mechanicznych i technologicznych wadach systemów lub infrastruktury zachodzących w czasie zwykłej działalności biznesowej oraz na skutek zdarzeń nadzwyczajnych, zarówno wewnętrznych, jak i zewnętrznych
HSBC	Ryzyko straty wynikającej z oszustwa, działalności bez upoważnienia, błędu, zaniedbania, nieefektywności, awarii systemów lub zdarzeń zewnętrznych
JP Morgan Chase	Ryzyko straty będącej wynikiem nieadekwatnych albo niewłaściwych procesów, systemów, czynnika ludzkiego lub zdarzeń zewnętrznych
Lloyd TSB	Ryzyko operacyjne zdefiniowane jest według wersji przyjętej przez Komitet Bazylejski z uwzględnieniem ryzyka utraty reputacji
Morgan Stanley	Ryzyko straty spowodowanej niewłaściwym lub nieautoryzowanym rozliczeniem i wykonaniem transakcji, awariami systemów informatycznych zarówno wewnętrznych, jak i zewnętrznych, nieadekwatnością lub wadliwością systemów kontrolnych. Definicja ta włącza do ryzyka operacyjnego ryzyko utraty reputacji i ryzyko regulacyjne
Swiss Re	W skład ryzyka operacyjnego wchodzą: ryzyko aktywów materialnych, ryzyko technologiczne, ryzyko związane z relacjami z otoczeniem, ryzyko kadrowe

Źródło: opracowanie własne na podstawie [Corporate Governance Survey 2003, s. 20] i [Jajuga i Jakóbczak 2004].

Jeżeli przyjrzymy się uważnie przytoczonym definicjom, okaże się, że obejmują one bardzo szerokie spektrum ryzyka i uwzględniają takie przypadki, jak oszustwo (które można odnieść to nieadekwatnych systemów i kontroli), ryzyko

regulacyjne (zarówno wadliwe systemy, jak i niewłaściwe zarządzanie), a także inne rodzaje ryzyka, od powodujących bezpośrednie straty klęsk żywiołowych po błędy administracyjne, których źródłem jest brak odpowiednio wykwalifikowanego personelu. Ryzyko operacyjne jest specyficznym rodzajem ryzyka występującym we wszystkich podmiotach działających na rynku.

Na podstawie analizy zaprezentowanych definicji można wysnuć wniosek o trójwymiarowym charakterze ryzyka operacyjnego. W pierwszym wymiarze ryzyko traktowane jest jako oczekiwane straty, które wynikają ze zdarzeń przewidzianych przez instytucje. Straty te stanowią wartość oczekiwaną rozkładu prawdopodobieństwa zagregowanych strat. Drugi wymiar ryzyka stanowią straty nieoczekiwane, najczęściej reprezentowane przez odchylenia standardowe rozkładu lub ich wielokrotność. Ostatnią płaszczyzną ryzyka operacyjnego są straty katastroficzne. Choć częstotliwość występowania zdarzeń powodujących takie straty jest niska, ich wpływ może zagrozić istnieniu podmiotu [Strupczewski 2008, s. 414]. Wielopłaszczyznowa natura ryzyka operacyjnego oraz trudny do oszacowania wpływ na osiągany dochód znacznie komplikują systematyczny i konsekwentny pomiar jego poziomu. W związku z tym w celu jak najbardziej precyzyjnego oszacowania poziomu ryzyka operacyjnego w praktyce gospodarczej pojawia się coraz silniejsza tendencja do całościowego podejścia do zarządzania ryzykiem operacyjnym, rozumianego jako połączenie jakościowego szacowania ryzyka, podejścia ilościowego określającego probabilistyczne miary ryzyka oraz wykorzystania KRI [Orzeł 2005, s. 7].

