

Grupa robocza ds. oceny i wdrażania

WSKAZÓWKI W ZAKRESIE PODEJŚCIA OPARTEGO NA RYZYKU  
DLA SEKTORA PODMIOTÓW ŚWIADCZĄCYCH USŁUGI PIENIĘŻNE  
(MSB)

*Niniejszy dokument uwzględnia dodatkowe komentarze przesłane do Sekretariatu FATF w sprawie projektu wskazówek w zakresie podejścia opartego na ryzyku dla sektora MSB, przekazanego do wszystkich delegacji na początku maja 2009 r.*

John CARLSON, tel. + 33 1 45 24 79 46; john.carlson@fatf-gafi.org  
Catherine MARTY, tel. + 33 1 45 24 94 89; catherine.marty@fatf-gafi.org  
Stephanie TALBOT, tel. + 33 1 45 24 96 44; stephanie.talbot@fatf-gafi.org

JT03267607

## SPIS TREŚCI

CZĘŚĆ PIERWSZA: WYKORZYSTANIE WSKAZÓWEK I CEL PODEJŚCIA OPARTEGO NA RYZYKU .....	4
Rozdział Pierwszy: Tło i kontekst .....	4
<i>Cel wskazówek:</i> .....	4
<i>Odbiorcy docelowi, status i treść wskazówek:</i> .....	5
Rozdział drugi: Podejście oparte na ryzyku – cel, korzyści i wyzwania .....	5
<i>Cel podejścia opartego na ryzyku</i> .....	5
<i>Potencjalne korzyści i wyzwania podejścia opartego na ryzyku</i> .....	7
Rozdział trzeci: FATF i podejście oparte na ryzyku .....	9
<i>Zasada ogólnego ryzyka</i> .....	9
<i>Odniesienia do szczególnego ryzyka</i> .....	10
<i>Możliwość zastosowania podejścia opartego na ryzyku do finansowania terroryzmu</i> ....	12
<i>Ograniczenia podejścia opartego na ryzyku</i> .....	14
<i>Rozróżnienie między nadzorem opartym na ryzyku a politykami i procesami opartymi na ryzyku</i> .....	15
CZĘŚĆ DRUGA: WSKAZÓWKI DLA WŁADZ PUBLICZNYCH .....	17
Rozdział pierwszy: Ogólne zasady tworzenia podejścia opartego na ryzyku .....	17
<i>Zasada pierwsza: zrozumienie i reagowanie na zagrożenia i najbardziej podatne/niebezpieczne obszary: krajowa ocena ryzyka</i> .....	17
<i>Zasada druga: ramy prawne/regulacyjne wspierające stosowanie podejścia opartego na ryzyku</i> .....	18
<i>Zasada trzecia: projekt ram nadzoru wspierający zastosowanie podejścia opartego na ryzyku</i> .....	18
<i>Zasada czwarta: identyfikacja głównych zaangażowanych podmiotów i zapewnienie spójności</i> .....	19
<i>Zasada piąta: wymiana informacji między sektorem publicznym a sektorem prywatnym</i> .....	20
Rozdział drugi: Wdrożenie podejścia opartego na ryzyku .....	21
<i>Ocena ryzyka kształtująca priorytety krajowe</i> .....	21
<i>Nadzór regulacyjny – Zasady ogólne</i> .....	23
CZĘŚĆ TRZECIA: WSKAZÓWKI DLA PODMIOTÓW ŚWIADCZĄCYCH USŁUGI PIENIĘŻNE (MSB) W ZAKRESIE WDRAŻANIA PODEJŚCIA OPARTEGO NA RYZYKU .....	28
Preambuła .....	28
Rozdział pierwszy: Kategorie ryzyka .....	29
<i>Ryzyko związane z krajem/obszarem geograficznym</i> .....	30
<i>Ryzyko związane z klientem</i> .....	31
<i>Ryzyko związane z produktem/usługą</i> .....	32
<i>Ryzyko związane z pośrednikami</i> .....	33
<i>Czynniki mogące wpłynąć na ocenę ryzyka</i> .....	34
<i>Kontrole w sytuacjach wysokiego ryzyka</i> .....	35
Rozdział drugi: Zastosowanie podejścia opartego na ryzyku .....	35
<i>Należyta staranność w kontaktach z klientami/poznaj swojego klienta</i> .....	35
<i>Monitoring klientów i transakcji</i> .....	37
<i>Raportowanie transakcji podejrzanych</i> .....	38
<i>Szkolenie i zwiększanie świadomości</i> .....	38
<i>Należyta staranność w kontaktach z pośrednikiem/poznaj swojego pośrednika</i> .....	39
<i>Monitorowanie pośredników</i> .....	41

<i>Szkolenie i zwiększanie świadomości</i> .....	42
Rozdział trzeci: Kontrole wewnętrzne .....	42
ZAŁĄCZNIK 1 ŹRÓDŁA DALSZYCH INFORMACJI.....	45
A. Dokumenty FATF.....	45
B. Akty prawne/wskazówki dot. podejścia opartego na ryzyku.....	45
C. Inne źródła informacji pomocnych instytucjom państwowym i finansowym w przeprowadzaniu oceny ryzyka kraju i działalności transgranicznej. ....	46
ZAŁĄCZNIK 2 GŁOSARIUSZ TERMINOLOGII .....	49
ZAŁĄCZNIK 3 CZŁONKOWIE ELEKTRONICZNEJ GRUPY DORADCZEJ .....	52

# **CZĘŚĆ PIERWSZA: WYKORZYSTANIE WSKAZÓWEK I CEL PODEJŚCIA OPARTEGO NA RYZYKU**

## **Rozdział Pierwszy: Tło i kontekst**

1. W lipcu 2007 r. FATF przyjął Wskazówki w zakresie opartego na ryzyku podejścia do zwalczania prania pieniędzy i finansowania terroryzmu: Ogólne zasady i procedury na wysokim szczeblu, które obejmują wskazówki dla władz publicznych i instytucji finansowych. Było to zwięźczone szerokie konsultacje prowadzonych z członkami sektora prywatnego i publicznego w ramach Elektronicznej Grupy Doradczej (Electronic Advisory Group – EAG) założonej przez FATF.

2. W 2008 r. FATF przyjął Wskazówki w zakresie opartego na ryzyku podejścia do zwalczania prania pieniędzy i finansowania terroryzmu: Ogólne zasady i procedury na wysokim szczeblu dla księgowych, kasyn, osób zajmujących się obrotem metalami szlachetnymi i osób zajmujących się obrotem kamieniami szlachetnymi, prawników, pośredników nieruchomości, osób świadczących usługi dla trustów i spółek.

3. Spotkanie odbyło się we wrześniu 2008 r. i uczestniczyły w nim organizacje reprezentujące podmioty świadczące usługi pieniężne (money services businesses MSB). Została ustanowiona Elektroniczna Grupa Doradcza (EAG), której przewodniczy Pan Ezra Levine (Okrągły Stół ds. Usług Pieniężnych, USA). W skład Grupy wchodzi członkowie i obserwatorzy FATF oraz przedstawiciele sektora MSB, którzy zgłosili się do pracy nad kwestią opartego na ryzyku podejścia do zwalczania prania pieniędzy i finansowania terroryzmu. Lista członków jest zawarta w Załączniku 3.

4. Po dalszych konsultacjach międzynarodowych zarówno z sektorem publicznym, jak i prywatnym, FATF przyjął Wskazówki RBA dla podmiotów świadczących usługi pieniężne na spotkaniu plenarnym w czerwcu 2009 r.

### **Cel wskazówek:**

5. Celem niniejszych Wskazówek jest:

- Wspieranie wypracowania wspólnego stanowiska względem kwestii podejścia opartego na ryzyku.
- Nakreślenie ogólnych zasad związanych z zastosowaniem podejścia opartego na ryzyku.
- Wskazanie dobrych praktyk sektora publicznego i prywatnego w projektowaniu i wdrażaniu skutecznego podejścia opartego na ryzyku.

6. Należy jednak zauważyć, że zastosowanie podejścia opartego na ryzyku nie jest obowiązkowe. Odpowiednio zastosowane podejście oparte na ryzyku niekoniecznie oznacza obniżenie obciążeń, chociaż powinno prowadzić do bardziej efektywnego pod względem kosztów wykorzystania zasobów. W niektórych krajach zastosowanie systemu opartego na regułach może dać lepsze efekty. Państwa będą musiały dokonać własnych ustaleń w zakresie tego, czy zastosować podejście oparte na ryzyku.

### ***Odbiorcy docelowi, status i treść wskazówek:***

7. Niniejsze Wskazówki są przede wszystkim adresowane do władz publicznych i MSB. MSB ogólnie rzecz biorąc stanowią podkategorię usług finansowych świadczonych przez instytucje finansowe. Niniejsze Wskazówki dotyczą głównie przekazu środków pieniężnych lub wartości majątkowych oraz wymiany pieniędzy i walut obsługiwanej przez MSB.

