Kategoryzacja strat operacyjnych w bankowości

Categorization of Operational Losses in Banking

*Maciej Piołunowicz**

Streszczenie

W ciągu ostatnich lat znacznie wzrosło znaczenie właściwej identyfikacji, pomiaru i zarządzania ryzykiem operacyjnym w działalności banków. Ta tendencja utrzyma się m.in. w wyniku wprowadzania nowych wymogów nadzorczych, zawartych w Nowej Umowie Kapitałowej oraz w unijnej dyrektywie Capital Requirements Directive (CRD). Wzrost tych wymogów wiąże się również ze zwiększeniem świadomości zagrożeń wynikających z ryzyka operacyjnego.

Jednym z podstawowych wymogów dotyczących ryzyka operacyjnego jest konieczność właściwej klasyfikacji strat operacyjnych. Celem niniejszego artykułu jest przedstawienie kategorii tych strat w podziale stosowanym w NUK, CRD oraz Rekomendacji M Komisji Nadzoru Bankowego. Autor posłużył się przykładami, aby wskazać, jakie straty operacyjne powinny być kwalifikowane do poszczególnych kategorii. Dodatkowym celem artykułu jest podkreślenie istotności zagadnień związanych z ryzykiem operacyjnym w działalności instytucji finansowych.

Słowa kluczowe: ryzyko operacyjne, straty operacyjne, zarządzanie ryzykiem, Nowa Umowa Kapitałowa, Dyrektywa CRD.

Abstract

The importance of generating appropriate operational risk identification, measurement and management processes in banks has increased significantly within the last few years. This trend will continue as a result of – among other reasons – implementation of new supervisory regulations stated in the New Basel Capital Accord and the UE Capital Requirements Directive. The introduction of these requirements is also associated with the increase in awareness of threats related to operational risk.

According to supervisory regulations, one of the fundamental requirements concerning operational risk is the necessity to categorize operational losses properly. This article aspires to present the categorization of losses, stated in the Capital Accord, CRD, and Recommendation M of the KNB. Author uses examples of losses to demonstrate which losses should be attributed to a particular loss category. Another aim of the article is to emphasize the importance of issues associated with operational risk management in financial institutions.

Keywords: operational risk, operational losses, risk management, New Basel Capital Accord, Capital Requirements Directive.

JEL: G32, G34

* Narodowy Bank Polski, Departament Audytu Wewnętrznego.

Wstęp

Ryzyko operacyjne w bankowości staje się coraz istotniejsze. Dostrzegają to przede wszystkim banki i inne instytucje finansowe, które coraz więcej czasu i środków przeznaczają na zarządzanie tym rodzajem ryzyka. Kwestie związane z ryzykiem operacyjnym stały się także przedmiotem zainteresowania instytucji nadzorczych oraz tworzących najlepsze praktyki, jak Bazylejski Komitet Nadzoru Bankowego (w Europie), U.S. Securities and Exchange Commission (w USA) czy Komisja Nadzoru Bankowego (w Polsce). Ryzykiem operacyjnym coraz szerzej interesują się również przedsiębiorstwa spoza branży finansowej, a także teoretycy i badacze naukowi.

W najbliższej przyszłości waga tego zagadnienia z pewnością będzie rosła, m.in. w związku z wdrażaniem Nowej Umowy Kapitałowej i związanych z nią dyrektyw europejskich, które wprowadzają obowiązek uwzględnienia ryzyka operacyjnego w pomiarze adekwatności kapitałowej oraz zarządzania tym rodzajem ryzyka w podobny sposób, jak ryzykiem kredytowym i rynkowym. Temat ten dotyczy zarówno Polski, jak i pozostałych krajów Unii Europejskiej, częściowo ze względu na ogólny obowiązek wprowadzania zapisów wynikających z unijnych dyrektyw, a częściowo z powodu globalizacji systemu finansowego, wymuszającej na bankach działających w Polsce dostosowanie się do zasad stosowanych przez banki na całym świecie.

W ostatnich latach w Polsce zagadnienie ryzyka operacyjnego stało się bardzo istotne, przede wszystkim w sektorze bankowym. Wiele banków, szczególnie większych, wprowadziło mniej lub bardziej zaawansowane systemy identyfikacji ryzyka operacyjnego, mierzenia go i zarządzania nim. Warto zauważyć, że wiele banków przejęło system zarządzania ryzykiem od spółki matki. Takie rozwiązanie ma oczywiste zalety – w postaci otrzymania gotowego, zaawansowanego systemu zarządzania ryzykiem. Wiąże się jednak również z niebezpieczeństwem, że otrzymany system może nie funkcjonować właściwie w specyficznym, lokalnym otoczeniu. Tematem ryzyka operacyjnego zajął się również nadzór bankowy, czego najważniejszym rezultatem była wydana w 2004 r. Rekomendacja M Komisji Nadzoru Bankowego, dotycząca zarządzania ryzykiem operacyjnym w bankach. W tej chwili trwają prace nad wprowadzeniem do polskiego porządku prawnego zapisów europejskiej dyrektywy Capital Requirements Directive (Parlament Europejski 2006a i 2006b)[1], wymuszających alokację kapitału regulacyjnego na równoważenie ryzyka operacyjnego występującego w działalności banków. Można podejrzewać, że spowoduje to przyśpieszenie prac nad systemami zarządzania ryzykiem operacyjnym.

Niniejszy artykuł przedstawia jeden z głównych aspektów ryzyka operacyjnego – kategoryzację strat operacyjnych według zdarzeń, które je powodują. Stosowania takiego podziału wymagają wszystkie najlepsze standardy w zakresie ryzyka operacyjnego. Przypisanie danej straty do konkretnej kategorii nie zawsze jest jednak oczywiste. Celem artykułu jest wskazanie, jakie straty powinny być zaliczane do poszczególnych kategorii, oraz opis przykładowych zjawisk z danej kategorii. Szczególną uwagę poświęcono przykładom strat znajdujących się na pograniczu kilku kategorii.

Pierwsza część artykułu zawiera ogólny opis problematyki ryzyka operacyjnego. W drugiej części zostały przedstawione kategorie strat operacyjnych, w podziale stosowanym przez większość instytucji nadzorczych, w tym Komisję Nadzoru Bankowego, wraz z opisem przykładów 2–3 strat z każdej kategorii. Większość z nich pochodzi z sektora bankowego. Ponieważ jednak ryzyko operacyjne dotyczy praktycznie wszystkich obszarów działalności biznesowej, w przypadku niektórych kategorii ryzyka zostały wskazane również przykłady strat operacyjnych w innych instytucjach. Trzecia i ostatnia część artykułu to ogólna analiza częstotliwości występowania różnych kategorii strat operacyjnych oraz wielkości pojedynczych strat wewnątrz danej kategorii, przede wszystkim na podstawie wyników ankiety wypełnianej przez banki dla Komitetu Bazylejskiego na potrzeby prac nad Nową Umową Kapitałową.

Historia ryzyka

Ryzyko towarzyszy bankom od początku ich działalności. Na jego istnieniu opiera się sama koncepcja funkcjonowania banku, którego podstawowa działalność – przyjmowanie depozytów i udzielanie kredytów – to w istocie transferowanie ryzyka. Oznacza to w praktyce, że banki z konieczności od bardzo dawna zarządzają podejmowanym ryzykiem. Ostatnie dekady przyniosły w tym zakresie bardzo duże zmiany, przede wszystkim formy, w której ten proces się odbywa. Kiedyś polegał on na nieformalnych działaniach, nakierowanych zwykle na badanie przyczyn już zaistniałych strat. Dzisiaj zarządzanie ryzykiem jest sformalizowane w postaci wielu procedur, modeli oraz wymogów i dotyczy praktycznie każdego pracownika banku, a jego celem jest raczej prewencja niż analiza strat *ex post*.

Niektórymi rodzajami ryzyka, takie jak ryzyko kredytowe czy płynności, banki zarządzają od początku swojego funkcjonowania. Banki zawsze przyzna-

[1] Pełna wersja dokumentów jest dostępna np. na oficjalnej stronie Komisji Europejskiej, http://ec.europa.eu

wały kredyty w zależności od spełnienia przez potencjalnego kredytobiorcę pewnych warunków. Ewentualne zabezpieczenia musiały spełniać określone wymogi, a spłaty kredytów były monitorowane. Jednocześnie banki starały się, by ich aktywa i pasywa były odpowiednio skorelowane, tak aby minimalizować potencjalne problemy z płynnością. Oczywiście, stopień skomplikowania systemów związanych z zarządzaniem tymi rodzajami ryzyka jest obecnie nieporównywalny z sytuacją sprzed lat. W szczególności bardzo zwiększyło się matematyczne i ekonometryczne zaawansowanie modeli wykorzystywanych do tych celów. Jednocześnie mimo tak dużego wzrostu wyrafinowania narzędzi i instrumentów fakt zarządzania tymi dwoma rodzajami ryzyka ma historię praktycznie tak długą, jak sama bankowość.