3. Kluczowe wskaźniki ryzyka

Kluczowe wskaźniki ryzyka definiowane są jako zestaw parametrów, które z dużym prawdopodobieństwem odzwierciedlają zmiany profilu ryzyka operacyjnego[1] tego procesu [Orzeł 2005, s. 4]. Wskaźniki KRI mają wszechstronne zastosowanie w szacowaniu ryzyka operacyjnego. Wykorzystywane są m.in. do określenia profilu ryzyka operacyjnego w metodologii OpVaR [Scandizzo 2005, s. 253]. Wskaźniki te występują w postaci statystyk odzwierciedlających dane empiryczne z poszczególnych okresów. KRI są ważnym narzędziem wykorzystywanym w procesie zarządzania ryzykiem operacyjnym, ułatwiającym monitorowanie i kontrolę ryzyka. Miara ta może być postrzegana jako wskaźnik ryzyka, jeżeli można jej używać do pomiaru następujących elementów:

[1] Profil ryzyka operacyjnego definiowany jest jako skala i struktura narażenia na ryzyko operacyjne. Ustalenie profilu ryzyka w bankowości dokonywane jest z wykorzystaniem m.in. posiadanych informacji na temat zdarzeń operacyjnych (w tym dotyczących ich częstości i dotkliwości) oraz informacji pochodzących z wykorzystywanych narzędzi zarządzania ryzykiem operacyjnym.

– wielkość narażenia na ryzyko (*risk exposure indicators*),

– efektywność kontroli przeprowadzanych w celu redukcji narażenia na ryzyko (*control effectiveness indicators*),

– efektywność zarządzania ryzykiem i skuteczność ustalonych schematów działania (*performance indicators*) [IOR 2010, s. 1].

Charakterystyki poszczególnych grup wskaźników zostały zaprezentowane w tabeli 3. Statystyki te w głównej mierze odzwierciedlają finansową stronę działalności organizacji. Głównymi technikami statystycznymi służącymi do analizy tego typu danych są analizy dyskryminacyjne oraz logitowe i probitowe [Sanyal 2005, s. 37].

Tabela 3. Charakterystyka wskaźników ryzyka

Grupa wskaźników	Wskaźniki narażenia na ryzyko	Wskaźnik efektywności kontroli	Wskaźnik efektywności zarządzania ryzykiem
Charakterystyka	Dostarczają informacji o wielkościach zagrożonych ryzykiem operacyjnym, występujących w danym czasie. Aby zapewnić te informacje, wskaźnik ryzyka musi wyraźnie odzwierciedlać zagrożenie związane z daną wielkością, np. liczba skarg konsumenckich – powiązanych z błędami procesowymi. Zmiany w wartościach tych wskaźników będą wpływały na stopień narażenia na ryzyko operacyjne, a w konsekwencji na ewentualną stratę operacyjną. Inne przykłady tych wskaźników to: rotacja pracowników, liczba błędów, wirusów czy ataków hakerskich	Dostarczają informacji o zakresie, w jakim przeprowadzana kontrola osiąga założone cele, jak np. zapobieganie stratom. Przykładowymi wskaźnikami tej kategorii są: liczba wykrytych przypadków pomyłek w identyfikacji klientów, co może oznaczać braki w kontroli bezpieczeństwa danych; liczba nieuprawnionych wejść do sieci firmy w danym okresie, które wskazują na słabość kontroli bezpieczeństwa systemów	Mierzą wyniki i stopień osiągnięcia celu. Najczęściej są rozpatrywane w aspekcie finansowym i księgowym, są też odpowiednie do oceny zarządzania ryzykiem operacyjnym w odniesieniu do oceny osiągnięcia celów takich jak zmniejszenie narażenia na ryzyko. Przykładem wskaźnika tej kategorii jest liczba godzin przestoju systemu IT, procent produktów lub transakcji, które zawierają błędy

Źródło: opracowanie własne na podstawie [IOR 2010, s. 1–2].

Ważną kwestią jest regularne omawianie KRI z osobami odpowiedzialnymi za obszar działalności, który wskaźniki mają identyfikować. Zapewni to aktualność wskaźników oraz bieżące informacje na temat możliwych zmian w ich strukturze.

