Ryzyko operacyjne na rynku instrumentów pochodnych – podział i metody jego minimalizacji

Agnieszka Wojtasiak

W ostatnim dziesięcioleciu ubiegłego stulecia znaczącą część katastrof finansowych związanych z instrumentami pochodnymi stanowiły katastrofy spowodowane ryzykiem operacyjnym. Na skutek ryzyka operacyjnego znaczące straty finansowe poniosły m.in. takie instytucje, jak: Barings Bank, Daiwa Bank, Procter&Gumble[1]. Zdarzenia te przyczyniły się do wzrostu znaczenia ryzyka operacyjnego wśród innych rodzajów ryzyka, na jakie narażone są podmioty działające na rynku instrumentów pochodnych.

Pojęcie ryzyka operacyjnego

Pierwsze kompleksowe analizy dotyczące ryzyka operacyjnego przypadają na wczesne lata 90., były one prowadzone przez Bankers Trust (1992 r.). We wrześniu 1998 r. Bazylejski Komitet ds. Nadzoru Bankowego opracował dokument dotyczący zarządzania ryzykiem operacyjnym (*White Paper on Operational Risk Management*), natomiast w styczniu 2001 r. Komitet Bazylejski wydał propozycję Nowej Umowy Kapitałowej, dotyczącą wymagań kapitałowych (The New Basle Capital Accord) na pokrycie różnego rodzaju ryzyka, w tym ryzyka operacyjnego. Przewiduje się, że propozycja ta wejdzie w życie w 2004 r.

Ryzyko operacyjne jest definiowane jako:

„Ryzyko, na które składają się:

– ryzyko aktywów będących środkami trwałymi – polega na uszkodzeniu lub stracie środka trwałego mającego wpływ na funkcjonowanie instytucji,

– ryzyko technologii – ryzyko spowodowane niesprawnością systemów, złą jakością danych, błędami w oprogramowaniu,

– ryzyko interakcji – ryzyko powstające w wyniku współpracy instytucji z podmiotami w otoczeniu, np. problemy z dostawcami, odbiorcami (klientami),

– ryzyko zasobów ludzkich – cele instytucji nie są osiągane na skutek niewłaściwej polityki personalnej dotyczącej np. systemu motywacji, podziału odpowiedzialności lub na skutek oszustw dokonywanych przez pracowników”[2].

Jedna z definicji przedstawionych przez Komitet Bazylejski pozwala na rozumienie ryzyka operacyjnego jako:

„Ryzyko bezpośredniej lub pośredniej straty wynikającej z niewłaściwych lub zawodnych procesów wewnętrznych, ludzi i systemów lub też ze zdarzeń zewnętrznych”[3].

[1] Na podstawie: R. Schwartz, C. Smith: *Derivatives handbook: risk management and control*. JohnWiley&Sons, New York 1997 s. 39–54.

[2] Na podstawie: J. Jakóbczak: *Rosnące znaczenie zarządzania ryzykiem operacyjnym*. Materiały z konferencji: Innowacje na rynkach finansowych, Warszawa 2001, P. Antal: Swiss Re New Market 2001.

[3] Basle Committee on Banking Supervision, Consultative Document, Supporting Document to the Basle Capital Accord. Basle, January 2001.

Definicje te obejmują ryzyko związane z poziomem wiedzy i odpowiedzialnością zarządzających, jakością dokumentacji, spójnością, przejrzystością i przestrzeganiem procedur operacyjnych.

Wielu autorów mianem ryzyka operacyjnego określa wszelkie ryzyko niezwiązane bezpośrednio ze zmiennością rynku bądź zdolnością kredytową partnerów. Komitet Bazylejski, obok definicji podanej powyżej, również przyjmuje właśnie takie rozumienie ryzyka operacyjnego. W tym kontekście podawana definicja brzmi następująco:

„Jakikolwiek rodzaj ryzyka niedający się zakwalifikować jako ryzyko rynkowe lub kredytowe"[4].

Podział ryzyka operacyjnego

Ze względu na charakter zagrożeń ryzyko operacyjne dzieli się na cztery zasadnicze klasy:

a) ryzyko relacji z otoczeniem – ryzyko to wiąże się m.in. z utratą reputacji przez daną instytucję, czyli z możliwością wystąpienia sytuacji, w której negatywna opinia na temat instytucji (prawdziwa lub nie) spowoduje utratę zaufania klientów, redukcję zysków lub obniżenie płynności,

b) ryzyko kadrowe – źródłem tego rodzaju ryzyka są celowe lub niezamierzone działania pracowników na szkodę pracodawcy,

c) ryzyko technologiczne – ryzyko to wiąże się z wadliwymi rozwiązaniami technologicznymi dotyczącymi dokonywanych transakcji[5],

d) operacyjne ryzyko dokumentacji – związane jest z prowadzeniem i przechowywaniem dokumentacji.

