Komisja Nadzoru Finansowego

# Rekomendacja M

dotycząca zarządzania ryzykiem operacyjnym w bankach

Warszawa, styczeń 2013 r.

# I. WSTĘP

## Uwagi ogólne

Niniejsza rekomendacja wydana jest na podstawie art. 137 pkt 5 ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe (Dz. U. z 2012 r. poz. 1376, 1385 i 1529) (zwanej dalej „ustawą Prawo bankowe") i stanowi zbiór zasad dobrej praktyki w zakresie ostrożnego i stabilnego zarządzania ryzykiem operacyjnym w bankach. Zastępuje ona wcześniejszą „Rekomendacje M dotyczącą zarządzania ryzykiem operacyjnym w bankach" opracowaną i wydaną w 2004 r.

Ryzyko operacyjne, ze względu na swój kompleksowy charakter może mieć znaczący wpływ na działalność i sytuację banków, zwłaszcza, że obok otoczenia oraz zdarzeń zewnętrznych, jego źródłem jest organizacja bankowa sama w sobie. Jak wynika z dostępnych opracowań, ryzyko operacyjne jest drugim najistotniejszym po ryzyku kredytowym rodzajem ryzyka w bankach. Co więcej, analizy spektakularnych strat w systemie finansowym na świecie wskazują, iż – mimo że ujawniły się one w obszarze ryzyka kredytowego lub rynkowego – ich faktycznym źródłem było ryzyko operacyjne.

Niniejsza rekomendacja ma na celu upowszechnienie dobrych praktyk w zarządzaniu ryzykiem operacyjnym w bankach, bez względu na złożoność struktury i procesów w bankach, z uwzględnieniem zasady proporcjonalności. Ma pomóc w pogłębianiu świadomości istnienia ryzyka operacyjnego, jego istotności i właściwości, oraz budowaniu odpowiedniej kultury organizacyjnej, która stanowi podstawę do wypracowania optymalnych mechanizmów zarządzania tym ryzykiem, zarówno w poszczególnych komórkach organizacyjnych, jak i zintegrowanego podejścia do tego ryzyka w skali całego banku.

Komisja Nadzoru Finansowego oczekuje, że **Rekomendacja M dotycząca zarządzania ryzykiem operacyjnym w bankach**, stanowiąca załącznik do uchwały Nr 8/2013 Komisji Nadzoru Finansowego z dnia 8 stycznia 2013 r. (Dz. Urz. KNF z 2013 poz. 6), zostanie wprowadzona nie później niż do dnia 30 czerwca 2013 r., z wyjątkiem pkt 17.3, w zakresie którego rekomendacja powinna zostać wprowadzona nie później niż do dnia 31 grudnia 2013 r. [1]

[1] W informacjach, o których mowa w pkt. 17.3, publikowanych w 2014 r. banki powinny uwzględnić również informacje w przedmiotowym zakresie jakich nie publikowały w 2013 r. mimo obowiązywania niniejszego dokumentu.

**Zakres i układ rekomendacji**

Zgodnie z definicją zawartą w § 1 załącznika nr 14 do Uchwały nr 76/2010 Komisji Nadzoru Finansowego z dnia 10 marca 2010 r. w sprawie zakresu i szczegółowych zasad wyznaczania wymogów kapitałowych z tytułu poszczególnych rodzajów ryzyka (Dz. Urz. KNF Nr 2, poz. 11 z późn. zm.) (zwanej dalej: „uchwałą w sprawie adekwatności kapitałowej"), przez ryzyko operacyjne należy rozumieć możliwość wystąpienia straty wynikającej z niedostosowania lub zawodności procesów wewnętrznych, ludzi i systemów lub ze zdarzeń zewnętrznych, obejmując również ryzyko prawne. Powyższa definicja nie obejmuje ryzyka reputacji i ryzyka strategicznego, które związane jest z ryzykiem biznesowym. Definicja ta określa tylko minimalny zakres ryzyka, natomiast bank w celach zarządzania ryzykiem operacyjnym może używać własnej, szerszej definicji, jednakże spójnej z powyższą. W kontekście ryzyka operacyjnego nie należy jednak zapominać o możliwości utraty reputacji na skutek zdarzeń ryzyka operacyjnego, w szczególności w obszarze ryzyka prawnego, co w konsekwencji może skutkować niepowodzeniem realizacji strategii biznesowej banku, w tym zmniejszeniem planowanych przychodów (np. na skutek spadku zaufania klientów i zakończenia przez nich współpracy z bankiem), czy spadkiem wartości firmy. W ślad za rekomendacjami Komitetu Bazylejskiego i przepisami Dyrektywy 2006/48/WE Parlamentu Europejskiego i Rady z dnia 14 czerwca 2006 r. w sprawie podejmowania i prowadzenia działalności przez instytucje kredytowe (wersja przeredagowana) (z późn. zm.) (Dz.U. L 177 z 30.6.2006, str. 1) (zwana również dyrektywą CRD), przepisy uchwały w sprawie adekwatności kapitałowej nakazują bankom stosującym metodę standardową (TSA) i zaawansowaną metodę pomiaru (AMA) do wyznaczania wymogów kapitałowych z tytułu ryzyka operacyjnego, o których mowa w § 2 ust. 1 załącznika nr 14 do uchwały w sprawie adekwatności kapitałowej, wyróżnić w działalności banku dla celów identyfikacji i zarządzania ryzykiem operacyjnym osiem linii biznesowych[2]. Wyodrębniając linie biznesowe należy stosować przepisy uchwały w sprawie adekwatności kapitałowej, odnoszące się do zasad przyporządkowania czynności do poszczególnych linii biznesowych oraz kryteria dezagregacji wskaźnika z metody standardowej wyznaczania wymogu kapitałowego z tytułu ryzyka operacyjnego pomiędzy linie biznesowe.

[2] Zgodnie z uchwałą w sprawie adekwatności kapitałowej, dla zaawansowanej metody pomiaru, ze względu na wyjątkowe okoliczności, straty, które mają wpływ na cały bank, mogą zostać przydzielone do dodatkowej linii biznesowej określonej jako „działalność ogólnobankowa".

Przepisy wyżej wymienionej uchwały definiują i systematyzują również rodzaje zdarzeń operacyjnych (zdarzeń związanych z działalnością banku, które mogą skutkować wystąpieniem strat finansowych z tytułu ryzyka operacyjnego). Klasyfikację rodzajów zdarzeń operacyjnych określono w załączniku nr 1 do niniejszej Rekomendacji. Przykłady zdarzeń operacyjnych zawartych w tym załączniku nie wyczerpują listy wszystkich możliwych zdarzeń operacyjnych.

Połączenie zestawienia linii biznesowych[3] z rodzajami zdarzeń operacyjnych określonych w załączniku nr 1 tworzy macierz linii biznesowych i rodzajów ryzyka operacyjnego – zwaną także macierzą bazylejską ryzyka operacyjnego – wykorzystywaną w procesie zarządzania ryzykiem operacyjnym. Komisja Nadzoru Finansowego oczekuje, że również banki stosujące metodę podstawowego wskaźnika (BIA), o której mowa w § 2 ust. 1 załącznika nr 14 do uchwały w sprawie adekwatności kapitałowej, z zachowaniem zasady proporcjonalności, będą stosować podobną systematykę w odniesieniu do linii biznesowych i rodzajów zdarzeń operacyjnych w celu ujednolicenia podejścia w skali całego sektora bankowego i ewentualnego dzielenia się informacjami i doświadczeniami z innymi bankami. Co więcej, stosowanie tej systematyki ułatwi im z czasem wykorzystanie bardziej zaawansowanych metod pomiaru i wyznaczania wymogu kapitałowego z tytułu ryzyka operacyjnego.

Uwzględniając najlepsze praktyki zarządzania ryzykiem operacyjnym, w tym wytyczne Bazylejskiego Komitetu Nadzoru Bankowego, Europejskiego Urzędu Nadzoru Bankowego (EBA, dawniej Komitet Europejskich Organów Nadzoru Bankowego CEBS) oraz chęć pokazania w sposób zintegrowany etapów procesu zarządzania ryzykiem operacyjnym, w niniejszym dokumencie przyjęto następujący układ rekomendacji:

1. Strategia zarządzania ryzykiem operacyjnym;
2. Środowisko wewnętrzne;
3. Identyfikacja ryzyka;
4. Ocena ryzyka;
5. Przeciwdziałanie ryzyku;
6. Kontrola;
7. Monitorowanie;
8. Raportowanie i przejrzystość działania.

[3] Linie biznesowe wraz z ich opisem przywołano w załączniku nr 2.

Przyjmując następujący układ treści dokumentu, Komisja Nadzoru Finansowego pragnie przekazać wszystkim bankom, jak należy prawidłowo postępować z ryzykiem operacyjnym, jakie elementy składają się na proces zarządzania tym ryzykiem oraz zwrócić uwagę, że proces zarządzania ryzykiem operacyjnym jest integralnym elementem procesu zarządzania bankiem. Oznacza to w szczególności, że informacje uzyskiwane w procesie zarządzania ryzykiem operacyjnym powinny być uwzględniane w procesach decyzyjnych dotyczących działalności biznesowej. Warto przy tym podkreślić, że poziom ryzyka operacyjnego banku zależy również od podejścia do ryzyka operacyjnego pracowników na poziomie poszczególnych komórek organizacyjnych lub w ramach procesów i od podejmowanych przez nich czynności obejmujących m.in. identyfikację i raportowanie ryzyka oraz kontrolę ryzyka.

Z uwagi na przyjęcie w niniejszej Rekomendacji podejścia, w którym pokazywane są poszczególne etapy procesu zarządzania ryzykiem operacyjnym, zadania i rola zarządu oraz rady nadzorczej zostały opisane na różnych etapach tego procesu w wielu miejscach dokumentu. W szczególności zadania i role zarządu oraz rady nadzorczej zostały przedstawione w poniższych rekomendacjach:

1. Rekomendacje 1 i 2 – w zakresie ustalania strategii zarządzania ryzykiem i jej weryfikacji;
2. Rekomendacja 3 – w zakresie opracowania systemu zarządzania ryzykiem operacyjnym i zapewnienia jego spójności ze strategią zarządzania tym ryzykiem;
3. Rekomendacja 4, pkt. 4.1, 4.2, 4.6, 4.10, 4.16, 4.17, 4.18, 4.20 i 4.21 – w zakresie tworzenia kultury organizacyjnej i budowy środowiska wewnętrznego w banku;
4. Rekomendacja 7, pkt. 7.11 – w zakresie wartości progowych do gromadzenia informacji o stratach operacyjnych;
5. Rekomendacja 8, pkt. 8.1 – w zakresie ustalania formalnych procedur pomiaru ryzyka operacyjnego;
6. Rekomendacja 10, Rekomendacja 11, Rekomendacja 12 - w zakresie przeciwdziałania ryzyku;
7. Rekomendacja 13 – w zakresie ustalania reguł kontroli zarządzania ryzykiem operacyjnym;
8. Rekomendacja 14 – w zakresie zapewnienia zgodności z wymogami wynikającymi z regulacji wewnętrznych i zewnętrznych, w tym prawnych;

9. Rekomendacja 15, pkt. 15.3 i 15.4 – w zakresie udziału w procesie monitorowania ryzyka operacyjnego;
10. Rekomendacja 16, pkt. 16.1 i 16.5 – w zakresie systemu raportowania w obszarze ryzyka operacyjnego;
11. Rekomendacja 17, pkt. 17.1, 17,2 i 17,3 – w zakresie przejrzystości działania i ujawnień w obszarze ryzyka operacyjnego.

Niniejsze wytyczne uwzględniają zasadę proporcjonalności, tj. przewidziano w nich, że powinny być wdrażane proporcjonalnie, z uwzględnieniem charakteru, skali i złożoności działalności danej instytucji, istotności procesów ich dotyczących, jak również jej profilu ryzyka. W szczególności zasada ta odnosi się do przyjętych metod pomiaru ryzyka operacyjnego, w tym również kalkulacji kapitału wewnętrznego z tytułu tego ryzyka. Nie oznacza to jednak, że mniejsze instytucje i/lub instytucje o mniej skomplikowanej strukturze są w mniejszym stopniu narażone na ryzyko operacyjne. Również one powinny stosować niniejszą rekomendację, w tym posiadać wydzieloną jednostkę lub funkcję do spraw zarządzania ryzykiem operacyjnym, a w bardzo małych instytucjach, przynajmniej powierzyć wyznaczonej osobie funkcję odpowiedzialną za zarządzanie tym ryzykiem. Należy mieć świadomość, że wymagania wynikające z treści niniejszego dokumentu, w których pozostawiono miejsce na zróżnicowanie sposobów ich spełnienia przez banki (np. w zakresie oceny czy kontroli ryzyka) mogą być realizowane wśród banków w sposób odmienny od siebie, ale zapewniający osiągnięcie celu ostrożnościowego w danym banku, a różnice mogą wynikać zwłaszcza z profilu ryzyka danej instytucji oraz skali i złożoności jej działalności. Jednoznaczne ustalanie czy dane rozwiązanie zastosowane przez bank w danym zakresie jest proporcjonalne w jego przypadku, powinno nastąpić w drodze dialogu pomiędzy bankiem a nadzorem. Każdy bank powinien wprowadzić rozwiązania, które jego zdaniem jak najpełniej realizują założony cel danej rekomendacji (przy czym w razie wątpliwości zawsze możliwe jest zwrócenie się o opinię nadzoru). Z kolei obowiązkiem nadzorcy jest ocenienie, w sposób niewykraczający poza założony cel ostrożnościowy danej rekomendacji, czy zastosowane przez bank rozwiązanie w danym zakresie spełnia w jego przypadku dany cel ostrożnościowy.

# II. SŁOWNIK POJĘĆ

**Istotny obszar działalności banku -** wskazana przez bank, dająca się wyodrębnić przedmiotowo, podmiotowo, terytorialnie lub organizacyjnie część działalności banku, wywierająca istotny wpływ na jego sytuację, a w szczególności stanowiąca istotne źródło finansowania lub istotne źródło przychodów, lub związana z istotnym ryzykiem.

**Kierownictwo banku** – zarząd banku oraz dyrektorów, kierowników komórek organizacyjnych i kierowników ds. kluczowych procesów w banku.

**Kluczowe procesy –** wskazane przez bank procesy w obrębie jego działalności, które warunkują realizację strategii banku (w tym strategii biznesowej i zarządzania ryzykiem).

**Krytyczne procesy –** wskazane przez bank procesy w obrębie jego działalności, w przypadku których szybkie odzyskanie sprawności działania może mieć istotne znaczenie z punktu widzenia ciągłości działania instytucji.

**Profil ryzyka operacyjnego –** skala i struktura ekspozycji na ryzyko operacyjne; określa stopień narażenia na ryzyko operacyjne i może być wyrażony w wybranych przez bank wymiarach strukturalnych (takich jak m.in. rodzaje zdarzeń operacyjnych, rodzaje linii biznesowych, kluczowe procesy) oraz wymiarach skali (takich jak m.in. oszacowana potencjalna wielkość straty); do jego ustalenia bank wykorzystuje m.in. posiadane informacje na temat zdarzeń operacyjnych (w tym dotyczące ich częstości i dotkliwości) oraz informacje pochodzące z wykorzystywanych narzędzi zarządzania ryzykiem operacyjnym.

**Strategia zarządzania ryzykiem operacyjnym –** element składowy strategii zarządzania ryzykiem, o której mowa w § 1 Uchwały nr 258/2011 Komisji Nadzoru Finansowego z dnia 4 października 2011 r. w sprawie szczegółowych zasad funkcjonowania systemu zarządzania ryzykiem i systemu kontroli wewnętrznej oraz szczegółowych warunków szacowania przez banki kapitału wewnętrznego i dokonywania przeglądów procesu szacowania i utrzymywania kapitału wewnętrznego oraz zasad ustalania polityki zmiennych składników wynagrodzeń osób zajmujących stanowiska kierownicze w banku (Dz. Urz. KNF Nr 11, poz. 42) (zwanej dalej: „uchwałą w sprawie funkcjonowania systemu zarządzania ryzykiem i systemu kontroli

wewnętrznej"); stanowi całościowy program wytyczania i osiągania celów instytucji w zakresie ryzyka operacyjnego, w szczególności powinna odzwierciedlać tolerancję/apetyt na ryzyko operacyjne oraz zrozumienie specyficznych cech tej kategorii ryzyka; powinna określać także sposób, w jaki instytucja planuje utrzymywać to ryzyko w ramach przyjętego apetytu/tolerancji, w tym wskazywać konkretne zakresy odpowiedzialności.