8. Firmy zajmujące się przekazem środków pieniężnych/wartości materialnych świadczą podstawowe usługi finansowe, często w regionach mniej rozwiniętych z ograniczonymi lub brakiem usług bankowych. Firmy zajmujące się przekazem środków pieniężnych/wartości materialnych działają na różne sposoby, ale zazwyczaj wysyłający pośrednik przyjmuje wpłatę na przekaz pieniężny (w tym opłaty), pobiera wymagane informacje identyfikacyjne i systematycznie rejestruje transakcję oraz odpowiednie dane identyfikacyjne nadawcy oraz wyznaczonego odbiorcy w miejscu pochodzenia. W przypadku lokalizacji międzynarodowych i różnych walut stosowane są stawki wymiany walut i są one systematycznie wymieniane. Przekaz pieniężny jest udostępniany ostatecznemu odbiorcy w odpowiedniej walucie, w lokalizacji pośrednika odbierającego w jurysdykcji wypłaty. Metody wypłaty różnią się w zależności od jurysdykcji, ale mogą obejmować gotówkę, czek, przekazy bankowe, karty płatnicze, depozyty bankowe lub kombinację metod.

9. Podmioty zajmujące się wymianą pieniędzy/walut są zaangażowane w działalność polegającą na przyjmowaniu waluty lub innego instrumentu pieniężnego denominowanego w walucie jednego kraju, w zamian za walutę lub inny instrument pieniężny denominowany w walucie jednego lub więcej innych krajów.

10. Cały dokument jest podzielony na trzy niezależne części. Część pierwsza przedstawia kluczowe elementy podejścia opartego na ryzyku i przedstawia podstawy dotyczące interpretacji części drugiej (Wskazówki dla władz publicznych) i części trzeciej (Wskazówki dla podmiotów świadczących usługi pieniężne MSB). Istnieje również Załącznik 1, który zawiera opis dodatkowych źródeł informacji.

11. Wskazówki mają na celu przedstawienie kluczowych elementów skutecznego podejścia opartego na ryzyku i określenia rodzajów kwestii, które zarówno władze publiczne jak i MSB mogą chcieć rozważyć w trakcie stosowania podejścia opartego na ryzyku.

12. Zgodnie ze wskazówkami każdy kraj i jego organy administracyjne, we współpracy z MSB, będą musiały określić najbardziej odpowiedni reżim dostosowany do rodzajów ryzyka występujących w poszczególnych krajach. Dlatego też Wskazówki nie zawierają jednego modelu podejścia opartego na ryzyku, ale poszukują możliwości przedstawienia wskazówek o szerokim zakresie, opartych na ogólnych zasadach i procedurach, które państwa mogą chcieć rozważyć przy stosowaniu podejścia opartego na ryzyku, pamiętając o tym, że niniejsze wskazówki nie są nadrzędne wobec zakresu władz państwowych.

## **Rozdział drugi: Podejście oparte na ryzyku – cel, korzyści i wyzwania**

### ***Cel podejścia opartego na ryzyku***

13. Zalecenia FATF ujęte są w sposób pozwalający krajom na przyjęcie podejścia opartego na ryzyku do zwalczania prania pieniędzy i finansowania terroryzmu, zgodnie z wymogami Standardów FATF. Język upoważnia także kraje do zezwolenia MSB na zastosowanie podejścia opartego na ryzyku przy realizacji określonych obowiązków związanych z przeciwdziałaniem praniu pieniędzy i finansowaniu terroryzmu. Poprzez przyjęcie podejścia opartego na ryzyku uprawnione organy i MSB mogą wprowadzić działania mające na celu zapobieżenie lub minimalizację ryzyka wystąpienia prania pieniędzy i finansowania

terroryzmu, które to działania będą współmierne do zidentyfikowanych zagrożeń. Pozwoli to na alokację środków w sposób najbardziej wydajny. Zasadą jest to, że środki powinny być kierowane zgodnie z priorytetami, tak żeby największą uwagę poświęcono najważniejszym zagrożeniom. Podejścia alternatywne polegają albo na równomiernej alokacji środków, tak żeby wszystkie MSB, klienci, produkty itd. otrzymały równą uwagę albo na nakierowaniu ich, ale na podstawie czynników innych niż ryzyko. Może to doprowadzić do podejścia „odhaczania”, koncentrującego się raczej na spełnianiu określonych wymogów niż skutecznym zwalczaniu prania pieniędzy i finansowania terroryzmu. Wreszcie, jest to najistotniejsze, by podejście oparte na ryzyku pozostało dynamiczne względem ryzyka; aby mogło ewoluować, tak by było zgodne ze zmienionym zagrożeniem, a tym samym żeby było elastyczne. MSB powinny mieć możliwość wskazania w jaki sposób ich strategia i podejście są zgodne ze zmieniającym się zagrożeniem określonym przez ich personel lub strony zewnętrzne z sektora publicznego.

14. Przyjęcie podejścia opartego na ryzyku wiąże się z wprowadzeniem procesu zarządzania ryzykiem do przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu. Proces ten składa się z rozpoznania istnienia ryzyka(ryzyk), przeprowadzenia oceny ryzyka(ryzyk) i przygotowania strategii mających na celu zarządzanie i zmniejszanie określonego ryzyka.

15. W celu określenia, na jakim obszarze istnieje największe ryzyko prania pieniędzy i finansowania terroryzmu musi zostać przeprowadzona i aktualizowana analiza ryzyka. Konieczne będzie zidentyfikowanie przez Państwa najbardziej podatnych obszarów i podjęcie odpowiednich działań. MSB będą musiały zidentyfikować klientów, produkty i usługi, włączając kanały dystrybucji i lokalizacje geograficzne charakteryzujące się wysokim ryzykiem. Oceny te nie są niezienne i będą się zmieniać w miarę upływu czasu, w zależności od rozwoju sytuacji i ewolucji zagrożeń. Wskazania przy tym wymaga, że przestępcy bardzo szybko identyfikują procedury kontrolne, które - choć pierwotnie były dostosowane do zagrożeń- nie zostały stosownie zmodyfikowane w ślad za zmieniającym się ryzykiem.

16. Strategie dotyczące zarządzania i ograniczania zidentyfikowanego ryzyka działalności związanej z praniem pieniędzy i finansowaniem terroryzmu w MSB, zazwyczaj mają na celu zapobieganie wystąpieniu tej przestępczej działalności poprzez szereg działań prewencyjnych (np. odpowiednie działania z zakresu zachowania należytej staranności w okolicznościach określonych w ust. 48), wykrywania (np. monitorowanie i zgłaszanie podejrzanych transakcji) oraz prowadzenie dokumentacji ułatwiającej prowadzenie śledztw.

17. W oparciu o ocenę ryzyka powinny być wprowadzone stosowne procedury. Obszary wysokiego ryzyka powinny być przedmiotem bardziej szczegółowych procedur dla MSB, obejmujących stosowanie wzmożonych środków należytej staranności i zwiększonego monitoringu transakcji. Konsekwencją jest także to, że w przypadkach niskiego ryzyka można stosować uproszczone i ograniczone kontrole.

18. Nie ma ogólnie przyjętych metodologii w pełni określających charakter i zakres podejścia opartego na ryzyku. Skuteczne podejście oparte na ryzyku obejmuje jednak identyfikację i kategoryzację zagrożeń związanych z praniem pieniędzy oraz ustanowienie racjonalnej kontroli opartej o zidentyfikowane zagrożenia. Skuteczne podejście oparte na ryzyku pozwoli MSB na stosowanie właściwej oceny biznesowej w odniesieniu do klientów. Zastosowanie racjonalnego i klarownego podejścia opartego na ryzyku uzasadni oceny MSB związane z zarządzaniem potencjalnych zagrożeń praniem pieniędzy i finansowaniem terroryzmu oraz pozwoli MSB na stosowanie odpowiedniej oceny biznesowej w odniesieniu do klientów. Celem podejścia opartego na ryzyku nie powinno być uniemożliwienie MSB zawierania transakcji z klientami lub kontaktów z potencjalnymi klientami, powinno raczej pomagać MSB w skutecznym zarządzaniu potencjalnym ryzykiem prania pieniędzy i finansowania terroryzmu.