W latach 80. XX w. banki (przede wszystkim amerykańskie) stanęły przed problemem dużych zmian stóp procentowych i silnie zmieniających się kursów walutowych. Stało się jasne, że sam monitoring ryzyka kredytowego nie wystarczy, by zapewnić im bezpieczeństwo. W ten sposób pojawiła się tematyka ryzyka rynkowego. Początkowo monitorowanie ryzyka rynkowego odbywało się jedynie przez wyznaczanie limitów ekspozycji na dane rodzaje instrumentów. Później, na podstawie prostych modeli statystycznych, rozpoczęto wyliczanie różnych miar i wskaźników określających zagrożenie tym rodzajem ryzyka. Typowym przykładem takiej miary ryzyka jest wartość zagrożona – Value at Risk. Wreszcie pojawiły się pomysły powiązania ryzyka z potencjalnymi zyskami i tak powstała koncepcja Risk Adjusted Performance Measurement, umożliwiająca uwzględnienie ryzyka danej działalności w pomiarze czerpanych z niej zysków. Do tego celu służą takie wskaźniki efektywności inwestycji, jak RAROC (*Risk Adjusted Return On Capital)* czy RORAC (*Return On Risk Adjusted Capital*). Dzisiaj, gdy banki angażują się w transakcje skomplikowanymi instrumentami finansowymi z wielookresowymi, warunkowymi płatnościami, straty związane z ryzykiem rynkowym mogą być bardzo duże. Jednocześnie nowoczesne systemy ryzyka rynkowego są już bardzo zaawansowane, zarówno pod względem technicznym, jak i merytorycznym. Coraz częściej mają one postać złożonych modeli matematycznych, stworzonych przez najlepszych fachowców, rozumiejących zarówno matematyczną, jak i biznesową stronę problemu.

Ryzyko operacyjne – nowy rodzaj rozpoznawanego ryzyka

Mogłoby się wydawać, że zaawansowane systemy zarządzania ryzykiem kredytowym i rynkowym zapewnią pełne bezpieczeństwo bankom. Tak jednak się nie stało. W dzisiejszym świecie coraz częściej i wyraźniej widoczna jest konieczność zwrócenia uwagi na ryzyko operacyjne i straty z nim związane. Warto zauważyć, że samo zjawisko ryzyka operacyjnego nie jest dla banków rzeczą nową. Nowa jest natomiast koncepcja, że ryzykiem operacyjnym można zarządzać w sposób zbliżony do tego, w jaki zarządzamy ryzykiem rynkowym czy kredytowym, czyli wykorzystując pewne narzędzia, procesy i odpowiednią strukturę. Wielu osobom niezaangażowanym bezpośrednio w zarządzanie ryzykiem operacyjnym możliwość sformalizowania tego procesu nadal może wydawać się obca. Warto jednak zauważyć, że jeszcze niedawno podobnie myślano o ryzyku rynkowym, podczas gdy dzisiaj instytucje finansowe prześcigają się w tworzeniu modeli mierzących poziom tego rodzaju ryzyka.

Sam termin „ryzyko operacyjne" po raz pierwszy pojawił się w szerszym użyciu po publikacji pierwszego raportu COSO[2] *Internal Control: Integrated Framework* w 1992 r. Faktycznie jednak został on rozpowszechniony dopiero w połowie lat 90., w dużej mierze z powodu kilku wielkich skandali związanych z ryzykiem operacyjnym, o których szerzej będzie mowa w dalszej części niniejszego artykułu. Od tego czasu można obserwować znaczny i stały wzrost popularności tego tematu, widoczny na przykład w postaci coraz większej liczby publikacji, książek i konferencji związanych z ryzykiem operacyjnym[3]. Ryzykiem operacyjnym zaczęły się również interesować różne instytucje nadzorcze bądź tworzące najlepsze praktyki. Istotnym momentem dla rozwoju zarządzania ryzykiem operacyjnym było zwrócenie na niego uwagi przez Bazylejski Komitet Nadzoru Bankowego. We wrześniu 1998 r. odniósł się on do tej problematyki w dokumencie *Operational Risk Management*[4] (Bazylejski Komitet Nadzoru Bankowego 1998). Wielkiego wzrostu znaczenia tematyki ryzyka operacyjnego dowodzi przede wszystkim Nowa Umowa Kapitałowa przygotowana przez Bazylejski Komitet Nadzoru Bankowego (Bazylejski Komitet Nadzoru Bankowego 2006). Z punktu widzenia tematu niniejszego artykułu najważniejszą zmianą zawartą w NUK jest uwzględnienie w nim ryzyka operacyjnego jako od-

[2] COSO – The Committee of Sponsoring Organizations of the Treadway Commission – to wpływowa organizacja, założona przez największe finansowe instytucje branżowe w USA, m.in. Institute of Internal Auditors. Jej celem jest poprawa jakości sprawozdawczości finansowej dzięki wzrostowi poziomu etyki biznesowej, zwiększaniu efektywności mechanizmów kontroli wewnętrznej oraz promowaniu zasad ładu korporacyjnego. Więcej informacji o COSO jest dostępnych na oficjalnej stronie internetowej COSO: www.coso.org

[3] Jako przykład można wskazać grupę Risk Waters (obecnie część Incisive Media), która w 2000 r. rozpoczęła publikację ukazującego się do dzisiaj miesięcznika "Operational Risk".

[4] Dokument ten jest dostępny między innymi na stronach internetowych Banku Rozrachunków Międzynarodowych w Bazylei, pod adresem http://www.bis.org/publ/bcbs42.htm

rębnej kategorii ryzyka, traktowanej podobnie jak ryzyko kredytowe oraz rynkowe. Warto podkreślić, że w Nowej Umowie Kapitałowej nie wskazano bezpośrednio, jak należy zarządzać ryzykiem operacyjnym. Po najlepsze praktyki w tym zakresie czytelnik jest odsyłany do wcześniejszego dokumentu Komitetu pt. *Sound Practices for the Management and Supervision of Operational Risk*[5] (Bazylejski Komitet Nadzoru Bankowego 2003b). Jest to obecnie najlepsze odzwierciedlenie dobrych praktyk w zarządzaniu ryzykiem operacyjnym. Na jego podstawie Komisja Nadzoru Bankowego wydała w 2004 r. Rekomendację M, dotyczącą zarządzania ryzykiem operacyjnym w bankach (Komisja Nadzoru Bankowego 2004)[6].

Jak wskazano, Nowa Umowa Kapitałowa koncentruje się na kwestiach związanych z alokacją odpowiedniego kapitału na pokrycie ryzyka operacyjnego. NUK (a także dyrektywa CRD) przewidują trzy sposoby wyliczania kapitału, różniące się poziomem wyrafinowania.

Według najprostszej metody, tzw. wskaźnika podstawowego, banki będą miały obowiązek utrzymywać kapitał w wysokości 15% średniego rocznego dochodu brutto z poprzednich trzech lat.

Druga pod względem skomplikowania jest metoda standardowa. Wymaga ona podziału działalności banku na 8 linii biznesowych i alokacji kapitału do każdej z nich. Dla każdej linii wysokość kapitału oblicza się (w przybliżeniu) jako średnią wielkość z pomnożenia dochodu brutto z danej linii biznesowej przez wskaźnik, wynoszący od 12% do 18%, w zależności od linii biznesowej. Średnia ta jest wyliczana dla ostatnich trzech lat.

Bankom najbardziej zaawansowanym w zarządzaniu ryzykiem operacyjnym Komitet Bazylejski sugeruje wykorzystanie zaawansowanych metod pomiaru wielkości kapitału na równoważenie ryzyka operacyjnego. To podejście opiera się na wykorzystywaniu przez banki wewnętrznych modeli kalkulacji ryzyka operacyjnego w celu wyznaczenia odpowiedniej wielkości kapitału. Wykorzystywanie tej metody jest możliwe dopiero po uzyskaniu akceptacji nadzoru i wymaga spełnienia wielu wymogów jakościowych i ilościowych, których dokładna analiza przekracza ramy niniejszego artykułu[7].

Po wielu aferach związanych z tzw. kreatywną księgowością (np. Enronu, Worldcomu czy Tyco International) problematyką ryzyka operacyjnego zajęły się również amerykańskie władze, zarówno legislacyjne, jak i nadzorcze. Rezultatem tych działań była przede wszystkim ustawa Sarbanes – Oxley Act (SOX) (Kongres USA, 2002). Co prawda nie wymieniono w niej wprost ryzyka operacyjnego, jednak nie ulega wątpliwości, że SOX w dużej mierze odnosi się właśnie do niego.

Mimo istnienia wielu publikacji na temat ryzyka operacyjnego dopiero od niedawna istnieje powszechnie akceptowana definicja tego zjawiska. Przygotował ją Komitet Bazylejski. Według niej ryzyko operacyjne to „ryzyko straty wynikającej z niewłaściwych lub błędnych procesów, działania ludzi, działania systemów lub ze zdarzeń zewnętrznych”[8]. Z elementów budzących w branży kontrowersje obejmuje ona ryzyko prawne, natomiast pomija ryzyko strategiczne oraz ryzyko utraty reputacji. Tę definicję zaakceptowała większość instytucji finansowych na całym świecie[9].

