Komisja Nadzoru Bankowego

Rekomendacja M

dotycząca zarządzania ryzykiem operacyjnym w bankach

Warszawa, 2004 r.

I. WSTĘP

1. Uwagi ogólne

Niniejsza rekomendacja wydana jest na podstawie art. 137 pkt 5 ustawy – Prawo bankowe i stanowi zbiór zasad dobrej praktyki w zakresie ostrożnego i stabilnego zarządzania ryzykiem operacyjnym w banku.
Zapisy Rekomendacji oparte zostały na opracowanym przez Komitet Bazylejski ds. nadzoru Bankowego i ogłoszonym w lutym 2003 r. tekście Zasad Dobrej Praktyki W Zakresie Zarządzania I Nadzoru Nad Ryzykiem Operacyjnym.
Ryzyko operacyjne, ze względu na swój kompleksowy charakter może mieć znaczący wpływ na działalność i kondycję banków, zwłaszcza, że obok otoczenia oraz zdarzeń zewnętrznych, jego źródłem jest organizacja bankowa sama w sobie. Rozwój technologii, powstawanie coraz bardziej złożonych technik i produktów bankowych oraz seria spektakularnych strat w międzynarodowych instytucjach finansowych skierowały uwagę regulatorów i menadżerów bankowych na znaczenie ryzyka o charakterze niefinansowym. Z analiz upadłości firm wynika, iż rzeczywiste powody znaczących strat miały podłoże operacyjne, chociaż wydawało się początkowo, iż straty te powstały w wyniku ryzyka kredytowego lub rynkowego. Znaczenie wpływu ryzyka operacyjnego na działalność bankową wzrosło także ze względu na rozwój automatyzacji i technologii informatycznych, powstanie bankowości elektronicznej, łączenie firm i integrację systemów zarządzania, rozwój outsourcingu, intensyfikację rozliczeń międzybankowych, kradzieże i oszustwa, kataklizmy, terroryzm etc. Nie bez znaczenia jest także coraz większa złożoność organizacji, jakimi są współczesne banki. Jednym z ważniejszych czynników ryzyka operacyjnego jest właśnie złożoność organizacji, stosowanych systemów oraz oferowanych produktów i usług.

Koncepcja zarządzania ryzykiem operacyjnym nie jest nowa - zawsze duże znaczenie dla banków miały takie elementy systemu zarządzania ryzykiem operacyjnym jak zapobieganie nadużyciom, redukcja błędów transakcyjnych czy też rozwój kontroli wewnętrznej. Jednakże relatywnie nowe jest podejście do zarządzania tym rodzajem ryzyka, jako zintegrowanego procesu porównywalnego z zarządzaniem ryzykiem finansowym, takim jak ryzyko rynkowe lub kredytowe.

Rosnąca świadomość ryzyka operacyjnego stanowi podstawę do wypracowania mechanizmów zarządzania tym ryzykiem w bankach i to nie tylko w poszczególnych komórkach operacyjnych, ale także zintegrowanego podejścia do tego ryzyka w skali całego banku.

2. Zakres

Dla potrzeb niniejszej rekomendacji, przyjmuje się za Bazylejskim Komitetem ds. Nadzoru Bankowego, że **ryzyko operacyjne należy rozumieć jako ryzyko straty wynikającej z niedostosowania lub zawodności wewnętrznych procesów, ludzi i systemów technicznych lub ze zdarzeń zewnętrznych.** W zakres ryzyka operacyjnego wchodzi ryzyko prawne, natomiast wyłącza się z niego ryzyko reputacji i strategiczne.

Zgodnie z rekomendacjami Komitetu Bazylejskiego, dla celów identyfikacji ryzyka operacyjnego i zarządzania tym ryzykiem, wyróżnia się w działalności banku osiem linii biznesowych:

- finansowanie przedsiębiorstw (Corporate Finance),
- sprzedaż i operacje spekulacyjne (Trading and Sales),
- bankowość detaliczna (Retail Banking),
- bankowość komercyjna (Commercial Bankimg),
- płatności i rozliczenia (Payment and Settlement),
- usługi pośrednictwa (Agency Services),
- zarządzanie aktywami na zlecenie (Asset Management),
- brokerskie usługi detaliczne (Retail Brokerage).

Wymieniona Rekomendacja definiuje i systematyzuje również kategorie zdarzeń operacyjnych (zdarzeń związanych z działalnością banku, które mogą skutkować wystąpieniem strat finansowych) na trzech poziomach szczegółowości:

Poziom 1 - podział zdarzeń operacyjnych na 7 głównych kategorii.
Poziom 2 - rodzaje zdarzeń w ramach kategorii
Poziom 3 - przykłady zdarzeń operacyjnych.

Systematyka zdarzeń operacyjnych.

Kategorie zdarzeń operacyjnych	**Rodzaje zdarzeń w ramach kategorii**	**Przykłady zdarzeń operacyjnych**
1. Oszustwo wewnętrzne - Straty z tytułu działań mających na celu zamierzone oszustwo, sprzeniewierzenie własności lub obejście regulacji, prawa lub polityki spółki, z wyłączeniem zdarzeń z zakresu różnicowania i dyskryminacji, dotyczące co najmniej jednej osoby wewnętrznej.	1. Działania nieuprawnione	1) działania nierejestrowane (zamierzone) 2) nieautoryzowane transakcje (poniesiona strata) 3) błędna wycena transakcji (zamierzona)
	2. Kradzież i oszustwo	1) oszustwo, oszustwo kredytowe, bezwartościowy depozyt 2) kradzież, wymuszenie, defraudacja, rabunek 3) sprzeniewierzenie aktywów 4) zamierzone zniszczenie aktywów 5) fałszerstwo 6) oszustwo czekowe 7) przemyt 8) przejęcie rachunku, mistyfikacja, itp. 9) niezgodności podatkowe, unikanie podatków (umyślne) 10) przekupstwo, łapówkarstwo 11) działalność na korzyść własną (nie na rachunek firmy)

2. Oszustwo zewnętrzne – Straty z tytułu działań mających na celu zamierzone oszustwo, sprzeniewierzenie własności lub obejście regulacji, prawa przez osobę trzecią.	1. Kradzież i oszustwo.	1) kradzież, rabunek 2) fałszerstwo 3) oszustwo czekowe
	2. Bezpieczeństwo systemów.	1) hakerstwo 2) kradzież informacji (poniesiona strata)
3. Praktyka kadrowa i bezpieczeństwo pracy - Straty wynikające z działań Banku niezgodnych z prawem pracy, przepisami BHP, porozumieniami zawartymi z pracownikami, lub z wypłat roszczeń z tytułu odszkodowań za wypadki przy pracy oraz zdarzeń z zakresu różnicowania i dyskryminacji.	1. Stosunki pracownicze	1) zdarzenia związane z wypłatą odszkodowań z tytułu wypłat wynagrodzeń, rozwiązywania umów o pracę, nieprzestrzegania przepisów prawa pracy przez Bank 2) zorganizowane działania związków zawodowych (strajki, protesty) 3) ujawnianie danych osobowych pracowników 4) nieobecność kluczowych pracowników w pracy
	2. Bezpieczeństwo środowiska pracy	1) wypadki na terenie administrowanym przez Bank 2) wypadki przy pracy z powodu nieprzestrzegania przez Bank przepisów BHP i ppoż. 3) inne zdarzenia skutkujące wypłatami odszkodowań dla pracowników
	3. Podziały i dyskryminacja	Wszelkie typy dyskryminacji pracowników (ze względu na wiek, płeć, przekonania, przynależność do partii politycznych, organizacji i związków zawodowych, itp.)
4. Klienci, produkty i praktyka biznesowa - Straty wynikające z niezamierzonego lub wynikającego z zaniedbania niewypełnienia zawodowych zobowiązań w stosunku do poszczególnych klientów (w tym wymagań dotyczących uczciwości i odpowiedzialności) albo też z charakteru lub struktury produktu.	1. Obsługa klientów, ujawnianie informacji o klientach, zobowiązania względem klientów	1) naruszenie zaufania, naruszenie wytycznych w zakresie obsługi klientów 2) zagadnienia dostosowania, pozyskiwanie informacji (poznaj swego klienta, itp.) 3) ujawnianie informacji dotyczących klientów indywidualnych 4) naruszenie prywatności 5) agresywna sprzedaż 6) agresywny handel na rachunek klienta w celu maksymalizacji prowizji 7) nieuprawnione użycie informacji poufnej 8) odpowiedzialność kredytodawcy
	2. Niewłaściwe praktyki biznesowe lub rynkowe	1) próby monopolizacji rynku 3) manipulacje rynkiem finansowym 3) handel na podstawie poufnych informacji (na konto Banku) 4) działanie poza zezwoleniem 5) pranie pieniędzy
	3. Wady produktów	1) wadliwie skonstruowane produkty bankowe (w tym błędy wzorów umów, regulaminów i innych tego typu dokumentów, brak autoryzacji) 2) błędy modeli (np. wycen instrumentów pochodnych)
	4. Klasyfikacja klienta i ekspozycje	1) dokonywanie oceny profilu klienta niezgodnie z wytycznymi 2) przekraczanie limitów zaangażowania względem klienta 3) błędy oceny profilu klienta
	5. Usługi doradcze	Spory o jakość działalności doradczej świadczonej przez Bank.