19. Bez względu na siłę i skuteczność kontroli w ramach przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu ustanowioną przez MSB, przestępcy wciąż będą próbowali przesuwać nielegalne fundusze, unikając wykrycia, i od czasu do czasu będą odnosić sukces. Racjonalnie określone i skutecznie wdrożone podejście oparte na ryzyku dostarczy odpowiednich i skutecznych ram dla kontroli mających na celu zarządzanie możliwym do zidentyfikowania ryzykiem prania pieniędzy i finansowania terroryzmu. Należy jednak uznać, że żadne zasadnie stosowane kontrole, w tym kontrole realizowane w wyniku racjonalnie wdrożonego podejścia opartego na ryzyku, nie zidentyfikują, ani nie wykryją wszystkich przypadków prania pieniędzy i finansowania terroryzmu. Dlatego też organy regulacyjne, organy ścigania i władze sądowe muszą uwzględnić i właściwie rozważyć racjonalnie uzasadnione podejście oparte na ryzyku MSB. W przypadkach, gdy MSB nieskutecznie zmniejsza ryzyko, ze względu na niewłaściwe wdrożenie adekwatnie zaprojektowanego podejścia opartego na ryzyku lub programu opartego na ryzyku, który nie był adekwatnie zaprojektowany organy regulacyjne, organy ścigania i władze sądowe powinny podjąć konieczne działania, w tym nałożenie kar lub innych odpowiednich środków egzekucyjnych/regulacyjnych.

### **Potencjalne korzyści i wyzwania podejścia opartego na ryzyku**

#### *Korzyści:*

20. Przyjęcie podejścia opartego na ryzyku w celu zwalczania prania pieniędzy i finansowania terroryzmu może przynieść korzyści dla wszystkich stron, w tym również dla całego społeczeństwa. Skutecznie wdrożone podejście powinno pozwolić MSB i organom nadzorującym na bardziej wydajne i efektywne wykorzystanie środków i minimalizację obciążeń dla klientów. Koncentracja na poważniejszych zagrożeniach powinna spowodować, że pozytywne skutki będzie można osiągnąć w sposób bardziej efektywny.

21. Starania związane ze zwalczaniem prania pieniędzy i finansowania terroryzmu powinny być elastyczne, aby umożliwiać ich adaptację w miarę ewolucji zagrożeń. W związku z tym MSB będą wykorzystywać swoją własną ocenę, wiedzę i doświadczenie w rozwijaniu odpowiedniego podejścia opartego na ryzyku w odniesieniu do swojej konkretnej formy organizacyjnej, struktury i działalności gospodarczej.

22. Ryzyko związane z praniem pieniędzy i finansowaniem terroryzmu może być skuteczniej zarządzane poprzez proces oparty na ryzyku, który pozwala na ocenę potencjalnego ryzyka i u podstaw którego leży rzeczywista współpraca pomiędzy uprawnionymi organami a MSB. Bez współpracy i zrozumienia pomiędzy tymi stronami, skuteczny proces oparty na ryzyku jest niemożliwy.

23. Podmioty zajmujące się praniem pieniędzy i finansowaniem terroryzmu posiadają dużą znajomość sektora finansowego i podejmują wszelkie działania, aby ukryć swoją działalność finansową i sprawić, by była nieodróżnialna od legalnych transakcji jakich dokonują. Celem podejścia opartego na ryzyku jest zwiększenie koncentracji na zidentyfikowanych działaniach o wysokim ryzyku, a tym samym utrudnienie przestępcom wykorzystania MSB do działań o charakterze przestępczym. Ponadto podejście oparte na ryzyku pozwala MSB na bardziej skuteczne i wydajne dostosowanie się i adaptację w miarę identyfikacji nowych metod prania pieniędzy i finansowania terroryzmu.

#### *Wyzwania:*

24. Podejście oparte na ryzyku nie jest łatwym rozwiązaniem i mogą istnieć bariery, które będzie trzeba pokonać przy wdrażaniu koniecznych działań. Niektóre wyzwania są

niezerwalnie związane z zastosowaniem podejścia opartego na ryzyku. Inne mogą wynikać z trudności w dokonaniu przejścia na system oparty na ryzyku. Jednak wiele wyzwań może być także postrzeganych jako punkt wyjścia dla wdrożenia bardziej skutecznego systemu. Wyzwania związane z wdrożeniem podejścia opartego na ryzyku w odniesieniu do finansowania terroryzmu zostało omówione bardziej szczegółowo w punktach 40 do 44 poniżej.

25. Podejście oparte na ryzyku stanowi wyzwanie zarówno dla podmiotów sektora publicznego, jak i prywatnego. Przy takim podejściu potrzebne są spore środki i wiedza fachowa, żeby gromadzić i interpretować informacje o zagrożeniach, zarówno na poziomie krajowym, jak i instytucjonalnym, opracowywać procedury i systemy, a także szkolić personel. Co więcej, wymaga ono zdolności do dokonywania rzetelnej i bazującej na wysokich kwalifikacjach oceny przy wdrażaniu procedur i systemów w instytucji i jej podzespołach. Z pewnością doprowadzi to do większego zróżnicowania praktyk, co powinno prowadzić do innowacji i lepszego przestrzegania zasad. Jednak może także spowodować niepewność co do oczekiwań, trudność w stosowaniu jednorodnego traktowania regulacyjnego oraz brak zrozumienia ze strony klientów co do wymaganych informacji.

26. Wdrożenie podejścia opartego na ryzyku wymaga, żeby MSB posiadały dogłębną wiedzę o zagrożeniach i były zdolne do dokonywania rzetelnych ocen. W celu wdrożenia tego podejścia konieczne jest budowanie wiedzy fachowej w MSB, w tym na przykład poprzez szkolenia, rekrutację, korzystanie z profesjonalnych porad oraz „uczenia się poprzez działanie”. W procesie tym zawsze będą wykorzystywane informacje przekazywane przez uprawnione organy, będą także wskazówki w zakresie dobrej praktyki. Próba postępowania zgodnie z podejściem opartym na ryzyku bez wystarczającej wiedzy fachowej może prowadzić do błędnych ocen dokonywanych przez MSB gdyż podmioty te mogą przeceniać ryzyko, co może prowadzić do marnowania środków, lub mogą nie doceniać zagrożeń, sprzyjając tym samym powstawaniu nadużyć.

27. Uznanie przez MBS, że niektórzy członkowie personelu mają problem z przeprowadzaniem ocen opartych na ryzyku może prowadzić do nadmiernej ostrożności przy podejmowaniu decyzji lub nieproporcjonalnej ilości czasu poświęconego na dokumentowanie uzasadnienia decyzji. Może to także dotyczyć kierownictwa na różnych szczeblach. Jednak w sytuacjach, gdy kierownictwo nie rozpozna lub zaniży ocenę ryzyka, może stać się regułą przeznaczenie nieadekwatnych środków na przestrzeganie norm, prowadząc do potencjalnie poważnego nieprzestrzegania norm. Organy nadzorujące powinny kłaść większy nacisk na to, żeby MSB dysponowały skutecznymi procesami podejmowania decyzji. W celu sprawdzenia skuteczności ogólnego zarządzania ryzykiem powinny być jednak stosowane wyrywkowe kontrole lub analiza poszczególnych decyzji (patrz ust. 87). Organy nadzorujące powinny brać pod uwagę, że chociaż MSB ustanowiło odpowiednie struktury i procedury zarządzania ryzykiem, które są aktualizowane regularnie, i że odpowiednie polityki, procedury i procesy są przestrzegane, MSB wciąż może podejmować decyzje niewłaściwe w świetle dodatkowych informacji, które w danym momencie nie były dostępne przy zastosowaniu racjonalnych działań.

28. Wdrażając podejście oparte na ryzyku, MSB powinny otrzymać możliwość dokonywania uzasadnionych ocen w kontekście ich konkretnych sytuacji. Może to oznaczać, że nie będzie dwóch podmiotów, które przyjmą taką samą szczegółową praktykę. Takie potencjalne zróżnicowanie praktyk będzie wymagać, żeby organy regulacyjne dołożyły większych starań w celu identyfikacji i rozpowszechniania wskazówek dotyczących racjonalnej praktyki i może stanowić wyzwanie dla pracowników nadzorującym przestrzeganie norm. Istnienie wskazówek dotyczących dobrej praktyki, szkoleń, analiz branżowych i innych dostępnych informacji i materiałów pomoże organom nadzorującym w określeniu, czy MSB dokonały właściwych ocen opartych na ryzyku.

*Potencjalne korzyści i potencjalne wyzwania mogą być podsumowane w następujący sposób:*

Potencjalne korzyści:

- Lepsze zarządzanie ryzykiem i korzyści płynące z poniesionych kosztów.
- Podmioty świadczące usługi pieniężne skupiają się na realnych zidentyfikowanych zagrożeniach.
- Elastyczność w adaptacji do zagrożeń zmieniających się w miarę upływu czasu.

Potencjalne wyzwania:

- Identyfikacja odpowiednich informacji celem przeprowadzenia solidnej analizy ryzyka.
- Rozwiązanie problemu krótkookresowych kosztów związanych ze zmianą systemu.
- Zwiększone zapotrzebowanie na lepiej wykwalifikowanych pracowników zdolnych do dokonywania rzetelnych ocen.
- Bieżące dostosowywanie regulacji odzwierciedlających potencjalne zmiany praktyk.