**System kontroli wewnętrznej** – zgodnie z ustawą Prawo bankowe, system funkcjonujący w ramach systemu zarządzania w banku, który obejmuje: mechanizmy kontroli ryzyka, badanie zgodności działania banku z przepisami prawa i regulacjami wewnętrznymi oraz audyt wewnętrzny; celem systemu kontroli wewnętrznej jest wspomaganie procesów decyzyjnych przyczyniające się do zapewnienia skuteczności i efektywności działania banku, wiarygodności sprawozdawczości finansowej oraz zgodności działania banku z przepisami prawa i regulacjami wewnętrznymi.

**System zarządzania** – zbiór zasad i mechanizmów odnoszących się do procesów decyzyjnych, zachodzących w banku oraz do oceny prowadzonej działalności bankowej; zgodnie z ustawą Prawo bankowe dzieli się na system zarządzania ryzykiem i system kontroli wewnętrznej; innym wymiarem podziału systemu zarządzania jest podział ze względu na obszary działalności, np. system zarządzania zasobami ludzkimi, system zarządzania bezpieczeństwem informacji, system zarządzania ciągłością działania.

**System zarządzania ryzykiem –** zgodnie z ustawą Prawo bankowe, obok systemu kontroli wewnętrznej, drugi element systemu zarządzania w banku; zbiór zasad, mechanizmów i narzędzi (w tym m.in. polityk i procedur dotyczących identyfikacji, pomiaru, monitorowania i kontroli ryzyka) odnoszących się do procesów dotyczących ryzyka; zadaniem systemu zarządzania ryzykiem jest identyfikacja, pomiar lub szacowanie oraz monitorowanie ryzyka występującego w działalności banku służące zapewnieniu prawidłowości procesu wyznaczania i realizacji szczegółowych celów prowadzonej przez bank działalności; w zakresie ryzyka operacyjnego określany jako system zarządzania ryzykiem operacyjnym – jest podstawowym środkiem realizacji przyjętej strategii zarządzania tym rodzajem ryzyka.

**Tolerancja/apetyt na ryzyko** – dwa pojęcia używane w dokumencie łącznie w celu opisania zarówno całkowitego ryzyka, na które instytucja jest gotowa i które jest skłonna podjąć *a priori* (co niekiedy nazywane jest apetytem na ryzyko), jak i faktycznych limitów w ramach

tego apetytu, jakie instytucja sobie wyznacza (zwane niekiedy tolerancją na ryzyko); termin z założenia pokrywający wszystkie definicje w przedmiotowym zakresie używane przez różne instytucje.

# III. LISTA REKOMENDACJI

**Rekomendacja 1**

***Zarząd banku odpowiada za opracowanie i wdrożenie pisemnej strategii zarządzania ryzykiem operacyjnym.***

**Rekomendacja 2**

***Rada nadzorcza banku akceptuje strategię zarządzania ryzykiem operacyjnym oraz (działając w zakresie swoich kompetencji) ocenia jej realizację i w razie konieczności zleca poddanie jej rewizji.***

**Rekomendacja 3**

***Zarząd banku odpowiada za opracowanie systemu zarządzania ryzykiem operacyjnym, jego wdrożenie, zapewnienie jego spójności ze strategią zarządzania tym ryzykiem oraz właściwe funkcjonowanie tego systemu w organizacji, w tym – jeśli to konieczne – wprowadzanie niezbędnych korekt w celu usprawnienia tego systemu.***

**Rekomendacja 4**

***Bank powinien posiadać strukturę, procesy i zasoby odpowiednie do skali i złożoności prowadzonej działalności, pozwalające na sprawne zarządzanie ryzykiem operacyjnym.***

**Rekomendacja 5**

***W strukturach banku powinna istnieć wydzielona jednostka lub funkcja do spraw zarządzania ryzykiem operacyjnym.***

**Rekomendacja 6**

***Bank, w miarę możliwości, zapewnia stosowanie jednolitych, spójnych zasad zarządzania ryzykiem operacyjnym w banku i podmiotach zależnych lub w podmiotach powiązanych z bankiem kapitałowo, organizacyjnie lub w inny sposób (np. poprzez uczestnictwo w***

***holdingu[4], lub konglomeracie finansowym), jeżeli powiązanie to może wywierać znaczący wpływ na sytuację banku.***

**Rekomendacja 7**

***Bank powinien realizować i dokumentować proces identyfikacji zagrożeń związanych z ryzykiem operacyjnym dla wszystkich istotnych obszarów działalności banku oraz tworzenia wszelkich nowych i modyfikacji już istniejących produktów, procesów i systemów.***

**Rekomendacja 8**

***Zarządzanie ryzykiem operacyjnym powinno opierać się na rzetelnej ocenie ryzyka, przeprowadzonej na podstawie zatwierdzonych procedur.***

**Rekomendacja 9**

***Bank w ramach oceny ryzyka operacyjnego powinien przeprowadzać testy warunków skrajnych, których programy są regularnie przeglądane i oceniane pod kątem efektywności i dopasowania do potrzeb, zarówno pod względem jakościowym, jak i ilościowym.***

**Rekomendacja 10**

***Bank powinien zdefiniować działania przeciwdziałające ryzyku, polegające na jego unikaniu, ograniczaniu lub transferowaniu, które są podejmowane w zależności od zidentyfikowanego poziomu ryzyka operacyjnego w stosunku do tolerancji/apetytu na ryzyko operacyjne zaakceptowanych przez radę nadzorczą.***

**Rekomendacja 11**

***Bank powinien posiadać system zarządzania ciągłością działania, w tym plany utrzymania ciągłości działania oraz plany awaryjne, zapewniający nieprzerwane działanie banku na określonym poziomie, uwzględniający profil ryzyka operacyjnego banku.***

**Rekomendacja 12**

***Bank powinien wykorzystywać optymalne mechanizmy transferu ryzyka, ale nie może traktować ich jako alternatywy dla właściwego zarządzania ryzykiem.***

[4] Przez holding rozumie się grupę podmiotów, o której mowa w art. 4 ust. 1 pkt 10-11c ustawy Prawo bankowe.

**Rekomendacja 13**

***Zarząd banku powinien zapewnić istnienie i funkcjonowanie reguł kontroli zarządzania ryzykiem operacyjnym i podejmować działania wspomagające ten proces.***

**Rekomendacja 14**

***Zarząd banku powinien zapewnić, że ryzyko niespełnienia wymogów wynikających z regulacji wewnętrznych i zewnętrznych (w tym prawnych) jest identyfikowane i kontrolowane.***

**Rekomendacja 15**

***Bank powinien posiadać system regularnego monitorowania zdarzeń operacyjnych oraz wyników pozostałych narzędzi w tym zakresie (np. KRI), umożliwiający obserwację profilu ryzyka operacyjnego oraz zapewniający regularne przekazywanie zarządowi i radzie nadzorczej stosownych informacji.***

**Rekomendacja 16**

***Bank powinien dokładać wszelkich starań, aby pozyskiwane przez niego dane do raportowania (w szczególności na potrzeby zarządcze) były rzetelne oraz charakteryzowały się wysoką jakością, w tym na bieżąco kontrolować tę jakość. Powinien również kontrolować wpływ jakości tych danych na proces zarządzania ryzykiem.***

**Rekomendacja 17**

***Bank powinien regularnie ogłaszać informacje na temat swojego podejścia do ryzyka operacyjnego służące ograniczeniu asymetrii informacji pomiędzy bankiem a jego otoczeniem.***

# IV. STRATEGIA ZARZĄDZANIA RYZYKIEM OPERACYJNYM

## 1. Rekomendacja 1

***Zarząd banku odpowiada za opracowanie i wdrożenie pisemnej strategii zarządzania ryzykiem operacyjnym[5].***

1.1. Strategia zarządzania ryzykiem operacyjnym powinna określać:

- przyjętą w banku definicję ryzyka operacyjnego, charakteryzującą w przejrzysty i jednoznaczny sposób ryzyko operacyjne,
- docelowy profil ryzyka operacyjnego banku, uwzględniający skalę i strukturę ryzyka operacyjnego obciążającego bank,
- tolerancję/apetyt banku na ryzyko operacyjne, w tym wartości progowe sum strat danej klasy zdarzeń[6] w określonym horyzoncie czasowym, oraz określone działania, które bank będzie podejmował w przypadkach, gdy wartości te zostaną przekroczone,
- ogólne zasady zarządzania ryzykiem operacyjnym, w tym zasady identyfikacji, oceny, monitorowania, zabezpieczania i transferu ryzyka operacyjnego,
- założenia dla systemu kontroli wewnętrznej w zakresie ryzyka operacyjnego.

1.2. Przedmiotowa strategia powinna również określać podstawowe procesy niezbędne do zarządzania ryzykiem operacyjnym. Stopień formalizacji i złożoności strategii zarządzania ryzykiem operacyjnym powinien być dostosowany do specyfiki działania banku i do aktualnego i docelowego profilu ryzyka. Strategia zarządzania ryzykiem operacyjnym powinna zostać opracowana z uwzględnieniem w szczególności:

- przedmiotu działalności banku,
- priorytetów działań zarządczych (w tym w zakresie zidentyfikowanych procesów kluczowych) i strategii biznesowej,

[5] KNF ma świadomość, że w sektorze bankowym nazwy dokumentów "polityka" i "strategia" są bardzo często używane zamiennie. Niezależnie od przyjętej przez bank nomenklatury w tym zakresie należy zapewnić aby zrealizowane zostały wytyczne wskazane w niniejszym rozdziale. Rekomendowana hierarchia i nazwy jej szczebli to: strategia, polityka, zasady.

[6] Klasy zdarzeń, o których tutaj mowa, mogą dotyczyć np. rodzajów zdarzeń czy kategorii zdarzeń, o których mowa w załączniku nr 1, jednak możliwe jest aby bank określił więcej i bardziej szczegółowe klasy wykraczające poza zakres przedstawiony w załączniku.

– dostępności środków na pokrycie strat,

– struktury organizacyjną banku,

– profilu ryzyka banku,

oraz zmian planowanych w powyższych obszarach.

## 2. Rekomendacja 2

***Rada nadzorcza banku akceptuje strategię zarządzania ryzykiem operacyjnym oraz (działając w zakresie swoich kompetencji) ocenia jej realizację i w razie konieczności zleca poddanie jej rewizji.***

2.1. W związku z szybko zmieniającymi się czynnikami zewnętrznymi i wewnętrznymi mającymi wpływ na ryzyko operacyjne, strategia i system zarządzania ryzykiem operacyjnym – a w tym zasady zarządzania tym ryzykiem – powinny być regularnie przeglądane przez zarząd oraz – jeśli zajdzie taka potrzeba – weryfikowane i aktualizowane. W ramach powyższych analiz należy w szczególności uwzględnić efektywność systemu zarządzania ryzykiem, zmiany zachodzące w otoczeniu banku, zmiany w strategii i działalności biznesowej, jakość systemu kontroli wewnętrznej, straty zachodzące w banku i w jego otoczeniu, zgodność z ustaloną tolerancją/apetytem na ryzyko operacyjne oraz zgodność z dobrymi praktykami w zakresie zarządzania tym rodzajem ryzyka. Rada nadzorcza musi być świadoma wyników tych przeglądów i odpowiednio reagować; w szczególności może nakazać zarządowi dokonanie rewizji strategii lub zasad zarządzania ryzykiem operacyjnym w banku. W celu umożliwienia radzie nadzorczej dokonania okresowej oceny realizacji założeń strategii zarządzania ryzykiem operacyjnym, zarząd banku powinien również okresowo przedkładać radzie nadzorczej syntetyczną informację na temat profilu ryzyka operacyjnego, na które narażony jest bank.

2.2. Rada nadzorcza banku powinna zapewnić, że zarząd banku posiada wiedzę i umiejętności niezbędne do realizacji strategii zarządzania ryzykiem operacyjnym w tym również weryfikować jego kompetencje w tym zakresie[7].

[7] Celem tych działań jest ustalenie czy w gronie członków zarządu są osoby posiadające kompetencje niezbędne do realizacji strategii zarządzania ryzykiem operacyjnym, które są w stanie zapewnić poprawne działanie systemu zarządzania tym rodzajem ryzyka. KNF oczekuje, że banki same wypracują – optymalne do celu jakiemu mają służyć – sposoby badania tych kompetencji, w szczególności nie wskazuje się, czy mają to być okresowo przeprowadzane testy kompetencyjne, czy też wystarczające będzie poświadczenie doświadczenia w pracy na danym stanowisku w danym obszarze lub określone tytuły naukowe wskazujące na kompetencje w danym obszarze.

## 3. Rekomendacja 3

***Zarząd banku odpowiada za opracowanie systemu zarządzania ryzykiem operacyjnym, jego wdrożenie, zapewnienie jego spójności ze strategią zarządzania tym ryzykiem oraz właściwe funkcjonowanie tego systemu w organizacji, w tym – jeśli to konieczne – wprowadzanie niezbędnych korekt w celu usprawnienia tego systemu.***

3.1. Zarząd banku zobowiązany jest zapewnić, że system zarządzania ryzykiem operacyjnym jest skuteczny – to znaczy, że proces zarządzania tym ryzykiem jest realizowany w sposób poprawny na każdym etapie, tj. etapach: identyfikacji, oceny, przeciwdziałania, kontroli monitorowania i raportowania.

3.2. Na skuteczność procesu zarządzania ryzykiem operacyjnym składa się szereg czynności podejmowanych na poziomie poszczególnych komórek organizacyjnych lub w ramach procesów, obejmujących m.in. kontrolę ryzyka, identyfikację ryzyka oraz raportowanie.

3.3. Aby zapewnić spójność systemu zarządzania ryzykiem operacyjnym ze strategią zarządzania tym ryzykiem oraz jego właściwe funkcjonowanie w organizacji zarząd banku powinien dysponować informacją umożliwiającą ocenę, czy system ten jest adekwatny do profilu ryzyka operacyjnego.

# V. ŚRODOWISKO WEWNĘTRZNE

## 4. Rekomendacja 4

***Bank powinien posiadać strukturę, procesy i zasoby odpowiednie do skali i złożoności prowadzonej działalności, pozwalające na sprawne zarządzanie ryzykiem operacyjnym.***

4.1. Odpowiedzialność za zapewnienie odpowiednich warunków organizacyjnych i technicznych oraz zasobów odpowiadających bieżącym i przyszłym wymaganiom banku spoczywa na zarządzie banku.

4.2. Warunki organizacyjne i techniczne powinny pozwalać na właściwe postępowanie z ryzykiem operacyjnym na poziomie poszczególnych komórek organizacyjnych lub w ramach procesów.

4.3. Struktura organizacyjna powinna umożliwiać skuteczne zarządzanie i kontrolę ryzyka operacyjnego – zarówno na poziomie dedykowanej jednostki/funkcji zarządzania ryzykiem operacyjnym, jak i jednostek biznesowych i ich wsparcia.

4.4. Struktura organizacyjna banku powinna przynajmniej raz w roku podlegać ocenie pod kątem skuteczności przyjętych rozwiązań z perspektywy zarządzania ryzykiem operacyjnym.

4.5. Zmiany dokonywane w strukturze organizacyjnej powinny być uzasadnione i dobrze zaplanowane, z uwzględnieniem konieczności dokonania przeglądu obowiązujących regulacji wewnętrznych i procedur w celu zapewnienia spójności wprowadzanych zmian z funkcjonującymi rozwiązaniami w zakresie zarządzania ryzykiem w banku.