Kryteria prawidłowego doboru KRI zaprezentowane zostały w tabeli 4. Prawidłowo przeprowadzony dobór wskaźników powinien zapewniać menadżerom obiektywne sygnały dotyczące zdarzeń, które mogą zakłócić działalność firmy, zanim sytuacja stanie się krytyczna [Rowe 2003, s. 47]. Warunkiem koniecznym skuteczności systemu zarządzania ryzykiem operacyjnym wykorzystującego KRI jest właściwa konstrukcja samego wskaźnika. Z uwagi na nieodłączny subiektywizm większości systemów KRI pojawia się konieczność skonstruowania odpowiedniego kryterium doboru tego typu wskaźników. Powinny one spełniać podstawowe kryteria w zakresie porównywalności, efektywności oraz łatwości użycia. Do głównych kryteriów zaliczyć należy: konieczność odzwierciedlania obiektywnego pomiaru, a nie subiektywnej oceny, mierzalność w zdefiniowanych momentach, przydatność z perspektywy procesów zarządzania, podatność na audyt, łatwość dokonywania pomiaru [Maderak 2010].

Tabela 4. Kryteria doboru wskaźnika KRI

Kryterium	Skuteczność	Porównywalność	Łatwość użytkowania
Opis	Wskaźnik powinien: – mieć zastosowanie do minimum jednego obszaru występowania ryzyka; – być mierzalny w określonych punktach czasowych; – odzwierciedlać obiektywny pomiar, a nie subiektywną ocenę; – śledzić co najmniej jeden aspekt profilu strat i historii zdarzeń; – dostarczać przydatnych informacji dotyczących procesu zarządzania	Wskaźnik powinien być: – wyrażony ilościowo lub procentowo – porównywalny w czasie, – porównywalny w ramach prowadzonej działalności, – identyfikowany jako porównywalny pomiędzy poszczególnymi podmiotami	Wskaźnik powinien być: – niezawodnie dostępny na czas; – opłacalny do monitorowania; – zrozumiały i przystępnie przekazywany

Źródło: opracowanie na podstawie [Davies i in. 2006, s. 7].

Pionierskie badania w zakresie wykorzystania współczynników KRI w zarządzaniu ryzykiem operacyjnym we współpracy z kilkudziesięcioma instytucjami finansowymi z całego świata przeprowadziło wspólnie z firmą RiskBusiness stowarzyszenie Risk Management Association [Taylor i Davis 2003, s. 59]. Najistotniejszymi celami projektu, które w efekcie przeprowadzonych badań udało się osiągnąć, były [Finlay 2004, s. 32]:

– budowa zestandaryzowanego schematu implementacji KRI,

– stworzenie mapy ryzyka zawierającej najistotniejsze obszary ryzyka operacyjnego,

– przygotowanie szczegółowej specyfikacji dla poszczególnych wskaźników,

– poszukiwanie benchmarku, który będzie mógł być wykorzystany jako standard do porównywania firm lub w celu wskazania optymalnych wartości wskaźników.

W przypadku wykorzystania wskaźników KRI w szacowaniu poziomu ryzyka operacyjnego niezbędne jest przyporządkowanie ich do poszczególnych obszarów i kategorii ryzyka. Umożliwia to precyzyjny opis sytuacji przedsiębiorstwa z perspektywy narażenia na ryzyko w każdym momencie i we wszystkich obszarach jego działalności[2]. Dodatkową korzyścią z przypisania wskaźników KRI do poszczególnych kategorii ryzyka jest uzyskanie możliwości śledzenia ich zmienności. Z kolei przypisanie wskaźników KRI do danej jednostki organizacyjnej pozwala monitorować jej sytuację za pomocą obserwacji zmienności wybranych wskaźników. Ocenę ryzyka można skwantyfikować z wykorzystaniem jednego z następujących wzorów [Orzeł 2005, s. 5]:

$$K = \frac{NS}{S}$$

lub

$$K = \frac{S}{NS + S},$$

gdzie:

NS – czynniki niesprzyjające danemu przedsięwzięciu lub KRI niespełniające wyznaczonych limitów,

S – czynniki sprzyjające danemu przedsięwzięciu lub KRI spełniające wyznaczone limity.

Analiza kształtowania się wybranych KRI może pozwolić na odpowiednią korektę prawdopodobieństwa i dotkliwości potencjalnych strat[3].