## **Rozdział trzeci: FATF i podejście oparte na ryzyku**

29. Zróżnicowanie stopni ryzyka prania pieniędzy i finansowania terroryzmu dla poszczególnych rodzajów MSB albo dla poszczególnych rodzajów klientów, produktów lub transakcji jest ważnym problemem leżącym u podstaw Zaleceń FATF. Zgodnie z Zaleceniami kraje mogą uwzględniać ryzyko na dwa sposoby: (a) istnieje zasada ogólna ryzyka, która stosuje się do MSB i która pozwala państwu w niektórych przypadkach na zastosowanie pewnych Zaleceń albo częściowo, albo w całości, zakładając, że spełniono pewne warunki; i (b) istnieją specjalne Zalecenia, w których stopień ryzyka jest problemem, który państwo albo musi uwzględnić (jeżeli istnieje podwyższone ryzyko), albo może uwzględnić (jeżeli istnieje niższe ryzyko). We wszystkich przypadkach w trakcie oceny ryzyka, należy zwrócić uwagę na atrakcyjność dla przestępców i terrorystów użycia kanałów, które identyfikują jako odpowiednie dla ich celów. Kanały niskiego ryzyka również mogą być czasem celem "nieprawidłowego" użycia.

### **Zasada ogólnego ryzyka**

30. Państwo może zdecydować, że zastosuje pełen zakres działań przeciwko praniu pieniędzy/finansowaniu terroryzmu określony w Zaleceniach 5-11, 13-15, 18 i 1-2 do wszystkich rodzajów instytucji finansowych<sup>1</sup>. Takie państwo może również zdecydować o uwzględnieniu ryzyka i o ograniczeniu zastosowania niektórych Zaleceń zakładając, że któryś z warunków określonych poniżej został spełniony. W przypadku gdy istnieją ograniczenia lub wyjątki, powinno być to przeprowadzone w sposób ściśle ograniczony i uzasadniony:

- W przypadku gdy działalność finansowa jest prowadzona przez osobę lub podmiot sporadycznie lub w bardzo ograniczonym zakresie (uwzględniając kryteria ilościowe i absolutne) tak, że istnieje niewielkie ryzyko prania pieniędzy lub finansowania terroryzmu, państwo może zdecydować, że zastosowanie działań przeciwko praniu pieniędzy nie jest konieczne w całości lub w części.

<sup>1</sup> Zob. Glosariusz Zaleceń FATF w celu zapoznania się z definicją „instytucji finansowej”

- W ściśle określonych lub uzasadnionych okolicznościach i w oparciu o udowodnione niskie ryzyko prania pieniędzy lub finansowania terroryzmu<sup>2</sup>, państwo może zdecydować się, by nie stosować niektórych lub wszystkich Czterdziestu Zaleceń do niektórych działalności finansowych.

### **Odniesienia do szczególnego ryzyka**

31. Poza zasadą ogólnego ryzyka, o której mowa powyżej, podejście oparte na ryzyku jest albo włączone do Zaleceń (i Metodologii) w sposób szczegółowy i ograniczony do wielu Zaleceń, albo jest nierozłączną częścią lub jest powiązany z Zaleceniami. W przypadku instytucji, podmiotów gospodarczych i grup zawodowych objętych Zaleceniami FATF ryzyko jest ujmowane na czterech podstawowych obszarach: (a) należyta staranność wobec klientów (Z. 5-9); (b) wewnętrzne systemy kontroli firm (Z. 15 i 22); (c) podejście do regulacji i nadzoru przez uprawnione organy (Z. 23); i (d) przepis dla państw pozwalający, by Wyznaczone Podmioty Nie-Finansowe i Grupy Zawodowe (DNFBP) uwzględniały ryzyko prania pieniędzy lub finansowania terroryzmu w podobny sposób co MSB (Z. 12, 16, 24).

#### *Należyta staranność wobec klientów (Z.5-9)*

32. Odwołania do ryzyka mają miejsce w kilku formach:

- a) Wysokie ryzyko – w ramach Zalecenia 5, państwo musi nałożyć na MSB wymóg zachowywania wzmożonej staranności w odniesieniu do klientów, stosunków gospodarczych i transakcji o wysokim ryzyku. Zalecenie 6 (osoby zajmujące eksponowane stanowiska polityczne) jest przykładem zastosowania tej zasady i jest uważane za przypadek wiążący się z podwyższonym ryzykiem wymagający zachowania wzmożonej należytej staranności w stosunkach z klientami.
- b) Niskie ryzyko – państwo może także pozwolić swoim MSB na wzięcie pod uwagę niskiego ryzyka przy decydowaniu o zakresie podejmowanych działań związanych z zachowaniem należytej staranności wobec klientów (zob. Metodologia - Kryterium 5.9). MSB mogą w ten sposób ograniczyć lub uprościć zakres wymaganych działań (ale nie mogą ich całkowicie zaniechać). Dwa możliwe przykłady wystąpienia niższego ryzyka prania pieniędzy/finansowania terroryzmu obejmują MSB, które podlegają wymogom zgodnym z Zaleceniami FATF i są nadzorowane pod względem zgodności z tymi wymogami, oraz notowane spółki publiczne, które podlegają wymogowi ujawniania informacji.
- c) Ryzyko wynikające z innowacji – zgodnie z Zaleceniem 8 państwa muszą wprowadzić wobec swoich MSB wymóg zwracania szczególnej uwagi na zagrożenia wynikające z nowych lub rozwijających się technologii, które sprzyjają anonimowości.
- d) Mechanizm oceny ryzyka – standardy FATF zakładają, że istnieje będzie adekwatny mechanizm, poprzez który uprawnione organy będą oceniać lub kontrolować procedury przyjmowane przez MSB w celu określenia stopnia ryzyka i sposobu zarządzania ryzykiem, jak również kontrolować rzeczywiste decyzje. Założenia te odnoszą się do wszystkich obszarów, do których zastosowanie ma podejście oparte na ryzyku. Dodatkowo, jeśli uprawnione organy wydały wytyczne dla MSB dotyczące właściwego podejścia do procedur opartych na ryzyku, ważne będzie ustalenie, czy MSB przestrzegało wytycznych. Zalecenia także uwzględniają fakt, że ryzyko związane z danym państwem jest koniecznym składnikiem każdego mechanizmu oceny ryzyka (Z. 5 i 9).

#### *Wewnętrzne systemy kontroli MSB (Z. 15 i 22)*

---

<sup>2</sup> Odniesienie do finansowania terroryzmu w tych dwóch stanowiskach zostało dodane w Metodologii FATF ust. 20 lit. a) i b).

33. W ramach Zalecenia 15, opracowanie „odpowiednich” polityk wewnętrznych oraz systemów szkoleniowych i audytowych będzie musiało szczegółowo i na bieżąco uwzględniać potencjalne zagrożenie praniem pieniędzy i finansowaniem terroryzmu związane z klientami, produktami i usługami, geograficznymi obszarami działalności itd. Nota interpretacyjna do Zalecenia 15 wyjaśnia, że kraje mogą zezwolić podmiotom gospodarczym przy określaniu rodzaju i zakresu koniecznych działań na wzięcie pod uwagę zagrożeń związanych z praniem pieniędzy i finansowaniem terroryzmu oraz wielkości firmy. W podobny sposób ryzyko państwa (i wdrożenie Zaleceń FATF) musi być wzięte pod uwagę przy ocenie działań podjętych przez oddziały i filie zagraniczne (Z. 22).

#### *Regulacja i nadzór przez uprawnione organy (Z. 23)*

34. W ramach Zalecenia 23 państwo może uwzględnić ryzyko prania pieniędzy lub finansowania terroryzmu w konkretnym sektorze finansowym w trakcie określania zakresu działań, aby udzielić licencji lub zarejestrować i odpowiednio regulować i nadzorować lub kontrolować te podmioty gospodarcze pod kątem prania pieniędzy i finansowania terroryzmu. W sytuacji kiedy dowiedziono niskiego ryzyka prania pieniędzy i finansowania terroryzmu mogą zostać podjęte działania na mniejszą skalę. Zakres działań dla osób świadczących usługi w zakresie przekazu środków pieniężnych lub wartości majątkowych oraz w zakresie wymiany pieniędzy/walut podlega określonym standardom minimalnym.

#### *Wyznaczone niefinansowe podmioty gospodarcze i grupy zawodowe (Z 12, 16, 24)*

35. W trakcie wdrażania działań zapobiegających praniu pieniędzy i finansowaniu terroryzmu w ramach Zalecenia 12 i 16 państwo może zezwolić, by DNFBP uwzględniło ryzyko prania pieniędzy i finansowania terroryzmu w trakcie określania zakresu należytej staranności, kontroli wewnętrznych itd. w sposób podobny do zezwolenia dla instytucji finansowych<sup>3</sup>.