### Zasoby Ludzkie

4.6. W banku powinien funkcjonować system zarządzania zasobami ludzkimi.

4.7. Ryzyko operacyjne dotyczące czynnika ludzkiego w funkcjonowaniu banku związane jest z dostępnością i kwalifikacjami pracowników, ich fluktuacją, zdolnością do adaptacji, kulturą pracy, absencją, zmęczeniem związanym z wykonywaniem pracy w godzinach nadliczbowych lub długotrwałym niewykorzystywaniem urlopu wypoczynkowego itp. W procesie zarządzania tym rodzajem ryzyka należy uwzględniać m.in. następujące kwestie:

- specyfikę i różnorodność uwarunkowań związanych z zarządzaniem zasobami ludzkimi w różnych obszarach działalności,

- możliwość negatywnego wpływu systemu wynagradzania pracowników na poziom ryzyka operacyjnego,
- prowadzenie polityki w zakresie wyboru, uzupełniania oraz monitorowania potrzeb kadrowych i planowania zaplecza kadrowego, w tym stosowanie przez bank mechanizmów zapewnienia ciągłości działania w sytuacjach nieobecności pracownika lub odejścia z pracy,
- wskaźniki ryzyka operacyjnego w obszarze zarządzania zasobami ludzkimi.

4.8. Należy zapewnić, aby pracownicy banku byli świadomi nałożonych na nich obowiązków i ról w ramach systemu zarządzania ryzykiem operacyjnym, a także by byli w stanie wykonywać nałożone na nich zadania, poprzez:

- wyraźne zdefiniowanie obowiązków i uprawnień kontrolnych,
- zapewnienie odpowiedniego wyposażenia (narzędzi pracy),
- jednoznaczny, spójny i przejrzysty podział obowiązków i nadzór nad ich wypełnianiem przez pracowników,
- obiektywne, spójne i przejrzyste zasady wynagradzania i motywowania pracowników (z uwzględnieniem zasad uczciwości i konsekwencji),
- przekazywanie jasnej i rzetelnej informacji zwrotnej,
- szkolenia podnoszące poziom kompetencji pracowników,
- tworzenie i dystrybucję materiałów dla pracowników dotyczących wprowadzania, stosowania oraz wycofywania procedur i wykorzystywania systemów (np. w formie podręczników lub ogólnie dostępnego serwisu w wewnętrznej sieci informatycznej).

4.9. Bank powinien posiadać sformalizowany, przejrzysty proces zatrudniania, oceny i awansu zawodowego pracowników uwzględniający ich kompetencje i zasady etyki zawodowej.

4.10. Zarówno rada nadzorcza, jak i zarząd banku zobowiązane są do stworzenia kultury organizacyjnej, w której nacisk kładzie się na efektywne zarządzanie ryzykiem operacyjnym, przestrzeganie procedur oraz stosowanie ustalonych reguł postępowania, w tym nienarażanie banku na utratę reputacji. Ponieważ ryzyko operacyjne - w odróżnieniu od innych ryzyk, takich jak kredytowe i rynkowe - dotyczy wszystkich komórek i obszarów działalności banku, proces zarządzania nim oraz zakresy odpowiedzialności obejmują znacznie szerszy krąg interesariuszy niż w przypadku innych rodzajów ryzyka. W związku z tym, bank poprzez

kulturę organizacyjną powinien promować aktywne włączanie się każdego pracownika w identyfikację i ograniczanie ryzyka operacyjnego.

4.11. W szczególności, ważnymi elementami kształtującymi kulturę organizacyjną są:

- zachowanie i postawa kierownictwa banku, tzw. „przykład z góry”,
- zasady etyczne,
- komunikowanie celów,
- jasne przypisanie pracownikom ustalonych zadań i celów,
- szkolenia i dzielenie się wiedzą,
- ustalenie zasad oceny działalności (w tym promujących rzetelne raportowanie o stratach),
- sposoby podejmowania decyzji,
- delegowanie uprawnień i odpowiedzialności na niższe szczeble.

**Systemy**[8]

4.12. Bank realizuje swoją strategię i założone cele wykorzystując różnorodne systemy użytkowane w procesach zachodzących w banku. Poprzez automatyzację procesów można redukować narażenie banku na ryzyko czynnika ludzkiego (np. poprzez redukcję błędów ludzkich, kontrolę dostępu), co zwiększy jednak zależność banku od wykorzystywanych systemów informatycznych. Zarówno na etapie projektowania, tworzenia, wdrażania, funkcjonowania, aktualizowania, rozbudowy, jak i wycofywania z użytku, systemy te mogą być źródłem strat operacyjnych (np. nieudane wdrożenia, błędy systemowe, awarie systemów, przestępstwa zewnętrzne). W związku z tym, w banku powinny być wdrożone zasady zarządzania systemami informatycznymi[9], których celem powinno być zapewnienie m.in.:

- odpowiednich rozwiązań organizacyjnych i systemu raportowania odnoszących się do procesów operacyjnych związanych z przygotowaniem i wykorzystaniem technologii (uwzględniających informacje dla kierownictwa banku),
- spójności strategii rozwoju i eksploatacji systemów informatycznych z ogólną strategią działania banku,

[8] Na potrzeby tej części Rekomendacji, o ile z kontekstu nie wynika inaczej, jako „systemy” rozumieć należy „systemy informatyczne”.

[9] Bardziej szczegółowe informacje w tym zakresie znajdują się w Rekomendacji D dotyczącej zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach.

- odpowiedniego wsparcia procesów realizowanych w banku przez rozwiązania informatyczne,
- wzajemnego dopasowania elementów środowiska teleinformatycznego banku w warstwach aplikacji, danych i infrastruktury,
- odpowiednich procedur nabywania, rozbudowy, wymiany i utrzymywania systemów (z uwzględnieniem adekwatności rozbudowy systemów telekomunikacyjnych i sieci w odniesieniu do obszarów operacyjnych),
- odpowiedniego wsparcia dla funkcjonowania systemów informatycznych (z uwzględnieniem zależności od podmiotów zewnętrznych w przypadku korzystania z rozwiązań zewnętrznych),
- odpowiedniego poziomu bezpieczeństwa związanego z użytkowaniem systemów informatycznych, m.in. poprzez właściwe zarządzanie uprawnieniami do korzystania z systemów w ramach obowiązujących regulacji wewnętrznych, w tym przypisanych do danego stanowiska, lub nadanych indywidualnie na kartach zadań, zapewnienie adekwatnego poziomu zabezpieczenia infrastruktury technologicznej oraz poprawne zarządzanie incydentami bezpieczeństwa,
- bezpiecznego i skutecznego funkcjonowania systemu identyfikacji klientów (w tym rejestru uwierzytelnień) korzystających z usług banku za pośrednictwem kanałów zdalnych.

4.13. Opracowując zasady zarządzania systemami informatycznymi należy uwzględnić:

- istotność i złożoność procesów i systemów wykorzystywanych w bankowych działaniach operacyjnych oraz stopień integracji tych systemów,
- konieczność prowadzenia monitoringu i kontroli w zakresie ryzyka wystąpienia awarii systemów i zawodności procesów, umożliwiających identyfikację i usuwanie błędów,
- kwestię zgodności tworzonych i użytkowanych procesów i systemów z wymogami prawnymi,
- konieczność stosowania przez bank mechanizmów zapewnienia ciągłości działania i planów awaryjnych w sytuacjach awarii lub zniszczenia systemu oraz nieprawidłowości w jego funkcjonowaniu,
- konieczność zapewnienia adekwatności tych zasad w poszczególnych obszarach działalności banku do związanych z nimi zagrożeń,

– kwestię spójności przyjętego systemu zarządzania ryzykiem operacyjnym związanym z systemami informatycznymi z całościowym systemem zarządzania ryzykiem operacyjnym w banku.

4.14. Dodatkowo, w celu usprawnienia obszaru kontroli jakości i bezpieczeństwa informacji, bank powinien:

– prowadzić odpowiednią dokumentację wykorzystywanych systemów informatycznych,

– prowadzić spójną politykę bezpieczeństwa informacji,

– prowadzić spójną politykę zarządzania danymi, wraz z dokumentacją procedur przetwarzania danych i zarządzania ich jakością,

– monitorować zasoby danych i systemy w celu identyfikacji ewentualnych błędów i prowadzić rejestr wykrytych błędów,

– określić zasady korygowania błędów danych.

**Procesy**

4.15. Bank powinien posiadać dokumentację wewnętrzną opisującą istniejące procesy, a także regularnie oceniać jej adekwatność, uwzględniając aktualność oraz zakres dystrybucji i wykorzystania. Realizowane przez bank procesy powinny być zinwentaryzowane i posiadać przypisanych właścicieli oraz być opisane (np. w formie spójnych procedur) na poziomie szczegółowości odpowiadającym istotności danego procesu dla banku. W dokumentacji należy też wskazać, które z nich są krytyczne z punktu widzenia ciągłości działania instytucji i kluczowe dla realizacji strategii banku. Dokładna i łatwo dostępna dla odpowiednich osób dokumentacja procesów i systemów[10] może zmniejszyć narażenie banku na niektóre kategorie zdarzeń operacyjnych, poprzez umożliwienie pogłębiania wiedzy w zakresie przebiegu procesów i funkcjonowania systemów, szczególnie w kontekście zapewnienia ciągłości działania. Ponadto, zinwentaryzowanie i opisanie procesów krytycznych jest niezbędne z punktu widzenia systemu zarządzania ciągłością działania. Bank powinien także zapewniać znajomość procedur poprzez okresowe szkolenia. Równie istotne dla ograniczenia ryzyka

[10] KNF nie narzuca tworzenia w banku odrębnego centralnego rejestru procesów czy procedur, do zawartości którego dostęp mieliby mieć poszczególni pracownicy w odpowiednim dla siebie zakresie. Niemniej jednak posiadanie i utrzymywanie aktualnego rejestru tego rodzaju może być korzystne dla banku.

operacyjnego jest zapewnienie aktualności dokumentacji, pozwala to bowiem na jej bieżące wykorzystywanie, a w konsekwencji na zmniejszenie ilości błędów w procesach.

4.16. Bank powinien zapewnić odpowiednią infrastrukturę technologiczną i zasoby ludzkie, odpowiadające bieżącym i przyszłym wymaganiom procesów realizowanych w banku. W tym celu należy zadbać m.in. o odpowiednią zdolność do działania (przepustowość) zarówno w warunkach normalnych, jak i skrajnych, zapewniając integralność, bezpieczeństwo i dostępność systemów i danych.

4.17. Bank powinien okresowo dokonywać przeglądu zgodności przebiegu procesów z procedurami, a także dostosowywać je do rzeczywistych i potencjalnych zmian warunków pod kątem zdolności do ograniczania faktycznych i potencjalnych strat.

4.18. Wnioski wynikające z okresowych przeglądów procesów zachodzących w banku powinny być podstawą działań zapewniających, że system zarządzania ryzykiem jest adekwatny do profilu ryzyka operacyjnego.

4.19. Wszyscy pracownicy banku powinni postrzegać ryzyko operacyjne jako ten rodzaj ryzyka, na który bank jest narażony nieustannie. W szczególności kierownictwo banku powinno dokładać wszelkich starań do stworzenia właściwej kultury organizacyjnej w zakresie ryzyka operacyjnego (obejmującej aspekty takie jak komunikowanie się wewnątrz firmy i z jej otoczeniem). W banku musi istnieć świadomość podziału działalności organizacji na podstawowe procesy operacyjne, tj. kluczowe i krytyczne procesy, których przebieg wiąże się z realizacją celów banku. Dla każdego z tych procesów powinien być określony wiodący właściciel procesu, odpowiedzialny za przestrzeganie procedur związanych z danym procesem oraz ich ewentualne modyfikacje. Powinno to umożliwić identyfikację możliwych zagrożeń w poszczególnych procesach oraz ich etapach.

4.20. W banku powinny zostać jednoznacznie określone kompetencje oraz schematy podległości służbowej w obszarze zarządzania na różnych szczeblach organizacyjnych. Zgodnie z przepisami § 8 ust. 2 uchwały w sprawie funkcjonowania systemu zarządzania ryzykiem i systemu kontroli wewnętrznej, podział kompetencji powinien zapobiegać przyporządkowaniu zakresu odpowiedzialności mogącemu prowadzić do konfliktów interesów. Przypisanie poszczególnym osobom bądź zespołom zakresu odpowiedzialności powodującego powstawanie konfliktu interesów może prowadzić do ukrywania szkód, błędów lub niewłaściwych działań. Tworząc, dokumentując i aktualizując schematy podległości należy identyfikować i eliminować potencjalne konflikty interesów.

4.21. Bank powinien ograniczać ryzyko operacyjne wynikające z powiązań personalnych osób, których zakres obowiązków jest kluczowy z punktu widzenia występującego w banku ryzyka. W tym celu bank powinien określić jak szeroki jest termin "powiązanie personalne" w zależności od tego jakie ryzyko z tego tytułu dostrzega, a następnie powinny być ponadto wprowadzone rozwiązania organizacyjne i procedury, które zapewnią odpowiednią ich niezależność, w tym w szczególności zasady podejmowania istotnych decyzji dotyczących funkcjonowania banku.

4.22. Rada nadzorcza powinna upewnić się, że wprowadzone przez zarząd rozwiązania organizacyjne oraz procedury mające na celu ograniczenie występowania konfliktu interesów i powiązań personalnych zapewniają w szczególności:

- rozdzielenie funkcji kierowania i zwierzchności organizacyjnej nad jednostkami operacyjnymi w banku (w tym uwzględniające podejmowanie decyzji w okresie zastępstw członków zarządu banku),
- niezależność i obiektywizm sprawowanej kontroli wewnętrznej,
- przestrzeganie określonych w banku zasad podejmowania decyzji przez osoby powiązane personalnie.

4.23. Konstrukcja procesów w banku powinna zapewniać bezpieczeństwo informacji związanych z prowadzoną działalnością.

4.24. Zakłócenia w przepływie, przetwarzaniu lub przechowywaniu informacji (m. in. występujących w formie papierowej albo elektronicznej – a także posiadanych przez pracowników, ale nie zarejestrowanych w żadnej formie) mogą prowadzić do znaczących strat operacyjnych w wymiarze finansowym, ale mogą również mieć wpływ na reputację banku i w konsekwencji powodować utratę potencjalnych zysków.

4.25. Bank musi posiadać odpowiedni system zarządzania bezpieczeństwem informacji, zapewniający[11]:

- poufność danych – właściwość danych stanowiącą, że dane powinny pozostać niedostępne lub niejawne dla nieuprawnionych osób, procesów lub innych podmiotów (zapewnienie poufności danych jest istotne w każdym aspekcie działalności banku),

[11] Poniższe definicje poufności, integralności, dostępności, niepodważalności i wiarygodności danych na podstawie ISO/IEC 27000:2009.

- integralność danych – właściwość danych stanowiącą o ich dokładności i kompletności (integralność danych wpływa na jakość działań podejmowanych przez bank na podstawie posiadanych informacji, przez co wpływa na ryzyko wystąpienia zdarzeń operacyjnych),
- dostępność danych – właściwość danych polegającą na tym, że są one dostępne i mogą być wykorzystywane na żądanie uprawnionej jednostki (dane będące w posiadaniu banku powinny być wykorzystywane w odpowiednich procesach i systemach, czyli powinny być dostępne w odpowiednim czasie dla określonych jednostek banku, przy zachowaniu poufności danych),
- niepodważalność danych – właściwość stanowiącą o jednoznaczności danych, uniemożliwiająca podważenie ich rzetelności i prawdziwości,
- wiarygodność danych – właściwość stanowiąca o tym, że wyniki działań podjętych w ramach przetwarzania danych będą zgodne z założeniami,
- uwierzytelnianie – odpowiednią identyfikację i weryfikację osoby lub systemu,
- odpowiednie procedury w zakresie odzyskiwania danych utraconych wskutek awarii systemu lub błędu człowieka.

4.26. Bank powinien zadbać o odpowiednią jakość dokumentacji zewnętrznej (obejmującej dokumenty opracowane przez bank i przekazywane klientom, kontrahentom i osobom trzecim, np. wzory umów, schemat wyciągów bankowych, broszury reklamowe, informacje prasowe, informacje w witrynach internetowych). Dokumentacja ta powinna być odpowiednio weryfikowana zarówno w procesie jej tworzenia (tj. jeszcze przed opublikowaniem) jak i okresowo po jej publikacji. Weryfikacji tej dokonywać powinna komórka prawna lub komórka ds. ryzyka braku zgodności, bądź przez zewnętrznych ekspertów. Analizie należy poddać:

- zgodność treści z wymogami prawnymi,
- zakres zastosowania i przyjęte w dokumentacji definicje wyrażeń standardowych (powszechnie obowiązujących) oraz niestandardowych (których znaczenie wcześniej nie było określone),
- sposób wydawania (publikowania) dokumentacji,
- objętość dokumentacji,
- jasność przekazu i przejrzystość dokumentu,

– zakres, w jakim wymagane jest potwierdzenie akceptacji dokumentów (np. podpis klienta lub potwierdzenie przez kontrahenta).