Warto zauważyć, że do niedawna definicja ta miała nieco inne brzmienie, zaczynała się bowiem od sformułowania „ryzyko pośredniej lub bezpośredniej straty”. Usunięcie tego fragmentu było spowodowane chęcią silniejszego rozgraniczenia ryzyka operacyjnego, które faktycznie może być fundamentalną przyczyną bardzo wielu różnego rodzaju strat, od ryzyka rynkowego i kredytowego. Podjęcie próby rozróżnienia tych rodzajów ryzyka było konieczne, chociaż związki między nimi są bardzo silne i w wielu przypadkach bardzo trudno jest precyzyjnie stwierdzić, do jakiej kategorii zakwalifikować daną stratę. Inne, dość popularne do niedawne definicje ryzyka operacyjnego to np. „ryzyko każdej straty, która nie jest zaliczana do strat kredytowych czy rynkowych” lub „ryzyko straty wynikającej z błędów ludzkich lub z niewłaściwego funkcjonowania technologii” (Davies et al. 1999; King 1998).

Przyczyny wzrostu istotności tematyki ryzyka operacyjnego

Widać więc, że ryzyko operacyjne szybko staje się coraz popularniejszym i istotniejszym tematem. Pozostaje pytanie, dlaczego tak się dzieje. Jak wskazano, jednym z czynników kierujących uwagę na to zagadnienie są wielkie skandale związane ze stratami ope-

[5] Dokument ten jest dostępny między innymi na stronach internetowych Banku Rozrachunków Międzynarodowych w Bazylei, pod adresem http://www.bis.org/publ/bcbs96.htm

[6] Dokument jest dostępny miedzy innymi na stronie internetowej Narodowego Banku Polskiego, pod adresem www.nbp.pl

[7] Nowa Umowa Kapitałowa jest dostępna między innymi na stronie Banku Rozrachunków Międzynarodowych, w części dotyczącej Komitetu Bazylejskiego, pod adresem www.bis.org/bcbs. Dyrektywę CRD można znaleźć np. na oficjalnej stronie Komisji Europejskiej, http://ec.europa.eu. Szczegółowe rozwiązania dotyczące ryzyka operacyjnego przyjęte przez GINB są dostępne na stronie Narodowego Banku Polskiego, www.nbp.pl, w części Publikacje nadzoru bankowego, w dokumentach konsultacyjnych dotyczących walidacji zaawansowanych metod wyliczania wymogów kapitałowych z tytułu ryzyka kredytowego i operacyjnego oraz metod prostych wyliczania wymogów kapitałowych z tytułu ryzyka operacyjnego.

[8] Definicja ta została zastosowana między innymi w Nowej Umowie Kapitałowej.

[9] Choć zdarzają się wyjątki. Przykładowo, International Association of Financial Engineers, choć nie prezentuje własnej definicji ryzyka operacyjnego, podkreśla, że prawidłowa definicja powinna również uwzględniać kwestie strategiczne, reputacyjne, a także pośrednie związki między ryzykiem operacyjnym a pozostałymi rodzajami ryzyka (tzn. ryzykiem rynkowym i kredytowym). Zob. www.iafe.org – oficjalna strona internetowa International Association of Financial Engineers.

racyjnymi. Jednak przyczyn faktycznego wzrostu zarówno rangi tematu, jak i zainteresowania nim jest dużo więcej. Można je podzielić z punktu widzenia banków na przyczyny wewnętrzne, to znaczy związane z ich rozwojem i zmianą sposobu funkcjonowania, oraz zewnętrzne, wywołane ogólnymi przemianami w światowym systemie finansowym. Przyczyny wewnętrzne to np.:

• Informatyzacja. Coraz szersze wykorzystanie systemów informatycznych powoduje zmniejszenie prawdopodobieństwa błędu ludzkiego, ale wzrost prawdopodobieństwa błędów systemowych, których potencjalne skutki są dużo większe. Nieprawidłowe działanie systemu może przynieść olbrzymie straty dla banku. Co więcej, pojawiło się ryzyko technologiczne, w postaci np. włamania do systemu, dokonywania nieautoryzowanych transakcji, kradzieży danych itp.

• Stopień skomplikowania produktów bankowych oraz instrumentów finansowych. Rozwój instrumentów finansowych, takich jak egzotyczne instrumenty pochodne[10], ułatwia zarówno popełnienie błędów, jak i różnego rodzaju oszustw, natomiast utrudnia ich wykrycie. Jednocześnie większe stają się potencjalne straty.

• Banki stosują coraz bardziej skomplikowane techniki zmniejszania ryzyka kredytowego i rynkowego (np. pochodne kredytowe, sekurytyzacja aktywów, skomplikowane formy zastawu), które jednocześnie są źródłem zwiększonego ryzyka operacyjnego (np. prawnego).

• System wynagradzania pracowników, szczególnie dealerów, oparty w mniejszym stopniu na stałym wynagrodzeniu, a w większym na premii za wyniki. Taki system motywacyjny, który zasadniczo pozytywnie wpływa na pracę dealerów, często wywołuje silną pokusę fałszowania wyników.

• Rosnąca rola outsourcingu, jako sposobu na obniżanie kosztów. Powoduje to m.in. wzrost ryzyka prawnego, a także ryzyka bezpieczeństwa instytucji związanego z dostępem osób spoza niej do pewnych danych.

Do przyczyn, które można określić jako zewnętrzne, należą:

• Wzrost wolumenu obrotów. Banki dokonują na rynku wielkich transakcji, wielokrotnie przewyższających ich kapitał własny. Wiąże się to m.in. z lepszymi metodami zarządzania ryzykiem rynkowym. Jednocześnie olbrzymie mogą być straty wynikające z oszustw lub błędów i coraz większa staje się pokusa nieuczciwego wzbogacenia się. Wzrost obrotów widać przede wszystkim na rynkach papierów wartościowych w rozwiniętych krajach. Coraz bardziej dotyczy to polskiego systemu bankowego, również ze względu na zależność większości banków działających w Polsce od wielkich światowych instytucji finansowych.

• Integracja różnych funkcji w ramach banku. Z jednej strony w bankach maleje znaczenie podziału na bankowość detaliczną, korporacyjną i inwestycyjną. Z drugiej strony banki sprzedają za pomocą swoich kanałów dystrybucji już nie tylko produkty typowo bankowe, ale także ubezpieczeniowe czy tradycyjnie łączone z funduszami inwestycyjnymi. Proces ten oznacza, że pracownicy banków w coraz większym stopniu są zmuszeni do zajmowania się sprawami, w których nie mają dużego doświadczenia i które często wymagają innych systemów kontrolnych niż dotąd stosowane.

• Globalizacja spowodowała zacieśnienie więzi między różnymi elementami systemu finansowego i, co za tym idzie, ryzyko, że problemy w jednej instytucji mogą pociągnąć za sobą kłopoty wielu innych.

• Fuzje i przejęcia, często dotyczące instytucji działających w zupełnie innych kulturach zarządczych, wywołują gruntowne zmiany nie tylko systemów informatycznych, ale również np. systemów kontroli wewnętrznej.

Dualizm ryzyka operacyjnego

Ryzyko operacyjne ma pewną charakterystyczną cechę, widoczną na tle innych rodzajów ryzyka. Jest ono niejednorodne – ma dwa różne aspekty, które zgodnie z najlepszymi praktykami w tej dziedzinie powinny być odmiennie traktowane. Większość strat operacyjnych wynika ze zdarzeń o relatywnie dużym prawdopodobieństwie, ale niskich potencjalnych skutkach. Z drugiej strony dla instytucji bardzo niebezpieczne mogą być zdarzenia, których prawdopodobieństwo wystąpienia jest niewielkie, lecz które mogą generować bardzo wysokie straty.

Straty należące do pierwszej z powyższych kategorii mogą być wywoływane przez najróżniejsze wydarzenia. Wydaje się, że jedną z ich najczęstszych przyczyn są ludzkie błędy. Oczywiście, podejmowane są próby ograniczania tego rodzaju strat, jednak ich całkowite zlikwidowanie nie jest możliwe. Prawdopodobnie nie byłoby to nawet korzystne dla danej instytucji, ze względu na relację kosztów zapobiegania stratom do korzyści związanych ze zmniejszeniem ich liczby bądź wielkości. Dla małych strat stosunek ten jest często niekorzystny, a więc opłaca się zrezygnować z dodatkowych działań zapobiegawczych, akceptując pewien poziom strat. Jednocześnie mówiąc o stratach operacyjnych, należy zawsze brać pod uwagę także inne negatywne skutki, które mogą wynikać z danego problemu, jak np. utrata reputacji przez instytucję.

[10] Np. opcje umożliwiające ich posiadaczowi wybór (do określonego momentu), czy będzie to opcja *call* czy *put*, lub typu *lookback*, którą można realizować po najkorzystniejszej cenie z danego okresu.