36. W odniesieniu do regulacji i monitorowania (Z. 24) państwo może uwzględnić ryzyko prania pieniędzy i finansowania terroryzmu w konkretnym sektorze DNFBP (poza kasynami, które zostały określone jako stwarzające wysokie ryzyko) w trakcie określania zakresu działań wymaganych do monitorowania i zapewniania zgodności z celami zapobiegania praniu pieniędzy i finansowaniu terroryzmu. Jeżeli dowiedziono niskiego ryzyka prania pieniędzy i finansowania terroryzmu mogą zostać podjęte działania na mniejszą skalę<sup>4</sup>.

#### *Inne Zalecenia*

37. W odniesieniu do Dziewięciu Specjalnych Rekomendacji FATF dotyczących finansowania terroryzmu Specjalna Rekomendacja VII ma na celu zwiększenie przejrzystości przepływu płatności poprzez zapewnienie, że jurysdykcja podejmuje spójne działania zapobiegające praniu pieniędzy i finansowaniu terroryzmu we wszystkich formach systemów przekazów środków pieniężnych/wartości majątkowych zwłaszcza tych, które tradycyjnie działają poza konwencjonalnym sektorem finansowym. Zgodnie z SR VII jurysdykcje wyznaczają jeden lub więcej uprawnionych organów do rejestrowania i/lub wydawania licencji osobom fizycznym i prawnym, które świadczą usługi przekazu środków pieniężnych lub wartości majątkowych w tym poprzez system nieformalny tak, aby osoby te podlegały odpowiednim Zaleceniom i Specjalnym Rekomendacjom FATF (zwłaszcza Z. 4-11, 13-15, 21-23, SR VII). Jednocześnie jurysdykcje powinny wymagać od każdej osoby dokonującej przekazów środków pieniężnych/wartości majątkowych posiadającej licencję lub będącej

<sup>3</sup> Podręcznik ust. 42 lit. e), i).

<sup>4</sup> Zob. Metodologię ust. 42 lit. f)

zarejestrowaną, by posiadała aktualizowaną listę swoich pośredników, która musi być dostępna dla uprawnionych organów.

Ponadto jurysdykcje powinny móc nałożyć sankcje w przypadku niedopełnienia wymogu nadawania licencji i/lub rejestracji i niedopełnienia Zaleceń FATF. W ramach Zalecenia 23 jurysdykcja może uwzględnić ryzyko prania pieniędzy lub finansowania terroryzmu w konkretnym sektorze finansowym w trakcie określania zakresu działań, aby udzielić licencji lub zarejestrować i odpowiednio regulować i nadzorować lub kontrolować te podmioty gospodarcze pod kątem prania pieniędzy i finansowania terroryzmu. Jeżeli dowiedziono niskiego ryzyka prania pieniędzy i finansowania terroryzmu mogą zostać podjęte działania na mniejszą skalę. Zakres działań dla osób świadczących usługi w zakresie przekazu środków pieniężnych lub wartości majątkowych oraz w zakresie wymiany pieniędzy/walut podlega określonym powyżej standardom minimalnym.

38. Również SR VIII odnosząca się do organizacji typu non-profit wskazuje na konieczność wzięcia pod uwagę ryzyka finansowania terroryzmu<sup>5</sup> oraz na fakt, że uwzględniając różnorodność w poszczególnych sektorach krajowych i różne stopnie, w jakich poszczególne części każdego sektora mogą być podatne na niewłaściwe wykorzystanie przez terrorystów, zasadnicze znaczenie ma ukierunkowane podejście zajmujące się zagrożeniem terroryzmu w odniesieniu do sektora organizacji typu non-profit (NPO). Podobnie dokument z najlepszymi praktykami wspierający SR IX zachęca państwa do oparcia swoich prac na ocenionym ryzyku i ocenach zagrożeń. Ryzyko figuruje również w metodologii wspierającej SR VII, gdzie instytucje finansowe beneficjenta powinny podlegać wymogowi przyjęcia skutecznych procedur opartych na ryzyku w celu identyfikacji i obsługi przekazów elektronicznych, którym nie towarzyszą pełne informacje o inicjatorze.

39. Zalecenie 25 wymaga dostarczania adekwatnych informacji zwrotnych do sektora finansowego i DNFBP. Tego typu informacje zwrotne pozwalają instytucjom i podmiotom gospodarczym na dokładniejszą ocenę ryzyka związanego z praniem pieniędzy i finansowaniem terroryzmu i dostosowanie programów oceniających ryzyko w odpowiedni sposób. To z kolei zwiększa prawdopodobieństwo otrzymywania lepszej jakości zgłoszeń o podejrzanych transakcjach. Poza tym, że są to zasadnicze dane do oceny ryzyka na skalę krajową lub sektorową, terminowość i treść informacji zwrotnych są również istotne do wdrażania skutecznego podejścia opartego na ryzyku.

## ***Możliwość zastosowania podejścia opartego na ryzyku do finansowania terroryzmu***

40. Istnieją zarówno podobieństwa, jak i różnice w stosowaniu podejścia opartego na ryzyku do finansowania terroryzmu i do prania pieniędzy. Obydwa obszary wymagają zastosowania procesu identyfikacji, jak i oceny ryzyka. Jednak charakterystyka finansowania terroryzmu utrudnia wykrycie ryzyka, a wdrożenie strategii zapobiegawczych może stanowić wyzwanie z powodu problemów takich jak relatywnie niska wartość transakcji związanych z finansowaniem terroryzmu, lub fakt, że fundusze mogą pochodzić z legalnych bądź nielegalnych źródeł.

41. Fundusze, które są wykorzystywane do finansowania terroryzmu, mogą pochodzić z działalności przestępczej, albo z legalnych źródeł, a charakter źródeł finansowania może różnić się w zależności od rodzaju organizacji terrorystycznej. W sytuacji gdy fundusze pochodzą z działalności przestępczej, tradycyjne mechanizmy monitorowania stosowane w przypadku identyfikacji prania pieniędzy mogą także być właściwe dla finansowania

---

<sup>5</sup> Podręcznik ust. 42 lit. f)

terroryzmu, mimo że podejrzana działalność może nie być zidentyfikowana jako finansowanie terroryzmu lub jako działalność z nim związana. Należy zauważyć, że transakcje związane z finansowaniem terroryzmu mogą opiewać na bardzo małe kwoty, które, przy zastosowaniu podejścia opartego na ryzyku, mogą być transakcjami, które są często uważane za transakcje o minimalnym ryzyku w odniesieniu do prania pieniędzy. Gdy fundusze pochodzą z legalnych źródeł jest jeszcze trudniej określić, czy mogły być wykorzystane dla celów związanych z terroryzmem. Dodatkowo działalność terrorystów może być jawna i pozornie nie wydawać się powiązana z łamaniem prawa, tak jak w przypadku zakupu materiałów i usług (np. powszechnie przechowywanych środków chemicznych, pojazdów silnikowych itd.) dla realizacji ich celów, kiedy to jedynym ukrywanym faktem jest zamierzone wykorzystanie zakupionych materiałów i usług. Dlatego, z uwagi na fakt, że fundusze terrorystów mogą pochodzić z działalności przestępczej lub z legalnych źródeł, transakcje związane z finansowaniem terroryzmu mogą nie wykazywać tych samych cech co konwencjonalne pranie pieniędzy. Jednak we wszystkich przypadkach nie jest obowiązkiem podmiotu gospodarczego określenie rodzaju podstawowej działalności przestępczej, ani zamierzonego celu terrorystycznego, rolą takiego podmiotu gospodarczego jest natomiast zgłaszanie podejrzanej działalności. Jednostka analityki finansowej i organy ścigania przeprowadzą następnie postępowanie w danej sprawie, aby określić, czy istnieje powiązanie z finansowaniem terroryzmu.

42. Zdolność MSB do wykrywania i identyfikacji potencjalnych transakcji finansujących terroryzm bez wskazówek dotyczących typologii finansowania terroryzmu lub bez działania na podstawie konkretnych danych wywiadowczych dostarczonych przez władze stanowi o wiele większe wyzwanie niż ma to miejsce w przypadku potencjalnego prania pieniędzy i innej podejrzanej działalności. Działania związane z wykrywaniem, bez konkretnych krajowych wskazówek i typologii, koncentrują się zwykle na monitorowaniu transakcji z krajami lub obszarami geograficznymi, o których wiadomo, że działają tam terroryści, lub transakcji, które oparte są na innych ograniczonych typologiach (z których wiele wskazuje na te same techniki, jakie są stosowane przy praniu pieniędzy).