4.27. Bank – niezależnie od lokalizacji, w jakich prowadzi swoją działalność oraz przyjętego modelu dystrybucji świadczonych usług – powinien zapewniać należyty poziom zarządzania ryzykiem operacyjnym, uwzględniający uwarunkowania lokalne właściwe dla danej jednostki. Należy rozpoznawać wpływ różnych lokalizacji i rozwiązań organizacyjnych (w tym np. *shared services center*) 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 politykę gospodarczą prowadzoną przez władze danego kraju) każdego z krajów działania banku (m.in. prawdopodobieństwo i ewentualny wpływ destabilizacji sytuacji politycznej, społecznej, gospodarczej lub różnic kulturowych na procesy dostawy usług),
– ograniczenia prawne związane z transferem informacji,
– zakres, w jakim lokalne wymogi regulacyjne i prawne mogą ograniczać zdolność banku do spełniania 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 i innymi jednostkami banku i kompatybilność systemów zarządzania ryzykiem.

4.28. Dla procesów, których wykonanie w części lub w całości jest powierzane podmiotom zewnętrznym, bank powinien posiadać pisemne procedury zarządzania ryzykiem związanym z czynnościami powierzonymi na zewnątrz, w tym plany awaryjne, które w wymagających tego przypadkach obejmować będą alternatywne źródło usług oraz zasoby niezbędne do zmiany dostawcy usług w odpowiednim czasie. Posiadanie takich planów, zapewniających poziom usług dla klientów na akceptowanym przez nich poziomie, ma kluczowe znaczenie z perspektywy reputacji banku. Powyższe procedury i plany powinny uwzględniać istotność poszczególnych procesów dla banku.

4.29. Powierzanie czynności na zewnątrz może zwiększać ryzyko operacyjne – zarówno dla banku, jak i jego klientów – poprzez ograniczoną kontrolę banku nad podmiotami wykonującymi te czynności. Bank odpowiada za czynności zlecone tak, jakby sam je wykonywał. W szczególności po utracie zaufania na skutek nieodpowiedniego działania

podmiotów, którym bank powierzył czynności, zaufanie to odbudowywać będzie musiał sam bank.

4.30. Zarządzając ryzykiem operacyjnym związanym z powierzaniem czynności na zewnątrz, w banku należy uwzględnić:

- strukturę organizacyjną i system raportowania w odniesieniu do usług zlecanych,
- zgodność zakresu i skali powierzanych czynności ze strategią działania banku,
- zapewnienie monitorowania i kontroli narażenia na ryzyko operacyjne wynikające ze zlecania czynności na zewnątrz (w tym wykonywanie kontroli wewnętrznej u zleceniobiorcy).

4.31. Przed zawarciem lub istotną zmianą umowy z podmiotem wykonującym powierzone czynności, bank powinien, uwzględniając istotność danej czynności, przynajmniej:

- dokonać analizy wpływu projektowanej umowy na strategię i profil ryzyka, zdolność banku do realizacji wymogów regulacyjnych oraz prowadzenie przez bank działalności zgodnie z przepisami prawa,
- 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,
- rozważyć przeprowadzenie wizyty w siedzibie usługodawcy,
- sprawdzić sytuację finansową podmiotu, z którym ma być zawarta umowa,
- dokonać analizy potencjalnych skutków ryzyka dla zachowania ciągłości działania w sytuacji, gdy jedna firma outsourcingowa obsługuje kilka podmiotów i w sytuacji awaryjnej może nie posiadać wystarczających zasobów,
- opracować i aktualizować adekwatne i wiarygodne plany awaryjne na wypadek zaprzestania świadczenia usług przez usługodawcę oraz sprawdzić, czy usługodawca posiada testowane plany zapewniające ciągłe i niezakłócone prowadzenie działalności w zakresie objętym umową,
- uwzględnić kwestie związane z bezpiecznym rozwiązaniem współpracy z usługodawcą.

## 5. Rekomendacja 5

***W strukturach banku powinna istnieć wydzielona jednostka lub funkcja do spraw zarządzania ryzykiem operacyjnym.***

5.1. Z uwagi na konieczność zapewnienia sprawnego zarządzania i należytego nadzoru nad procesami w ramach zarządzania ryzykiem operacyjnym, w każdym banku powinna zostać wyodrębniona komórka do spraw ryzyka operacyjnego, lub co najmniej wyznaczona osoba, odpowiedzialna za zarządzanie tym ryzykiem[12].

5.2. Pracownicy, o których mowa w punkcie 5.1. powinni posiadać odpowiednie doświadczenie i kwalifikacje, powinni być wyposażeni w odpowiednie środki techniczne i mieć zapewniony dostęp do niezbędnych zasobów. Powinni oni również współpracować w odpowiednim zakresie z osobami odpowiedzialnymi za zarządzanie ryzykiem kredytowym i rynkowym (z uwagi na możliwość występowania strat z pogranicza tych ryzyk i ryzyka operacyjnego) oraz – w przypadku, gdy wnosiłoby to dodatkową wartość z perspektywy całościowego zarządzania ryzykiem banku – również z osobami odpowiedzialnymi za zarządzanie innymi rodzajami ryzyka, z właścicielami procesów, z osobami zajmującymi się zlecaniem czynności na zewnątrz, zajmujących się ubezpieczaniem banku, a także z przedstawicielami jednostek odpowiedzialnych za bezpieczeństwo i audyt wewnętrzny. Współpraca ta powinna mieć na celu zapobieganie powstawaniu luk w systemie zarządzania oraz nakładaniu się zakresów odpowiedzialności za poszczególne obszary zarządzania.

## 6. Rekomendacja 6

***Bank, w miarę możliwości, zapewnia stosowanie jednolitych, spójnych zasad zarządzania ryzykiem operacyjnym w banku i podmiotach zależnych lub w podmiotach powiązanych z bankiem kapitałowo, organizacyjnie lub w inny sposób (np. poprzez uczestnictwo w holdingu[13], lub konglomeracie finansowym), jeżeli powiązanie to może wywierać znaczący wpływ na sytuację banku.***

6.1. Ponieważ bezpieczeństwo ekonomiczne banków zależy również od rodzaju i stopnia powiązań z innymi podmiotami oraz od procesu zarządzania ryzykiem (w tym operacyjnym)

[12] Zgodnie z przepisami § 16 i § 37 Załącznika nr 14 do uchwały w sprawie adekwatności kapitałowej, obowiązek posiadania takiej komórki istnieje w przypadku banków stosujących do wyznaczania wymogu kapitałowego z tytułu ryzyka operacyjnego metodę standardową lub metodę zaawansowanego pomiaru, jednak – dla celów sprawnego zarządzania tym ryzykiem – również banki stosujące metodę podstawowego wskaźnika powinny posiadać taką komórkę lub jednostkę.

[13] Przez holding rozumie się grupę podmiotów, o której mowa w art. 4 ust. 1 pkt 10-11c ustawy Prawo bankowe.

generowanym przez te podmioty, bank powinien dysponować niezbędnymi informacjami dotyczącymi podmiotów powiązanych, w tym dotyczącymi tego, w jaki sposób zarządzają one ryzykiem, oraz gromadzić i analizować przypadki wystąpienia strat operacyjnych w podmiotach powiązanych i badać ich wpływ na ryzyko operacyjne w banku. Powiązania pomiędzy bankiem a innymi podmiotami mają wpływ na jego bezpieczeństwo i stabilność, dlatego np. w przypadku podmiotów zależnych od banku – zgodnie z przepisami § 21 ust. 1 uchwały w sprawie funkcjonowania systemu zarządzania ryzykiem i systemu kontroli wewnętrznej – w banku sprawowany jest nadzór nad ryzykiem związanym z działalnością tych podmiotów.

6.2. Kierownictwo podmiotu dominującego identyfikując profil ryzyka operacyjnego całej grupy i określając systemy zarządzania ryzykiem operacyjnym dla poszczególnych podmiotów powinno uwzględniać nie tylko grupę jako całość, ale także zakres i rodzaj powiązań podmiotów wchodzących w jej skład, jak również specyfikę i skalę działalności poszczególnych podmiotów.

6.3. Wdrożenie jednolitych, spójnych zasad w tych podmiotach może być uzależnione od ograniczeń w przepisach prawa lub ograniczeń organizacyjnych samych podmiotów, warunkowane relacją korzyści do kosztów wprowadzenia takiego ujednolicenia.

6.4. Osiągnięcie powyższych celów przez bank może wykraczać poza kompetencje organu zarządzającego, dlatego powinno być przedmiotem dążenia także pozostałych organów, a w konsekwencji także – podmiotu dominującego.

# VI. IDENTYFIKACJA RYZYKA

## 7. Rekomendacja 7

***Bank powinien realizować i dokumentować proces identyfikacji zagrożeń związanych z ryzykiem operacyjnym dla wszystkich istotnych obszarów działalności banku oraz tworzenia wszelkich nowych i modyfikacji już istniejących produktów, procesów i systemów.***

7.1. Zarządzanie ryzykiem operacyjnym obejmuje szczegółową analizę tego ryzyka, do której punkt wyjścia stanowi trafna identyfikacja ryzyka operacyjnego. Efektywna identyfikacja ryzyka operacyjnego powinna pozwalać na przeprowadzenie poprawnej oceny ryzyka i uwzględniać:

- czynniki wewnętrzne (takie jak struktura organizacyjna banku i jej zmiany, specyfika działalności banku, użytkowane systemy informatyczne, jakość i rotacja kadr, skargi od klientów banku czy też związane z zależnością banku od innych podmiotów w grupie),
- czynniki zewnętrzne (czynniki otoczenia gospodarczego, w tym polityczne, prawne, socjodemograficzne, rynkowe czy dotyczące zmian technologicznych).

7.2. Proces identyfikacji powinien odbywać się na podstawie ustalonych procedur, a materiały powstające w wyniku tego procesu powinny pozwalać na jego weryfikację.

7.3. Bank powinien samodzielnie identyfikować ryzyko właściwe dla wszystkich produktów, procesów i systemów występujących w banku, również w przypadku, gdy identyfikacja ryzyka została przeprowadzona przez podmiot inny niż sam bank. Niezależna identyfikacja powinna zostać przeprowadzona na poziomie zarówno samego banku, jak i z uwzględnieniem grupy, w skład której wchodzi.

7.4. Bank powinien przykładać szczególną wagę do identyfikacji ryzyka operacyjnego w sytuacji, gdy:

- angażuje się w nowe rodzaje działalności lub tworzy nowe produkty (szczególnie, gdy produkt taki lub działalność, nie są ściśle związane z podstawową działalnością banku),
- wchodzi na nowe, nieznane rynki – również poza granicami kraju,
- dokonuje zmian w strukturze organizacyjnej,

– wprowadza nowe systemy informatyczne,

– uczestniczy w procesie fuzji lub przejęcia,

– dokonuje restrukturyzacji.

7.5. W celu właściwej identyfikacji ryzyka operacyjnego, która stanowi warunek konieczny do prawidłowej oceny tego ryzyka, bank – niezależnie od metody stosowanej do wyznaczania wymogu kapitałowego z tytułu ryzyka operacyjnego – powinien gromadzić historyczne dane o zdarzeniach operacyjnych powstających wewnątrz banku oraz w miarę możliwości o zdarzeniach operacyjnych poniesionych przez podmioty funkcjonujące w otoczeniu banku, np. przez inne instytucje finansowe, przy czym dane o zdarzeniach zewnętrznych muszą być gromadzone odrębnie od danych o zdarzeniach wewnętrznych. Gromadzone dane muszą umożliwiać rzetelną ocenę ryzyka i pozwalać na weryfikację przyczyn powstawania strat. Powinny obejmować przynajmniej rodzaj zdarzenia, okoliczności i przyczyny jego zajścia, wielkość jego rzeczywistych i potencjalnych skutków finansowych, informację o tym, co zrobiono w sprawie odzyskania kwoty straty (odwrócenia) i kwotę tego odzysku (odwrócenia), oraz wpływ ubezpieczenia.

7.6. Identyfikując zdarzenia operacyjne, bank powinien zwracać uwagę na przypadki zdarzeń z pogranicza ryzyka operacyjnego i innych rodzajów ryzyka. O ile w przypadku wyznaczania wymogu kapitałowego z tytułu ryzyka operacyjnego odrębne traktowanie zdarzeń operacyjnych, które pierwotnie zaliczane były do ryzyka kredytowego (tj. nie włączanie tych zdarzeń do zbioru danych do kalkulacji wymogu kapitałowego) jest dopuszczone przez przepisy uchwały w sprawie adekwatności kapitałowej (dopóki traktuje się je jako straty wynikłe z ryzyka kredytowego do celów obliczania minimalnych wymogów kapitałowych), o tyle dla celów zarządzania ryzykiem operacyjnym ich włączanie do analizy tego rodzaju ryzyka jest celowe. Przykładem zdarzenia z pogranicza ryzyka operacyjnego i kredytowego może być wyłudzenie kredytu[14].

7.7. Podstawowym rodzajem strat, które bank powinien uwzględniać w procesie identyfikacji ryzyka operacyjnego, są wszystkie dotychczas zaewidencjonowane straty operacyjne brutto, tj. nie uwzględniające pomniejszeń o wartości odzyskane bezpośrednio

[14] Więcej przykładów i przydatnych informacji w zakresie identyfikacji ryzyka znaleźć można w dokumencie *CEBS Compendium of Supplementary Guidelines on implementation issues of operational risk*.

oraz z tytułu mechanizmu transferu ryzyka[15]. Straty te można podzielić na zrealizowane, tj. takie których skutki zostały ujęte (zgodnie z przyjętymi zasadami rachunkowości) w rachunku zysków i strat lub kapitałach własnych banku, jak i niezrealizowane, których maksymalna kwota jest oszacowana ale nie ujęta w rachunku zysków i strat lub kapitałach. Do kategorii niezrealizowanych strat operacyjnych należą zdarzenia typu *pending-loss*, czyli takie, których wpływ został już określony, ale który nie został jeszcze uwzględniony w wynikach finansowych banku (np. znajduje się na kontach „przejściowych" lub „do wyjaśnienia"). Zdarzenia tego typu, których wpływ uznaje się za istotny, powinny być jak najszybciej uwzględnione w ocenie ryzyka.

7.8. Bank w procesie identyfikacji ryzyka powinien także uwzględniać zdarzenia typu *near-miss* i *rapidly recovered loss events*. Zdarzenia operacyjne typu *near-miss*, czyli zdarzenia "prawie strat" to zdarzenia o charakterze zamkniętym[16], w przypadku których istniało realne zagrożenie wystąpienia bezpośrednich lub pośrednich strat finansowych, ale których to strat ostatecznie uniknięto. Mianem zdarzeń typu *rapidly recovered loss events* określa się zdarzenia operacyjne, których skutki finansowe w krótkim czasie (zwykle pomiędzy okresami sprawozdawczymi) zostają w pełni odwrócone i przez to nie są odzwierciedlane w rachunku wyników (np. błąd w rozliczeniu transakcji po wykryciu zostanie usunięty, a kwoty transferów pieniężnych odpowiednio skorygowane i korekty te często nie spowodują żadnych materialnych strat finansowych). Analizowanie tych dwóch kategorii zdarzeń może dostarczyć cennych informacji z uwagi na fakt, iż każde takie zdarzenie może wystąpić w przyszłości, skutkując trwałą stratą finansową.

7.9. Identyfikując zdarzenia i wynikające z nich straty finansowe należy zwrócić uwagę na grupy strat „powiązanych" i „rozciągniętych w czasie". Straty powiązane (z ang. *multiple-effect losses*) to rodzaj strat występujących w różnych liniach biznesowych, podmiotach z grupy itp., ale mających swoje źródło w tym samym zdarzeniu operacyjnym. Straty rozciągnięte w czasie (z ang. *multiple-time losses*) to straty powtarzające się w różnych okresach, ale mające swoje źródło w tym samym zdarzeniu operacyjnym.