5. Uszkodzenia aktywów - Straty wynikające z utraty bądź zniszczenia fizycznych aktywów w wyniku klęsk żywiołowych lub innych zdarzeń.	Klęski żywiołowe i inne zdarzenia.	1) straty powstałe w wyniku klęsk żywiołowych 2) straty wynikające z działalności terrorystycznej, wandalizmu
6. Zakłócenia działalności i błędy systemów - Straty wynikające z zakłóceń w działalności i błędów systemów.	Systemy	1) nieprawidłowe działanie sprzętu 2) błędy oprogramowania 3) nieprawidłowe działanie sieci telekomunikacyjnych, komputerowych, Internetu 4) przerwy w dopływie energii elektrycznej oraz nieprawidłowe działanie urządzeń podtrzymujących zasilanie.
7. Dokonywanie transakcji, dostawa oraz zarządzanie procesami - Straty wynikające z błędów podczas przeprowadzania transakcji lub zarządzania procesami, jak również z relacji z kontrahentami i dostawcami	1. Wprowadzanie do systemu, wykonywanie, rozliczanie i obsługa transakcji	1) błędy w czasie komunikacji 2) błędy wprowadzania, utrzymania i ładowania danych 3) przeoczenie terminu lub niewywiązanie się z ciążącego obowiązku 4) błędne działanie modelu lub systemu 5) błędy księgowe, błędy atrybutów rejestracji 6) błędy wykonania innych zadań 7) niewykonanie dostawy 8) błędy w procesie zarządzania zabezpieczeniami 9) utrzymywanie danych referencyjnych
	2. Monitorowanie i sprawozdawczość	1) niewykonanie obowiązku sprawozdawczego 2) sporządzenie niedokładnego sprawozdania zewnętrznego (poniesiona strata)
	3. Dokumentacja dotycząca klienta	1) zagubienie dokumentacji dotyczącej udzielenia, odwołania pełnomocnictwa 2) zagubienie, niekompletność dokumentacji innej niż wymieniona w pkt 1 3) błędy w informacji na etapie pozyskania klienta
	4. Zarządzanie rachunkami klientów	1) udzielenie dostępu do rachunku osobom nieuprawnionym 2) wprowadzenie błędnych danych na rachunku (poniesiona strata) 3) wyrządzenie szkody lub straty w aktywach klienta wskutek zaniedbania
	5. Uczestnicy procesów niebędący klientami banku (np. izby rozliczeniowe)	1) błąd kontrahenta 2) spory z kontrahentami.
	6. Sprzedawcy i dostawcy	1) wadliwie sporządzone umowy o wykonywanie przez podmioty zewnętrzne czynności należących do zakresu działania Banku oraz ich niewłaściwe realizowanie 2) spory z sprzedawcami i dostawcami

Nadzór bankowy oczekuje, że banki będą stosować podobną systematykę w odniesieniu do linii biznesowych i zdarzeń operacyjnych w celu ujednolicenia podejścia w skali całego sektora bankowego, a także ewentualnie w celu dzielenia się informacjami i doświadczeniami.

II. CZYNNIKI RYZYKA OPERACYJNEGO

1. Ludzie

W banku powinien być opracowany system zarządzania ryzykiem operacyjnym związanym z pracownikami. Ta kategoria ryzyka operacyjnego związana jest z dostępnością i kwalifikacjami pracowników, ich fluktuacją, zdolnościami do adaptacji, kulturą pracy, absencją kadry, zmęczeniem pracowników związanym z wykonywaniem pracy w godzinach nadliczbowych lub długotrwałym niewykorzystywaniem urlopu wypoczynkowego itp. W procesie zarządzania tą kategorią ryzyka rekomenduje się uwzględnić m.in. następujące kwestie:

- specyfika i różnorodność uwarunkowań związanych z zarządzaniem zasobami ludzkimi w różnych obszarach działalności,
- możliwość negatywnego wpływu systemu wynagradzania pracowników na efektywność ich pracy. Powinno się rozważyć, w jakim stopniu system wynagrodzeń i efektywność pracowników mogą wpływać na poziom ryzyka operacyjnego oraz czy kategorie te są przydatne do mierzenia rzeczywistego narażenia banku na ryzyko operacyjne,
- zgodność systemu zarządzania ryzykiem operacyjnym z wymogami prawnymi dotyczącymi bezpieczeństwa socjalnego i sytuacji pracowników,
- stosowanie przez bank mechanizmów zapewnienia ciągłości działania (plany utrzymania ciągłości działania i plany awaryjne) w sytuacjach nieobecności pracownika lub odejścia z pracy,
- relacja pomiędzy kategorią ryzyka kadrowego (np. godziny nadliczbowe, zwolnienia lekarskie, fluktuacja kadr) a rzeczywiście poniesionymi stratami operacyjnymi,
- w miarę możliwości - stosowanie powyższych zasad wobec pracowników zatrudnionych w podmiotach zależnych oraz wykonujących zlecone czynności (outsourcing).

Należy zadbać, aby pracownicy banku byli świadomi nałożonych na nich obowiązków i roli w procesie zarządzania ryzykiem operacyjnym, oraz byli w stanie wykonywać nałożone na nich zadania, poprzez:

- wyraźne zdefiniowanie obowiązków i uprawnień kontrolnych,
- zapewnienie odpowiedniego wyposażenia (narzędzi pracy),
- odpowiedni podział obowiązków i nadzór nad ich wypełnianiem przez pracowników,
- odpowiednie zasady zatrudniania pracowników i późniejszy proces weryfikacji (z uwzględnieniem zasad uczciwości, etyki zawodowej, reputacji, stopnia integracji, kompetencji, a także sytuacji finansowej),
- tworzenie i dystrybucję materiałów dla pracowników dotyczących stosowania procedur i wykorzystywania systemów (np. w formie podręczników lub ogólnie dostępnego serwisu w wewnętrznej sieci informatycznej),
- szkolenia podnoszące poziom kompetencji pracowników,
- przejrzystą politykę kadrową oraz odpowiednie zasady wprowadzania i wycofywania stosowanych procedur zatrudniania.

2. Procesy i systemy

Bank realizuje swoją strategię i założone cele wykorzystując różnorodne systemy (zarówno tradycyjne jak i teleinformatyczne) użytkowane w procesach bankowych. Zarówno na etapie tworzenia, wdrażania, jak i funkcjonowania, systemy te mogą być źródłem strat operacyjnych (np. błędy systemowe, awarie systemów, przestępstwa zewnętrzne). W związku z tym w banku powinien być opracowany system zarządzania ryzykiem operacyjnym związanym z procesami lub systemami, w którym rekomenduje się uwzględnić:

- istotność i złożoność procesów i systemów wykorzystywanych w bankowym cyklu operacyjnym (np. czy systemy są odpowiednio zunifikowane, w szczególności w najbardziej znaczących sferach działalności banku),
- kontrole zapobiegające awariom systemów i procesów umożliwiające identyfikację i usuwanie błędów,
- zgodność tworzonych i użytkowanych procesów i systemów z wymogami prawnymi,
- stosowanie przez bank mechanizmów zapewnienia ciągłości działania i planów awaryjnych w sytuacjach awarii lub zniszczenia systemu oraz nieprawidłowości funkcjonowania procesów,
- relację pomiędzy tą kategorią ryzyka (np. niekompatybilność, kompensowanie sald, błędy w dokumentacji) a rzeczywiście poniesionymi stratami operacyjnymi.

2.1. Systemy teleinformatyczne

System teleinformatyczny to zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci urządzenia końcowego.

Poprzez automatyzację procesów i systemów można redukować narażenie banku na ryzyko czynnika ludzkiego (np. poprzez redukcję błędów ludzkich, kontrolę dostępu), zwiększając jednak zależność banku od wykorzystywanych systemów teleinformatycznych.

W banku powinien być wdrożony system zarządzania i kontroli systemów teleinformatycznych, którego celem powinno być zapewnienie:

- odpowiedniej struktury organizacyjnej i systemu raportowania odnoszących się do procesów technologicznych (uwzględniających nadzór wyższego kierownictwa),
- spójności strategii rozwoju i eksploatacji systemów teleinformatycznych z ogólną strategią działania banku,
- odpowiednich procedur nabywania, rozbudowy i utrzymywania systemów (z uwzględnieniem adekwatności rozbudowy systemów telekomunikacyjnych i sieci w odniesieniu do obszarów operacyjnych),
- odpowiedniego wsparcia funkcjonowania systemów teleinformatycznych.

2.2. Dokumentacja wewnętrzna

Dokumentacja wewnętrzna związana z przeprowadzanymi procesami i wykorzystywanymi systemami może zmniejszyć narażenie banku na niektóre kategorie ryzyka operacyjnego poprzez umożliwienie pogłębiania wiedzy w zakresie funkcjonowania systemów i zapewnienie ciągłości działania. W zarządzaniu ryzykiem operacyjnym bank powinien ocenić adekwatność dokumentacji wewnętrznej, uwzględniając jej aktualizację, dystrybucję i wykorzystanie.

2.3. Dokumentacja zewnętrzna

Dokumentacja zewnętrzna obejmuje dokumenty opracowane przez bank i przekazywane klientom, kontrahentom i osobom trzecim. Bank stosuje dokumentację zewnętrzną (np. w postaci: kontraktów i umów, wyciągów bankowych, broszur reklamowych) w celu przedstawienia swoich produktów, prowadzonej działalności i strategii (np. poprzez informacje prasowe) oraz wizerunku.