Na podstawie przedstawionych powyżej definicji oraz podziału ryzyka operacyjnego można przyjąć, że ryzyko operacyjne jest to ryzyko wynikające ze źródeł zarówno wewnętrznych, jak i zewnętrznych w stosunku do danej instytucji, spowodowane niesprawnością systemów, celowymi lub niezamierzonymi błędami w działaniach ludzkich, odnoszącymi się zarówno bezpośrednio, jak i pośrednio do transakcji dokonywanych w instytucji. Przyczyną tego ryzyka są także relacje z otoczeniem.

W związku z faktem, że ryzyko operacyjne w takim samym stopniu odnosi się do opcji, kontraktów terminowych i kontraktów *swap*, zostanie ono rozpatrzone ogólnie dla wszystkich tych instrumentów. Opis będzie dokonany zgodnie z powyższym podziałem ryzyka operacyjnego.

[4] Basle Committee on Banking Supervision, Sound Practices for the Management and Supervision of Operational Risk. Bank for International Settlements, Basle, December 2001.

[5] Na podstawie: L. Sołtysik: *Ryzyko operacyjne – nowe wyzwania*. „Rynek Terminowy" nr 1/2001, s. 68.

Ryzyko operacyjne na rynku instrumentów pochodnych

Ryzyko relacji z otoczeniem

Ryzyko relacji z otoczeniem wiąże się z utratą zaufania klientów do instytucji oferujących instrumenty pochodne. Może być to związane ze skargami, procesami sądowymi prowadzonymi przeciw danej firmie, o których dowiadują się jej klienci. Reputację firmy kształtują także media. Informacje prasowe mogą w znacznym stopniu zaszkodzić postrzeganiu jej przez klientów.

Ryzyko relacji z otoczeniem wiąże się również z możliwością wystąpienia błędów operacyjnych na skutek nieprzestrzegania regulacji, zewnętrznych w stosunku do danej instytucji, dotyczących działalności na rynku instrumentów pochodnych.

Ryzyko kadrowe[6]

Ryzyko kadrowe wiąże się z zaniedbaniami osób odpowiedzialnych za pracę działu dokonującego transakcji instrumentami pochodnymi lub bezpośrednio z błędami osób dokonujących tych transakcji. Zarówno oszustwa, jak i niecelowe działania na szkodę instytucji dotyczą m.in. błędnego wprowadzania danych, zagubienia umów, niewprowadzania bieżących danych, niekontrolowania dopuszczalnych limitów prowadzonych transakcji na rynku instrumentów pochodnych, błędów natury rachunkowej. Wymienione błędy mogą być popełniane przez wykwalifikowanych pracowników, jednak liczba błędów niecelowych jest zdecydowanie większa wśród kadry, której brakuje kwalifikacji do wykonywania określonych operacji. Firmy, które mają problemy z pozyskaniem wykwalifikowanej kadry, są więc narażone na większe ryzyko operacyjne.

Ryzyko związane z brakiem wiedzy i doświadczenia w zawieraniu transakcji na rynku instrumentów pochodnych pojawia się przede wszystkim na rynkach rozwijających się.

Przyczyną ryzyka operacyjnego na poziomie kadrowym jest także niewłaściwe zarządzanie ryzykiem, na co składa się m.in.: brak środków monitorowania ryzyka, brak określonych limitów zaangażowania, niewłaściwa praktyka zatrudnienia, struktura organizacyjna i zarządzania oraz błędnie kształtowana kultura organizacyjna. Nieodpowiednie ujęcie w strukturze organizacyjnej jednostki sprawującej nadzór nad komórkami dokonującymi transakcji instrumentami pochodnymi powoduje, że nadzór ten jest niedostateczny lub spełniany przez niewłaściwe jednostki organizacyjne. Często popełnianym błędem jest powierzenie jednej

[6] Na podstawie: R. Schwartz, C. Smith: *Derivatives handbook: risk management and control*. New York 1997 JohnWiley&Sons, s. 39–54.

osobie odpowiedzialności za dokonywanie transakcji, ich ewidencjonowanie i rozliczanie. Niewłaściwa polityka kadrowa prowadzi więc do błędnego podziału pracy i odpowiedzialności. Całkowity brak nadzoru, powierzenie jednej osobie odpowiedzialności za ewidencjonowanie i rozliczanie transakcji były przyczyną upadku Banku Barings w 1995 r.