W trakcie oceny ryzyka dane dotyczące takich zdarzeń i strat mogą podlegać agregacji (np. przed włączeniem ich do zestawu danych do wyliczania miar ryzyka takich jak Value-at-Risk) jednak na potrzeby zarządcze korzystniejsze może być posiadanie informacji

[15] Dane o stratach operacyjnych na bazie netto mogą być wykorzystywane do oceny skuteczności działań mitygujących.
[16] Nie oczekuje się wystąpienia dalszych strat finansowych z ich tytułu.

zdezagregowanych, przy czym powinny być one oznaczone dodatkowym wyróżnikiem pozwalającym na identyfikację powiązań z innymi stratami.

7.10. W celu weryfikacji kompletności wykorzystywanych baz danych o zdarzeniach i stratach operacyjnych, dane w nich zawarte powinny być zestawiane z innymi źródłami danych (takimi jak rejestr skarg i reklamacji, rejestr incydentów bezpieczeństwa, wyniki audytów, wyniki rekoncyliacji z księgami finansowymi).

7.11. Zarząd banku powinien odpowiednio zdefiniować w strategii zarządzania ryzykiem operacyjnym minimalne wartości progowe dla gromadzonych informacji o stratach operacyjnych. Dla celów zarządzania ryzykiem operacyjnym wartości progowe dla gromadzonych informacji o stratach mogą być definiowane oddzielnie dla poszczególnych rodzajów zdarzeń operacyjnych, przy czym bank musi być w stanie wiarygodnie uzasadnić, że wyznaczone wartości progowe:

- są adekwatne do rodzajów zdarzeń operacyjnych, do których są przypisane,
- nie pomijają istotnych (pod względem liczebności) zdarzeń operacyjnych,
- nie zniekształcają istotnie miar ryzyka operacyjnego.

7.12. Przyjęcie minimalnych wartości progowych do gromadzenia informacji o stratach jest istotne z uwagi 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 kwotę straty). Jednakże, 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 zagrożeń. Trzeba mieć bowiem świadomość, że pomijanie lub lekceważenie drobnych strat może prowadzić do licznych nadużyć i pozostawia nieodkryte istotne źródło strat, które może prowadzić do znacznie większej straty. Dlatego też banki ustalając te progi powinny kompleksowo szacować koszty i korzyści wynikające z przyjętych wartości progowych oraz weryfikować te wartości w ramach przeglądów systemu zarządzania ryzykiem operacyjnym.

7.13. Identyfikacja ryzyka operacyjnego wynikającego z nowych lub zmienianych produktów, procesów i systemów powinna nastąpić przed ich wprowadzeniem w życie i zastosowaniem. 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 odpowiedniej ocenie przed ich formalnym zatwierdzeniem. Bank powinien zagwarantować, że dokonano niezbędnych inwestycji w wymagane technologie i zasoby ludzkie niezbędne do wprowadzenia nowych produktów i usług. Pomoże to uniknąć ewentualnych strat i utraty reputacji.

7.14. Banki powinny w miarę możliwości dokonywać wymiany informacji z innymi bankami na temat przypadków wystąpienia strat operacyjnych w sposób zapewniający poufność odpowiednich danych.

# VII. OCENA RYZYKA

## 8. Rekomendacja 8

***Zarządzanie ryzykiem operacyjnym powinno opierać się na rzetelnej ocenie ryzyka, przeprowadzonej na podstawie zatwierdzonych procedur.***

8.1. Jednym z kluczowych zadań systemu zarządzania ryzykiem jest pomiar lub szacowanie występującego w działalności banku ryzyka. Stanowi to podstawę oceny tego ryzyka, co jest niezbędne dla realizacji założonych celów zarządczych odnośnie do danego rodzaju ryzyka. W ramach tego systemu bank stosuje sformalizowane procedury, zatwierdzone przez kierownictwo banku lub właściwy komitet.

8.2. Ocena ryzyka powinna polegać w szczególności na określeniu prawdopodobieństwa wystąpienia i wielkości możliwych przyszłych strat z tytułu ryzyka operacyjnego. Do określenia tych dwóch wielkości wykorzystuje się zarówno mierniki ilościowe (takie jak m.in. historyczne informacje o stratach), jak i jakościowe. Dokonując oceny należy analizować zagrożenia zarówno wewnętrzne, jak i zewnętrzne.

8.3. Trafna ocena ryzyka operacyjnego umożliwi bankowi odpowiednie określenie jego profilu i właściwe dostosowanie mechanizmów zarządzania nim. Pomocne w tym zakresie mogą być tzw. „mapy ryzyka operacyjnego" – narzędzia ułatwiające ujawnienie słabych punktów oraz nadanie priorytetu dalszym działaniom zarządczym[17].

8.4. Należy pamiętać, że łączny poziom ryzyka operacyjnego banku może nie być prostą sumą wynikającą z ryzyka poszczególnych transakcji czy poszczególnych obszarów działalności banku, gdyż pojedyncze zagrożenia mogą nie być wzajemnie od siebie niezależne. Łączny poziom ryzyka jest zdeterminowany wielkościami pojedynczych zagrożeń, prawdopodobieństwami ich wystąpienia oraz powiązaniami między nimi. Przykładowo, w wyniku synergii, łączny efekt zmaterializowania się więcej niż jednego zagrożenia może być większy niż suma efektów pojedynczych zagrożeń.

8.5. Bank powinien posiadać udokumentowany proces oceny wrażliwości banku na zidentyfikowane zagrożenia, tj. m.in. badania możliwego wpływu ich skutków finansowych

[17] Mapy ryzyka operacyjnego omówiono szerzej w załączniku nr 3: „Przykłady narzędzi do oceny ryzyka".

na wynik z działalności. W procesie tym należy także określić wpływ mechanizmów ograniczania ryzyka.

8.6. Ocena ryzyka operacyjnego wynikającego z nowych lub zmienianych produktów, procesów i wykorzystywanych systemów, jak również ze zmian organizacyjnych, powinna stanowić integralny element procesu zarządzania i nastąpić przed ich wprowadzeniem w życie i zastosowaniem[18].

**Testy warunków skrajnych (z ang. *stress tests*)**

## 9. Rekomendacja 9

***Bank w ramach oceny ryzyka operacyjnego powinien przeprowadzać testy warunków skrajnych, których programy są regularnie przeglądane i oceniane pod kątem efektywności i dopasowania do potrzeb, zarówno pod względem jakościowym, jak i ilościowym.***

9.1. § 16 uchwały w sprawie funkcjonowania systemu zarządzania ryzykiem i systemu kontroli wewnętrznej nakłada na bank obowiązek przeprowadzania testów warunków skrajnych w ramach pomiaru ryzyka.

9.2. Testy mogą polegać na analizie wrażliwości (jednoczynnikowej – na zmianę jednego czynnika, lub wieloczynnikowej – na zmianę większej liczby czynników) lub analizie scenariuszy. Mogą mieć też one formę odwrotnych testów warunków skrajnych (tj. takich, w których wychodzi się od założonej straty i szuka się zdarzenia/scenariusza mogącego do niej doprowadzić wraz z prawdopodobieństwem jego zajścia). Metodyka testów musi być regularnie przeglądana i oceniana pod kątem jej efektywności i dopasowana do potrzeb, w tym bieżącego wykorzystania, zarówno pod względem jakościowym, jak i ilościowym. Testy powinny być odpowiednio zintegrowane z procesem zarządzania i działaniami zarządu banku. Zakładane w testach zmiany czynników muszą być wystarczająco dotkliwe, a zdarzenia w nich zachodzące muszą być we właściwy sposób ze sobą łączone, aby dawały one prawidłowy obraz strat w warunkach skrajnych i umożliwiały poprawne wskazanie działań prewencyjnych.

[18] KNF nie wskazuje sposobu dokumentowania przeprowadzanej w takim przypadku analizy ryzyka operacyjnego, zaleca jedynie, aby stopień jej szczegółowości był przynajmniej skorelowany z wyznaczonym w toku takiej analizy poziomem ryzyka operacyjnego. Przykładowym rozwiązaniem w tym zakresie może być dołączenie stosownej analizy ryzyka operacyjnego w ramach funkcjonującej w banku dokumentacji projektowej, wniosków itp.

9.3. Gama testów powinna w szczególności uwzględniać elementy specyficzne dla danej instytucji, takie jak uwarunkowania regionalne, sektorowe, nowe i specyficzne produkty, linie biznesowe (w tym nowe linie biznesowe) czy wewnętrzne polityki.. Ponadto należy mieć świadomość, że założenie o liniowości reakcji na szok[19] nie zawsze jest poprawne.

9.4. Testy warunków skrajnych należy przeprowadzać z wykorzystaniem zdarzeń zarówno historycznych (w tym takich, które wydarzyły się w systemie bankowym na świecie), jak i hipotetycznych[20]. Ze względu na rosnącą nieciągłość zmian na rynkach finansowych i w gospodarce realnej scenariusze testowe muszą uwzględniać nieliniowość reakcji na zakłócenia, być dynamiczne i wybiegać w przyszłość, jak również zakładać równoczesne występowanie zdarzeń w obrębie instytucji (tj. nie w oderwaniu od innych linii biznesowych czy procesów). Konieczna jest także otwartość w przyjmowaniu dotkliwych założeń dotyczących warunków skrajnych.

9.5. Banki przeprowadzające testy warunków skrajnych powinny zakładać wystąpienie dotkliwych strat, konfrontować ich wielkość z dostępnym kapitałem i oceniać wpływ ich wystąpienia na swoją działalność.

9.6. Banki stosujące metody proste do wyznaczania wymogu kapitałowego na ryzyko operacyjne (tj. BIA lub TSA) w ramach testów warunków skrajnych powinny przeprowadzać wiarygodną analizę swoich głównych zagrożeń operacyjnych i posiadanych środków mitygujących. W szczególności bank powinien przeanalizować adekwatność posiadanego kapitału wewnętrznego na tle innych środków mitygujących. W tym celu, w ramach testu, bank może założyć odpowiednio dotkliwe zwiększenie poziomu strat i odzwierciedlić je w wynikach finansowych (pomniejszyć je) stanowiących podstawę do obliczania wymogu kapitałowego na ryzyko operacyjne, zgodnie z przepisami załącznika nr 14 do uchwały w sprawie adekwatności kapitałowej. Powstałą różnicę w regulacyjnym wymogu kapitałowym może następnie porównać z różnicą pomiędzy wymaganym kapitałem wewnętrznym i regulacyjnym, co pozwoli ustalić, na ile zwiększenie poziomu strat może zostać zaabsorbowane przez utrzymywany kapitał.

W odniesieniu do wyników przeprowadzanych testów instytucje powinny określać wiarygodne działania zarządcze, mające na celu zapewnienie ich bezpieczeństwa w czasie

[19] Tj. stałej, proporcjonalnej reakcji na zmiany w danym interwale czasu, w stosunku do poprzedniego interwału czasu.

[20] Kryzys finansowy zapoczątkowany w 2008 roku wykazał, że opieranie się wyłącznie na zdarzeniach historycznych jest niewystarczające i dlatego należy poświęcić większą uwagę zdarzeniom hipotetycznym.

scenariusza skrajnego. Wśród działań zarządczych uwzględnić można szeroki zakres technik ograniczających skutki tego ryzyka oraz plany awaryjne, w tym dotyczące planów kapitałowych.

9.7. Banki stosujące zaawansowane metody pomiaru do obliczania wymogu kapitałowego z tytułu ryzyka operacyjnego muszą zapewnić, że istotne zmienne modelu, w tym te obejmujące cztery podstawowe elementy – tj. wewnętrzne i zewnętrzne dane, analizy scenariuszy oraz czynniki otoczenia gospodarczego i kontroli – są odpowiednio testowane przy kalkulacji wymogu pierwszo- i drugofilarowego oraz walidacji AMA[21].

9.8. Jako że przepisy § 42 - 60 załącznika nr 14 do uchwały w sprawie adekwatności kapitałowej, nie narzucają sposobu i proporcji, w jakiej bank musi wykorzystać w modelu wewnętrzne i zewnętrzne dane, analizę scenariuszową oraz czynniki otoczenia gospodarczego i kontroli, bank musi odpowiednio uwzględnić jego specyfikę w ramach programu testów warunków skrajnych. Jeżeli dodatkowo zaawansowana metoda pomiaru jest łączona z metodami prostymi[22] do wyznaczania wymogu na ryzyko operacyjne (tzw. „wdrożenie częściowe"), wyniki testów dla tych ostatnich i działania zarządcze z nich wynikające powinny być zintegrowane z takimi działaniami wynikającymi z testów w ramach metod zaawansowanych.

[21] Należy odróżnić wykorzystywanie zdarzeń katastrofalnych w procesie budowy i/lub walidacji modelu od wykorzystywania tego rodzaju zdarzeń w procesie testowania.

[22] Łączenie metody zaawansowanego pomiaru (AMA) z metodami prostymi (BIA lub TSA) możliwe jest po uzyskaniu zgody KNF, o której mowa w § 2 ust. 4 Załącznika nr 14 do uchwały w sprawie adekwatności kapitałowej.

# VIII. PRZECIWDZIAŁANIE RYZYKU

## 10. Rekomendacja 10

***Bank powinien zdefiniować działania przeciwdziałające ryzyku, polegające na jego unikaniu, ograniczaniu lub transferowaniu, które są podejmowane w zależności od zidentyfikowanego poziomu ryzyka operacyjnego w stosunku do tolerancji/apetytu na ryzyko operacyjne zaakceptowanych przez radę nadzorczą.***

10.1. W banku muszą być zdefiniowane sposoby traktowania zidentyfikowanego ryzyka operacyjnego, tj. jego:

- akceptowanie (świadome niepodejmowanie działań mających na celu ograniczenie prawdopodobieństwa lub skutków zmaterializowania się danego zagrożenia, wraz z ewentualnym zapewnieniem środków na pokrycie potencjalnie związanych z nim strat),
- ograniczanie (przede wszystkim poprzez odpowiednie zdefiniowanie procesów, produktów, systemów, ich opis/procedury oraz wprowadzenie mechanizmów kontrolnych),
- transferowanie (przeniesienie części lub całości ryzyka związanego z danym zagrożeniem na podmiot zewnętrzny, w szczególności poprzez zlecanie wykonywania czynności zewnętrznym dostawcom usług lub stosowanie ubezpieczeń),
- unikanie (niepodejmowanie działań, z którymi wiąże się dane zagrożenie).

10.2. W przypadku ryzyka operacyjnego, związanego z daną klasą zdarzeń operacyjnych, którego bank nie może zaakceptować (tj. przykładowo takich, w przypadku których istnieje duże zagrożenie utratą reputacji), transferować, ani nie jest możliwe ich ograniczanie, należy podjąć decyzję, czy ograniczyć dany rodzaj działalności, czy też całkowicie się z takiej działalności wycofać. Narzędzia ograniczające ryzyko operacyjne, stosowane w celu zmniejszenia zagrożenia i/lub częstości oraz dotkliwości zdarzenia operacyjnego, powinny być stosowane jako uzupełnienie pozostałych elementów systemu kontroli wewnętrznej, a nie jako ich zastąpienie. Należy zachować dużą ostrożność przy ocenie, czy narzędzia ograniczania ryzyka faktycznie redukują ryzyko operacyjne lub transferują skutki zdarzeń związanych z tym ryzykiem do innych sektorów (np. ubezpieczenia), nie tworząc w zamian nowych kategorii ryzyka w obrębie działalności banku, m.in. w ramach ryzyka operacyjnego

(np. ryzyka prawnego, czy ryzyka niepewności wypłacenia odszkodowania), przez co suma ryzyk nie zmniejszy się.

10.3. Mechanizmy ograniczające ryzyko powinny obejmować działania, polityki i procedury, w wyniku których zwiększa się prawdopodobieństwo osiągnięcia zamierzonych celów zarządzania ryzykiem operacyjnym poprzez ograniczenie prawdopodobieństwa lub potencjalnych skutków strat z tytułu tego ryzyka lub utraty reputacji na skutek zmaterializowania się tego ryzyka.