W procesie tworzenia, dokumentacja zewnętrzna powinna być odpowiednio zweryfikowana jeszcze przed jej opublikowaniem (np. w departamentach: prawnym, marketingu i departamencie odpowiedzialnym za tę dokumentację lub przez zewnętrznych doradców). W związku z powyższym analizie należy poddać:

- zgodność z wymogami prawnymi,
- zakres zastosowania i przyjęte w dokumentacji definicje standardowych wyrażeń (powszechnie obowiązujących) lub wyrażeń niestandardowych (których znaczenie wcześniej nie było określone),
- sposób wydawania (publikowania) dokumentacji,
- zakres, w jakim wymagane jest potwierdzenie akceptacji dokumentów (np. podpis klienta lub potwierdzenie przez kontrahenta).

2.4. Bezpieczeństwo informacyjne

Informacja w banku może istnieć w wielu różnych formach, m.in.: fizycznej, elektronicznej, lub może być znana przez pracowników, ale nie zarejestrowana w żadnej formie. Błędy w przetwarzaniu informacji lub ochronie ich przechowywania mogą prowadzić do znaczących strat operacyjnych i narazić bank nie tylko na straty finansowe, ale wpłynąć na jego reputację.

Bank powinien wprowadzić odpowiedni system zarządzania ryzykiem związanym z bezpieczeństwem informacyjnym, poprzez zapewnienie:

- poufności danych[*]: właściwości danych, wskazującej obszar, w którym te dane nie powinny być dostępne lub ujawniane nieuprawnionym osobom, procesom lub innym podmiotom,
- integralności danych[*]: właściwości danych polegającej na tym, że dane nie zostały wcześniej zmienione lub zniszczone w nieautoryzowany sposób,

[*] Definicje zgodne z PN-ISO/IEC 2382-8 i PN-I-02000

- integralności systemu*: właściwości, polegającej na tym, że system realizuje swoją zamierzoną funkcję w nienaruszony sposób, wolny od nieautoryzowanej manipulacji, celowej lub przypadkowej,
- dostępności danych*: właściwości danych lub zasobów polegającej na tym, że mogą być one dostępne i wykorzystywane na żądanie uprawnionej jednostki,
- uwierzytelnienia: odpowiedniej weryfikacji i identyfikacji osoby lub systemu.

2.5. Lokalizacja

Lokalizacja banku lub jego poszczególnych placówek może mieć wpływ na jego profil ryzyka operacyjnego, związany z funkcjonowaniem systemów. Należy więc rozpoznawać wpływ różnych lokalizacji na funkcjonowanie systemu całego banku.

Jeśli bank działa w różnych krajach, powinien rozważyć między innymi następujące uwarunkowania:

- środowisko biznesowe (w szczególności: uwarunkowania formalno-prawne oraz polityka gospodarcza prowadzoną przez władze danego kraju) każdego z krajów działania banku (m.in. prawdopodobieństwo i ewentualny wpływ destabilizacji sytuacji politycznej lub różnic kulturowych na dostawy usług),
- ograniczenia prawne związane z transferem informacji za granicę,
- zakres w jakim lokalne wymogi regulacyjne i prawne mogą ograniczać zdolność banku do wypełniania wymogów regulacyjnych w kraju macierzystym (np. poufność informacji o klientach, dostęp do informacji uzyskiwanych od nadzorców kraju macierzystego, jednostki kontroli wewnętrznej, czy audytorów zewnętrznych),
- wymiana informacji z centralą banku i kompatybilność systemów zarządzania ryzykiem.

3. Zdarzenia zewnętrzne

Narażenie banku i jego klientów na ryzyko operacyjne może wynikać ze zmian w środowisku biznesowym, w jakim funkcjonuje dany bank. Znaczący wpływ mogą mieć następujące zjawiska:

- działania firm, takie jak przejęcia, fuzje, podział,
- restrukturyzacja firm, włączając zmiany wynikające z wprowadzania, modyfikacji lub rezygnacji ze zlecania czynności na zewnątrz (outsourcing),
- zmiany w systemie regulacyjnym i prawnym lub sądowe rozstrzygnięcia dotyczące stosowania i interpretacji przepisów.

3.1. Zdarzenia przewidywalne

Przed, w trakcie i po znaczących zmianach w otoczeniu, bank powinien ocenić i monitorować ich wpływ na jego profil ryzyka. W celu zabezpieczenia się przed tymi zagrożeniami i w celu zarządzania ryzykiem wynikającym z przewidywanych zmian rekomenduje się:

* Definicje zgodne z PN-ISO/IEC 2382-8 i PN-I-02000

- dostosowanie organizacji i systemu raportowania dla celów efektywnego zarządzania zmianami (włączając odpowiedni nadzór kierownictwa wyższego szczebla),
- zweryfikowanie adekwatności programu i systemu zarządzania dla celów zarządzania zmianami (uwzględniając: planowanie, akceptację, wdrażanie, kontrolę),
- wprowadzenie niezbędnych zmian w komunikowaniu się z pracownikami.

3.2. Zdarzenia nieprzewidywalne

Zagrożeniem dla ciągłości działania banku mogą być zdarzenia nieprzewidywalne, skutkujące np.: utratą zasobów. Zagrożenia te mogą powodować znaczące straty operacyjne. W związku z powyższym należy ocenić możliwość wystąpienia i ewentualny wpływ tych zdarzeń na działalność banku. Ocena taka powinna między innymi uwzględniać:

a) rodzaje zdarzeń uznanych za najbardziej prawdopodobne, np.:
   - awaria zasobów zewnętrznych (np. zakłócenia dostaw energii elektrycznej),
   - wandalizm, wojna, lub kataklizmy,

b) czas trwania zdarzenia.

W celu ochrony przed skutkami tych zdarzeń bank powinien podjąć odpowiednie kroki, między innymi:

- działania zmierzające do zmniejszenia prawdopodobieństwa wystąpienia niekorzystnych zdarzeń oraz ich skutków, takie jak: plany utrzymania ciągłości działania, plany awaryjne, wybór alternatywnych dostawców usług, podwojenie procesów, przechowywanie kopii zapasowych oprogramowania, replikowanie danych,
- działania redukujące wpływ powstałych zniszczeń: procesy i systemy alternatywne, umowy ochronne w razie wypadku, ubezpieczenia.

4. Zlecanie czynności na zewnątrz (outsourcing)

Przekazanie przez bank podmiotowi zewnętrznemu czynności istotnych dla działalności bankowej nie wiąże się z przeniesieniem odpowiedzialności za ich wykonanie. Wobec klienta i nadzoru bankowego bank odpowiada za czynności zlecone tak jakby sam je wykonywał.

Celem przekazywania części prowadzonej przez banki działalności do podmiotów powiązanych lub niezależnych podmiotów trzecich jest najczęściej: obniżanie kosztów, poprawa efektywności i redukcja ryzyka. Niezależnie od przytaczanych korzyści zarówno dla banku jak i jego klientów zlecanie czynności na zewnątrz może powiększać ryzyko operacyjne poprzez: ograniczoną kontrolę banku nad podmiotami wykonującymi zlecone czynności w działalności zleconej na zewnątrz.

Zarządzając ryzykiem operacyjnym związanym ze zlecaniem czynności na zewnątrz, w banku należy rozważyć:

- strukturę organizacyjną i system raportowania w odniesieniu do usług zlecanych,
- zgodność umów ze strategią działania banku,
- czy zawierane przez bank umowy oraz system zarządzania umożliwiają monitorowanie i kontrolę narażenia na ryzyko operacyjne wynikającej ze zlecania czynności na zewnątrz.

Przed zawarciem lub istotną zmianą umowy z podmiotem wykonującym zlecone czynności, bank powinien między innymi:

- dokonać analizy wpływu projektowanej umowy na strategię i profil ryzyka, na zdolność banku do realizacji wymogów regulacyjnych oraz na prowadzenie przez bank działalności zgodnie z przepisami prawa,
- sprawdzić sytuację finansową podmiotu, z którym ma być zawarta umowa,
- rozważyć najmniej uciążliwy sposób ewentualnej transformacji systemów,
- dokonać analizy potencjalnych skutków ryzyka koncentracji (np. zachowanie ciągłości działania w sytuacji gdy jedna firma outsourcingowa obsługuje kilka podmiotów),
- opracować adekwatne i wiarygodne plany awaryjne na wypadek zaprzestania świadczenia usług przez usługodawcę oraz sprawdzić czy usługodawca posiada plany zapewniające ciągłe i niezakłócone prowadzenie działalności w zakresie objętym umową,
- sprawdzić, czy powierzenie wykonywania czynności nie wpłynie niekorzystnie na ostrożne i stabilne zarządzanie bankiem, skuteczność systemu kontroli wewnętrznej w banku, możliwość wykonywania obowiązków przez biegłego rewidenta upoważnionego do badania sprawozdań finansowych banku na podstawie zawartej z bankiem umowy oraz ochronę tajemnicy prawnie chronionej.