4. Zastosowanie kluczowych wskaźników ryzyka

Istotą analizy KRI jest tzw. system wczesnego ostrzegania kierownictwa przedsiębiorstwa o wszelkich zachodzących w organizacji zmianach mających związek z szeroko rozumianym ryzykiem operacyjnym. W tym kontekście istotnym elementem jest nadawanie priorytetów wskaźnikom ryzyka. Zabieg ten pomaga skoncentrować się na tych wskaźnikach, które mogą mieć największe znaczenie

[2] Aczkolwiek precyzyjne przyporządkowanie zdarzeń do poszczególnych kategorii ryzyka nie jest proste z uwagi na to, że zachodzą trudności w jednoznacznym określeniu granic określonych kategorii. Szczególnie w dużych organizacjach to samo zdarzenie może zostać przypisane do różnych kategorii lub podkategorii, zob. [McLenaghen 2007, s. 25–31].

[3] Szczegółowo zob. [Thlon 2012, s. 85–90].

dla instytucji. Nadawanie priorytetów może być zautomatyzowane w pełnym zakresie[4], jednak zazwyczaj konieczne jest włączenie się w ten proces komórki odpowiedzialnej za zarządzanie ryzykiem operacyjnym. Wśród czynników, które mogą wpływać na priorytet nadawany poszczególnym wskaźnikom, dominującą rolę odgrywają następujące [IOR 2006, s. 17–18]:

– wartość wskaźnika – w aspekcie zarówno bezwzględnym, jak i względnym uważana jest za jeden z głównych czynników determinujących jego znaczenie. W praktyce w tym zakresie wykorzystywany jest system limitów i wartości progowych przyporządkowanych do poszczególnych stref związanych ze stopniem istotności wskaźnika. Tabela 5 zawiera przykładowe zestawienie znaczenia wskaźnika wraz z przyporządkowanym sposobem reakcji w podziale na trzy płaszczyzny istotności. Wskaźnik znajdujący się wewnątrz strefy II (pomarańczowej) powinien uzyskać wyższy priorytet w stosunku do wskaźnika ze strefy I (zielonej), jednak niższy od wskaźnika ze strefy III (czerwonej);

– trend – monitorowanie trendu obrazującego kształtowanie się poziomu ryzyka operacyjnego w instytucji pozwala antycypować, czy w najbliższej przyszłości przekroczone zostaną ustalone wartości progowe. Analiza trendów dostarcza ponadto informacji dotyczących dynamiki przyrostu lub spadku poszczególnych wartości ryzyka operacyjnego. Przykładowo nawet jeżeli wskaźnik znajduje się w zielonej I strefie, może zaistnieć sytuacja, w której należy nadać mu wyższy priorytet, ponieważ trend wskaźnika sugeruje, że powiązany z nim poziom ryzyka rośnie;

– zależność między wskaźnikami – użyteczną metodą prezentacji wskaźników KRI jest przedstawianie ich w starannie dobranych parach, w celu uzyskania bardziej kompletnej perspektywy dotyczącej ekspozycji na ryzyko.

Główna korzyść stosowania wskaźników wynika z ich zdolności do wskazania relacji pomiędzy rzeczywistym a pożądanym poziomem narażenia na ryzyko. Poprzez monitorowanie właściwie dobranych wskaźników ryzyka oraz sprawdzenie ich aktualnych wartości i trendów w stosunku do ustalonych limitów instytucja jest w stanie ocenić, czy narażenie na ryzyko operacyjne pozostaje na pożądanym poziomie, czy też znacznie od niego odbiega.

Dane, na których podstawie budowane są wskaźniki, są gromadzone w kolejnych okresach, dzięki czemu zarząd dysponuje porównywalnymi informacjami. Informacje o kluczowych wskaźnikach lub wskaźnikach o ekstremalnie wysokich lub niskich wartościach powinny być przekazywane do zarządzających najwyższych szczebli w celu podjęcia przez nich odpowiednich działań w momencie przekroczenia przez te wskaźniki ustalonego poziomu.

[4] Zazwyczaj z wykorzystaniem limitów i wartości progowych.