Ten typ ryzyka operacyjnego jest dość podobny do innych rodzajów ryzyka. Jeśli dysponujemy odpowiednio dużą bazą danych, która właściwie odzwierciedla faktyczne straty operacyjne ponoszone przez instytucję w dłuższym czasie, to możemy podejmować próby dopasowania ich do odpowiedniego rozkładu prawdopodobieństwa. Następnie, korzystając z metod statystycznych, można wyliczyć prawdopodobne straty na wybranym poziomie ufności. Jest to więc metoda podobna do tej, którą stosuje się przy wyliczaniu wartości Value at Risk. Oczywiście, problemem jest posiadanie odpowiedniej bazy danych. Jest to trudne ze względu na kłopoty z precyzyjnym wyznaczeniem wielkości faktycznie poniesionych strat operacyjnych, a także z powodu kosztowej efektywności procesu rejestrowania strat. Większość banków wpisuje do bazy jedynie straty powyżej pewnej granicy, uznając, że przy niższych stratach ich rejestrowanie jest po prostu nieopłacalne.

Z drugiej strony istnieją straty operacyjne występujące rzadko, ale za to wiążące się z dużymi konsekwencjami. Zarządzanie ryzykiem operacyjnym w tym zakresie znacznie różni się od zarządzania jakimkolwiek innym ryzykiem. Wynika to przede wszystkim z faktu, że tego typu straty są dla pojedynczej instytucji rzadkością. Na podstawie danych z jednej bądź nawet kilku instytucji nie sposób budować bazy danych o odpowiednich rozmiarach. Sprawę pogarszają jeszcze problemy z uzyskaniem wiarygodnych danych na ten temat. Wiele instytucji, które poniosły bardzo duże straty operacyjne, z powodów prestiżowych nie chce publicznie ujawniać wszystkich szczegółów z nimi związanych. Przyczynami tego typu strat mogą być przede wszystkim oszustwa, najczęściej popełniane przez pracowników samej instytucji, systemowe wady oprogramowania bądź klęski żywiołowe lub podobne przyczyny zewnętrzne. Warto również wspomnieć, że w niektórych przypadkach potencjalne skutki wystąpienia zdarzeń z zakresu ryzyka operacyjnego mogą zostać zmniejszone dzięki ubezpieczeniu. Jednocześnie trzeba podkreślić, iż nawet pełne ubezpieczenie danego elementu ryzyka operacyjnego (np. strat z tytułu klęsk żywiołowych) zwykle nie oznacza, że dane wydarzenie nie będzie przyczyną kosztów dla banku, ze względu na podwyżkę składki ubezpieczeniowej po jego wystąpieniu.

W praktyce dualizm ryzyka operacyjnego oznacza konieczność różnego sposobu zarządzania jego dwoma aspektami. Zarządzanie całością zagadnień związanych z ryzykiem operacyjnym w sposób zbliżony do zarządzania innymi rodzajami ryzyka rynkowego, a więc właściwy dla ryzyka operacyjnego o dużym prawdopodobieństwie i małych skutkach, z którą można się dość często spotkać, jest podejściem zdecydowanie niewystarczającym.

Kategorie ryzyka operacyjnego

Jak wskazano, problem z ryzykiem operacyjnym polega między innymi na trudnościach z jego precyzyjnym opisaniem. Definicja Bazylejskiego Komitetu Nadzoru Bankowego, przytoczona na początku niniejszego artykułu, w praktyce nie wystarcza do zarządzania ryzykiem. Instytucje zarządzające ryzykiem muszą wypracować ściślejsze metody określania, gdzie występuje ryzyko operacyjne. Z tego względu Komitet Bazylejski, a za jego przykładem również inne instytucje nadzorcze, między innymi Komisja Nadzoru Bankowego, wyróżniły 7 ogólnych kategorii strat operacyjnych. Są one następujące:

– oszustwo wewnętrzne (*internal fraud*),

– oszustwo zewnętrzne (*external fraud*),

– praktyka kadrowa i bezpieczeństwo pracy (*employment practices and workplace safety*),

– klienci, produkty i praktyka biznesowa (*clients, products and business practices*),

– uszkodzenia aktywów (*damage to physical assets*),

– zakłócenia działalności i błędy systemów (*business disruptions and system failures*),

– dokonywanie transakcji, dostawa oraz zarządzanie procesami (*execution, delivery and process management*)[11].

Dla każdej kategorii ryzyka zostały wskazane jego podkategorie oraz przykłady możliwych strat w każdej z nich. Organy nadzorcze powszechnie przyjęły tę kategoryzację. W dalszej części artykułu postaram się przybliżyć każdą z powyższych kategorii i dla każdej z nich wskazać przykłady publicznie znanych strat operacyjnych.

Oszustwo wewnętrzne

Ta kategoria strat operacyjnych jest najczęściej kojarzona z terminem „ryzyko operacyjne". To właśnie wielkie oszustwa, dokonywane przez pracowników danej instytucji, przyciągają uwagę świata finansowego, a niekiedy również mediów. Według definicji KNB, w skład tej kategorii strat wchodzą wszelkie zamierzone oszustwa, łamanie i obejście prawa, regulacji lub polityki spółki, niszczenie albo kradzież aktywów, fałszerstwa, celowe (niedozwolone) unikanie podatków, przekraczanie limitów, przekraczanie uprawnień itp. Wyłączono z niej jedynie zdarzenia związane z dyskryminacją i niedozwolonym różnicowaniem pracowników i stworzono dla nich odrębną kategorię strat. Warunkiem umieszczenia danego zdarzenia w kategorii „oszustwo wewnętrzne" jest udział w nim przynajmniej jednego pracownika danej instytucji.

[11] Polskie nazwy kategorii ryzyka zostały zaczerpnięte z *Rekomendacji M* Komisji Nadzoru Bankowego, natomiast nazwy angielskie – z terminologii Komitetu Bazylejskiego, wykorzystywanej m.in. w Nowej Umowie Kapitałowej.

Przykład. Jednym z najważniejszych przykładów, który zwrócił uwagę świata finansowego na istotność tematyki ryzyka operacyjnego, był upadek w 1995 r. Barings Bank, najstarszego brytyjskiego banku inwestycyjnego.

Kłopoty Barings Bank spowodowała działalność Nicholasa Leesona, dyrektora zarządzającego (General Manager) małej jednostki zależnej Barings Bank – Barings Futures Singapore. Leeson miał dokonywać transakcji arbitrażowych, których celem było wykorzystanie różnic między cenami kontraktów *futures* na indeks NIKKEI na giełdach japońskiej i singapurskiej. Teoretycznie miał bardzo ograniczone uprawnienia do przeprowadzania transakcji, jednak faktycznie dokonywał wielu ryzykownych transakcji na opcjach i kontraktach *futures*. Gdy zaczął ponosić na tych transakcjach duże straty, bardzo szybko powiększał ich wolumen, w nadziei na szybkie odrobienie strat. Jednocześnie ponoszone straty były księgowane na koncie „Błędy", które pozostawało do jego dyspozycji, mimo że cały proces księgowania odbywał się w Londynie. Leeson korzystał z tego konta praktycznie od chwili jego utworzenia w 1992 r. Do ujawnienia jego faktycznej działalności przyczynił się gwałtowny spadek akcji na giełdzie tokijskiej po trzęsieniu ziemi w Japonii w 1995 r. Pozycja Leesona była dochodowa, gdy zmienność kursu akcji była mała, więc w wyniku powyższego spadku jego straty wzrosły wielokrotnie, a desperackie próby ich zmniejszenia, poprzez zakupy kontraktów *futures* na indeks NIKKEI, tylko powiększały straty. Do chwili ujawnienia całej sprawy Leeson był uznawany za „gwiazdę" banku, ponieważ co roku jego działalność przynosiła, według raportów, bardzo duże zyski. Pod koniec lutego 1995 r., kiedy skandal został wykryty, okazało się, że w wyniku zawieranych przez niego transakcji Barings Bank poniósł w sumie straty wynoszące prawie 1,5 mld USD. Ostatecznym skutkiem całej sprawy było wykupienie większości aktywów i pasywów Barings Bank – najstarszego i do niedawna cieszącego się dobrą opinią brytyjskiego banku inwestycyjnego – przez ING Bank za dokładnie 1 funta.

Podstawową, głęboką przyczyną upadku Barings Bank było faktyczne niefunkcjonowanie systemu kontroli wewnętrznej. Istnieje wiele zasad sprawowania kontroli nad dealerami – w Baringsie złamane zostały niemal wszystkie. Po pierwsze, w Singapurze faktycznie nie było rozdzielenia funkcji *front* i *back office*. Leeson zarówno dokonywał transakcji, jak i kierował ich rozliczaniem. Na ten problem zwrócił uwagę audyt wewnętrzny w raporcie z sierpnia 1994 r., wydając rekomendację, aby te dwie funkcje zostały rozdzielone. Nie została ona nigdy spełniona. Po drugie, zasady kontroli wewnętrznej wymagają, aby kierownictwo instytucji miało świadomość rodzaju prowadzonej działalności i akceptowało poziom związanego z nią ryzyka. W przypadku Baringsa kierownictwo było zainteresowane jedynie zyskami uzyskiwanymi przez singapurską komórkę. Nikt nie zainteresował się, jak to możliwe, że działalność, która teoretycznie wiąże się z bardzo małym ryzykiem, może przynosić tak wysokie dochody. Jak wykazały późniejsze raporty badających całą sprawę, kierownictwo nie rozumiało natury instrumentów pochodnych i nie wnikało, dlaczego komórka Leesona domaga się coraz większych środków na swoje działania. Kierownictwo Baringsa nie reagowało nawet na pytania podmiotów zewnętrznych, dotyczące wielkich pozycji Leesona[12] i wykrywanych nieregularności, nawet gdy zadawały je takie instytucje, jak Bank Rozrachunków Międzynarodowych w Bazylei. Po trzecie, ponieważ działalność Leesona miała się wiązać z niewielkim ryzykiem, nie nałożono na niego żadnych limitów. Po czwarte, w matrycowej strukturze podległości, funkcjonującej w Barings Banku, Leeson miał teoretycznie wielu przełożonych, ale jak się okazało po ujawnieniu skandalu, każdy z nich twierdził, że nadzór nad działaniami Leesona jest faktycznie obowiązkiem kogoś innego (zobacz np. Bank of England 1995).