Należy pamiętać, że niezależnie od oferowanych bankom rozwiązań technicznych, organizacyjnych lub prawnych, nie można przekazać usługodawcy odpowiedzialności za bezpieczeństwo gromadzonych środków oraz za prowadzenie działalności zgodnie z obowiązującym prawem.

III. REKOMENDACJE

Rekomendacja 1

Członkowie organów banku - rady nadzorczej i zarządu banku - powinni być świadomi ważnych aspektów ryzyka operacyjnego w banku, jako odrębnego i podlegającego zarządzaniu rodzaju ryzyka i powinni znać profil ryzyka wynikającego z działalności banku.

Rekomendacja 2

Rada nadzorcza w ramach wypełniania swoich funkcji zatwierdza (akceptuje) opracowane przez zarząd założenia strategii prowadzenia działalności. Założenia te powinny uwzględniać występowanie ryzyka operacyjnego wynikającego z działalności banku, a w szczególności określać ogólne zasady zarządzania tym ryzykiem.

Rada nadzorcza powinna dokonywać okresowej oceny realizacji przez zarząd założeń strategii (w szczególności w odniesieniu do zasad zarządzania ryzykiem operacyjnym banku). W tym celu zarząd banku powinien okresowo przedkładać radzie nadzorczej syntetyczną informację na temat skali i rodzajów ryzyka operacyjnego, na które narażony jest bank, prawdopodobieństwa jego występowania, jego skutków i metod zarządzania ryzykiem operacyjnym.

Rekomendacja 3

Zarząd banku odpowiada za opracowanie i wdrożenie strategii zarządzania ryzykiem, w tym za zorganizowanie i funkcjonowanie procesu zarządzania ryzykiem operacyjnym, oraz jeśli to konieczne - wprowadzanie niezbędnych korekt w celu usprawnienia tego procesu. Zasady i procedury zarządzania ryzykiem operacyjnym powinny obejmować pełen zakres działalności banku.

Rekomendacja 4

Kontrola i ocena systemu zarządzania ryzykiem operacyjnym oraz jego regularne przeglądy powinny być dokonywane przez komórkę audytu wewnętrznego, niezależną pod względem operacyjnym i zatrudniającą kompetentny, odpowiednio wyszkolony personel. Rada Nadzorcza sprawuje nadzór nad kontrolą systemu zarządzania ryzykiem operacyjnym oraz ocenia jej adekwatność i skuteczność.

Rekomendacja 5

W banku powinny w jasny sposób zostać określone kompetencje oraz schematy podległości służbowej w obszarze zarządzania ryzykiem operacyjnym na różnych szczeblach organizacyjnych.

Rekomendacja 6

W banku powinien istnieć udokumentowany proces identyfikacji i oceny zagrożeń związanych z ryzykiem operacyjnym dla wszystkich istotnych obszarów działalności banku oraz wszelkich nowych produktów, procesów i systemów. Identyfikacja i ocena ryzyka operacyjnego wynikającego z nowych produktów, zachodzących procesów i wykorzystywanych systemów powinny nastąpić przed ich wprowadzeniem w życie i zastosowaniem. Bank powinien posiadać udokumentowany

proces: oceny wrażliwości banku na zidentyfikowane zagrożenia, badania ich możliwego wpływu na wynik z działalności oraz określenia możliwych zabezpieczeń.

Rekomendacja 7

Wdrożony w banku system regularnego monitorowania zdarzeń operacyjnych powinien umożliwiać obserwację profilu ryzyka operacyjnego oraz regularne przekazywanie zarządowi informacji w tym zakresie.

Rekomendacja 8

Bank powinien dokonywać okresowej weryfikacji skuteczności funkcjonowania wdrożonego systemu zarządzania ryzykiem operacyjnym oraz jego adekwatności do aktualnego profilu ryzyka banku.

Rekomendacja 9

Bank powinien posiadać plany utrzymania ciągłości działania (w tym plany awaryjne), zapewniające nieprzerwane działanie banku na określonym poziomie, uwzględniające kategorie i czynniki ryzyka operacyjnego.

Rekomendacja 10

Bank powinien ujawniać otoczeniu rynkowemu informacje umożliwiające dokonanie oceny podejścia banku do zarządzania ryzykiem operacyjnym.

IV. ROLA ORGANÓW BANKU

1. Środowisko zarządzania ryzykiem operacyjnym

Błędy w identyfikacji i zarządzaniu ryzykiem operacyjnym, obecnym faktycznie w całej działalności banku, mogą zwiększyć możliwość nierozpoznania lub niekontrolowania niektórych kategorii tego ryzyka. Wszyscy pracownicy banku powinni postrzegać ryzyko operacyjne jako ten rodzaj ryzyka, na które bank jest narażony w coraz większym stopniu. Zarówno rada nadzorcza jak i zarząd banku zobowiązane są do stworzenia kultury organizacyjnej, w której nacisk kładzie się na efektywne zarządzanie ryzykiem operacyjnym i stosowanie ustalonych reguł postępowania (procedur).

W banku musi istnieć świadomość podziału organizacji na podstawowe procesy operacyjne, których przebieg wiąże się z realizacją celów banku. Dla każdego z tych procesów powinna być określona jednostka organizacyjna (osoba) odpowiedzialna za przestrzeganie procedur związanych z danym procesem oraz ich ewentualne modyfikacje (tzw. linie odpowiedzialności). Umożliwia to identyfikację możliwych zagrożeń w poszczególnych procesach i na określonych ich etapach.

Należy zapewnić pewną równowagę pomiędzy formalną strategią a kulturą organizacyjną banku. Dla ryzyka operacyjnego istotne są takie aspekty kultury organizacyjnej jak komunikowanie się wewnątrz firmy i z otoczeniem. W szczególności ważnymi elementami kultury organizacyjnej są:

- tzw. przykład z góry,
- zasady etyczne,
- komunikowanie celów,
- jasne przypisanie pracownikom ustalonych zadań i celów,
- szkolenia i dzielenie się wiedzą,
- ustalenie zasad oceny działalności,
- sposób podejmowania decyzji,
- przekazywanie uprawnień i odpowiedzialności na niższe szczeble.

Zarządzanie ryzykiem operacyjnym jest bardziej efektywne w bankach, w których istnieją wysokie standardy etycznych zachowań na wszystkich poziomach działalności banku.

2. Rada nadzorcza

Rekomendacja 1

Członkowie organów banku - rady nadzorczej i zarządu banku - powinni być świadomi ważnych aspektów ryzyka operacyjnego w banku, jako odrębnego i podlegającego zarządzaniu rodzaju ryzyka i powinni znać profil ryzyka wynikającego z działalności banku.

Rekomendacja 2

Rada nadzorcza w ramach wypełniania swoich funkcji zatwierdza (akceptuje) opracowane przez zarząd założenia strategii prowadzenia działalności. Założenia te powinny uwzględniać występowanie ryzyka operacyjnego wynikającego z działalności banku, a w szczególności określać ogólne zasady zarządzania tym ryzykiem.

Rada nadzorcza powinna dokonywać okresowej oceny realizacji przez zarząd założeń strategii (w szczególności w odniesieniu do zasad zarządzania ryzykiem operacyjnym banku). W tym celu zarząd banku powinien okresowo przedkładać radzie nadzorczej syntetyczną informację na temat skali i rodzajów ryzyka operacyjnego, na które narażony jest bank, prawdopodobieństwa jego występowania, jego skutków i metod zarządzania ryzykiem operacyjnym.

Nieznajomość profilu ryzyka (struktury ryzyka, obszarów powstawania zagrożeń i skali) wynikającego z działalności banku może negatywnie wpływać na jakość strategii zarządzania ryzykiem operacyjnym i przyczyniać się do wzrostu tego ryzyka. Stopień formalizacji i złożoności strategii zarządzania ryzykiem operacyjnym powinien być dostosowany do specyfiki działania banku i do określonego profilu ryzyka.
Strategia powinna określać podstawowe procesy niezbędne do zarządzania ryzykiem operacyjnym.

Członkowie rady nadzorczej powinni uzyskać przekonanie, że kierownictwo banku posiada niezbędne kompetencje do wdrożenia tej strategii. W związku z szybko zmieniającymi się czynnikami zewnętrznymi i wewnętrznymi kształtującymi ryzyko operacyjne strategia, a w tym zasady zarządzania ryzykiem operacyjnym, powinna podlegać regularnym przeglądom oraz jeśli zajdzie taka potrzeba - weryfikacji i aktualizacji. Rada nadzorcza może nakazać zarządowi poddanie rewizji zasad zarządzania ryzykiem operacyjnym w banku.

3. Zarząd banku

Rekomendacja 3

Zarząd banku odpowiada za opracowanie i wdrożenie strategii zarządzania ryzykiem, w tym za zorganizowanie i funkcjonowanie procesu zarządzania ryzykiem operacyjnym, oraz jeśli to konieczne - wprowadzanie niezbędnych korekt w celu usprawnienia tego procesu. Zasady i procedury zarządzania ryzykiem operacyjnym powinny obejmować pełen zakres działalności banku.

Opracowując strategię, zarząd banku powinien uwzględnić występowanie dwóch klas strat operacyjnych:

- powstałych w wyniku zdarzeń o wysokiej częstotliwości występowania ale generujących niewielkie straty,
- powstałych w wyniku zdarzeń o niskiej częstotliwości występowania ale generujących duże straty.