Tabela 5. Znaczenie wskaźników ryzyka

Strefa istotności	Sposób reakcji
I strefa – zielona	Wartość wskaźnika jest w zakresie standardowych parametrów, co wskazuje na brak narażenia na istotne dla instytucji ryzyko Nie ma potrzeby podejmowania działań zaradczych, ponieważ wskaźnik i skorelowane z nim kategorie ryzyka operacyjnego są pod odpowiednią kontrolą
II strefa – pomarańczowa	Wartość wskaźnika odchyla się od standardowych parametrów, co wskazuje, że instytucja może być wystawiona na ryzyko o podwyższonym poziomie Wymagany jest wzmożony monitoring zagrożonych procesów i przygotowanie działań zaradczych, które mogą zostać wdrożone w niedalekiej przyszłości
III strefa – czerwona	Wartość wskaźnika zdecydowanie odbiega od wartości standardowych, co wskazuje na potencjalnie znaczące narażenie na ryzyko Wymagane jest niezwłoczne podjęcie działań mających na celu redukcję poziomu ryzyka do akceptowalnego poziomu

Źródło: opracowanie własne na podstawie [IOR 2010, s. 17–18].

W praktyce funkcjonują dwa podejścia w zakresie wyboru wskaźników, które instytucja zamierza monitorować [IOR 2010, s. 8]:

– podejście *top-down*,

– podejście *bottom-up*.

Podejście *top-down* inicjowane jest przez menedżerów wyższego szczebla, którzy dokonują wyboru wskaźników podlegających monitoringowi w całej firmie. Decyzja o zastosowaniu tej koncepcji doboru KRI oznacza, że selekcja powinna być przeprowadzona według następujących kryteriów:

– wybrany KRI musi odzwierciedlać profil ryzyka operacyjnego działów, sektorów branżowych, kraju bądź regionu lub całej organizacji, w zależności od poziomu, na którym został wyselekcjonowany,

– wskaźnik musi ułatwiać agregację pozyskiwanych danych, które mogą zostać na odpowiednim poziomie zarządzania,

– KRI powinien mieć zastosowanie do wszystkich części struktury organizacyjnej poniżej poziomu, do którego został odniesiony.

W podejściu *top-down* KRI są zwykle dobrane w połączeniu z grupą funkcji i mogą odnosić się do ogólnych przyczyn lub konkretnego procesu, potencjalnej awarii lub zdarzenia. Wskaźniki tego typu określane są przez główne grupy funkcyjne, np. [Davies i in. 2006, s. 8]:

– prawne – całkowita liczba i wartość roszczeń wobec firmy, ogółem oraz z podziałem na linie biznesowe;

– finansowe – liczba incydentów na koniec okresu sprawozdawczego, liczba błędów rachunkowych lub nieuzasadnione różnice;

– IT – liczba prób ataków zewnętrznych na zaporę typu firewall.

Z kolei podejście *bottom-up* pozwala dokonywać wyboru i monitorować zestawy wskaźników na każdym szczeblu struktury organizacyjnej. Proces wyboru KRI zgodnie z tą koncepcją powinien uwzględniać [IOR 2010, s. 8–9]:

– wyniki szacunkowego pomiaru ryzyka operacyjnego metodami samooszacowania, zapewniające, że wskaźniki są identyfikowane w celu ułatwienia ciągłego monitorowania określonych zagrożeń,

– wyniki audytu, które ułatwią identyfikację nieprawidłowości dotyczących kontroli lub monitorowania,

– spostrzeżenia „właścicieli" ryzyka (np. operacyjnych menedżerów poszczególnych linii biznesowych) oraz komórki do spraw ryzyka operacyjnego,

– wszelkie wnioski, które mogły zostać wyciągnięte w związku z zaistniałymi w ostatnim okresie wydarzeniami skutkującymi stratami,

– zmiany w otoczeniu instytucji, które mogą oznaczać, że niektóre KRI stały się bardziej istotne[5].

Obecnie wiele instytucji łączy obydwa podejścia, dostosowując sposób wyboru KRI do specyfiki prowadzonej działalności. Każda organizacja musi przed wdrożeniem zestawu wskaźników opracować procedury dotyczące sposobu interpretacji danych oraz wartości progowych, a także działań podejmowanych w momencie przekroczenia ustalonych limitów. Założeniem funkcjonowania limitów czy wartości progowych jest ich ustalenie w taki sposób, by po ich przekroczeniu osoby odpowiedzialne za zarządzanie ryzykiem operacyjnym były na bieżąco informowane o potencjalnie istotnej zmianie w narażeniu na ryzyko.