**Plany ciągłości działania i plany awaryjne**

## 11. Rekomendacja 11

***Bank powinien posiadać system zarządzania ciągłością działania, w tym plany utrzymania ciągłości działania oraz plany awaryjne, zapewniający nieprzerwane działanie banku na określonym poziomie, uwzględniający profil ryzyka operacyjnego banku.***

11.1. W wyniku zdarzeń, które mogą pozostawać poza kontrolą, 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 oraz problemów dla całego systemu finansowego. Sytuacje takie wymagają od banku posiadania wdrożonych planów awaryjnych odtworzenia/wznowienia funkcjonowania istotnych dla jego działalności systemów, uwzględniających różne możliwe scenariusze zdarzeń, na które bank może być narażony i odzwierciedlających skalę i złożoność działalności banku. Posiadanie planów, zapewniających poziom usług dla klientów na akceptowanym przez nich poziomie, ma kluczowe znaczenie dla reputacji banku. Zgodnie z przepisami uchwały w sprawie funkcjonowania systemu zarządzania ryzykiem i systemu kontroli wewnętrznej, w ramach działań zabezpieczających w banku są opracowane i wprowadzone:

- **plany utrzymania ciągłości działania** zapewniające ciągłe i niezakłócone działanie banku,
- **plany awaryjne** służące zapewnieniu możliwości odtworzenia działalności banku i ograniczeniu strat w przypadku wystąpienia niekorzystnych zdarzeń wewnętrznych i zewnętrznych zakłócających tą działalność.

11.2. W tym celu należy zidentyfikować procesy krytyczne, w przypadku których szybkie odzyskanie sprawności działania może mieć istotne znaczenie z punktu widzenia banku, w szczególności te, w przypadku których występuje zależność od źródeł zewnętrznych lub osób trzecich. Dla takich procesów bank powinien określić alternatywne mechanizmy sprawnego funkcjonowania lub wznowienia działania w przypadku awarii.

11.3. Szczególną uwagę należy zwrócić na tworzenie kopii bezpieczeństwa oraz umiejętność odzyskiwania danych elektronicznych (w tym z kopii bezpieczeństwa) i przechowywanych w innej postaci, 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, bezpiecznej lokalizacji 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.

11.4. Opracowując plany awaryjne i plany utrzymania ciągłości działania należy ustalić w szczególności:

- w jakich sytuacjach i w jakim trybie podejmowana będzie decyzja o aktywacji planu awaryjnego?
- jak będą podejmowane decyzje w sytuacji kryzysowej?
- które procesy są krytyczne, ile czasu maksymalnie może trwać ich przywrócenie i jakich zasobów będzie to wymagało?
- jakie są najistotniejsze zagrożenia dla krytycznych procesów i jaki może być ich wpływ na funkcjonowanie tych procesów?
- jak będą realizowane krytyczne procesy w sytuacji, gdy bank będzie miał do dyspozycji ograniczone zasoby?
- w jaki sposób realizowana będzie komunikacja z klientami banku i innymi zainteresowanymi stronami w przypadku zajścia sytuacji kryzysowej?
- jak i kiedy zostaną przywrócone dane i zasoby?
- jak zapewnić odpowiednią jakość danych, w szczególności ich spójność, kompletność i aktualność?
- ile czasu bank może prowadzić działalność w ośrodku zapasowym?
- ile czasu potrwa zorganizowanie niezbędnej przestrzeni biurowej?
- ile czasu potrwa dostarczenie niezbędnego wyposażenia i gdzie powinno ono zostać dostarczone?

11.5. Należy dokonywać okresowych przeglądów planów awaryjnych i planów utrzymania ciągłości działania, w szczególności należy oceniać, czy odpowiadają one zmianom zachodzącym w działalności banku oraz jego otoczeniu.

11.6. W celu zapewnienia odpowiedniego funkcjonowania planów awaryjnych i planów utrzymania ciągłości działania w przypadku zaistnienia niekorzystnych zdarzeń lub awarii, powinny być one przedmiotem okresowych testów, realizowanych z odpowiednią częstotliwością; testy takie powinny być przeprowadzane również w przypadku wprowadzenia istotnych zmian w przebiegu procesów kluczowych. Testując plany awaryjne i plany utrzymania ciągłości działania należy uwzględnić przygotowane wcześniej scenariusze zakładające jednoczesne zajście jednego lub kilku zdarzeń operacyjnych. W testach planów awaryjnych oraz planów ciągłości działania powinny brać udział wszystkie komórki organizacyjne banku niezbędne do realizacji danego planu. Pracownicy banku powinni być świadomi i przeszkoleni w zakresie tych planów w celu sprawnego ich zastosowania w sytuacji awaryjnej. Testy planów ciągłości działania i planów awaryjnych należy w miarę możliwości przeprowadzać przy współudziale kluczowych dostawców.

11.7. W przypadku powierzania wykonywania czynności dostawcy zewnętrznemu, bank zobowiązany jest do weryfikacji jakości i skuteczności planów ciągłości działania i planów awaryjnych dostawcy zapewniających ciągłe i niezakłócone prowadzenie działalności w zakresie objętym umową.

11.8. Dla procesów, których wykonanie w części lub w całości jest zlecane podmiotom zewnętrznym, plany utrzymania ciągłości działania i plany awaryjne banku powinny obejmować – w wymagających tego przypadkach – alternatywne źródło usług oraz zasoby niezbędne do zmiany dostawcy usług w niezbędnym czasie. Należy przy tym zadbać by zagwarantować sobie właściwymi zapisami w umowach z takimi podmiotami możliwość zmiany dostawcy w określonej przez bank sytuacji awaryjnej.

## Transferowanie ryzyka

### 12. Rekomendacja 12

***Bank powinien wykorzystywać optymalne mechanizmy transferu ryzyka, ale nie może traktować ich jako alternatywy dla właściwego zarządzania ryzykiem.***

**Ubezpieczenia**

12.1. Ubezpieczenia służą zabezpieczaniu przed skutkami trudnych do przewidzenia błędów lub zdarzeń operacyjnych o znaczących skutkach finansowych. Przed zawarciem umowy ubezpieczenia bank powinien dokonać wstępnej symulacji efektów redukcji ryzyka operacyjnego wynikających z zakresu i sumy ubezpieczenia, uwzględniając skutki ewentualnego niedopasowania zakresów ubezpieczenia[23]. Ma to na celu ustalenie czy ubezpieczający nie zawiera ubezpieczenia w zbyt małym jak dla siebie zakresie (zarówno kwotowym jak i zdarzeń).

12.2. Bank powinien oceniać i monitorować niepewność dotyczącą płatności kwoty z ubezpieczenia oraz wpływ tych kwestii na profil ryzyka operacyjnego.

Niepewność płatności kwoty z ubezpieczenia może wynikać m.in. z:

- ubezpieczenia się w zbyt małym zakresie (mismatch in coverage),
- zdolności ubezpieczyciela do wywiązania się z zawartej umowy (zawarta umowa ubezpieczenia wykracza poza możliwości ubezpieczyciela),
- zawarcia umowy pozostawiającej ubezpieczycielowi duże pole do zakwestionowania zgłoszonej szkody („słaba umowa ubezpieczenia").

**Zlecanie czynności na zewnątrz (outsourcing)**

12.3. Bank może przyjąć również politykę redukcji ryzyka operacyjnego poprzez zlecanie zadań na zewnątrz. Zlecanie działalności na zewnątrz umożliwia redukcję ryzyka instytucji poprzez transfer niektórych czynności związanych z działalnością bankową wraz z obciążającym je ryzykiem operacyjnym do innej instytucji, posiadającej większe doświadczenie i lepszą infrastrukturę do prowadzenia danej działalności z uwagi na skalę, w jakiej prowadzi tę działalność (jak to ma miejsce np. w przypadku usługi konwojowania lub liczenia środków pieniężnych). Zlecając czynności na zewnątrz bank musi zwrócić szczególną uwagę na zgodność takiego działania z obowiązującym prawem. Należy jednak zwrócić uwagę, że zlecanie czynności na zewnątrz zmienia również profil ryzyka banku, tj. pewne zagrożenia są zastępowane innymi związanymi ze współpracą z dostawcą usług.

[23] Bank dokonując symulacji efektów redukcji ryzyka operacyjnego poprzez ubezpieczenie może m.in. porównywać wielkości ekspozycji na daną kategorię ryzyka operacyjnego i jej różne charakterystyki z zakresem i sumą ubezpieczenia.

12.4. Korzystanie z usług innych firm nie zwalnia kierownictwa banku z odpowiedzialności za kontrolę, czy działalność takich firm prowadzona jest zgodnie z obowiązującym prawem (np. czy zagwarantowane jest bezpieczeństwo tajemnicy prawnie chronionej w zakresie czynności powierzonych przez bank), w sposób bezpieczny oraz należycie staranny. 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.

12.5. Bank powinien prowadzić analizę działalności oraz sytuacji finansowej podmiotów, którym powierzane są czynności, pod kątem zdolności do wywiązania się z przyjętych zobowiązań oraz ryzyka operacyjnego wynikającego z ograniczonej kontroli nad tymi podmiotami, biorąc pod uwagę m.in. doświadczenie rynkowe podmiotów, dostępne certyfikaty i opinie niezależnych audytorów w zakresie związanego z nimi ryzyka operacyjnego oraz jakości świadczonych usług.

**Inne mechanizmy transferu ryzyka**

12.6. Zanim bank zacznie wykorzystywać inne mechanizmy transferu ryzyka na potrzeby obliczania wymogu kapitałowego z tytułu ryzyka operacyjnego metodą zaawansowanego pomiaru, powinien posiadać doświadczenie w korzystaniu z nich w ramach zarządzania ryzykiem operacyjnym.

12.7. W celu zapewnienia efektywności stosowania innych mechanizmów transferu ryzyka (z ang. *other risk transfer mechanisms*), takich jak np. opcje katastroficzne czy *Operational Risk Swaps*, bank powinien podejmować działania mające na celu ustalenie prawdopodobieństwa pokrycia strat przez te narzędzia oraz terminowości związanych z nimi płatności, w tym gromadzić odpowiednie dane zewnętrzne i wewnętrzne. Jest to szczególnie wymagane w przypadku nowatorskich produktów, których funkcjonowanie jest obarczone znaczną niepewnością.

# IX. KONTROLA

## 13. Rekomendacja 13

***Zarząd banku powinien zapewnić istnienie i funkcjonowanie reguł kontroli zarządzania ryzykiem operacyjnym i podejmować działania wspomagające ten proces.***

13.1. Zarząd banku odpowiada za realizację procesu kontroli ryzyka operacyjnego (m.in. jego ciągłość i skuteczność działania), nadzorując (również pośrednio poprzez analizę raportów komórki audytu wewnętrznego) zakres i częstotliwość kontroli wewnętrznej w celu zapewnienia jej adekwatności do profilu ryzyka operacyjnego banku.

13.2. System zarządzania ryzykiem operacyjnym powinien być dostosowany do profilu ryzyka. Bank powinien dokonywać okresowej weryfikacji skuteczności funkcjonowania wdrożonego systemu zarządzania ryzykiem operacyjnym oraz jego adekwatności do profilu ryzyka operacyjnego banku. Częstotliwość weryfikacji systemu zarządzania ryzykiem operacyjnym powinna być dostosowana do profilu ryzyka operacyjnego. W uzasadnionych przypadkach bank powinien dokonać niezbędnych zmian w tym zakresie.

13.3. Weryfikacja i ocena systemu zarządzania ryzykiem, w tym jego regularne przeglądy powinny być dokonywane przez komórkę audytu wewnętrznego lub – w przypadku banków spółdzielczych nieposiadających komórki audytu – przez komórkę audytu banku zrzeszającego. Komórka audytu nie może jednak wypełniać bezpośrednio funkcji zarządzania ryzykiem.

13.4. System kontroli wewnętrznej odgrywa kluczową rolę w ograniczaniu całości ryzyka na jakie narażony jest w swojej działalności bank, jest także istotnym elementem zarządzania ryzykiem operacyjnym**.** Wadliwie funkcjonujące mechanizmy kontroli wewnętrznej i zarządzania bankiem mogą prowadzić do wzrostu zagrożenia z tytułu ryzyka operacyjnego.

13.5. Sprawdzenie, czy system kontroli wewnętrznej jest efektywny, adekwatny i czy działa poprawnie – czyli czy właściwie odgrywa swoją rolę w zarządzaniu ryzykiem – należy między innymi do zadań komórki audytu wewnętrznego lub – w przypadku banków spółdzielczych nieposiadających komórki audytu – do komórki audytu banku zrzeszającego.

13.6. Zgodnie z przepisami § 5 uchwały w sprawie funkcjonowania systemu zarządzania ryzykiem i systemu kontroli wewnętrznej, podejmując decyzje w ramach zarządzania bankiem zarząd banku uwzględnia rezultaty badań prowadzonych przez komórkę audytu

wewnętrznego oraz zewnętrznego (np. biegłych rewidentów). Raport pokontrolny powinien wskazywać istniejące niepożądane zjawiska zwiększające ryzyko operacyjne oraz powinien zawierać zalecenia podjęcia stosownych działań.

13.7. Wykorzystanie przez komórkę audytu wewnętrznego informacji uzyskanych przy pomocy narzędzi zarządzania ryzykiem operacyjnym (np. samooceny jednostek, bazy zdarzeń operacyjnych, mapy ryzyka, analizy scenariuszy) w ramach przygotowywania planów audytu umożliwia lepszą identyfikację obszarów badania audytu (w tym tych, w których występuje podwyższone ryzyko).

## 14. Rekomendacja 14

***Zarząd banku powinien zapewnić, że ryzyko niespełnienia wymogów wynikających z regulacji wewnętrznych i zewnętrznych (w tym prawnych) jest identyfikowane i kontrolowane.***

14.1. Zadania funkcjonującej w banku komórki ds. zarządzania ryzykiem braku zgodności powinny być wyraźnie określone. W przypadku, gdy część zadań odnoszących się do ryzyka braku zgodności jest wykonywana przez jednostkę inną niż komórka ds. zarządzania ryzykiem braku zgodności (np. przez departament prawny) powinien być wyraźnie określony podział obowiązków pomiędzy te jednostki.

14.2. Funkcjonująca w banku komórka ds. zarządzania ryzykiem braku zgodności powinna być w odpowiednim stopniu niezależna, zarówno na poziomie organizacyjnym jak również budżetu i wynagrodzenia pracowników tej jednostki, w szczególności jej kierownik, nie powinien być zaangażowany w działalność, która mogłaby rodzić konflikt interesów z jego obowiązkami w ramach komórki ds. zarządzania ryzykiem braku zgodności.

14.3. Komórka ds. zarządzania ryzykiem braku zgodności musi mieć zapewnione odpowiednie zasoby niezbędne do efektywnego wykonywania jej zadań. W szczególności jej personel powinien posiadać odpowiednie kwalifikacje i doświadczenie, które umożliwią mu właściwe wykonywanie powierzonych obowiązków oraz mieć zapewniony dostęp do informacji niezbędnych do wykonywania swoich obowiązków.

14.4. Należy stworzyć odpowiedni mechanizm współpracy pomiędzy komórką ds. zarządzania ryzykiem braku zgodności a pozostałymi jednostkami organizacyjnymi banku (np. w odniesieniu do dostarczania i wymiany istotnych informacji i uwag),

gwarantujący skuteczność wykonywania obowiązków w ramach zarządzania ryzykiem braku zgodności. Mechanizm współpracy powinien być zatwierdzony przez zarząd banku. Kierownik tej jednostki powinien mieć zapewnione możliwości raportowania do rady nadzorczej banku lub odpowiedniego komitetu przy tej radzie.

14.5. Komórka ds. zarządzania ryzykiem braku zgodności powinna w szczególności być zaangażowana w identyfikację i ocenę ryzyka związanego z rozwijaniem nowych modeli biznesowych lub tworzeniem nowych produktów. W szczególności tworzone nowe produkty nie mogą mieć na celu obchodzenia powszechnie obowiązujących przepisów[24].

14.6. Komórka ds. zarządzania ryzykiem braku zgodności powinna zapewnić wprowadzenie przez właściwe jednostki organizacyjne banku rozwiązań kontrolujących ryzyko braku zgodności związane z klientami i transakcjami (np. tworzenie listy kontrahentów[25], z którymi bank nie zamierza podejmować współpracy, na której znajdują się kontrahenci z krajów o niejasnej sytuacji prawno-politycznej, czy kontrahenci, z którymi współpraca może być obarczona ryzykiem utraty reputacji, lub wykorzystywanie istniejących list podmiotów podejrzewanych o wspieranie terroryzmu, objętych sankcjami itp., czy których działalność może być sprzeczna z powszechnie obowiązującymi przepisami).