Opracowana przez zarząd strategia powinna określać:

- przyjętą w banku definicję ryzyka operacyjnego charakteryzującą w przejrzysty sposób ryzyko operacyjne w danym banku,
- profil ryzyka banku obejmujący skalę i strukturę ryzyka operacyjnego obciążającego bank,
- zasady zarządzania ryzykiem operacyjnym, w tym zasady: identyfikacji, oceny, monitorowania, zabezpieczania przed ryzykiem operacyjnym,
- system kontroli wewnętrznej w zakresie ryzyka operacyjnego.

Strategia powinna określać tolerancję banku na ryzyko operacyjne, uwzględniając:

- kierunki zarządzania tym ryzykiem,

- priorytet działań zarządczych,
- zakres oraz sposób transferowania ryzyka operacyjnego poza bank,
- główne zasady identyfikacji, oceny, monitorowania, zabezpieczania,
- system kontroli.

Obowiązkiem zarządu jest opracowanie szczegółowej strategii oraz zorganizowanie i wdrożenie zasad zarządzania ryzykiem, w tym odpowiednio - ryzykiem operacyjnym, wynikających z założeń zatwierdzonych przez radę nadzorczą. Zarząd banku odpowiada za przełożenie strategii banku na szczegółowe pisemne zasady zarządzania ryzykiem operacyjnym oraz ich wprowadzenie w organizacji.

Kierownictwo każdego szczebla jest odpowiedzialne za adekwatność i efektywność prowadzonej polityki i kontroli na swoim szczeblu. Zarząd banku zobowiązany jest do oceny czy na poszczególnych poziomach procesu zarządzania prowadzi się odpowiednio: identyfikację, ocenę, monitorowanie, raportowanie i kontrolę oraz czy kierownictwo każdego szczebla efektywnie zarządza ryzykiem operacyjnym na swoim szczeblu.

Kierownictwo banku powinno zapewnić funkcjonowanie w banku systemu efektywnego komunikowania się i znajomość polityki zarządzania ryzykiem operacyjnym przez pracowników banku we wszystkich obszarach działalności narażonych na ryzyko operacyjne. Pewne elementy zarządzania ryzykiem operacyjnym w codziennym prowadzeniu działalności mogą być delegowane do odpowiednich komórek banku. Może także powstać wydzielona w strukturach banku komórka do spraw zarządzania tym rodzajem ryzyka.

Pracownicy zajmujący się zarządzaniem i monitorowaniem ryzyka operacyjnego powinni posiadać odpowiednie doświadczenie, kwalifikacje, powinni być wyposażeni w odpowiednie środki techniczne i mieć zapewniony dostęp do niezbędnych zasobów. Pracownicy odpowiedzialni za zarządzanie ryzykiem operacyjnym powinni również ściśle współpracować z osobami odpowiedzialnymi za zarządzanie ryzykiem kredytowym, rynkowym oraz z osobami zajmującymi się ubezpieczeniami i zlecaniem funkcji na zewnątrz. Współpraca ta winna mieć na celu zapobieganie powstawaniu luk w zarządzaniu lub nakładaniu się zakresów odpowiedzialności za poszczególne obszary zarządzania.

Zarząd banku powinien aktywnie uczestniczyć w procesie kontroli zarządzania ryzykiem operacyjnym i podejmować działania wspomagające ten proces. Udział zarządu w procesie kontroli może mieć duży wpływ na szybkość podejmowanych działań naprawczych, a więc także na ich efektywność.

Szczególną uwagę należy zwrócić na kontrolę jakości dokumentacji i praktyk transakcyjnych w banku. Polityka, procesy i procedury związane z zaawansowanymi technologiami (w szczególności dotyczy to obsługi dużych transakcji) powinny być udokumentowane i przekazane pracownikom zajmującym się tymi transakcjami.

Aby wymogi w zakresie ryzyka operacyjnego mogły być właściwie wypełnione, w banku powinien być opracowany i wdrożony system raportowania, dostarczający informacji niezbędnych do zarządzania tym ryzykiem - pozwalających na identyfikację, ocenę, monitorowanie i kontrolowanie ryzyka operacyjnego. Zarząd banku powinien dysponować informacją umożliwiającą ocenę, czy w banku istnieje adekwatny system zarządzania ryzykiem operacyjnym, obejmujący kontrolę ze strony zarządu i kierownictwa wyższego szczebla.

4. Rola komórki kontroli wewnętrznej

Rekomendacja 4

Kontrola i ocena systemu zarządzania ryzykiem operacyjnym oraz jego regularne przeglądy powinny być dokonywane przez komórkę audytu wewnętrznego, niezależną pod względem operacyjnym i zatrudniającą kompetentny, odpowiednio wyszkolony personel. Rada Nadzorcza sprawuje nadzór nad kontrolą systemu zarządzania ryzykiem operacyjnym oraz ocenia jej adekwatność i skuteczność.

Rada nadzorcza banku powinna nadzorować (pośrednio przez komitet audytu wewnętrznego) zakres i częstotliwość kontroli wewnętrznej oraz jej adekwatność do poziomu narażenia banku na ryzyko operacyjne.

System kontroli wewnętrznej odgrywa kluczową rolę dla bezpiecznego działania banku, jest także istotnym elementem zarządzania ryzykiem operacyjnym**.** Wadliwie funkcjonujące mechanizmy kontroli wewnętrznej i zarządzania bankiem mogą prowadzić do wzrostu zagrożenia z tytułu ryzyka operacyjnego. Skutkiem mogą być między innymi straty finansowe powstałe w wyniku zdarzeń związanych z ryzykiem operacyjnym.

Sprawdzenie czy system kontroli wewnętrznej działa poprawnie i jest skuteczny, czyli czy właściwie odgrywa swoją rolę w zarządzaniu ryzykiem, należy do zadań komórki audytu wewnętrznego. Z tego między innymi wynika potrzeba powiązania audytu wewnętrznego z zarządzaniem ryzykiem. **Należy jednak wyraźnie podkreślić, że komórka audytu wewnętrznego nie powinna wypełniać bezpośrednio funkcji zarządzania ryzykiem, powinna natomiast dostarczać obiektywnej oceny: efektywności, adekwatności i skuteczności funkcjonującego systemu zarządzania oraz jakości przeprowadzanych operacji bankowych**.

Banki powinny posiadać skuteczną kontrolę wewnętrzną, bez względu na przyjęte techniki i narzędzia wykorzystywane w ramach funkcjonującego w nim systemu kontroli.

Narażenie na ryzyko operacyjne może być bardzo znaczące w sytuacji, gdy: banki angażują się w nowe rodzaje działalności lub tworzą nowe produkty (szczególnie, gdy produkt taki lub działalność nie są ściśle związane z podstawową działalnością banku), wchodzą na nowe nieznane rynki, angażują się w przedsięwzięcia znacząco oddalone geograficznie od centrali banku oraz dokonują zmian w strukturze organizacyjnej. Należy pamiętać, iż komórka audytu wewnętrznego powinna szczególnie dokładnie analizować takie dziedziny, ponieważ największe straty, związane z ryzykiem operacyjnym, ponoszone w ostatnich latach przez banki, związane były z takimi właśnie sytuacjami.

Zasadne jest także zapewnienie zachowania niezależności osób odpowiedzialnych za kontrolę ryzyka operacyjnego od ocenianej jednostki operacyjnej, która generuje ryzyko.

V. ZARZĄDZANIE RYZYKIEM OPERACYJNYM

Zdarzenia związane z ryzykiem operacyjnym są coraz częstsze, jednakże rzeczywisty wymiar tego ryzyka jest niezwykle trudno określić. Dlatego też celowe jest zorganizowanie i wdrożenie procesu zarządzania w banku tym rodzajem ryzyka, polegającego na:

- identyfikacji,

- ocenie,
- zastosowaniu narzędzi redukcji ryzyka,
- monitorowaniu efektywności redukcji ryzyka,
- raportowaniu.

Jednym z podstawowych elementów odpowiedniego zarządzania ryzykiem operacyjnym jest również opracowanie i wdrożenie udokumentowanych procedur oraz określenie zakresów odpowiedzialności na różnych szczeblach organizacyjnych. Proces zarządzania powinien być **dostosowany do skali i specyfiki działania banku.** Zasady zarządzania ryzykiem operacyjnym powinny być opracowane w formie pisemnej.

Rekomendacja 5

W banku powinny w jasny sposób zostać określone kompetencje oraz schematy podległości służbowej w obszarze zarządzania ryzykiem operacyjnym na różnych szczeblach organizacyjnych.

W banku można wyróżnić następujące grupy jednostek, osób i funkcji odpowiedzialnych za czynności związane z zarządzaniem ryzykiem na wszystkich szczeblach (poziomach) organizacji:

- jednostki organizacyjne zajmujące się zarządzaniem ryzykiem w swej codziennej działalności (poziom pierwszy - podstawowy),
- osoby zajmujące stanowiska kierownicze, pełniące kontrolę funkcjonalną (poziom drugi),
- główną funkcję zarządzania ryzykiem (poziom trzeci – nadrzędny).

Podział kompetencji powinien zapobiegać przyporządkowaniu zakresu odpowiedzialności mogącego prowadzić do konfliktów interesów. Przypisanie poszczególnym osobom bądź zespołom zakresu odpowiedzialności powodującego powstawanie konfliktu interesów może im umożliwić ukrywanie szkód, błędów lub niewłaściwych działań. Dlatego należy identyfikować i ograniczać obszary potencjalnych konfliktów interesów przy zastosowaniu dokładnego monitorowania i przeglądów.