5. Schemat funkcjonowania systemu wskaźników KRI w banku

Istotą funkcjonowania systemu wskaźników KRI jest przetworzenie danych o wskaźnikach biznesowych banku, które potencjalnie mogą mieć wpływ na urzeczywistnienie się i skutki zdarzeń o charakterze operacyjnym. KRI w ujęciu pragmatycznym jest miarą używaną w zarządzaniu, obrazującą, jak ryzykowna jest dana działalność, może więc odnosić się zarówno do relatywnej lub potencjalnej dotkliwości i (lub) częstości strat, jak i zdarzeń typu *near-miss*[6]. Ważnym elementem KRI jest właściwe ustalenie wartości krytycznej i progowej poszczególnych wskaźników. Przez wartość krytyczną rozumie się taką wartość KRI,

[5] Np. wskaźnik ryzyka związanego z potencjalnymi oszustwami może uzyskać wyższy priorytet w okresie recesji.

[6] Zdarzenia operacyjne typu *near-miss*, czyli „o mały włos", to zdarzenia o charakterze zamkniętym, w przypadku których istniało realne zagrożenie wystąpienia bezpośrednich lub pośrednich strat finansowych, ale których to strat ostatecznie uniknięto, zob. [Thlon 2012].

która odpowiada nieakceptowanemu poziomowi ryzyka. Natomiast wartość progowa rozumiana jest jako taka wartość KRI, której przekroczenie oznacza, że istnieje poważne ryzyko osiągnięcia wartości krytycznej w określonym czasie. Krótko mówiąc, przekroczenie wartości progowej jest bezpośrednim sygnałem ostrzegawczym. W praktyce występuje kilka metod wykorzystywanych do wyznaczania wartości progowych, m.in. modele logistyczne, metody oparte na szeregach czasowych, metody oparte na historycznych rozkładach strat, analizy rentowności, analizy eksperckie[7]. Sposób wyznaczania wartości krytycznych i progowych powinien uwzględniać dostępność danych. Każda ze wskazanych metod ma istotne ograniczenia, z tego względu zalecane jest zbudowanie odpowiednich modeli hybrydowych, np. powiązanie modelu logistycznego z analizą rentowności lub z szeregiem czasowym pozwala na ograniczenie wad poszczególnych rozwiązań [Korona 2011].

KRI musi mieć zdefiniowaną metrykę, w skład której wchodzą informacje definiujące poszczególne wskaźniki. W tabeli 6 zaprezentowano informacje, które powinny być wprowadzone, by możliwy był monitoring przykładowego wskaźnika KRI.

Tabela 6. Metryka przykładowego wskaźnika KRI

I. Informacje ogólne	
Nazwa wskaźnika	liczba podjętych prób wyłudzenia
Typ wskaźnika	podstawowy
Jednostka systemowa	…
Jednostka monitorująca, linia biznesowa	bankowość korporacyjna
Obszar ryzyka	proces obsługi klientów
Kategoria ryzyka operacyjnego	oszustwo zewnętrzne
II. Szczegółowe informacje o KRI	
ID wskaźnika KRI	001
Jednostka miary wskaźnika KRI	liczba podjętych prób wyłudzenia
Wartość progowa KRI	55
Wartość krytyczna KRI	70
Częstotliwość monitorowania	miesięczna
Okres przejściowy	brak
Data utworzenia KRI	1.01.2014
Data modyfikacji KRI	–

[7] Algorytmy poszczególnych metod z uwzględnieniem ich wad i zalet zostały zaprezentowane w publikacji [Korona 2011]. Wyznaczanie wartości progowych i krytycznych KRI, PRMIA – zob. http://start5g.ovh.net/~prmia/prezentacje/12.09.2011KRI.pdf (dostęp: 5.05.2014).