[24] Bardziej szczegółowe spojrzenie na zagadnienia identyfikacji i pomiaru ryzyka braku zgodności znaleźć można m.in. w dokumencie Komitetu Bazylejskiego: Basel Committee on Banking Supervision (2005), *Compliance and the compliance function in banks.*

[25] Wprowadzając takie narzędzie należy zwrócić uwagę na ograniczenia prawne w tym zakresie, takiej jak przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U.2002.101.926 j.t. z późn. zm.).

# X. MONITOROWANIE

## 15. Rekomendacja 15

***Bank powinien posiadać system regularnego monitorowania zdarzeń operacyjnych oraz wyników pozostałych narzędzi w tym zakresie (np. KRI), umożliwiający obserwację profilu ryzyka operacyjnego oraz zapewniający regularne przekazywanie zarządowi i radzie nadzorczej stosownych informacji.***

15.1. Regularne monitorowanie stanowi podstawę szybkiego wykrycia słabości występujących w systemie zarządzania ryzykiem. Szybka identyfikacja i analiza okoliczności związanych z odnotowanym zdarzeniem i stratą operacyjną pozwala określić część lub wszystkie przyczyny wystąpienia zdarzenia operacyjnego i odpowiednie zapobieganie ich powtórzeniu. Szybkie uzyskanie precyzyjnych informacji w zakresie wykrytych nieprawidłowości może pozwolić na podjęcie działań niwelujących negatywny odbiór banku przez otoczenie, wyprzedzających ewentualną utratę reputacji albo działań, które pozwolą szybko ją odbudować.

15.2. Monitorowaniu powinien podlegać co najmniej przebieg wszystkich kluczowych procesów w banku.. Proces ten powinien umożliwiać obserwację profilu ryzyka operacyjnego. Monitorowanie powinno obejmować zdarzenia operacyjne, ich źródła, czynniki otoczenia gospodarczego i kontroli oraz skuteczność działań kontrolnych i odwracających (naprawczych) i innych metod ograniczania lub transferu ryzyka, umożliwiając podjęcie działań wyprzedzających powstanie straty.

15.3. Członkowie rady nadzorczej i zarządu powinni być świadomi profilu ryzyka operacyjnego występującego w banku, wiedzieć i rozumieć w jaki sposób został on wyznaczony i jak sposób jego wyznaczenia mógł wpłynąć na to że wyznaczony profil odbiega od rzeczywistego. Powinni też upewnić się, że całościowa strategia banku uwzględnia uwarunkowania wynikające z tego profilu.

15.4. Złożoność systemu monitorowania i częstotliwość wykonywania czynności monitorujących powinna wynikać ze świadomie akceptowanych (z góry określonych przez zarząd i zatwierdzonych przez radę nadzorczą) tolerancji/apetytu na ryzyko operacyjne, profilu tego ryzyka oraz częstotliwości i natury zmian w banku i jego otoczeniu.

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

- rodzaj i istotność zdarzeń operacyjnych,
- rodzaje, stopień skomplikowania i wartość realizowanych oraz planowanych operacji,
- złożoność wykorzystywanych systemów,
- zależności pomiędzy bankiem a podmiotami powiązanymi,
- poziom kwalifikacji pracowników oraz zmiany kadrowe,
- złożoność struktury organizacyjnej i poziom jej zmienności.

# XI. RAPORTOWANIE I PRZEJRZYSTOŚĆ DZIAŁANIA

## Raportowanie

### 16. Rekomendacja 16

***Bank powinien dokładać wszelkich starań, aby pozyskiwane przez niego dane do raportowania (w szczególności na potrzeby zarządcze) były rzetelne oraz charakteryzowały się wysoką jakością, w tym na bieżąco kontrolować tę jakość. Powinien również kontrolować wpływ jakości tych danych na proces zarządzania ryzykiem.***

16.1. Banki powinny opracować system sprawozdawczości wewnętrznej (informacji zarządczej) w zakresie ryzyka operacyjnego umożliwiający ocenę ich narażenia na ryzyko operacyjne oraz skuteczne zarządzanie tym ryzykiem. Co więcej, odpowiednio dla przyjętego systemu zarządzania, kierownictwo banku powinno otrzymywać regularne raporty z poszczególnych linii biznesowych, komórek (komórki) zarządzania ryzykiem, jak i komórki audytu wewnętrznego, zarówno w warunkach normalnych, jak i skrajnych. Raporty dotyczące ryzyka operacyjnego powinny zawierać co najmniej informacje wymagane przepisami uchwały w sprawie funkcjonowania systemu zarządzania ryzykiem i systemu kontroli wewnętrznej. W szczególności w informacjach tych należy uwzględnić:

- wykorzystanie założonych tolerancji/apetytu na ryzyko operacyjne danego rodzaju,
- szczegółową charakterystykę ostatnich znaczących wewnętrznych zdarzeń operacyjnych z wewnętrznej bazy zdarzeń operacyjnych i strat z nimi związanych,
- informacje dotyczące istotnych zdarzeń zewnętrznych oraz prawdopodobieństwa zajścia takich zdarzeń w banku i ich potencjalnego wpływu m.in. na wynik finansowy i wymóg kapitałowy z tytułu ryzyka operacyjnego,
- informacje pochodzące z innych wykorzystywanych w banku narzędzi zarządzania ryzykiem operacyjnym.

16.2. W raportach powinny być odpowiednio opisane zarówno zidentyfikowane zdarzenia, jak i działania je korygujące, które pomogą uniknąć strat związanych z zajściem podobnych zdarzeń w przyszłości. Szybkie zaraportowanie precyzyjnych informacji w zakresie wykrytych nieprawidłowości może pozwolić na podjęcie działań niwelujących negatywny odbiór banku przez otoczenie, wyprzedzających ewentualną utratę reputacji albo działań, które pozwolą szybko ją odbudować.

16.3. Raporty powinny być przekazywane na odpowiednie poziomy zarządzania oraz do linii biznesowych banku, których te dane dotyczą lub mogą wspomagać procesy w nich zachodzące. Raportowanie powinno wspierać proces decyzyjny, a częstotliwość tego raportowania powinna być uzależniona od skali działalności, profilu ryzyka i stopnia złożoności prowadzonej działalności, co oznacza m.in., że przed ostatecznym terminem, kiedy dana decyzja musi być podjęta, bank dokłada wszelkich starań, żeby dostępne były potrzebne do tego informacje.

16.4. W celu poprawy jakości zarządzania ryzykiem operacyjnym w banku należy zapewnić odpowiednie zasady wewnętrznej dystrybucji informacji dotyczącej tego rodzaju ryzyka.

16.5. W ramach kontroli poprawności systemów raportów dotyczących ryzyka i kontroli, kierownictwo powinno regularnie weryfikować jakość systemu raportowania.

**Przejrzystość działania**

## 17. Rekomendacja 17

***Bank powinien regularnie ogłaszać informacje na temat swojego podejścia do ryzyka operacyjnego służące ograniczeniu asymetrii informacji pomiędzy bankiem a jego otoczeniem.***

17.1. Asymetria informacji pomiędzy bankiem a jego udziałowcami oraz klientami, deponującymi w nim swoje środki czy prowadzącymi za jego pośrednictwem rozliczenia, jest zjawiskiem niepożądanym z punktu widzenia bezpieczeństwa systemu bankowego, stąd jednym z kluczowych elementów regulacji bankowych jest dyscyplina rynkowa. Obowiązek ogłaszania informacji na temat ogólnego podejścia do zarządzania ryzykiem operacyjnym ma wpływ na poprawę dyscypliny rynkowej, gdyż umożliwia inwestorom i klientom banku ocenę, czy bank efektywnie zarządza tym rodzajem ryzyka. Dotyczy to zarówno banków korzystających z zaawansowanych metod pomiaru ryzyka operacyjnego, jak i pozostałych. Dodatkowo, działanie to ma wpływ na poprawę efektywności zarządzania ryzykiem w systemie bankowym (np. poprzez wymianę informacji) i może pomóc w utrzymaniu reputacji.

17.2. Odpowiedzialność za ogłaszanie informacji, o których mowa w pkt. 17.1 spoczywa na zarządzie banku.

17.3. Zakres ogłaszanych informacji nie powinien ograniczać się tylko do minimum określonego w Uchwale nr 385/2008 Komisji Nadzoru Finansowego z dnia 17 grudnia 2008 r. w sprawie szczegółowych zasad i sposobu ogłaszania przez banki informacji o charakterze jakościowym i ilościowym dotyczących adekwatności kapitałowej oraz zakresu informacji podlegających ogłaszaniu (Dz. Urz. KNF Nr 8, poz. 39 z późn. zm.) (tj. do podania informacji o metodzie stosowanej do wyznaczania wymogu kapitałowego z tytułu ryzyka operacyjnego, czy ewentualnie użytego w tej metodzie mechanizmu transferu ryzyka), ale – w zależności od wielkości banku, profilu ryzyka i stopnia złożoności prowadzonej przez niego działalności – powinien obejmować także inne informacje służące ograniczeniu asymetrii informacji pomiędzy bankiem a jego otoczeniem. Działanie takie będzie zgodne z § 4. ust. 3 ww. uchwały. Ogłaszając informacje z zakresu adekwatności kapitałowej, w obszarze ryzyka operacyjnego bank powinien dawać świadectwo bezpiecznego zarządzania ryzykiem operacyjnym w oparciu o dobre praktyki rynkowe, w szczególności wykazując, że stara się wypełniać zalecenia wynikające z niniejszego dokumentu. Powinien przy tym również informować otoczenie o sumach strat brutto z tytułu ryzyka operacyjnego odnotowanych w danym roku, w podziale na klasy zdarzeń, w tym co najmniej w podziale na kategorie zdarzeń w ramach rodzaju zdarzenia (zgodnie z załącznikiem nr 1), oraz o tym, jakie działania mitygujące[26] w związku z tym zostały podjęte w celu uniknięcia ich w przyszłości.

Bank powinien również rozważyć publikację bardziej szczegółowych informacji o najpoważniejszych, jego zdaniem, zdarzeniach operacyjnych, jakie wystąpiły u niego w minionym roku. W szczególnych sytuacjach, kiedy publikacja informacji mogłaby zagrażać bieżącemu bezpieczeństwu procesów operacyjnych banku (np. w sytuacji, gdy usuwanie przyczyn zdarzenia operacyjnego jest w toku, a podanie informacji o nim do publicznej wiadomości mogłoby stwarzać zagrożenie, czy też opóźnić usunięcie przyczyny zdarzenia) publikacja informacji o danym zdarzeniu powinna zostać opóźniona do czasu kolejnego ogłoszenia.

[26] Publikując informacje na temat działań mitygujących należy zadbać, by zawarte informacje nie ujawniały wrażliwych szczegółów mechanizmów zabezpieczających banku, przez co mogłyby znacząco zwiększyć narażenie banku na ryzyko operacyjne.

# XII. SPIS TREŚCI


I. WSTĘP ... 2
Uwagi ogólne ... 2
Zakres i układ rekomendacji ... 3
II. SŁOWNIK POJĘĆ ... 7
III. LISTA REKOMENDACJI ... 10
IV. STRATEGIA ZARZĄDZANIA RYZYKIEM OPERACYJNYM ... 13
V. ŚRODOWISKO WEWNĘTRZNE ... 16
Zasoby Ludzkie ... 16
Systemy ... 18
Procesy ... 20
VI. IDENTYFIKACJA RYZYKA ... 28
VII. OCENA RYZYKA ... 33
Testy warunków skrajnych (z ang. *stress tests*) ... 34
VIII. PRZECIWDZIAŁANIE RYZYKU ... 37
Plany ciągłości działania i plany awaryjne ... 38
Transferowanie ryzyka ... 40
Ubezpieczenia ... 41
Zlecanie czynności na zewnątrz (outsourcing) ... 41
Inne mechanizmy transferu ryzyka ... 42
IX. KONTROLA ... 43
X. MONITOROWANIE ... 46
XI. RAPORTOWANIE I PRZEJRZYSTOŚĆ DZIAŁANIA ... 48
Raportowanie ... 48
Przejrzystość działania ... 49
XII. SPIS TREŚCI ... 51
ZAŁĄCZNIK NR 1 ... 52
ZAŁĄCZNIK NR 2 – PODZIAŁ NA LINIE BIZNESOWE ... 55
ZAŁĄCZNIK NR 3 – PRZYKŁAD NARZĘDZI DO OCENY RYZYKA ... 57



Opracowano w:
Departamencie Regulacji Bankowych i Instytucji Płatniczych

## ZAŁĄCZNIK NR 1

| Rodzaj zdarzenia | Definicja | Kategoria zdarzenia w ramach rodzaju | Przykłady zdarzeń operacyjnych |
|---|---|---|---|
| 1.Oszustwa wewnętrzne | Straty spowodowane celowym działaniem polegającym na defraudacji, sprzeniewierzeniu majątku, obejściach regulacji, przepisów prawa lub przepisów wewnętrznych przedsiębiorstwa, wyłączając straty wynikające z różnicowania/dyskryminacji pracowników, które dotyczą co najmniej jednej strony wewnętrznej. | 1) Działania nieuprawnione | 1) Działania nierejestrowane (zamierzone)<br>2) Nieautoryzowane transakcje (poniesiona strata)<br>3) Błędna wycena transakcji (zamierzona) |
| | | 2) Kradzież i oszustwo | 1) Oszustwo, oszustwo kredytowe, bezwartościowy depozyt<br>2) Kradzież, wymuszenie, defraudacja, rabunek<br>3) Sprzeniewierzenie aktywów<br>4) Zamierzone zniszczenie aktywów<br>5) Fałszerstwo<br>6) Oszustwo czekowe<br>7) Przemyt<br>8) Przejęcie rachunku, podszycie, itp.<br>9) Niezgodności podatkowe, unikanie podatków (umyślne)<br>10) Przekupstwo, łapówkarstwo<br>11) Wykorzystanie poufnych informacji w transakcji w celu osiągnięcia korzyści (nie na rachunek banku) |
| 2.Oszustwa zewnętrzne | Straty spowodowane celowym działaniem polegającym na defraudacji, sprzeniewierzeniu majątku lub obejściu regulacji prawnych przez stronę trzecią. | 1) Kradzież i oszustwo | 1) Kradzież, rabunek<br>2) Fałszerstwo<br>3) Oszustwo czekowe |
| | | 2) Bezpieczeństwo systemów | 1) Uszkodzenia na skutek działań hakerskich<br>2) Kradzież informacji (poniesiona strata) |

| | | | |
|---|---|---|---|
| 3.Zasady dotyczące zatrudnienia oraz bezpieczeństwo w miejscu pracy | Straty powstałe na skutek działań niezgodnych z przepisami lub porozumieniami dotyczącymi zatrudnienia, bezpieczeństwa i higieny pracy, wypłaty odszkodowań z tytułu uszkodzenia ciała lub straty wynikające z nierównego traktowania i dyskryminacji pracowników. | 1) Stosunki pracownicze | 1) Zdarzenia związane z wypłatą wynagrodzeń, przekazywaniem innych korzyści oraz z rozwiązywaniem współpracy z pracownikiem,<br>2) Zorganizowane działania związków zawodowych (strajki, protesty) |
| | | 2) Bezpieczeństwo środowiska pracy | 1) Wypadki na terenie administrowanym przez bank<br>2) Wypadki przy pracy z powodu nieprzestrzegania przez bank przepisów BHP i ppoż.<br>3) Inne zdarzenia skutkujące wypłatami odszkodowań dla pracowników |
| | | 3) Podziały i dyskryminacja | Wszelkie typy dyskryminacji pracowników |
| 4.Klienci, produkty i praktyki operacyjne | Straty wynikające z niewywiązania się z obowiązków zawodowych względem określonych klientów, będące skutkiem działań nieumyślnych lub zaniedbania (w tym wymagań powierniczych i stosownego zachowania) lub też związane z charakterem bądź konstrukcją produktu. | 1) Obsługa klientów, ujawnianie informacji o klientach, zobowiązania względem klientów | 1) Nadużycie zaufania, naruszenie wytycznych w zakresie obsługi klientów<br>2) Zagadnienia dotyczące należytej staranność w zakresie weryfikacji klienta i dopasowaniem oferowanych mu produktów (poznaj swego klienta, itp.)<br>3) Ujawnianie informacji dotyczących klientów indywidualnych<br>4) Naruszenie prywatności<br>5) Agresywna sprzedaż<br>6) Agresywny handel na rachunek klienta w celu maksymalizacji prowizji<br>7) Nieuprawnione użycie informacji poufnej<br>8) Odpowiedzialność kredytodawcy |
| | | 2) Niewłaściwe praktyki biznesowe lub rynkowe | 1) Pogwałcenie przepisów antymonopolowych<br>2) Niewłaściwe praktyki handlowe/rynkowe<br>3) Manipulacje rynkiem finansowym<br>4) Wykorzystanie poufnych informacji w transakcji w celu osiągnięcia korzyści (na rachunek banku)<br>5) Działanie bez licencji<br>6) Pranie pieniędzy |
| | | 3) Wady produktów | 1) Wadliwie skonstruowane produkty bankowe (w tym błędy wzorów umów, regulaminów i innych tego typu dokumentów, brak właściwej autoryzacji)<br>2) Błędy modeli |
| | | 4) Klasyfikacja klienta i ekspozycje | 1) Dokonywanie oceny profilu klienta niezgodnie z wytycznymi<br>2) Przekraczanie limitów ekspozycji względem klienta |
| | | 5) Usługi doradcze | Spory o jakość działalności doradczej świadczonej przez bank |