Ryzyko technologiczne

Ryzyko technologiczne wiąże się z wadliwymi rozwiązaniami technologicznymi dotyczącymi transakcji dokonywanych na rynku instrumentów pochodnych. Mogą one dotyczyć:

– nieprawidłowości w działaniu systemów i wyborze modeli wyceny instrumentów pochodnych (błędy oprogramowania, brak aktualnych danych do modelu, nieefektywne przetwarzanie danych, słaba ochrona danych);

– błędów w kanałach komunikacyjnych (niesprawność systemów informatycznych i komunikacyjnych, brak możliwości uzyskania istotnych informacji lub uzyskiwanie błędnych informacji, opóźnienia w dostarczaniu informacji, brak integracji systemu);

– niewłaściwego wyposażenia do dokonywanych transakcji na rynku instrumentów pochodnych (niedostosowanie wyposażenia do potrzeb instytucji);

– problemów z dostawą kluczowych usług (np. prąd, telekomunikacja)[7].

Operacyjne ryzyko dokumentacji

Ryzyko w tym kontekście dotyczy przechowywania dokumentacji w niewłaściwym miejscu, możliwości dostępu do dokumentacji osób niepowołanych, dokumentowania operacji w niewłaściwy sposób.

Minimalizacja ryzyka operacyjnego

Zarządzanie ryzykiem operacyjnym jest realizowane zarówno wewnątrz instytucji, jak i poprzez jej interakcje z otoczeniem. Składają się na nie opisane poniżej metody.

System kontroli wewnętrznej i regulacji wewnątrz organizacji

System kontroli wewnętrznej ma na celu:

a) stworzenie metod, narzędzi i procedur do analizy i kontroli ryzyka operacyjnego,

b) minimalizację błędów popełnianych przez człowieka,

c) zarządzanie ryzykiem dokumentacji.

Stworzenie metod, narzędzi i procedur do analizy i kontroli ryzyka operacyjnego

Poniżej opisano tworzenie metod oraz dobór narzędzi do analizy i kontroli ryzyka operacyjnego.

1. Wybór metody analizy ryzyka operacyjnego

W celu właściwego oszacowania i monitorowania ryzyka operacyjnego należy ustalić sposób jego analizy. Analiza ryzyka operacyjnego polega na badaniu związków między kapitałem, jego zagrożeniami i wrażliwością badanej instytucji na to ryzyko a możliwymi zabezpieczeniami. Jej celem jest określenie poziomu istniejącego ryzyka oraz możliwości jego zredukowania za pomocą dostępnych zabezpieczeń.

Wśród praktyków istnieją dwa zasadnicze podejścia do analizy ryzyka operacyjnego: *top-down*, *bottom-up*. W podejściu *top-down* przyjmuje się za punkt wyjścia faktyczne lub hipotetyczne zdarzenia powodujące stratę finansową. Poprzez analizę owych zdarzeń i wewnętrznych zabezpieczeń można określić prawdopodobieństwo i wielkość potencjalnych strat. W podejściu tym zakłada się, że ryzyko operacyjne jest większe na tych obszarach, gdzie występuje więcej aktywów narażonych na ryzyko. Podejście *bottom-up* koncentruje się na źródłach ryzyka. Źródłem tym jest korelacja między działaniem ludzi, technologii i procedur w organizacji (wrażliwość i zabezpieczenia) a określonymi zdarzeniami wewnętrznymi i zewnętrznymi. Instytucja zostaje podzielona zgodnie z obszarami działalności. Następnie w każdym z obszarów jest mierzone ryzyko, które w ostatnim etapie jest sumowane dla całej instytucji[8].

2. Wybór modeli matematycznych i statystycznych

Wewnętrzne zarządzanie ryzykiem operacyjnym obejmuje wybór modeli matematycznych i statystycznych do pomiaru i zarządzania ryzykiem. Wskazane jest także porównywanie wyników dostępnych z różnych systemów w ramach organizacji. Przykładem może być estymacja spodziewanych wyników dokonywana przez *back office* i porównywana ze stratami i przychodami oczekiwanymi przez *middle office*.

3. Kontrola systemów

Kontroli powinna podlegać sprawność i aktualność systemów: gromadzenia danych, przetwarzania danych, rozliczania transakcji i tworzenia raportów z transakcji. Należy tu zwrócić uwagę na: scentralizowany charakter bazy danych, możliwości wykorzystania danego systemu, zintegrowany charakter danego systemu, pozwalający na całościowe ujęcie wartości strat lub przychodów towarzyszących operacjom w danej instytucji, przystosowanie operacji do zmiennych warunków rynkowych.

[7] Na podstawie: L. Sołtysik: *Ryzyko operacyjne – nowe wyzwania*, op.cit., s. 68.