cd. tabeli 6

III. Dodatkowe informacje o KRI	
Informacje na temat budowy wskaźnika	odnotowane próby wyłudzenia dotyczą przede wszystkim procesu udzielania kredytów i gwarancji
Powiązanie wskaźnika z ryzykiem operacyjnym	wzrost wartości wskaźnika może wskazywac na wzrost poziomu ryzyka operacyjnego w kategorii oszustwo zewnętrzne
Zastosowanie wskaźnika	– prognozowanie liczby prób wyłudzeń – monitoring nieprawidłowości w działalności działu obsługi klienta – poprawa jakości obsługi klienta
Data weryfikacji KRI	–
Słowa kluczowe	wyłudzenie, oszustwo
Źródło danych	…
Metoda wprowadzenia danych	ręcznie
IV. Tryb przekazania informacji do jednostki monitorującej KRI	
Nazwa jednostki przekazującej informacje	…
Częstotliwość lub termin przekazywania informacji	miesięcznie, na koniec każdego miesiąca
Forma przekazywanych informacji	zestawienie w pliku Excel
Sposób przekazywania informacji	online
V. Działania ograniczające poziom ryzyka w przypadku przekroczenia wartości progowej	
Nazwa jednostki odpowiedzialnej za podjęcie działań	…
Opis działania ograniczającego poziom ryzyka	analiza przyczyn wzrostu wartości wskaźnika i podjęcie działań ograniczających poziom ryzyka, polegających np. na aktualizacji procedur dotyczących analiz kredytowych
VI. Działania ograniczające poziom ryzyka w przypadku przekroczenia wartości krytycznej	
Nazwa jednostki odpowiedzialnej za podjęcie działań	…
Opis działania ograniczającego poziom ryzyka	analiza przyczyn wzrostu wartości wskaźnika i podjęcie działań ograniczających poziom ryzyka, polegających np. na aktualizacji procedur dotyczących analiz kredytowych

Źródło: opracowanie własne na podstawie [Karwański 2012, s. 56].

6. Podsumowanie

KRI stanowią mierzalną wartość pozwalającą śledzić zmienność narażenia na ryzyko operacyjne w poszczególnych liniach biznesowych. Wskaźnik taki staje się kluczowy, gdy potrafi śledzić szczególnie ważne rodzaje narażenia na ryzyko. Przykładowo w miarę zwiększania się liczby skarg klientów rośnie prawdopodobieństwo wystąpienia ukrytych, potencjalnych błędów systemowych lub ludzkich. Innymi słowy jest podstawą do twierdzenia, przynajmniej w pewnym zakresie, że zmiany wartości wskaźnika są prawdopodobnie związane ze zmianami wielkości narażenia na ryzyko czy też z zagrożeniem poniesieniem straty operacyjnej.

Efektywny proces monitorowania KRI jest niezbędny we wczesnym wykrywaniu i korekcie sytuacji wynikających z zagrożeń o charakterze operacyjnym. Może służyć jako baza dla szacowania ryzyka operacyjnego oraz wdrażania strategii łagodzących. Raporty dotyczące wskaźników ryzyka operacyjnego mogą być tworzone na każdym poziomie podejmowania decyzji, począwszy od zarządu, a skończywszy na menedżerach pojedynczych zespołów. Należy pamiętać, że zarząd powinien monitorować jedynie ogólne narażenie organizacji na ryzyko, używając relatywnie małej liczby wskaźników, natomiast osoby zajmujące kolejne szczeble w hierarchii jednostki powinny zajmować się szerszym zakresem danych bądź informacjami dotyczącymi wyłącznie poszczególnych działów [IOR 2010, s. 15].

Literatura

Allen L., Bali T. [2004], *Cyclicality in Catastrophic and Operational Risk Measurements*, City University of New York.

BCBS [2004], *International Convergence of Capital Measurement and Capital Standards*, Basel Committee on Banking Supervision, Basel.

BITS Financial Services Roundtable [2004], *Developing a KRI Program: Guidance for the Operational Risk Manager*, www.bits.org/publications/doc/KRIprogram0904.doc.

Bourque W. [2003], *Buy Side Operational Risk*, Conference Society of Actuaries Conference Investment Risk: The Operational Side, Montreal.

Corporate Governance Survey 2003 part I, *Op Risk Disclosure: a Long Road Ahead* [2003], Operational Risk, June 1st 2003 / vol. 4, no 6, http://db.riskwaters.com/public/showPage.html?page=277094.

Cruz M. [2002], *Modeling, Measuring and Hedging Operational Risk*, John Wiley & Sons, Chichester.