Drugim przykładem ryzyka operacyjnego związanego z oszustwem wewnętrznym, mającym podobne przyczyny, była sprawa Daiwa Bank, która również miała miejsce w 1995 r. W tym przypadku dealer nowojorskiego oddziału banku, Toshihide Iguchi, w ciągu 11 lat zdefraudował ponad 1,1 mld USD. Podobnie jak w przypadku Baringsa, Iguchi poza zawieraniem transakcji był również kierownikiem *back office* i dzięki temu mógł odpowiednio fałszować raporty, tak by ukrywać swoje straty. Interesujące jest, że to oszustwo trwało aż 11 lat, bez podejrzeń ze strony kierownictwa. Co więcej, cała sprawa wyszła na jaw tylko dzięki temu, że Iguchi napisał do kierownictwa banku list, w którym przyznał się do swoich działań.

Podobnie jak w przypadku Barings Bank, również Daiwa ignorowała wszystkie złe sygnały. Posunięte to było do tego stopnia, że w 1993 r., po uwagach ze strony nadzoru, zapewniono, że funkcje *front* i *back office* będą rozdzielone, choć nigdy tak się nie stało.

Symptomatyczne może być zachowanie kierownictwa banku po otrzymaniu listu Iguchiego. Cztery dni później Iguchi przysłał kolejny list, wyjaśniając, w jaki sposób należy działać, by całą sprawę ukryć. Kierownictwo banku zgodziło się i podjęło działania mające na celu ukrycie całej sprawy przed amerykańskim nadzorem. Proces ten trwał ponad 2 miesiące[13]. To właśnie ta próba ukrycia prawdy przed nadzorem

[12] W pewnym momencie posiadał on np. około połowy wszystkich wystawionych kontraktów na indeks NIKKEI.

[13] Pierwszy list ujawniający sprawę został wysłany 13 lipca 1995 r., natomiast amerykański nadzór został powiadomiony 18 września tego roku.

spowodowała bardzo ostrą reakcję nadzorców amerykańskich. Ostatecznym rezultatem były: usunięcie Daiwa Bank z amerykańskiego rynku, ugoda z bankiem w sprawie kryminalnej, w wyniku czego bank zapłacił karę w wysokości 340 mln USD, oraz wielkie straty reputacji, zarówno przez Daiwa Bank, jak też japońskie banki jako całość.

Oszustwo zewnętrzne

Jest to kategoria zbliżona do oszustwa wewnętrznego, z tym że dotyczy oczywiście oszustw dokonywanych przez osoby trzecie, bez udziału pracowników danej instytucji. W jej skład wchodzą straty związane z kradzieżami, oszustwami i fałszerstwami oraz straty wynikające z kradzieży informacji i ataku hakerów.

Przykład. W 2001 r. Republic New York Corporation zgodziła się wypłacić 611 mln USD jako odszkodowanie za oszustwa dokonywane przez firmę Princeton Economics International. Republic pełniła funkcję powiernika dla Princeton i jej założyciela, Martina Armstronga. Princeton sprzedawał papiery (tzw. *princeton notes*) z funduszu popularnego wśród japońskich inwestorów instytucjonalnych. Uzyskane w ten sposób środki, które miały być księgowane na wydzielonym koncie i inwestowane w określone papiery o małym ryzyku, były faktycznie inwestowane w ryzykowne przedsięwzięcia, przynoszące poważne straty. Republic New York Corporation była oskarżana o to, że nie dochowała należytej ostrożności i nadzoru, w szczególności w związku z faktem, że Armstrong już wcześniej, jeszcze przed przyłączeniem się do firmy, miał niezbyt dobrą reputację. Według pozwu złożonego przez grupę japońskich inwestorów przeciwko Republic Bank powinien był wykryć jeden z bardzo wielu sygnałów ostrzegawczych, wskazujących na niewłaściwe zarządzanie kontami Princeton.

Innym, dość typowym przykładem tego typu ryzyka jest kradzież prawie 70 mln USD z oddziału banku centralnego Brazylii w mieście Fortaleza. Miało to miejsce w sierpniu 2005 r. Bandyci wykopali 80-metrowy podkop, aby dostać się do skarbca. Praca nad nim trwała kilka miesięcy. Przestępcy wynajęli na ten okres dom w pobliżu banku i udawali firmę zajmująca się ogrodnictwem, aby uwiarygodnić wywożenie dużej ilości ziemi z posesji. Ze skarbca ukradziono jedynie używane banknoty o nominale 50 realów[14], których łączna waga przekroczyła 3,5 tony. Skradzione pieniądze nie były ubezpieczone, gdyż według rzecznik banku ryzyko ich kradzieży było tak małe, że nie opłacało się ponosić kosztów składki ubezpieczeniowej.

Oczywiście, tak duże kradzieże dokonywane przez fizyczne włamanie się do skarbca banku są dziś rzadkością. Podstawowym zagrożeniem są raczej włamania do systemu informatycznego. W tym kontekście warto także wspomnieć o tzw. phishingu, czyli wyłudzaniu od klientów danych potrzebnych do przejęcia kontroli nad ich kontem, poprzez przesyłanie przez oszustów podszywających się pod bank fałszywych maili z prośbą o podanie numeru konta i hasła do niego. Tego typu sytuacje są coraz częstsze. Przykładowo w okresie od marca 2005 r. do czerwca 2006 r. do klientów Citibanku zostały rozesłane 32 różne maile tego typu. Warto podkreślić, że choć większość kosztów takich ataków ponosi klient, który ujawnił swoje dane, coraz częściej i w coraz większym stopniu banki przejmują odpowiedzialność za takie straty, co oczywiście skutkuje wzrostem strat operacyjnych z tego tytułu.

Praktyka kadrowa i bezpieczeństwo pracy

Ta kategoria zawiera wszystkie kwestie związane z nieprzestrzeganiem prawa pracy, przepisów BHP lub porozumień z pracownikami. Należą do niej także straty związane z dyskryminacją i różnicowaniem pracowników. Należy tu również uwzględnić wszelkie odszkodowania dla pracowników za wypadki na terenie instytucji i inne roszczenia. Na polskim rynku ta kategoria ryzyka nie jest jeszcze w praktyce zbyt istotna, jednak na świecie często przynosi poważne straty. Warto zauważyć, że akurat w tej kategorii straty operacyjne mogą dotyczyć zarówno instytucji finansowej, jak i każdej innej.

Przykład. W 2004 r. Morgan Stanley uzgodnił warunki ugody w sprawie zgłoszonej przez ponad 300 pracownic średniego i wyższego szczebla. Oskarżały one firmę o systematyczne niższe wynagradzanie kobiet i pomijanie przy ich awansie. W ramach ugody Morgan Stanley zapłacił im 54 mln USD.

Jako przykład spoza branży finansowej można wskazać Microsoft Corporation. W 1992 r. firma zatrudniła dużą grupę pracowników tymczasowych. Zostali oni wyłączeni z programu zakupu akcji firmy na preferencyjnych warunkach. W tej sytuacji 8.600 pracowników wniosło pozew sądowy w tej sprawie. W 2001 r. sprawa zakończyła się ugodą, według której Microsoft zapłacił im 97 mln USD.

Klienci, produkty i praktyka biznesowa

To jedna z najszerszych kategorii ryzyka operacyjnego. Najogólniej rzecz ujmując, w jej skład wchodzą wszelkie kwestie związane z niewłaściwą realizacją obowiązków wobec klientów, oraz z wadami produktów oferowanych przez bank. Kategoria ta obejmuje m.in.:

- Niewłaściwe działania wobec klientów, takie jak naruszenie zasad powiernictwa, wprowadzenie klienta w błąd, nieuczciwa reklama, zawarcie transakcji z klientem nieuprawnionym do danego rodzaju transakcji itp.

[14] Około 25 USD.