43. Poszczególne osoby, organizacje lub państwa mogą podlegać sankcjom związanym z finansowaniem terroryzmu, w jakimkolwiek państwie. W takich przypadkach lista osób, organizacji lub państw, do których mają zastosowanie sankcje oraz zobowiązanie do przestrzegania tych sankcji nałożone na podmiot gospodarczy ustalane są przez poszczególne państwa i nie są funkcją ryzyka. Naruszenie takich sankcji może skutkować przestępstwem lub sankcjami, jeżeli fundusze lub usługi finansowe są udostępnione dla podmiotu podlegającego sankcjom lub jego pośrednika.

44. Z tego względu niniejsze Wskazówki nie wyczerpują problemu zastosowania procesu opartego na ryzyku w odniesieniu do finansowania terroryzmu. Byłoby zdecydowanie lepiej, gdyby podejście oparte na ryzyku było zastosowane tam, gdzie będzie to wykonalne przy zastosowaniu racjonalnych środków. W tym zakresie potrzebne są dalsze konsultacje z kluczowymi zainteresowanymi stronami, tak aby zidentyfikować pełniejszy zestaw wskaźników metod i technik wykorzystywanych do finansowania terroryzmu, które potem mogą stać się podstawą dla opracowania strategii oceny zagrożeń związanych z finansowaniem terroryzmu i opracowania działań im zapobiegających. MSB będą wtedy miały dodatkową podstawę dla pełniejszego zaawansowania i wdrożenia procesu opartego na ryzyku w odniesieniu do finansowania terroryzmu.

## **Ograniczenia podejścia opartego na ryzyku**

45. Istnieją okoliczności, w których podejście oparte na ryzyku nie ma zastosowania lub może być zastosowane w ograniczonym stopniu. Istnieją także okoliczności, w których podejście oparte na ryzyku może nie mieć zastosowania na wstępnych etapach realizacji wymogu lub procesu, ale będzie mieć zastosowanie na późniejszych etapach. Ograniczenia dotyczące podejścia opartego na ryzyku są zwykle rezultatem wymogów prawnych lub regulacyjnych, które nakazują podejmowanie pewnych działań.

46. Wymagania zamrożenia aktywów zidentyfikowanych osób lub podmiotów w krajach, w których takie wymagania obowiązują, są niezależne od jakiegokolwiek oceny ryzyka. Wymóg zamrożenia jest bezwzględny i nie może na niego wpłynąć proces oparty na ryzyku. Podobnie, choć identyfikacja potencjalnie podejrzanych transakcji może być usprawniona poprzez podejście oparte na ryzyku, zgłaszanie już zidentyfikowanych podejrzanych transakcji nie jest oparte na ryzyku.

47. Istnieje kilka elementów należytej staranności wobec klientów – identyfikacja i weryfikacja tożsamości klientów i ich rzeczywistych beneficjentów, otrzymywanie informacji o celach i zamierzonym charakterze przedsięwzięć gospodarczych oraz ciągle zachowanie należytej staranności. Ze wskazanych powyżej elementów identyfikacja i weryfikacja tożsamości klientów stanowi wymogi, które muszą być spełnione bez względu na podejście oparte na ryzyku dla wszystkich klientów, którzy posiadają rachunek lub stosunki biznesowe, a tam gdzie ma to zastosowanie, w przypadku gdy osiągnięte zostały progi pieniężne (nie wyższe niż USD/EUR 15 000 dla okazjonalnych transakcji lub nie wyższe niż USD/EUR 1 000 dla przekazów elektronicznych). Dotyczy to przekazów transgranicznych i krajowych funduszy pomiędzy instytucjami finansowymi w tym MSB.

Rzeczywiście Specjalna Rekomendacja VII wymaga, by każde państwo podejmowało działania zmierzające do egzekwowania od instytucji finansowych, w tym MSB, by te załączały dokładne i właściwe informacje o inicjatorze (nazwę, adres i numer rachunku) do przekazów funduszy i powiązanych wiadomości, które są przesyłane; informacje te powinny pozostać załączone do przekazu lub powiązanych wiadomości w całym łańcuchu płatności. Przy czym w przypadku przekazów krajowych, zlecający MSB może zawrzeć pełne informacje o inicjatorze lub tylko numer rachunku inicjatora lub unikalny numer identyfikacyjny, zakładając, że pełna informacja dot. inicjatora będzie dostępna dla instytucji finansowej beneficjenta i dla uprawnionych organów w ciągu trzech dni roboczych.

48. Jednak w odniesieniu do wszystkich innych składników zachowania należytej staranności wobec klientów rozsądnie wdrożone podejście oparte na ryzyku może pozwolić na podjęcie decyzji o zakresie i ilości wymaganych informacji oraz mechanizmów, które mają być zastosowane, aby spełnić te minimalne standardy. Gdy tylko te decyzje zostaną podjęte, zobowiązanie do prowadzenia ewidencji i przechowywania dokumentów otrzymanych dla celów zachowania należytej staranności, podobnie jak dokumentów księgowych, nie będzie zależne od poziomów ryzyka.

49. Państwa mogą zezwolić MSB na stosowanie ograniczonych lub uproszczonych środków, gdy ryzyko prania pieniędzy lub finansowania terroryzmu jest niskie. Jednak te ograniczone lub uproszczone środki niekoniecznie mają zastosowanie do wszystkich aspektów zachowania należytej staranności w stosunkach z klientami. Co więcej, gdy zwolnienia te są uzależnione od spełnienia pewnych warunków, konieczne jest zweryfikowanie, czy dane warunki zostały spełnione, a gdy zwolnienia stosowane są poniżej pewnej wartości progowej, powinny być przedsięwzięte środki zapobiegające sztucznemu dzieleniu transakcji celem uniknięcia progu. Dodatkowo dla adekwatnej oceny ryzyka mogą być potrzebne informacje wykraczające poza określenie tożsamości klientów, takie jak lokalizacja klienta. Proces ten będzie miał charakter iteracyjny: początkowe informacje uzyskane na temat klienta powinny być wystarczające do

określenia, czy należy postępować dalej, a w wielu przypadkach monitorowanie klientów i dostarczy dodatkowych informacji.

50. Pewna forma monitorowania, niezależnie od tego czy jest zautomatyzowana czy ręczna, czy jest ot kontrola sprawozdań z wyjątków czy kombinacja dozwolonych opcji, w zależności od przedstawionego ryzyka, potrzebna jest w celu wykrycia nietypowych, a tym samym być może podejrzanych transakcji. Nawet w przypadku klientów niskiego ryzyka monitorowanie jest konieczne do weryfikacji, czy transakcja spełnia początkowy kryterium niskiego ryzyka, a jeśli nie, to następuje rozpoczęcie procesu właściwej oceny ryzyka w odniesieniu do klienta. Podobnie, ryzyko związane z niektórymi klientami może zostać stwierdzone po rozpoczęciu transakcji albo przez rachunek, albo w inny sposób w relacji z MSB. Odpowiednie i rozsądne monitorowanie transakcji z klientami staje się zatem kluczowym składnikiem właściwie zaprojektowanego podejścia opartego na ryzyku, jednak w tym kontekście powinno być jasne, że nie wszystkie transakcje, rachunki lub klienci będą monitorowani w dokładnie ten sam sposób. Co więcej, gdy istnieje rzeczywiste podejrzenie prania pieniędzy lub finansowania terroryzmu, może to być uważane za scenariusz wysokiego ryzyka i powinna być zachowana wzmożona należyta staranność bez względu na wszelkie progi lub zwolnienia.

### ***Rozróżnienie między nadzorem opartym na ryzyku a politykami i procesami opartymi na ryzyku***

51. Polityki i procesy oparte na ryzyku w MSB powinny być odróżnione od nadzoru opartego na ryzyku. Metodologia przyjęta przez organy regulacyjne do określania alokacji środków na nadzór powinna obejmować zakres działalności firmy, profil ryzyka i środowisko kontroli wewnętrznej i powinna umożliwiać istotne porównania między MSB. Metodologia wykorzystywana do określania alokacji środków będzie wymagała bieżącej aktualizacji tak, aby odzwierciedlić charakter, wagę i zakres ryzyka, na które wystawione są poszczególne MSB. W konsekwencji, priorytety te powinny prowadzić organy nadzorujące do zwracania baczniejszej uwagi pod kątem tworzenia regulacji w odniesieniu do MSB, które angażują się w działalność ocenioną jako stwarzająca wysokie ryzyko prania pieniędzy.

53. Jednak należy także zauważyć, że czynniki ryzyka brane pod uwagę przy ustalaniu priorytetów dla pracy organów nadzorujących będą zależeć nie tylko od wewnętrznego ryzyka związanego z podejmowaną działalnością, ale także od jakości i skuteczności systemów zarządzania ryzykiem wprowadzanych w celu przeciwstawiania się takim zagrożeniom.