Davies J., Finlay M., McLenaghen T., Wilson D. [2006], *Key Risk Indicators – Their Role in Operational Risk Management and Measurement*, „RiskBusiness International", February.

Finlay M. [2004], *A Structured Framework for KRIs*, „OpRisk&Compliance", July.

Goodhart Ch. [2001], *Operational Risk*, LSE Financial Market Group, Special Paper Series, London.
Harmantzis F. [2004], *Operational Risk Management in Financial Services and the New Basel Accord*, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=579321.
IOR [2010], *Operational Risk Sound Practice Guidance: Key Risk Indicators*, Institute of Operational Risk (IOR), November.
Jajuga K., Jakóbczak J. [2004], *Operational Risk – New Tendencies in Measurement*, prezentacja, Warszawa, czerwiec, http://www.kdpw.pl/konferencje.
Jamson R. [2002], *The True Cost of Operational Risk*, „Erisk", February.
Jorion P. [2007], *Financial Risk Manager*, Handbook, John Wiley & Sons, New Jersey.
Karwański M. [2012], *Model integracji danych dla prognoz eksperckich w informatycznych systemach zarządzania ryzykiem*, SGGW, Warszawa 2012.
King J. [2001], *Operational Risk: Measurement and Modelling*, John Wiley & Sons, Chichester.
Korona R. [2011], *Wyznaczanie wartości progowych i krytycznych KRI*, PRMIA, http://start5g.ovh.net/~prmia/prezentacje/12.09.2011KRI.pdf.
Maderak K. [2010], *Ewolucja metod kwantyfikacji ryzyka*, „Bank", nr 9 (214).
Marshall C. [2001], *Measuring and Managing Operational Risk in Financial Institutions*, John Wiley & Sons, Singapore.
McLenaghen T. [2007], *The Data Puddle Challenge*, „Oprisk&Compliance", 1 August.
Orzeł J. [2005], *Na drodze do zaawansowanych metod ilościowego pomiaru ryzyka operacyjnego – KRI*, „Bank i Kredyt" nr 6.
Rowe D. [2003], *The Operational Risk Pyramid*, „Risk", August.
Sanyal A. [2005], *A Pragmatic Approach to Modelling KRIs and Their Impact on OpVaR*, „Operational Risk", May.
Scandizzo S. [2005], *Risk Mapping and Key Risk Indicators in Operational Risk Management*, „Economic Notes", vol. 34, nr 2, July, http://dx.doi.org/10.1111/j.0391-5026.2005.00150.x.
Strupczewski G. [2008], *Pojęcie i struktura procesu zarządzania ryzykiem ze szczególnym uwzględnieniem ryzyka katastroficznego* [w:] *Ubezpieczenia wobec wyzwań XXI wieku*, red. W. Ronka-Chmielowiec, Prace Naukowe Akademii Ekonomicznej we Wrocławiu nr 1197, Wrocław.
Taylor Ch., Davies J. [2003], *Getting Traction with KRIs: Laying the Groundwork*, „The RMA Journal", November.
Thlon M. [2012], *Zarządzanie ryzykiem operacyjnym przedsiębiorstwa. Metoda szacowania ryzyka Delta-EVT*, Wydawnictwo Uniwersytetu Ekonomicznego w Krakowie, Kraków.

The Use of Key Risk Indicators in Operational Risk Management in Banks

Operational risk is defined as the possibility of losses resulting from the failure, deficiency or inadequacy of internal processes, people and systems or from external events. Operational risk measurement methods are different from techniques applicable to other types of risk. The particular issues involved in operational risk and the difficulty of estimating its impact on the level of income earned significantly complicate the measurement.

Therefore, in order to estimate the level of operational risk there is a tendency to take a comprehensive approach to operational risk management, understood as the combination of qualitative risk estimation, quantitative measurement methods and Key Risk Indicators (KRI). The main objective of the paper is to analyse the most important aspects of the use of KRI in managing operational risk. This objective determines the paper's structure. I analyse the definition, characteristics, applications and quantification methods of KRI, in that order.

Keywords: risk, operational risk, risk measurement methods, Key Risk Indicators KRI.