Poziom trzeci (nadrzędny) - w zależności od przyjętego modelu zarządzania ryzykiem, może funkcjonować w formie:

- scentralizowanej - ryzykiem operacyjnym zarządza wydzielona komórka lub komitet (rozwiązanie to jest najbardziej efektywne zwłaszcza w bankach uniwersalnych),
- zdecentralizowanej – ryzykiem operacyjnym zarządzają wytypowane jednostki organizacyjne, jeśli odpowiada to charakterowi działalności banku (rozwiązanie takie może wiązać się z problemami z przepływem informacji i koordynacji procesu w skali całej instytucji, rozwiązanie takie jest odpowiednie w przypadku wyspecjalizowanych i małych banków, nie oferujących złożonych produktów i usług, wymaga jednak większego zaangażowania zarządu banku, który faktycznie pełni rolę lidera procesu zarządzania ryzykiem operacyjnym).

Należy założyć, że niektóre banki, szczególnie duże, będą stosować nieco odmienne rozwiązania.

1. Identyfikacja i ocena

Rekomendacja 6

W banku powinien istnieć udokumentowany proces identyfikacji i oceny zagrożeń związanych z ryzykiem operacyjnym dla wszystkich istotnych obszarów działalności banku oraz wszelkich nowych produktów, procesów i systemów. Identyfikacja i ocena ryzyka operacyjnego wynikającego z nowych produktów, zachodzących procesów i wykorzystywanych systemów powinny nastąpić przed ich wprowadzeniem w życie i zastosowaniem. Bank powinien posiadać udokumentowany proces: oceny wrażliwości banku na zidentyfikowane zagrożenia, badania ich możliwego wpływu na wynik z działalności oraz określenia możliwych zabezpieczeń.

Aktywne zarządzanie ryzykiem operacyjnym powinno obejmować szczegółową analizę tego ryzyka, zaś złożoność tej analizy zależy w znacznej mierze od samooceny danego banku na temat skali i wagi podejmowanego ryzyka operacyjnego.

1.1. Identyfikacja

Bez względu na poziom złożoności systemu, punkt wyjścia stanowić powinna trafna identyfikacja ryzyka operacyjnego. Efektywna identyfikacja ryzyka operacyjnego powinna uwzględniać:

- czynniki wewnętrzne (takie jak: struktura organizacyjna banku, specyfika działalności banku, użytkowane systemy informatyczne, specyfika klientów banku, skargi od klientów banku, jakość kadr, zmiany organizacyjne oraz rotacja kadr),
- czynniki zewnętrzne (otoczenie działania banku: czynniki polityczne, prawne, socjo-demograficzne, konkurencję, postęp technologiczny), które mogą wpływać negatywnie na realizację celów banku.

Trudność wyboru czynników ryzyka do analizy może często wynikać z braku bezpośrednich mierzalnych związków pomiędzy różnymi czynnikami ryzyka a wielkością i częstotliwością strat. Bank powinien identyfikować ryzyko właściwe dla wszystkich produktów, procesów, działań i systemów występujących w banku. W ramach identyfikacji kategorii ryzyka narażających bank na potencjalnie największe straty, bank powinien oszacować wrażliwość (podatność) na to ryzyko. Trafna identyfikacja ryzyka umożliwi bankowi odpowiednie określenie profilu ryzyka i właściwe dostosowanie mechanizmów zarządzania tym ryzykiem.

Pomocne w tym zakresie są mapy ryzyka, stanowiące odwzorowanie powiązań poszczególnych czynników ryzyka operacyjnego z poszczególnymi pionami operacyjnych. W procesie konstruowania „mapy ryzyka" poszczególne kategorie ryzyka operacyjnego przyporządkowuje się pionom operacyjnym, funkcjom organizacyjnym i procesom. „Mapa ryzyka" umożliwia ujawnienie słabych punktów oraz nadanie priorytetu dalszym działaniom zarządczym. Zmiany administracyjno-organizacyjne i technologiczne oraz wprowadzanie nowych produktów i usług powinny być uwzględniane w procesie zarządzania ryzykiem operacyjnym, przed ich formalnym zatwierdzeniem i wprowadzeniem, zaś ryzyko operacyjne, które może być z nimi związane, powinno podlegać odpowiednim procedurom oceny.

1.2. Ocena

Bank ocenia swoje operacje i działania na podstawie listy potencjalnych zagrożeń związanych z ryzykiem operacyjnym. Stosowane na przykład „karty ocen" (scorecard) umożliwiają zamianę ocen jakościowych na dane ilościowe. To z kolei umożliwia określenie systemu ratingu narażenia na różne kategorie ryzyka. System ratingu może odnosić się do poszczególnych pionów operacyjnych lub też poziom ryzyka może być przypisany do kilku różnych pionów operacyjnych jednocześnie. Ponadto rating może zarówno odnosić się do konkretnego rodzaju ryzyka, jak i do sposobu kontroli i zabezpieczania się przed nim.

Należy pamiętać, że łączne ryzyko operacyjne dla banku nie jest prostą sumą zagrożeń wynikających z ryzyka poszczególnych transakcji i poszczególnych pionów działalności banku, gdyż pojedyncze zagrożenia nie są od siebie wzajemnie niezależne. Tak, więc łączne ryzyko jest zdeterminowane przez wielkości pojedynczych zagrożeń, prawdopodobieństwo ich wystąpienia oraz poziom korelacji między nimi.

Do oceny ryzyka przydatne może być określenie zestawu wskaźników ryzyka operacyjnego. Mogą to być statystyki i/lub miary (np. finansowe), na podstawie których można określić m.in. wrażliwość banku na ryzyko, w tym ryzyko operacyjne. Wskaźniki te można określać na podstawie danych okresowych (miesięcznych lub kwartalnych). Analiza wskaźników ryzyka ma na celu ostrzeganie banku o możliwych zmianach związanych z ryzykiem operacyjnym. Wskaźniki te mogą zawierać np.: liczby nieudanych transakcji, wskaźniki zmian kadrowych, częstotliwość błędów.

Istotne źródło informacji o skali ryzyka operacyjnego mogą stanowić skargi od klientów banku, które często pokazują nieprawidłowości i ułomności procedur, procesów lub systemów banku z innej perspektywy.

1.3. Bazy danych o stratach

Banki powinny gromadzić dane o stratach powstających wewnątrz banku oraz w miarę możliwości o stratach zewnętrznych (poniesionych w otoczeniu banku). W miarę potrzeb należy rozszerzać i systematyzować wprowadzone rozwiązania służące analizie rodzajów i poziomu ryzyka operacyjnego, na które bank jest narażony. Celem gromadzenia i analizy danych na temat dotychczasowych strat banku ma być ułatwienie działań zmierzających do ograniczenia możliwości wystąpienia straty wywołanej działaniami czynników wewnętrznych.

Należy jednak zwrócić uwagę na fakt, że stosunkowo niedużym stratom (np. spowodowanym przez błąd człowieka) mogą towarzyszyć duże koszty związane z identyfikacją ich przyczyn i korektą problemów (czasami koszty badania mogą przewyższać stratę). W każdym przypadku trzeba rozstrzygnąć, na ile podjęte działania mogą być opłacalne nie tylko ze względu na rachunek ekonomiczny (np. relacja kosztu wykrycia i korekty problemu do wielkość straty), ale także z punktu widzenia przyszłych zagrożeń. Oznacza to, że trzeba uwzględniać powszechnie obowiązującą zasadę, zgodnie z którą koszt kontroli powinien być współmierny do wartości poniesionej lub potencjalnej straty, ale z drugiej strony trzeba uświadamiać sobie, że pomijanie lub lekceważenie drobnych strat może być początkiem dużych problemów lub wręcz nadużyć. Dlatego też banki powinny szacować koszty i korzyści alternatywnych strategii ograniczania i kontroli ryzyka operacyjnego.

Banki powinny w miarę możliwości dokonywać wymiany informacji z innymi bankami na temat przypadków wystąpienia strat finansowych oraz gromadzić te informacje i je analizować. Analiza danych zewnętrznych powinna obejmować weryfikację przyczyn i poziomu strat (na przykład odnotowanym awariom w systemie teleinformatycznym częstokroć trudno jest przypisać straty określonej wielkości).

W celu umożliwienia projektowania systemu pomiaru ryzyka operacyjnego niezbędne jest gromadzenie danych historycznych na temat strat operacyjnych w każdym banku i tworzenie własnych baz danych w oparciu o dane wewnętrzne i zewnętrzne, służących do analizy rodzajów i poziomów ryzyka operacyjnego. Wykorzystywanie danych zewnętrznych umożliwić może zabezpieczenie się przed tzw. "ryzykiem zarażenia", gdy problemy i straty finansowe występujące w innych instytucjach finansowych mogą bardzo szybko przenieść się na bank.

2. Monitorowanie i raportowanie

Rekomendacja 7

Wdrożony w banku system regularnego monitorowania zdarzeń operacyjnych powinien umożliwiać obserwację profilu ryzyka operacyjnego oraz regularne przekazywanie zarządowi informacji w tym zakresie.