[8] Tamże, s. 68.

4. Ustalenie i monitorowanie przestrzegania przedziałów transakcji

Narzędziem kontroli ryzyka jest ustalanie i monitorowanie przestrzegania dopuszczalnych przedziałów wartości transakcji. Mając określone kluczowe parametry danych transakcji, można określić limity tolerancji danego parametru. Przekroczenie owego limitu powinno wywołać reakcję. Systemy ustalonych przedziałów tolerancji pozwalają także na obserwacje zdarzeń odbiegających od wartości oczekiwanych.

Minimalizacja błędów popełnianych przez pracowników

W związku z faktem, że błędy popełniane przez człowieka – zarówno celowe, jak i niecelowe – są częstą przyczyną strat, niezwykle istotne jest zarządzanie ryzykiem związanym z zasobami ludzkimi. Służy temu podział zadań i odpowiedzialności za dokonywane transakcje i wyraźne oddzielenie *front office* od *back office*. Osoby, które są odpowiedzialne za dokonywane transakcje, nie mogą odpowiadać za ich ewidencjonowanie i rozliczanie. Ważnym elementem minimalizacji ryzyka operacyjnego na poziomie kadrowym są także szkolenia pracowników.

Zarządzanie ryzykiem dokumentacji

Z procedurami zabezpieczania danych nierozerwalnie wiąże się kwestia miejsca ich przechowywania. Kopie danych są przekazywane do innych miejsc w danym kraju lub innych rejonów geograficznych. Instytucje, które nie mogą sobie pozwolić na przerwy w działalności, wynajmują pomieszczenia, do których będzie przeniesiona siedziba w sytuacji zagrożenia. Częstym błędem przy transakcjach instrumentami pochodnymi jest nieudokumentowanie w formie pisemnej warunków ustalonych ustnie. Niejednokrotnie upływa sporo czasu między zawarciem ustnej umowy a podpisaniem jej przez strony transakcji. Z powodu tego opóźnienia jedna ze stron może odmówić pokrycia należności powstałych w tym okresie. Dlatego wszelkie uzgodnienia ustne powinny być natychmiast udokumentowane w formie pisemnej.

System kontroli zewnętrznej

Zarządzanie ryzykiem operacyjnym opiera się także na zachowywaniu właściwych relacji z otoczeniem. Polega to przede wszystkim na dostosowywaniu się do regulacji związanych z ryzykiem operacyjnym.

Dostosowywanie do wymogów międzynarodowych odnosi się do wzorowania działalności na ustalonych rekomendacjach międzynarodowych w zakresie kontroli, pomiaru, zapobiegania ryzyku (np.: Group of Thirty Recommendations). Najnowsze międzynarodowe standardy dotyczące ryzyka operacyjnego zostały zawarte w dyrektywach Komitetu Bazylejskiego. Są to: obowiązujący dokument Operational Risk Management (September 1998) oraz dokumenty konsultacyjne: Operational Risk (January 2001) oraz Sound Practices for the Management and Supervision of Operational Risk (December 2001).

*

Powyższe rozważania dowodzą, że ryzyko operacyjne na rynku instrumentów pochodnych odnosi się do bardzo odmiennych obszarów. Jego źródeł należy poszukiwać zarówno w nieprawidłowym działaniu systemów, relacjach z otoczeniem, jak i w błędach popełnianych przez człowieka. W związku z tym metody jego minimalizacji powinny zapewnić możliwość analizy i kontroli przez instytucję każdego ze źródeł ryzyka

Literatura

1. Group of Thirty, Derivatives: Practices and Principles, Global Derivatives Study Group.
2. R. Kendall: *Zarządzanie ryzykiem dla menedżerów*. Warszawa 2000 LIBER.
3. J. Jakóbczak: *Rosnące znaczenie zarządzania ryzykiem operacyjnym*. Materiały z konferencji: *Innowacje na rynkach finansowych*, Warszawa 2001.
4. Basle Committee on Banking Supervision, Operational Risk Management. Basle, September 1998.
5. Basle Committee on Banking Supervision, Consultative Document, Supporting Document to the Basle Capital Accord. Basle, January 2001.
6. Basle Committee on Banking Supervision, Sound Practices for the Management and Supervision of Operational Risk. Bank for International Settlements, Basle, December 2001.
7. L. Sołtysik: *Ryzyko operacyjne – nowe wyzwania.* „Rynek Terminowy" nr 1/2001.
8. R. Schwartz, C. Smith: *Derivatives handbook: risk management and control*, JohnWiley&Sons, New York 1997.
9. H. Riehl: *Managing risk in the foreign exchange, money and derivatives markets*. New York 1998 McGraw Hill.