#### Ramka podsumowująca:

#### **Oparte na ryzyku podejście do przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu na poziomie krajowym: elementy kluczowe dla osiągnięcia sukcesu**

- Podmioty świadczące usługi pieniężne i organy regulacyjne powinny mieć dostęp do wiarygodnych i przydatnych w działaniu informacji o zagrożeniach.
- Musi być położony nacisk na rozwiązania promujące współpracę między twórcami polityki, organami ścigania, organami regulacyjnymi i sektorem prywatnym.
- Władze powinny publicznie uznać fakt, że podejście oparte na ryzyku nie wyeliminuje wszystkich elementów ryzyka.

- Władze są zobowiązane do stworzenia warunków, w których podmioty świadczące usługi pieniężne nie będą musiały obawiać się sankcji regulacyjnych w sytuacjach, gdy postępowali odpowiedzialnie i wdrażali adekwatne wewnętrzne systemy i kontrole.
- Pracownicy nadzorujący organów regulacyjnych muszą być dobrze wyszkoleni w zakresie podejścia opartego na ryzyku, zarówno stosowanego przez wyznaczonych nadzorujących, jak i przez podmioty świadczące usługi pieniężne.
- Wymogi i nadzór na poziomie krajowym powinny być spójne w podobnych sektorach.

## **CZĘŚĆ DRUGA: WSKAZÓWKI DLA WŁADZ PUBLICZNYCH**

### **Rozdział pierwszy: Ogólne zasady tworzenia podejścia opartego na ryzyku**

53. Stworzenie opartego na ryzyku podejścia do przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu pozwoli uprawnionym organom i MSB wykorzystywać ich środki w najbardziej efektywny sposób. Niniejszy rozdział określa pięć ogólnych zasad, które państwa powinny wziąć pod uwagę przy projektowaniu podejścia opartego na ryzyku. Powinny one być uznawane za ogólne ramy dobrej praktyki.

54. Tych pięć zasad określonych w niniejszym opracowaniu ma za zadanie pomóc krajom w ich wysiłkach zmierzających do ulepszenia reżimów przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu. Nie mają one charakteru normatywnego i powinny być stosowane w sposób przemyślany i dopasowany do konkretnych okoliczności panujących w danym kraju.

#### ***Zasada pierwsza: zrozumienie i reagowanie na zagrożenia i najbardziej podatne/niebezpieczne obszary: krajowa ocena ryzyka***

55. Skuteczne wdrożenie opartego na ryzyku podejścia do zwalczania prania pieniędzy i finansowania terroryzmu zależy od dobrego zrozumienia zagrożeń i najbardziej podatnych obszarów. Jeśli państwo stara się wprowadzić podejście oparte na ryzyku na poziomie krajowym, jest to dużo łatwiejsze przy dobrym zrozumieniu zagrożeń, na jakie kraj jest narażony. Wiedza ta może pochodzić z krajowej oceny ryzyka.

56. Krajowa ocena ryzyka powinna być dopasowana do okoliczności panujących w danym kraju. Z wielu powodów, włączając strukturę uprawnionych organów i charakter sektora usług finansowych, ocena ryzyka w każdym kraju będzie jedyna w swoim rodzaju, podobnie jak decyzje o sposobie wdrożenia krajowej oceny w praktyce. Ocena krajowa nie musi być jednym formalnym dokumentem. Powinna być postrzegana jako proces, który jest zaprojektowany w celu osiągnięcia konkretnych rezultatów. Pożądanym rezultatem jest oparcie decyzji dotyczącej alokacji obowiązków i środków na poziomie krajowym na wyczerpującej i aktualnej wiedzy o zagrożeniach. Uprawnione organy, w porozumieniu z sektorem prywatnym, powinny rozważyć, jak najlepiej osiągnąć ten cel, równocześnie biorąc pod uwagę ryzyko dostarczenia informacji na temat słabych punktów ich systemów finansowych i niefinansowych osobom piorącym pieniądze, finansującym terroryzm i innym przestępcom<sup>6</sup>.

---

<sup>6</sup> Zob. Raport FATF dot. strategii szacowania ryzyka związanego z praniem pieniędzy i finansowaniem terroryzmu, przyjęty w czerwcu 2008 r.

## ***Zasada druga: ramy prawne/regulacyjne wspierające stosowanie podejścia opartego na ryzyku***

57. Państwa powinny rozważyć, czy ich ramy prawne i regulacyjne sprzyjają zastosowaniu podejścia opartego na ryzyku. Gdy będzie to wskazane, zobowiązania nakładane na MSB powinny być kształtowane przy uwzględnieniu rezultatów krajowej oceny ryzyka.

58. Podejście oparte na ryzyku nie oznacza braku jasnego określenia tego, czego wymaga się od MSB. Jednak przy podejściu opartym na ryzyku MSB powinny posiadać pewien stopień elastyczności w zakresie wdrażania polityk i procedur, stanowiących adekwatną odpowiedź na ich własną ocenę. W konsekwencji wdrożone standardy mogą być dopasowane i/lub ulepszone przez dodatkowe działania, zgodnie z zagrożeniami stojącymi przed poszczególnymi MSB. Fakt, że polityki i procedury, zgodnie z poziomami ryzyka, mogą być stosowane elastycznie w stosunku do różnych produktów, usług, klientów oraz lokalizacji nie oznacza, że polityki i procedury nie muszą być jasno zdefiniowane.

59. Podstawowe minimalne wymagania w zakresie przeciwdziałania praniu pieniędzy mogą współistnieć z podejściem opartym na ryzyku. Rzeczywiście, rozsądne minimalne standardy, pozostawiające możliwość ich intensyfikacji w sytuacji uzasadnionego zagrożenia, powinny stanowić istotę opartych na ryzyku wymogów, dotyczących przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu. Standardy te powinny jednak być zorientowane na rezultaty (zwalczanie poprzez przeciwdziałanie, wykrywanie i zgłaszanie przypadków prania pieniędzy i finansowania terroryzmu), a nie stosowanie wymogów prawnych i regulacyjnych w czysto mechaniczny sposób do każdego klienta.

## ***Zasada trzecia: projekt ram nadzoru wspierający zastosowanie podejścia opartego na ryzyku***

60. Jeśli uprawnionym organom przypisano obowiązek nadzorowania kontroli związanych z przeciwdziałaniem praniu pieniędzy i finansowaniu terroryzmu, państwa mogą rozważyć, czy takie organy i branżowe organizacje samorządowe otrzymały konieczny zakres uprawnień, żeby wdrożyć oparte na ryzyku podejście do nadzoru. Do barier w tym zakresie należeć może nadmierne poleganie na szczegółowych wymaganiach normatywnych zawartych w regulaminach organów regulacyjnych. Te wymogi mogą z kolei wynikać z prawa, które determinuje realizację uprawnień przez organ regulacyjny.

61. W odpowiednich sytuacjach organy regulacyjne powinny starać się dostosować podejście oparte na ryzyku do nadzoru kontroli MSB w celu zwalczania prania pieniędzy i finansowania terroryzmu. Podstawą powinna być dogłębna i wyczerpująca wiedza o rodzajach prowadzonej działalności finansowej i ryzyka związanego z praniem pieniędzy i finansowaniem terroryzmu, na jakie są one wystawiane. Organy regulacyjne będą prawdopodobnie musiały ustalić priorytety wykorzystania środków w oparciu o całościową ocenę tego, gdzie ogniskują się zagrożenia, jakie instytucje są najbardziej zagrożone i inne czynniki.

62. Organy regulacyjne, mające inny zakres kompetencji niż te związane z przeciwdziałaniem praniu pieniędzy i finansowaniu terroryzmu będą musiały wziąć również to ryzyko pod uwagę, równoległe z oceną ryzyka wynikającą z pozostałych obowiązków organów regulacyjnych. Podobnie, należy dołożyć starań, aby zapewnić odpowiednią współpracę pomiędzy uprawnionymi organami, które nadzorują podobne działania.

63. Takie oceny ryzyka powinny pomóc organom regulacyjnym w wyborze miejsca wykorzystania środków w swoim programie nadzoru, mając na celu wykorzystanie ograniczonych środków dla osiągnięcia jak najlepszego efektu. Ocena ryzyka może także wskazywać, że organ regulacyjny nie posiada adekwatnych środków, żeby zajmować się

takimi zagrożeniami<sup>7</sup>. W takiej sytuacji organ regulacyjny może być zmuszony do uzyskania dodatkowych środków lub przyjęcia innych strategii, aby zarządzać niedopuszczalnym pozostałym ryzykiem lub je zminimalizować.