2.1. Monitorowanie

Banki powinny wprowadzić proces monitorowania ryzyka operacyjnego, niezbędny dla adekwatnego zarządzania tym rodzajem ryzyka. Regularne monitorowanie stanowi podstawę szybkiego wykrycia i weryfikacji słabości występujących w systemie zarządzania tym rodzajem ryzyka. Natychmiastowe wykrycie i przeanalizowanie okoliczności związanych z odnotowaną stratą operacyjną pozwala zidentyfikować część lub całość przyczyn powstania tej straty, co z kolei będzie wpływało na możliwości redukcji potencjalnych strat w przyszłości.

Procesowi monitorowania powinien być poddany przebieg wszystkich ważnych procesów składających się na działalność bankową. Proces ten powinien umożliwiać obserwację profilu ryzyka operacyjnego banku. Banki powinny wdrożyć systemy bieżącego monitorowania narażenia na ryzyko operacyjne i powstawania strat w pionach operacyjnych. Monitorowanie powinno obejmować kluczowe źródła strat z tytułu ryzyka operacyjnego (sygnały i parametry ostrzegawcze). Ma to na celu umożliwienie podjęcia działań wyprzedzających powstanie straty.

Monitorowanie ryzyka operacyjnego powinno być integralną częścią działalności bankowej. Świadomie podejmowany, z góry określony poziom ryzyka operacyjnego, określona wrażliwość banku na to ryzyko oraz częstotliwość i natura zmian w otoczeniu operacyjnym powinny określać częstotliwość i złożoność systemu monitorowania.

Banki powinny wypracowywać własne mechanizmy monitorowania ryzyka operacyjnego, biorąc pod uwagę w szczególności:

- rodzaj i istotność błędów,
- rodzaje, stopień skomplikowania i wartość zawieranych oraz planowanych transakcji,
- wahania osiąganych i przewidywanych zysków,

- posiadany system teleinformatyczny,
- poziom kwalifikacji pracowników oraz zmiany kadrowe i organizacyjne.

Efektywny sposób zbierania informacji o zdarzeniach generujących ryzyko operacyjne powinien opierać się na systematycznym wyszukiwaniu i zbieraniu danych o przyczynach strat oraz informacji na temat ich wielkości, częstotliwości, dotkliwości etc. Mechanizmy monitorowania powinny być ukierunkowane w sposób pozwalający na wykorzystanie ich dla celów pomiaru ryzyka. Mechanizmy te powinny zapewniać systematyczne monitorowanie ryzyka operacyjnego. Będą one poddawane ocenie przez nadzór bankowy w czasie czynności nadzorczych.

2.2. Raportowanie

Dane uzyskiwane w procesie monitorowania powinny stanowić podstawę regularnego raportowania dla kierownictwa banku oraz powinny być wykorzystywane przez komórkę audytu wewnętrznego i komórkę zarządzania ryzykiem. Banki powinny opracować system sprawozdawczości wewnętrznej w zakresie ryzyka operacyjnego umożliwiający ocenę ich narażenia na ryzyko operacyjne oraz skuteczne zarządzanie tym ryzykiem. Zakres przekazywanych sprawozdań wewnętrznych może być uzależniony od struktury organizacyjnej banku, jego wielkości, złożoności i rodzajów prowadzonej działalności. Mając świadomość, że banki są w trakcie rozwijania technik i metod zarządzania ryzykiem operacyjnym, zaś poziom ich zaawansowania w tej dziedzinie jest bardzo różny, można się spodziewać, że regularne przekazywanie informacji dotyczącej ryzyka operacyjnego wewnątrz banku niewątpliwie wpłynie na poprawę zarządzania ryzykiem operacyjnym.

W zależności od przyjętego systemu zarządzania, zarząd banku powinien otrzymywać regularne raporty z poszczególnych linii biznesowych, komórek (komórki) zarządzania ryzykiem jak i komórki audytu wewnętrznego. Raporty dotyczące ryzyka operacyjnego powinny zawierać wewnętrzne dane finansowe, operacyjne oraz dane o stratach jak i zewnętrzne dane rynkowe o zdarzeniach i warunkach, niezbędne w procesie podejmowania decyzji. W raportach powinny być odpowiednio opisane zarówno zidentyfikowane problemy jak i działania je korygujące.

Raporty powinny być przekazywane na odpowiednie poziomy zarządzania oraz do linii biznesowych banku, dla których dane te mogą być ważne. Częstotliwość raportowania powinna być uzależniona od skali działalności, profilu ryzyka i stopnia złożoności prowadzonej działalności.

W ramach kontroli poprawności systemu raportów na temat ryzyka i kontroli kierownictwo powinno regularnie weryfikować poprawność i dokładność systemu raportowania oraz systemu kontroli wewnętrznej (w tym funkcjonowania mechanizmów kontrolnych). Dla oceny użyteczności i wiarygodności raportów wewnętrznych kierownictwo może współpracować z instytucjami zewnętrznymi i wykorzystywać również raporty przygotowane przez źródła zewnętrzne (audytorów, nadzorców).

Banki powinny dokonywać okresowo przeglądu operacji pod względem ich funkcjonowania, dostosowania do rzeczywistych i potencjalnych zmian warunków, zdolności banku do ograniczania faktycznych i potencjalnych strat.

3. Podmioty powiązane

Banki działają w określonym środowisku gospodarczym i dlatego ich bezpieczeństwo ekonomiczne zależy również od rodzaju i stopnia powiązań z innymi podmiotami oraz od procesu zarządzania ryzykiem (również operacyjnym) generowanym przez te podmioty. Powiązania pomiędzy bankiem a innymi podmiotami mają wpływ na jego bezpieczeństwo i stabilność, dlatego bank powinien zarządzać ryzykiem operacyjnym w kontekście tych powiązań. Bank powinien dysponować niezbędnymi danymi dotyczącymi podmiotów powiązanych oraz gromadzić i analizować przypadki wystąpienia strat finansowych w podmiotach powiązanych oraz ich wpływ na ryzyko operacyjne w banku. W tym celu należy rozpatrzyć różne rodzaje powiązań z innymi podmiotami, np.:

- powiązania właścicielskie (kapitałowe) – gdzie bank jest podmiotem zależnym, stowarzyszonym bądź dominującym,
- powiązania przez osoby wewnętrzne,
- powiązania gospodarcze.

Rekomenduje się, aby w grupach podmiotów powiązanych kapitałowo i organizacyjnie, podmiotach blisko powiązanych oraz podmiotach działających w jednym holdingu z bankiem stosowano, w miarę możliwości, jednolite zasady zarządzania ryzykiem operacyjnym. Zarząd podmiotu dominującego powinien zidentyfikować profil ryzyka operacyjnego całej grupy oraz określił zasady, procedury i procesy zarządzania ryzykiem operacyjnym, uwzględniając: nie tylko specyfikę i skalę działalności poszczególnych podmiotów, ale także grupy jako całości oraz rodzaj powiązań i ich zakres.

VI. KONTROLA RYZYKA OPERACYJNEGO I DZIAŁANIA ZABEZPIECZAJĄCE

1. Kontrola

Rekomendacja 8

Bank powinien dokonywać okresowej weryfikacji skuteczności funkcjonowania wdrożonego systemu zarządzania ryzykiem operacyjnym oraz jego adekwatności do aktualnego profilu ryzyka banku.

W banku powinna być przeprowadzana okresowa weryfikacja funkcjonującego systemu zarządzania ryzykiem operacyjnym, mająca na celu m. in. sprawdzenie, czy w dalszym ciągu odpowiada on profilowi ryzyka operacyjnego, na które bank jest narażony. Dostosowanie systemu zarządzania ryzykiem operacyjnym do profilu ryzyka ma istotne znaczenie dla jakości zarządzania tym ryzykiem. W uzasadnionych przypadkach, Bank powinien dokonać niezbędnych zmian w tym zakresie.

2. Działania zabezpieczające

Rekomendacja 9

Bank powinien posiadać plany utrzymania ciągłości działania (w tym plany awaryjne), zapewniające nieprzerwane działanie banku na określonym poziomie, uwzględniające kategorie i czynniki ryzyka operacyjnego.

W banku należy podjąć decyzję, w jaki sposób traktować poszczególne kategorie zidentyfikowanego ryzyka operacyjnego:

- poprzez uruchomienie odpowiednich procedur kontroli i/lub ograniczenia ryzyka,
- poprzez podjęcie ryzyka przy świadomej rezygnacji z zabezpieczania się.

W przypadku kategorii ryzyka, których bank nie może kontrolować, należy podjąć decyzję: czy zaakceptować ten poziom ryzyka, czy ograniczyć ten rodzaj działalności, czy też całkowicie się z niej wycofać.

Narzędzia i programy ograniczające ryzyko operacyjne, stosowane w celu zmniejszenia zagrożenia i/lub częstotliwości oraz skutków krytycznego zdarzenia powinny być stosowane jako uzupełnienie szczegółowej kontroli wewnętrznej, a nie jej zastąpienie. Dużą rozwagę zachować należy w obszarach, gdzie narzędzia ograniczania ryzyka faktycznie redukują ryzyko operacyjne lub transferują skutki zdarzeń związanych z ryzykiem operacyjnym do innych sektorów (np. ubezpieczenia), ale w zamian tworzą nowe kategorie ryzyka (np. ryzyko prawne, ryzyko kontrahenta).