| | | | |
|---|---|---|---|
| 5.Szkody związane z aktywami rzeczowymi | Straty powstałe na skutek straty lub szkody w aktywach rzeczowych w wyniku klęski żywiołowej lub innych wydarzeń. | Klęski żywiołowe i inne zdarzenia | 1) Straty powstałe w wyniku klęsk żywiołowych<br>2) Straty wynikające z działalności terrorystycznej, wandalizmu |
| 6.Zakłócenia działalności banku i awarie systemów | Straty powstałe na skutek zakłóceń działalności banku lub awarii systemów. | Systemy | 1) Nieprawidłowe działanie sprzętu<br>2) Nieprawidłowe działanie oprogramowania<br>3) Nieprawidłowe działanie sieci telekomunikacyjnych i komputerowych<br>4) Przerwy w dopływie energii elektrycznej oraz nieprawidłowe działanie urządzeń podtrzymujących zasilanie |
| 7.Wykonanie transakcji, dostawa i zarządzanie procesami operacyjnymi | Straty powstałe na skutek nieprawidłowego rozliczenia transakcji lub wadliwego zarządzania procesami operacyjnymi oraz wynikłe ze stosunków z kontrahentami i sprzedawcami. | 1) Wprowadzanie do systemu, wykonywanie, rozliczanie i obsługa transakcji | 1) Błędy w komunikacji<br>2) Błędy wprowadzania, utrzymania i ładowania danych<br>3) Przeoczenie terminu lub niewywiązanie się z ciążącego obowiązku<br>4) Błędne działanie modelu lub systemu<br>5) Błędy księgowe/ błędne przypisanie do rachunku<br>6) Błędy wykonania innych zadań<br>7) Niewykonanie dostawy<br>8) Błędy w zakresie zarządzania zabezpieczeniami transakcji<br>9) Utrzymywanie danych referencyjnych |
| | | 2) Monitorowanie i sprawozdawczość | 1) Niewykonanie obowiązku sprawozdawczego<br>2) Opublikowanie nierzetelnego sprawozdania (poniesiona strata) |
| | | 3) Napływ i dokumentacja klientów | 1) Zagubienie dokumentacji dotyczącej udzielenia, odwołania pełnomocnictwa oraz klauzul<br>2) Brak/niekompletność dokumentacji prawnej |
| | | 4) Zarządzanie rachunkami klientów | 1) Udzielenie dostępu do rachunku osobom nieuprawnionym<br>2) Błędne dane klienta (poniesiona strata)<br>3) Wyrządzenie szkody lub straty w aktywach klienta wskutek zaniedbania |
| | | 5) Kontrahenci niebędący klientami banku (np. izby rozliczeniowe) | 1) Błąd kontrahenta niebędącego klientem banku<br>2) Spory z kontrahentami niebędącymi klientami banku |
| | | 6) Sprzedawcy i dostawcy | 1) Wadliwie sporządzone umowy dotyczące powierzania wykonywania czynności bankowych podmiotom zewnętrznym oraz ich niewłaściwe realizowanie<br>2) Spory ze sprzedawcami i dostawcami |

# ZAŁĄCZNIK NR 2 – PODZIAŁ NA LINIE BIZNESOWE

| | Rodzaje czynności |
|---|---|
| Bankowość inwestycyjna | Gwarantowanie emisji instrumentów finansowych lub subemisja instrumentów finansowych z gwarancją przejęcia emisji<br><br>Usługi związane z gwarantowaniem emisji<br><br>Doradztwo inwestycyjne<br><br>Doradztwo dla podmiotów gospodarczych w zakresie struktury kapitałowej, strategii branżowej i zagadnień pokrewnych oraz doradztwo i usługi w zakresie fuzji i przejęć podmiotów gospodarczych<br><br>Badania inwestycyjne i analizy finansowe oraz inne formy ogólnych zaleceń w sprawie transakcji związanych z instrumentami finansowymi |
| Działalność dealerska | Zawieranie transakcji na własny rachunek<br><br>Usługi brokerskie na rynku pieniężnym<br><br>Przyjmowanie oraz przekazywanie zleceń związanych z instrumentami finansowymi<br><br>Wykonywanie zleceń w imieniu klienta<br><br>Subemisja instrumentów finansowych bez gwarancji przejęcia emisji<br><br>Operacje w alternatywnym systemie obrotu określonym w art. 3 pkt 2 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi |
| Detaliczna działalność brokerska<br>(obsługa osób fizycznych lub małych i średnich przedsiębiorstw spełniających warunki, o których mowa w § 21 załącznika nr 4 do uchwały w sprawie adekwatności kapitałowej) | Przyjmowanie oraz przekazywanie zleceń związanych z instrumentami finansowymi<br>Wykonywanie zleceń w imieniu klienta<br>Subemisja instrumentów finansowych z gwarancją przejęcia emisji |
| Bankowość komercyjna (w tym obsługa małych i średnich przedsiębiorstw niespełniających warunków, o których | Przyjmowanie depozytów i innych wkładów pieniężnych płatnych na żądanie<br>Udzielanie kredytów i pożyczek gotówkowych<br>Leasing finansowy<br>Gwarancje i inne zobowiązania pozabilansowe |

| | |
|---|---|
| mowa w § 21 załącznika nr 4 do uchwały w sprawie adekwatności kapitałowej) | |
| Bankowość detaliczna (obsługa osób fizycznych lub małych i średnich przedsiębiorstw spełniających warunki, o których mowa w § 21 załącznika nr 4 do uchwały w sprawie adekwatności kapitałowej) | Przyjmowanie depozytów i wkładów pieniężnych płatnych na żądanie<br>Udzielanie kredytów i pożyczek gotówkowych<br>Leasing finansowy<br>Gwarancje i inne zobowiązania pozabilansowe |
| Płatności i rozliczenia | Usługi związane z transferem środków pieniężnych<br>Emitowanie instrumentów płatniczych i administrowanie nimi |
| Usługi pośrednictwa (agencyjne) | Przechowywanie instrumentów finansowych i administrowanie nimi na rachunkach klientów, w tym usługi powiernicze i podobne, takie jak zarządzanie gotówką lub zabezpieczeniami |
| Zarządzanie aktywami | Zarządzanie portfelem<br>Zarządzanie instytucjami zbiorowego inwestowania<br>Inne formy zarządzania aktywami |

# ZAŁĄCZNIK NR 3 – PRZYKŁAD NARZĘDZI DO OCENY RYZYKA

Banki w procesie oceny ryzyka prawie zawsze wykorzystują kombinacje różnych metod oceny ryzyka. Mogą to być zarówno metody statystyczne oparte na danych ilościowych, jak i metody oparte na samoocenie ryzyka (z ang. *risk self-assesment*). Mianem samooceny określa się szereg narzędzi do zarządzania ryzykiem, w których źródłem danych są odpowiedzi przedstawicieli obszarów biznesowych na predefiniowane pytania, lub odpowiedzi otrzymane w trakcie warsztatów eksperckich (osoby dobrze znające zagrożenia występujące w danym obszarze działalnosci banku), które mają dać obraz występującego w banku ryzyka. W miarę potrzeb należy rozszerzać i systematyzować wprowadzone rozwiązania służące ocenie ryzyka operacyjnego, na które bank jest narażony. Przykładowe narzędzia służące do oceny ryzyka zostały zaprezentowana poniżej.

**Statystyczne modele ryzyka oparte o rozkład strat (z ang. *loss distribution approach*)** to rozwiązanie, w którym bank – na podstawie posiadanych przez siebie danych ilościowych o stratach – ustala i analizuje łączny rozkład strat danego rodzaju. Danymi do analizy mogą być historyczne dane wewnętrzne, wewnętrzne dane uzyskane na podstawie analiz jakościowych, czy dane zewnętrzne. Łączny rozkład strat to rozkład uzyskany w drodze połączenia ustalonych odrębnie rozkładów częstości i dotkliwości strat. Rozkłady częstości i dotkliwości strat ustala się poprzez dopasowanie do rozkładu empirycznego rozkładu (bądź rozkładów) teoretycznych. Przykładowo, dla częstości występowania strat często dopasowywanym rozkładem jest rozkład Poisson'a, a dla dotkliwości rozkład Pareto (lub jego uogólnienie) czy też rozkład lognormalny[27]. W idealnym przypadku ustalanie i analiza rozkładu strat powinno się odbywać dla pojedynczych komórek bazylejskiej macierzy ryzyka operacyjnego (czyli danego rodzaju zdarzenia w obrębie danej linii biznesowej), jednak z uwagi na częste problemy z odpowiednią ilością danych dopuszcza się agregacje zdarzeń należących do różnych komórek pod warunkiem, że łączone rodzaje zdarzeń (niezależnie czy z tej samej linii biznesowej, czy z różnych) stworzą zbiory homogeniczne zarówno statystycznie, jak i pod kątem czynników ryzyka.

Za homogeniczne statystycznie uznać można zbiory zawierające dane o maksymalnie zbliżonych własnościach statystycznych, w tym charakteryzujących się identycznością rozkładu dotkliwości i częstości z dokładnością do czynnika skalującego.

Homogeniczność pod kątem czynników ryzyka może natomiast wynikać z zależności zdarzeń zawartych w zbiorze od podobnych, kluczowych czynników ryzyka, czy też podobieństw zarządzania z perspektywy ryzyka operacyjnego.

[27] Często stosowane są również rozkłady należące do klasy uogólnionych rozkładów wartości ekstremalnych (*Generalised Extreme Value Distributions*), np. rozkład Weibulla, rozkład Fréchet'a, rozkład Gumbela.

**Analiza scenariuszowa ryzyka operacyjnego** polega na analizie funkcjonowania instytucji (np. powstałe straty, utracone korzyści, wąskie gardła, działanie planów awaryjnych, itp.) w sytuacji wystąpienia badanego scenariusza przygotowanego przez bank na podstawie wkładu informacyjnego z rejestrów zdarzeń operacyjnych (rejestrów strat), zewnętrznych źródeł informacji o stratach, przy uzględnieniu czynników otoczenia gospodarczego i kontroli.

**Karta ocen (z ang. *scorecard*)** to narzędzie umożliwiające określenie ratingu narażenia na różne klasy zdarzeń operacyjnych. Na podstawie wkładu informacyjnego z różnych źródeł (np. dane o stratach operacyjnych, wyniki analiz scenariuszowych, czynniki otoczenia gospodarczego i kontroli) bank opracowuje pewnego rodzaju system scoringowy, w którym różne informacje związane ze zdarzeniami danej klasy są odpowiednio zważone i dają jednostkowy wynik rangujący ryzyko dla danej klasy zdarzeń operacyjnych. Rating może odnosić się do poszczególnych pionów operacyjnych lub też może być przypisany do kilku różnych pionów operacyjnych jednocześnie. Ponadto, rating może odnosić się zarówno do konkretnej klasy zdarzenia, jak i do sposobu kontroli i zabezpieczania się przed nim.

**Kluczowe wskaźniki ryzyka (z ang. *key risk indicators*)** tworzy zestaw syntetycznych wskaźników przydatnych do oceny 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 to narzędzie o charakterze proaktywnym, badające zarówno poziomy, jak i tendencje zmian tych wskaźników, mające na celu ostrzeganie banku o możliwych zmianach związanych z ryzykiem operacyjnym. Do wskaźników tych można na przykład zaliczyć: częstotliwość błędów (np. związanych z przetwarzaniem przelewów), czasy niedostępności systemów w stosunku do średniego czasu ich wykorzystywania, wskaźniki zmian kadrowych (np. liczba zmian personalnych na danym stanowisku w określonym przedziale czasu). Istotne źródło informacji o skali ryzyka operacyjnego mogą stanowić również skargi od klientów banku, które często pokazują nieprawidłowości i ułomności procedur, procesów lub systemów banku z innej perspektywy. W praktyce często stosuje się także kluczowe wskaźniki kontroli (z ang. *key control indicators*) i kluczowe wskaźniki efektywności (z ang. *key performance indicators*) . Kluczowe wskaźniki kontroli są używane do określenia środowiska kontroli wewnętrznej, monitorowania poziomu tej kontroli w stosunku do tolerancji na ryzyko. Kluczowe wskaźniki efektywności są zestawem wskaźników wykorzystywanym do oceny procesu realizacji celów. Ich rolą jest kwantyfikacja stanu wybranego elementu w procesie tak, aby można było ocenić postęp i podjąć ewentualną korektę, zapewniając efektywną realizację założonego w nim celu. Wskaźniki efektywności ustalane są zgodnie ze strategią organizacji i zalicza się je wraz z kluczowymi wskaźnikami

kontroli i kluczowymi wskaźnikami ryzyka do czynników otoczenia gospodarczego i kontroli wewnętrznej (z ang. *Business Environment and Internal Control Factors).*

**Mapy ryzyka operacyjnego (z ang. *operational risk mapping*)** to narzędzie służące zarówno do identyfikacji, jak i oceny ryzyka operacyjnego. Jego ideą jest analiza ryzyka wykonywana przez jednostki operacyjne. Mapy ryzyka mogą odwzorowywać powiązania poszczególnych czynników ryzyka operacyjnego z poszczególnymi liniami biznesowymi, pionami operacyjnymi, funkcjami organizacyjnymi i procesami. Proces konstruowania „mapy ryzyka" można rozpocząć od wypunktowania w komórkach wspomnianej we wstępie do niniejszego dokumentu bazylejskiej macierzy ryzyka operacyjnego już zarejestrowanych i/lub potencjalnie możliwych zdarzeń operacyjnych wraz z poziomem ich dotkliwości. Wypełnianie komórek przez pracowników poszczególnych obszarów biznesowych, polegające na określaniu poziomu ryzyka dla danych zdarzeń i tego, jaką mają nad nim kontrolę, odbywa się na bazie historycznej, ale także hipotetycznej (w tym w oparciu o informacje dot. zdarzeń typu *near-miss*)[28]. Dodatkowo, do poszczególnych zagrożeń mogą być wskazane działania ograniczające.

Zdarzenia operacyjne uwzględnione w ramach powyższej analizy mogą być również przedstawiane na wykresie punktowym, gdzie na osiach wskazuje się odpowiednio częstość i dotkliwość. Wykres ten jest następnie dzielony na cztery części w których znajdą się:

- zdarzenia o niskiej częstości i dotkliwości,
- zdarzenia o wysokiej częstości i dotkliwości,
- zdarzenia o niskiej częstości, ale wysokiej dotkliwości,
- zdarzenia o wysokiej częstości, ale niskiej dotkliwości.

W zależności od zatwierdzonych przez odpowiednie władze w banku punktów podziału dla zdarzeń w poszczególnych częściach wykresu podejmowane mogą być inne działania.

[28] Może do tego posłużyć szereg formularzy umożliwiających szybkie wypełnienie i agregację informacji, przy czym jednocześnie należy zadbać o to, by uniemożliwiały one zwyczajne kopiowanie ich zawartości z formularzy z wcześniejszych okresów i od innych ankietowanych.