• Niewłaściwe praktyki biznesowe, takie jak niedozwolone manipulacje rynkiem finansowym, *insider trading* (na rachunek banku), działania bez zezwolenia czy pranie pieniędzy. W skład tej kategorii wchodzą również straty wynikające z niewłaściwej klasyfikacji klientów bądź z przekraczania limitów zaangażowania przypadających na poszczególnych klientów, a także straty wynikające z nieprzestrzegania zasad typu *Know Your Customer* (KYC). Warto podkreślić, że w ostatnich latach, kładzie się duży nacisk na zwalczanie prania brudnych pieniędzy oraz kwestie przeciwdziałanie finansowaniu terroryzmu, co spowodowało wzrost znaczenia KYC.

• Straty wynikające ze sporów o jakość usług doradczych świadczonych przez bank.

• Straty wynikające z wad produktów, np. błędów w umowach bądź błędów w wewnętrznych modelach bankowych.

Przykład. Duże straty operacyjne z tej kategorii poniosła spółka ubezpieczeniowa Prudential Insurance Company. Została ona pozwana do sądu przez 10,7 mln swoich klientów, którzy zarzucili agentom spółki niedozwoloną, agresywną sprzedaż. Według pozwu, agenci namówili klientów do zakupu polis, których ci nie potrzebowali. W 1995 r. doszło do ugody, w ramach której Prudential Insurance Company wypłacił klientom około 2 mld USD, częściowo w formie refundacji kosztów, a częściowo w postaci poprawy warunków obecnie wykupionych polis ubezpieczeniowych.

Jako inny przypadek można wymienić Merrill Lynch, który w maju 2002 r. uzgodnił warunki ugody z prokuratorem generalnym Nowego Jorku, Earlem Spitzerem. Firmie zarzucano, że jej analitycy sporządzali korzystniejsze opinie dotyczące niektórych akcji, kierując się przede wszystkim dochodami, jakie z ich sprzedaży miała uzyskiwać część inwestycyjna firmy. Merrill Lynch nie przyznał się do winy, ale zgodził się zapłacić 100 mln USD, z czego 48 mln dla Nowego Jorku, a pozostałe 52 mln dla poszczególnych stanów, oraz wprowadzić nową politykę podziału obowiązków wśród pracowników.

Kolejny przykład jest interesujący ze względu na wyraźne przenikanie się ryzyka rynkowego i operacyjnego. Są to głośne kłopoty funduszu hedgingowego Long Term Capital Management (LTCM). Fundusz ten jest dobrym przykładem tego, że w praktyce różne rodzaje ryzyka często są ze sobą ściśle powiązane. Bez wątpienia w LTCM wystąpiły poważne problemy z ryzykiem rynkowym, które łącznie spowodowały utratę płynności finansowej przez LTCM. Wyraźnie też widać, że źródłem wielu problemów LTCM było ryzyko operacyjne. Było ono widoczne na przykład w postaci lekceważenia w funduszu wyników pewnych stress-testów przyjętego modelu, które były niezgodne z oczekiwaniami kierujących. Jednak podstawowym problemem funduszu było wystąpienie ryzyka modelu, zaliczanego do ryzyka operacyjnego.

Fundusz LTCM zgromadził najlepszych na rynku specjalistów od rynku kapitałowego, w tym dwóch laureatów Nagrody Nobla, w celu stworzenia matematycznego modelu kształtowania się cen pewnych instrumentów. Uważali oni, że przygotowali model zapewniający funduszowi zyski przy praktycznie minimalnym ryzyku. Był on oparty na zajmowaniu przeciwstawnych pozycji w instrumentach, których ceny podlegały w dłuższym okresie bardzo silnej korelacji. Zajmowanie pozycji następowało w chwili, gdy jeden z instrumentów miał korzystną cenę. W długim okresie ceny obu tych instrumentów miały zmieniać się podobnie, a ponieważ jeden z nich został kupiony po korzystnej cenie, LTCM miał osiągać zyski przy bardzo małym ryzyku. Jednocześnie uzyskanie odpowiednio wysokich zysków wymagało zainwestowania bardzo dużych środków. LTCM uzyskał takie środki, lecz kosztem bardzo dużej dźwigni finansowej.

Przez kilka lat ta strategia przynosiła spodziewane efekty. Kryzys nadszedł w 1998 r. Rosja zawiesiła realizację swoich zobowiązań wynikających z wyemitowanych obligacji. Spowodowało to poniesienie przez LTCM strat, które jednak nie były na tyle duże, by stanowiły zagrożenie dla istnienia funduszu. O wiele gorsza była reakcja rynków światowych, które zaczęły uciekać w stronę bezpieczniejszych instrumentów, w szczególności obligacji amerykańskich. Z tego powodu korelacja między cenami najważniejszych aktywów LTCM, która wynosiła normalnie około 95%, spadła do około 80%. Do tego inwestorzy zaczęli domagać się zwrotu pieniędzy ulokowanych w LTCM. Fundusz, który miał bardzo wysoką dźwignię finansową, zaczął tracić płynność i został zmuszony do likwidacji swoich pozycji po bardzo niekorzystnych cenach.

Skomplikowany model matematyczny działał dobrze w normalnych warunkach rynkowych, ale nie był odpowiednio przygotowany na dużą zmianę korelacji cen aktywów i na problemy z płynnością. Taka sytuacja ujawniła poważne wady w jego konstrukcji, których rezultatem było poniesienie przez fundusz strat w wysokości około 4,4 mld USD. Upadku LTCM udało się uniknąć tylko dzięki pierwszemu w historii pakietowi ratunkowemu dla funduszu inwestycyjnego, przygotowanemu przez Bank Rezerwy Federalnej w Nowym Jorku, z udziałem największych banków i funduszy. Warto dodać, że LTCM jako fundusz hedgingowy nie był objęty nadzorem SEC.

Uszkodzenia aktywów

Kolejną kategorią ryzyka operacyjnego są uszkodzenia aktywów, wynikające przede wszystkim z klęsk żywiołowych, działalności terrorystycznej lub wandalizmu.

Przykład. Wszelkie klęski żywiołowe, takie jak huragany, powodzie czy trzęsienia ziemi wiążą się ze stratami należącymi do tej kategorii. Będą tu również uwzględnione straty poniesione przez instytucje w związku z atakami na World Trade Center 11 września 2001 r. Jako przykład można wskazać Bank of New York, który w wyniku tych ataków poniósł straty w wysokości około 140 mln USD.

Szczęśliwie w Polsce nie zdarzyło się nic, co można byłoby porównać z atakiem na WTC. Jednak rangę tej kategorii ryzyka operacyjnego obrazuje powódź z 1997 r. Zalanie między innymi Wrocławia i Opola spowodowało duże straty i przestoje w funkcjonowaniu wielu przedsiębiorstw, m.in. z sektora finansowego.

Warto zauważyć, że jest to specyficzny rodzaj ryzyka operacyjnego, bowiem bardzo trudno jest przeciwdziałać jego wystąpieniu. Działania podejmowane przez instytucje muszą być skoncentrowane na minimalizowaniu skutków tego rodzaju ryzyka. Dlatego istotne są plany ciągłości działania (Business Continuity Plan) i planów odzyskania sprawności (Disaster Recovery Plan), które w czasie normalnej pracy mogą być postrzegane jako niepotrzebny, biurokratyczny wymysł, ale w sytuacji awaryjnej mogą oznaczać obniżenie wysokości poniesionych strat o wiele milionów.

Zakłócenia działalności i błędy systemów

Kolejna kategoria ryzyka operacyjnego pokrywa przede wszystkim ryzyko technologiczne, związane z nieprawidłowym funkcjonowaniem lub awariami oprogramowania, sprzętu informatycznego i sieci komputerowych lub telekomunikacyjnych. Należy tu również wliczać straty związane z przerwami w dopływie energii elektrycznej.

Przykład. Zapewne każda instytucja ma większe lub mniejsze problemy z funkcjonowaniem szeroko pojętego sprzętu informatycznego. Jako przykład można wskazać problemy Sallie Mae, jednego z największych kredytodawców w zakresie kredytów studenckich na rynku amerykańskim. W kwietniu 2003 r. firma ujawniła, że w wyniku niewłaściwie działającego oprogramowania naliczyła zbyt niskie raty ponad 800 tysięcy udzielonych kredytów. W większości przypadków udało się odzyskać dodatkowe kwoty po ponownym naliczeniu rat, jednak w sumie, w ocenie samej firmy, wskutek tego błędu poniosła ona straty w wysokości około 8 mln USD.

Interesująca historia, która co prawda nie przyniosła żadnych strat, ale wyraźnie wykazała istotność ryzyka technologicznego, miała miejsce w 1996 r. i dotyczyła First National Bank of Chicago. W maju tego roku do kont 823 klientów banku, w wyniku błędu w działaniu oprogramowania, została dopisana kwota 924.844.208,32 USD. W sumie dodatkowe kwoty na kontach klientów wyniosły ponad 760 mld USD, czyli ponad 6 razy więcej niż suma aktywów banku. W tym przypadku bank szybko zorientował się w sytuacji i w ciągu kilku godzin naprawił błąd. Według oficjalnych informacji nie poniósł on strat w wyniku tej sytuacji.