Ważną rolę w ograniczaniu ryzyka operacyjnego odgrywają także inwestycje w odpowiednie technologie informatyczne i zabezpieczenia technologiczne. Jednak należy mieć na uwadze, że rosnąca automatyzacja może zmienić częste i mało dotkliwe straty w sporadyczne, ale istotne. Problemy związane z utratą, bądź przedłużającą się awarią systemów spowodowaną przyczynami wewnętrznymi lub powstałymi poza bankiem, mogą zagrozić podstawowej działalności banku.

W ramach działań zabezpieczających w banku powinny być opracowane i wprowadzone:

- plany utrzymania ciągłości działania służące zapewnieniu bezawaryjnego działania krytycznych funkcji biznesowych na wymaganym przez Bank poziomie,
- plany awaryjne na wypadek zaistnienia awarii, mające na celu odtworzenie/wznowienie działalności działania krytycznych procesów biznesowych zgodnie z przyjętymi celami odtworzenia.

2.1. Plany awaryjne

W wyniku zdarzeń, które mogą pozostawać poza kontrolą banku, bank może utracić zdolność do realizacji części bądź całości swoich zobowiązań. Problemy takie mogą mieć miejsce szczególnie w sytuacji awarii lub zniszczenia infrastruktury informatycznej, telekomunikacyjnej lub fizycznej i mogą być przyczyną znaczących strat finansowych dla banku i problemów dla całego systemu finansowego. Sytuacje takie wymagają od banku opracowania i wdrożenia planów awaryjnych

odtworzenia/wznowienia działalności ważniejszych i większych systemów, uwzględniających różne możliwe scenariusze zdarzeń, na które bank może być narażony i odzwierciedlających skalę i złożoność działalności banku.

W banku należy zidentyfikować krytyczne procesy biznesowe, dla których szybkie odzyskanie sprawności działania może mieć istotne znaczenie, włączając również takie, w których występuje zależność od źródeł zewnętrznych lub osób trzecich. Dla procesów takich, bank powinien określić alternatywne mechanizmy sprawnego funkcjonowania lub wznowienia działania w przypadku awarii. Szczególną uwagę należy zwrócić na umiejętność odzyskiwania (lub tworzenia kopii bezpieczeństwa) danych elektronicznych i fizycznych niezbędnych dla ponownego rozpoczęcia działalności. Jeśli dane takie przechowywane są poza siedzibą banku lub bank przenosi operacje bankowe w nowe miejsce, musi ono znajdować się w odpowiedniej odległości i być dobrze zabezpieczone, aby w sytuacji zagrożenia zminimalizować ryzyko utraty nie tylko danych głównych, ale także ich kopii oraz podstawowego i alternatywnego ośrodka przetwarzania danych.

Należy dokonywać okresowych przeglądów planów awaryjnych i planów ciągłości działania, w szczególności należy oceniać, czy odpowiadają one zmieniającej się działalności banku.

Plany awaryjne powinny być okresowo testowane w celu zapewnienia ich odpowiedniego funkcjonowania w przypadku zaistnienia niekorzystnych zdarzeń lub awarii.

2.2. Ubezpieczenia

Ubezpieczenia służą zabezpieczaniu przed skutkami trudnych do przewidzenia błędów lub zdarzeń operacyjnych o znaczących skutkach finansowych. Najczęściej stosowane są w przypadku strat będących rezultatem: reklamacji/skarg/roszczeń osób trzecich z tytułu błędów, przeoczeń, fizycznej utraty papierów wartościowych, kradzieży dokonywanych przez pracowników lub osoby trzecie, kataklizmów. Przed zawarciem umowy ubezpieczenia warto wstępnie dokonać symulacji efektów redukcji ryzyka operacyjnego wynikających z możliwości zastosowanych ubezpieczeń.

Należy także podkreślić, że ubezpieczenie nie powinno być w żadnym przypadku traktowane jako alternatywa dla właściwego zarządzania ryzykiem oraz kontroli wewnętrznej (firmy ubezpieczeniowe przed przejęciem ryzyka będą szukały potwierdzenia, że ubezpieczana instytucja jest dobrze zarządzana i ich ocena będzie miała wpływ na warunki ubezpieczenia).

2.3. Zlecanie czynności na zewnątrz (outsourcing)

Bank może przyjąć również politykę redukcji ryzyka operacyjnego poprzez zlecanie funkcji na zewnątrz. Zlecanie działalności na zewnątrz umożliwia redukcję ryzyka instytucji poprzez transfer niektórych czynności (zgodnie z obowiązującym prawem) wraz z obciążającym je ryzykiem operacyjnym do innej instytucji posiadającej większe doświadczenie i skalę działalności dla podjęcia tego ryzyka. Jednocześnie jednak zlecanie działalności na zewnątrz może powiększać narażenie banku na ryzyko operacyjne poprzez: ograniczoną kontrolę nad podmiotami wykonującymi zlecone czynności w działalności zleconej na zewnątrz.

Korzystanie z usług innych firm nie zwalnia kierownictwa banku z odpowiedzialności za kontrolę - czy działalność takich firm prowadzona jest w sposób bezpieczny i zgodny z obowiązującym prawem (np. czy zagwarantowana jest ochrona tajemnicy prawnie chronionej w zakresie czynności powierzonych przez bank). Umowy z podmiotami wykonującymi zlecone czynności powinny być

szczegółowe i zawierać zapisy o jakości świadczonych usług, zapewniać wyraźny podział odpowiedzialności pomiędzy usługodawcą a bankiem zlecającym oraz nie powinny zawierać postanowień ograniczających lub wyłączających odpowiedzialność przedsiębiorcy w związku z niewykonaniem lub nienależytym wykonaniem tej umowy.

Bank powinien przeprowadzić analizę działalności podmiotów, którym powierzane będą czynności, pod kątem zdolności do wywiązania się z przyjętych zobowiązań oraz ryzyka operacyjnego biorąc m.in. pod uwagę doświadczenie rynkowe podmiotów, dostępne certyfikaty i opinie niezależnych audytorów w zakresie ich ryzyka operacyjnego oraz świadczonej jakości usług.

Bank powinien posiadać dla krytycznych procesów, których wykonanie w części lub w całości jest zlecane podmiotom zewnętrznym, plany awaryjne obejmujące alternatywne źródło usług oraz zasoby niezbędne do zmiany dostawcy usług w niezbędnym czasie.

VII. PRZEJRZYSTOŚĆ DZIAŁANIA

Rekomendacja 10

Bank powinien ujawniać otoczeniu rynkowemu informacje umożliwiające dokonanie oceny podejścia banku do zarządzania ryzykiem operacyjnym.

Regularne publiczne ujawnianie ogólnych informacji na temat podejścia do ryzyka operacyjnego przez banki może mieć wpływ na poprawę dyscypliny rynkowej oraz poprawę efektywności zarządzania ryzykiem w systemie bankowym (np. poprzez wymianę informacji). Zakres ujawnianych informacji powinien być uzależniony od wielkości banku, profilu ryzyka i stopnia złożoności działalności prowadzonej przez bank.

Ujawnianie informacji na temat ogólnego podejścia do zarządzania ryzykiem operacyjnym umożliwi inwestorom i kontrahentom banku ocenę, czy bank efektywnie zarządza tym rodzajem ryzyka.

SPIS TREŚCI

I. WSTĘP **2**
1. Uwagi ogólne 2
2. Zakres 3

II. CZYNNIKI RYZYKA OPERACYJNEGO **6**
1. Ludzie 6
2. Procesy i systemy 7
2.1. Systemy teleinformatyczne 7
2.2. Dokumentacja wewnętrzna 8
2.3. Dokumentacja zewnętrzna 8
2.4. Bezpieczeństwo informacyjne 8
2.5. Lokalizacja 9
3. Zdarzenia zewnętrzne 9
3.1. Zdarzenia przewidywalne 9
3.2. Zdarzenia nieprzewidywalne 10
4. Zlecanie czynności na zewnątrz (outsourcing) 10

III. REKOMENDACJE **12**

IV. ROLA ORGANÓW BANKU **14**
1. Środowisko zarządzania ryzykiem operacyjnym 14
2. Rada nadzorcza 14
3. Zarząd banku 15
4. Rola komórki kontroli wewnętrznej 17

V. ZARZĄDZANIE RYZYKIEM OPERACYJNYM **17**
1. Identyfikacja i ocena 19
1.1. Identyfikacja 19
1.2. Ocena 20
1.3. Bazy danych o stratach 20
2. Monitorowanie i raportowanie 21
2.1. Monitorowanie 21
2.2. Raportowanie 22
3. Podmioty powiązane 23

VI. KONTROLA RYZYKA OPERACYJNEGO I DZIAŁANIA ZABEZPIECZAJĄCE **23**
1. Kontrola 23
2. Działania zabezpieczające 24
2.1. Plany awaryjne 24
2.2. Ubezpieczenia 25
2.3. Zlecanie czynności na zewnątrz (outsourcing) 25

VII. PRZEJRZYSTOŚĆ DZIAŁANIA **26**

Opracowano:
w Wydziale Regulacji Ostrożnościowych
Biura Polityki Nadzorczej GINB

Aprobował:

Wojciech Kwaśniak
Generalny Inspektor Nadzoru Bankowego