Jako przykład mieszczący się na pograniczu oszustwa wewnętrznego i wadliwego działania oprogramowania można wskazać problemy UBS Paine Webber, spółki córki UBS. W 2002 r. jeden z administratorów systemu, niezadowolony z warunków pracy w firmie, złożył wypowiedzenie. Jednocześnie przygotował wirusa komputerowego, w postaci tzw. logicznej bomby, która uaktywniła się po jego odejściu z pracy. Bomba zaatakowała około 1.000 pracujących w sieci komputerów firmy, kasując na ich dyskach wiele plików. W wyniku tej sytuacji UBS Paine Webber poniósł straty w wysokości około 3 mln USD. Relatywnie niski poziom strat wynikał z szybkiej reakcji i odpowiednich zasad przygotowywania zapasowych kopii danych.

Dokonywanie transakcji, dostawa oraz zarządzanie procesami

To kolejna bardzo szeroka kategoria ryzyka. W jej skład wchodzą takie wydarzenia, jak:

– przyjęcie, rejestrowanie, wykonywanie, rozliczanie i obsługa transakcji,

– sprawozdawczość (np. sporządzenie raportu sprawozdawczego z błędnymi danymi),

– relacje z kontrahentami, dostawcami i podmiotami świadczącymi usługi outsourcingu,

– utrzymywanie pełnej dokumentacji klienta,

– zarządzanie rachunkami klientów (np. wprowadzenie błędnych danych bądź umożliwienie dostępu do rachunku nieuprawnionej osobie).

Przykład. Dla każdego banku można wskazać bardzo wiele przykładów tego typu strat. Z reguły jednak pojedyncza strata nie będzie zbyt duża. Interesującym przykładem bardzo dużych strat operacyjnych, mieszczących się na pograniczu tej kategorii (w zakresie sprawozdawczości) i kategorii oszustwa wewnętrznego, jest sprawa banku JP Morgan Chase. W połowie 2005 r. bank ten uzgodnił warunki ugody w procesie sądowym dotyczącym jego udziału w aferze Enronu. Akcjonariusze Enronu oskarżali go o niewłaściwe raportowanie o rodzaju produktów sprzedawanych Enronowi (chodziło o bardzo skomplikowane transakcje pozabilansowe, które faktycznie oznaczały udzielanie kredytów Enronowi, natomiast na potrzeby sprawozdawcze były raportowane jako zwykłe transakcje dealerskie). Według ustalonych warunków ugody JP Morgan zapłacił akcjonariuszom odszkodowania w wysokości 2,2 mld USD.

W tej kategorii mieszczą się również straty związane z ujawnieniem poufnych danych, np. danych o klientach instytucji. Przykładowo, do poważnego ujawnienia danych doszło w firmie ChoicePoint w 2005 r. ChoicePoint zajmuje się zbieraniem danych, które są następnie wykorzystywane przez różnego rodzaju uprawnione instytucje. W ciągu ponad roku, do lutego 2005 r., ChoicePoint udostępnił wiele informacji o ponad 145 tys. klientów osobom legitymującym się fałszywymi danymi i niemającym prawa do tych informacji. Doprowadziło to do 750 przypadków podszycia się przez oszustów pod inne osoby. Według samej firmy, w związku z przekazaniem danych poniosła ona ponad 11 mln USD strat – częściowo w związku z koniecznością wzmożonej komunikacji z klientami, których dane zostały przekazane, oraz z monitorowaniem tej sprawy, a częściowo w związku ze zwiększonymi kosztami prawnymi. Dodatkowo wewnętrzne zmiany, mające ustrzec firmę przed ponownym wystąpieniem takiej sytuacji, mają kosztować około 15–20 mln USD.

Liczba strat operacyjnych

Z powyższych przykładów widać więc, jak wielkie mogą być straty operacyjne. W niektórych przypadkach stają się wręcz przyczyną upadku danej instytucji. Pozostaje jednak pytanie, jak często występują tego typu straty. Tutaj dostępne dane są raczej skąpe. W latach 1993–2003 w instytucjach finansowych miało miejsce ponad 100 strat operacyjnych, przekraczających 100 mln USD (de Fontnouvelle et al. 2003). Liczba mniejszych strat rośnie wykładniczo. Na przykład jeden z producentów oprogramowania wspierającego proces zarządzania ryzykiem operacyjnym podaje, że w swojej bazie ma ponad 10 tysięcy publicznie znanych danych o stratach operacyjnych przekraczających milion dolarów[15].

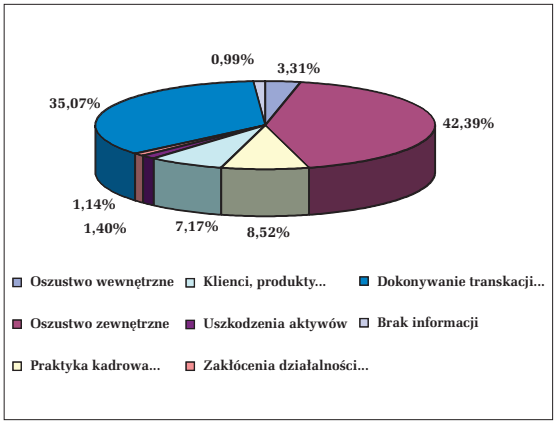
Najszersze informacje na temat wielkości strat operacyjnych można uzyskać z badań Bazylejskiego Komitetu Nadzoru Bankowego, który w 2003 r. opublikował wyniki ankiety dotyczącej strat operacyjnych, przeprowadzonej na potrzeby przygotowywanej Nowej Umowy Kapitałowej (Bazylejski Komitet Nadzoru Bankowego 2003a). Zgodnie z danymi uzyskanymi przez Komitet od 89 banków w 2001 r. zarejestrowały one 47.269 strat operacyjnych przekraczających 10 tys. euro[16]. Oznacza to, że średnio na każdy z nich przypada 528 strat operacyjnych w ciągu zaledwie jednego roku. Wśród tych strat około 2% to straty przekraczające 1 mln USD. Procentowo jest to niewielka liczba, jednak oznacza to, że średnio każdy z banków biorących udział w ankiecie poniósł w 2001 r. ponad 10 strat operacyjnych, przewyższających milion USD. Według danych banków uczestniczących w ankiecie poniosły one straty operacyjne na łączną sumę 7,8 mld euro, czyli na każdy bank przypada średnio 14 mln euro w ciągu tego jednego roku.

Warto również zauważyć, że prawdopodobnie wskazane tu liczby stanowią jedynie część strat operacyjnych, które faktycznie wystąpiły w instytucjach finansowych. Wynika to z dwóch czynników. Banki mogą ukrywać pewne zdarzenia, których upublicznienie naraziłoby je na ryzyko utraty reputacji. Kolejnym czynnikiem są problemy z gromadzeniem danych przez banki. W czasie badania prowadzonego przez Komitet Bazylejski odzwierciedleniem tych czynników był bardzo nierównomierny rozkład zdarzeń operacyjnych przypadających na poszczególne linie biznesowe oraz kategorie zdarzeń. Oczywiście można się spodziewać pewnej nierównomierności. Na przykład naturalne jest, że straty operacyjne związane z bankowością detaliczną będą niewielkie, jeśli chodzi o wielkość pojedynczej straty, natomiast będzie ich dużo. Równocześnie bardzo duże zróżnicowanie wielkości i liczby zdarzeń, zarówno w obrębie pojedynczego banku, jak i pomiędzy różnymi bankami, świadczy jednak o brakach w danych (zobacz również de Fontnouvelle et al. 2003).

Analiza Komitetu Bazylejskiego jest interesująca, jeśli chodzi o liczbę zidentyfikowanych strat operacyjnych w poszczególnych kategoriach.

Widać wyraźnie, że spośród ponad 47 tys. zidentyfikowanych strat prawie 80% dotyczy dwóch kategorii: oszustwo zewnętrzne i dokonywanie transakcji, dostawa oraz zarządzanie procesami. Z kolei w kate-

Wykres 1 *Liczba strat operacyjnych w bankach wg danych Komitetu Bazylejskiego*



Źródło: Bazylejski Komitet Nadzoru Bankowego (2003a).

[15] Zobacz http://www.sas.com/industry/fsi/oprisk/brochure.pdf, oficjalna strona internetowa SAS Institute.

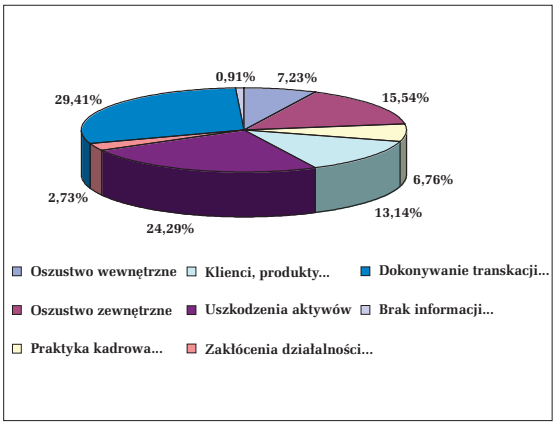
[16] Komitet Bazylejski wskazał 10 tys. euro jako minimalną wielkość strat operacyjnych, które należy zgłaszać na potrzeby badania. Jednocześnie 12 banków, spośród 89, zgłosiło jedynie straty powyżej większej kwoty, a kolejne 2 – powyżej 10 tysięcy dla niektórych linii biznesowych i powyżej większej kwoty dla innych linii. Dodatkowo 5 banków zgłaszało niektóre straty niższe niż 10 tysięcy euro. W praktyce oznacza to, że przy rygorystycznym przestrzeganiu zasad badania zarówno wartość, jak i liczba strat byłyby większe, niż faktycznie zgłoszono.

gorii oszustwa zewnętrzne prawie 90% zidentyfikowanych zdarzeń wiąże się z bankowością detaliczną. Po analizie dokładniejszych danych widać, że są to straty związane z oszustwami oraz kradzieżami. Prawdopodobnie są to drobne oszustwa dokonywane przez klientów detalicznych banku. W zakresie kategorii „dokonywanie transakcji, dostawa oraz zarządzanie procesami" większość strat jest związanych z wprowadzaniem do systemu, wykonywaniem, rozliczaniem i obsługą transakcji. Można więc sądzić, że są to głównie błędy ludzkie bądź systemowe, które zostały zakwalifikowane do tej kategorii.

W ramach analizy przeprowadzonej dla Komitetu Bazylejskiego poproszono banki również o określenie wartości strat operacyjnych poniesionych w 2001 r. W sumie 89 badanych banków wskazało w tym okresie straty operacyjne w wielkości 7,8 mld euro. Rozkład strat przedstawiony przez banki zilustrowano na wykresie 2.

Można zaobserwować, że liczba strat operacyjnych z danej kategorii nie wiąże się bezpośrednio z ich wielkością. Wydarzenia z kategorii oszustwo zewnętrzne, które stanowią ilościowo ponad 42% wszystkich zidentyfikowanych przypadków strat operacyjnych, pod względem wartości przynoszą bankom średnio jedynie 15,5% wszystkich strat. Podobnie, choć w mniejszym stopniu, wygląda sytuacja ze stratami z kategorii „dokonywanie transakcji, dostawa oraz zarządzanie procesami". W ujęciu ilościowym stanowiły one ponad 35% ogółu strat, natomiast były przyczyną jedynie 29% strat w ujęciu wartościowym. Z drugiej strony uszkodzenia aktywów, które zdarzają się rzadko (1,4% wszystkich strat), powodują jednocześnie bardzo duże straty, w ujęciu wartościowym stanowiące ponad 24% ogółu. Oczywiście powstaje pytanie, na ile rezultaty tego badania są reprezentatywne dla ogółu banków światowych w dłuższym okresie. Trzeba bowiem pamiętać, że badanie było przeprowadzone na relatywnie niewielkiej próbie 89 banków, głównie dużych, i dotyczyło jedynie strat z 2001 r. W tej sytuacji straty poniesione przez niektóre instytucje w atakach na World Trade Center miały zapewne poważny wpływ na wielkość strat z tej kategorii.

Wykres 2 *Wielkość strat operacyjnych w bankach wg danych Komitetu Bazylejskiego*



Źródło: Bazylejski Komitet Nadzoru Bankowego (2003a).

Nie jest jasne, jak kształtują się straty operacyjne w mniejszych, „lokalnych" instytucjach. Między dużymi a małymi bankami widać jednak zdecydowane różnice w sposobie podchodzenia do zarządzania ryzykiem operacyjnym. W dużych, międzynarodowych instytucjach ryzyko operacyjne jest formalnie identyfikowane, mierzone i zarządza się nim za pomocą zaawansowanych metod. W małych bankach w tym zakresie często pozostaje jeszcze dużo do zrobienia. Wydaje się, że największy wpływ na taką sytuację ma wciąż niewystarczająca świadomość istotności ryzyka operacyjnego w mniejszych instytucjach. Innym ważnym czynnikiem jest prawdopodobnie zbyt mała liczba ekspertów zajmujących się tą dziedziną. Ponadto wiele banków mylnie uważa, że system zarządzania ryzykiem operacyjnym wiąże się z tak dużymi kosztami, że przewyższają one korzyści płynące z jego wprowadzenia. Można jednak sądzić, że również w mniejszych instytucjach sytuacja w zakresie ryzyka operacyjnego będzie się poprawiała, głównie w wyniku rosnącej presji regulacyjnej.

Podsumowanie

W celu efektywnego zarządzania ryzykiem operacyjnym niezbędne są narzędzia, umożliwiające działania w dwóch dziedzinach. Po pierwsze, konieczna jest możliwość wyliczenia poziomu ryzyka w danym procesie, a po drugie – możliwość realnego oddziaływania na jego wielkość. W idealnej sytuacji powinniśmy mieć narzędzia, które umożliwią obniżenie ryzyka operacyjnego do konkretnego, akceptowalnego przez nas poziomu. Jeśli to nie jest możliwe, powinniśmy mieć chociaż przekonanie, że stosowane przez nas narzędzia są właściwe do obniżenia ryzyka operacyjnego w danej kategorii.

Przedstawiona powyżej klasyfikacja ryzyka wyraźnie wskazuje na bardzo dużą różnorodność zdarzeń generujących ryzyko operacyjne. Do redukcji ryzyka w różnych dziedzinach potrzebne będą różne narzędzia. W tej sytuacji umiejętność prawidłowego rozumienia, rozróżniania i klasyfikowania strat jest warunkiem koniecznym właściwego funkcjonowania procesu zarządzania ryzykiem. Właściwa klasyfikacja zdarzeń musi łączyć dwa elementy – mieścić się w ramach wskazanych przez nadzór, a jednocześnie być efektywnym narzędziem zarządzania ryzykiem operacyjnym. W przeciwnym razie

istnieje niebezpieczeństwo, że podejmowane próby redukcji ryzyka będą nieskuteczne, ze względu na niewłaściwość zastosowanych w tym celu środków. To z kolei będzie powodowało nadmierne koszty zarządzania ryzykiem operacyjnym, a jednocześnie faktyczny brak jego istotnej redukcji. Prawidłowa kategoryzacja poszczególnych zdarzeń operacyjnych nie jest prostym zadaniem. Wydaje się jednak, że powszechnie przyjęte w tym zakresie kategorie ryzyka, które zostały szeroko opisane powyżej, umożliwiają właściwe funkcjonowanie tego procesu i w konsekwencji stworzenie dobrych podstaw efektywnego zarządzania ryzykiem operacyjnym w instytucji.

Bibliografia

Bank of England (1995), *Report of the Board of Banking Supervision Inquiry into the Circumstances of the Collapse of Barings*, Bank of England, Londyn.

Bazylejski Komitet Nadzoru Bankowego (1998), *Operational Risk Managemen*t, Bank for International Settlements, Bazylea.

Bazylejski Komitet Nadzoru Bankowego (2003a), *Operational Risk Loss Data Collection Exercise 2002: Summary of Data Collected*, Bank for International Settlements, Bazylea.

Bazylejski Komitet Nadzoru Bankowego (2003b), *Sound Practices for the Management and Supervision of Operational Risk*, Bank for International Settlements, Bazylea.

Bazylejski Komitet Nadzoru Bankowego (2006), *International Convergence of Capital Measurement and Capital Standards: A Revised Framework Comprehensive Version*, Bank for International Settlements, Bazylea.

Davies J., Ong M., Wilmot J., Mark B., Hoffman D., Belton A., Williams L. (1999), *Round Table: The struggle to define and measure goes on*, "Risk", No. 7/1999, Operational Risk Supplement, za http://www.financewise.com/public/edit/riskm/oprisk/opr-rt.htm

de Fontnouvelle P., DeJesus – Rueff V., Jordan J., Rosengren E. (2003), *Capital and Risk: New Evidence on Implications of Large Operational Losses*, Federal Reserve Bank of Boston, Boston.

Generalny Inspektorat Nadzoru Bankowego (2005), *Dokument Konsultacyjny DK/04/OPR, dotyczący metod prostych wyliczania wymogów kapitałowych z tytułu ryzyka operacyjnego*, GINB, Warszawa.

Generalny Inspektorat Nadzoru Bankowego (2006), *Dokument Konsultacyjny DK/9/Walidacja, dotyczący walidacji zaawansowanych metod wyliczania wymogów kapitałowych z tytułu ryzyka kredytowego i operacyjnego*, GINB, Warszawa.

King J. (1998), *Defining operational risk*, "ALGO Research Quarterly", Vol 1, No. 2, s. 37-42.

Komisja Nadzoru Bankowego (2004), *Rekomendacja M dotycząca zarządzania ryzykiem operacyjnym w bankach*, KNB, Warszawa,

Kongres USA (2002) *Sarbanes – Oxley Act of 2002*, H.R. 3763, Kongres USA, Waszyngton.

Parlament Europejski (2006a), *Directive 2006/48/EC of the European Parliament and of the Council of 14 June 2006 relating to the taking up and pursuit of the business of credit institutions*, Urzędowy Dziennik Unii Europejskiej, Bruksela.

Parlament Europejski (2006b), *Directive 2006/49/EC of the European Parliament and of the Council of 14 June 2006 on the capital adequacy of investment firms and credit institutions*, Urzędowy Dziennik Unii Europejskiej, Bruksela.