64. Zastosowanie podejścia opartego na ryzyku do nadzoru wymaga, żeby pracownicy organów regulacyjnych byli zdolni do podejmowania decyzji bazując na obowiązujących zasadach, w sposób podobny do tego, jakiego oczekiwać można od MSB, które przyjęło podejście oparte na ryzyku. Decyzje te będą obejmowały adekwatność rozwiązań MSB związanych ze zwalczaniem prania pieniędzy i finansowania terroryzmu. Organ regulacyjny może zechcieć rozważyć najlepszy sposób szkolenia swoich pracowników w zakresie praktycznego zastosowania podejścia opartego na ryzyku do nadzoru. Pracownicy nadzorujący będą musieli być dobrze zaznajomieni z ogólnymi zasadami podejścia opartego na ryzyku, możliwymi metodami zastosowania i tym, jak podejście oparte na ryzyku wygląda po skutecznym zastosowaniu przez MSB.

### **Zasada czwarta: identyfikacja głównych zaangażowanych podmiotów i zapewnienie spójności**

65. Przyjmując podejście oparte na ryzyku do zwalczania prania pieniędzy i finansowania terroryzmu państwa powinny rozważyć, kim są główne zaangażowane strony. Sytuacja będzie się różnić w poszczególnych krajach. Należy zastanowić się nad najbardziej skutecznym sposobem podziału obowiązków między tymi stronami oraz tym, jak wymieniać się informacjami, aby uzyskać najlepszy skutek. Przykładowo, można zastanowić się nad tym, który organ lub organy są najbardziej odpowiednie do dostarczenia wskazówek dla MSB dotyczących wdrażania podejścia opartego na ryzyku do przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu.

66. Do listy potencjalnych zainteresowanych stron należą:

- Administracja rządowa – może obejmować władzę ustawodawczą, wykonawczą i sędziowską.
- Organy ścigania – mogą one obejmować policję, służbę celną itd.
- Jednostki wywiadu finansowego (FIU), służby specjalne, inne podobne agencje, itd..
- Organy regulujące usługi finansowe.
- Sektor prywatny MSB – może obejmować firmy MSB lub stowarzyszenia handlowe.
- Społeczeństwo – rozwiązania zaprojektowane w celu przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu są ostatecznie zaprojektowane tak, żeby chroniły przestrzegającą prawo część społeczeństwa. Jednak te rozwiązania mogą także nakładać obciążenia na klientów firm MSB.
- Inne – ci, którzy mają możliwość przyczynienia się do opracowania podstawy pojęciowej podejścia opartego na ryzyku, takie zainteresowane strony mogą obejmować uczelnie i media.

66. Oczywiście władze krajowe nie będą w stanie skutecznie wpływać na wszystkie z tych zainteresowanych stron w równym stopniu. Jednak to rząd będzie mógł najlepiej ocenić, jak można zachęcić wszystkie strony zainteresowane do wspierania działań związanych ze zwalczaniem prania pieniędzy i finansowania terroryzmu.

67. Kolejnym elementem jest rola, jaką władze krajowe odgrywają w staraniach o nadanie odpowiedniej rangi podejściu opartemu na ryzyku przez uprawnione organy. Odpowiednie władze mogą wspomóc ten proces poprzez wydawanie jasnych i spójnych oświadczeń dotyczących podejścia opartego na ryzyku wobec tego co następuje:

---

<sup>7</sup> Zob. Zalecenie FATF nr 30.

- Od MSB można oczekiwać elastyczności w dostosowywaniu swoich wewnętrznych systemów i kontroli biorąc pod uwagę niskie i wysokie ryzyko, o ile systemy te są racjonalne. Jednak istnieją minimalne wymogi prawne i regulacyjne oraz elementy, które stosują się bez względu na poziom ryzyka, na przykład zgłaszanie podejrzanych transakcji i minimalne standardy należytej staranności w stosunkach z klientami.
- Uznanie, że zdolność MSB do wykrywania i powstrzymywania prania pieniędzy i finansowania terroryzmu może czasami być z konieczności ograniczona, oraz że informacje o czynnikach ryzyka nie są zawsze rzetelne i łatwo dostępne. Dlatego powinny istnieć racjonalne oczekiwania wobec polityki i nadzoru w zakresie tego, co MSB może osiągnąć przy dobrej kontroli mającej za zadanie zapobieganie praniu pieniędzy i finansowaniu terroryzmu. MSB może działać w dobrej wierze podejmując rozsądne i uzasadnione kroki, aby zapobiec praniu pieniędzy, dokumentując powody swoich decyzji, i wciąż paść ofiarą przestępcy.
- Uznanie, że nie wszystkie sytuacje wskazujące na wysokie ryzyko są takie same i w konsekwencji nie zawsze wymagają zachowania dokładnie tego samego rodzaju wzmożonej należytej staranności.

### **Zasada piąta: wymiana informacji między sektorem publicznym a sektorem prywatnym**

69. Skuteczna wymiana informacji między sektorem publicznym a sektorem prywatnym będzie stanowić integralną część krajowej strategii zwalczania prania pieniędzy i finansowania terroryzmu. W wielu przypadkach pozwoli to sektorowi prywatnemu na dostarczenie uprawnionym organom informacji pozyskanych w rezultacie wywiadu uprzednio przeprowadzonego przez organy administracji rządowej.

70. Władze publiczne, czy to w postaci organów ścigania, organów regulacyjnych czy innych, posiadają uprzywilejowany dostęp do informacji, które mogą pomóc MSB w osiągnięciu popartych wiedzą ocen przy stosowaniu opartego na ryzyku podejścia do prania pieniędzy i finansowania terroryzmu. Podobnie MSB rutynowo zawierają transakcje z dużą liczbą klientów każdego dnia i są w stanie w miarę dobrze zrozumieć działalność swoich klientów. Organy publiczne i prywatne powinny współpracować przy określaniu, jakie informacje są wartościowe przy zwalczaniu prania pieniędzy i finansowania terroryzmu oraz opracowywaniu metod, poprzez które te informacje mogą być rozpowszechniane w sposób terminowy i skuteczny.

71. Z punktu widzenia sprawności, wymianie informacji między sektorem publicznym a sektorem prywatnym powinna towarzyszyć odpowiednia wymiana informacji między organami władzy publicznej. Jednostki analityki finansowego, nadzorujący i organy ścigania powinny być w stanie przekazywać sobie informacje, ocenę rezultatów oraz informacje o zidentyfikowanych słabych punktach, tak żeby sektorowi prywatnemu można było przekazać spójne i istotne dane. Wszystkie strony powinny, rzecz jasna, wziąć pod uwagę środki ochronne potrzebne dla adekwatnej ochrony informacji wrażliwych posiadanych przez organy publiczne przed nadmiernym rozpowszechnieniem.

72. Zainteresowane strony powinny pracować nad utrzymaniem dialogu, żeby wiadomo było, jakie informacje okazały się użyteczne przy zwalczaniu prania pieniędzy i finansowania terroryzmu<sup>8</sup>. Na przykład rodzaje informacji, których wymiana pomiędzy sektorem publicznym a sektorem prywatnym mogłaby okazać się użyteczna, obejmować mogą (o ile są dostępne) następujące pozycje:

<sup>8</sup> Przykłady takich dialogów są zawarte w załączniku 1 niniejszych wskazówek.

- Ocena ryzyka danego kraju.
- Typologia i ocena tego, jak osoby piorące pieniądze i terroryści nadużywali systemu finansowego.
- Informacja zwrotna na temat zgłoszeń podejrzanych transakcji i innych istotnych raportów.
- Ukierunkowany jawny wywiad. W specyficznych okolicznościach oraz przy przestrzeganiu odpowiednich zabezpieczeń, odpowiednie może także być przekazywanie MSB przez władze ukierunkowanych informacji poufnych.
- Kraje, osoby lub organizacje, których aktywa lub transakcje powinny być zamrożone.

73. Wybierając rodzaj informacji, które mogą być odpowiednio i efektywnie przekazywane, władze publiczne mogą chcieć zwrócić uwagę sektora usług finansowych na fakt, że informacje od organów publicznych powinny kształtować, ale nie zastępować własną ocenę dokonaną przez instytucje. Przykładowo, kraje mogą podjąć decyzję o nieopracowywaniu ostatecznych krajowych list klientów niskiego ryzyka. Zamiast tego władze publiczne mogą preferować przekazywanie informacji, które będą wkładem w proces decyzyjny MSB, razem z istotnymi informacjami, które są dostępne dla MSB.

## **Rozdział drugi: Wdrożenie podejścia opartego na ryzyku**

### ***Ocena ryzyka kształtująca priorytety krajowe***

74. Podejście oparte na ryzyku powinno być zbudowane na solidnych fundamentach: należy najpierw dołożyć starań, żeby zapewnić dobre zrozumienie zagrożeń. Podejście oparte na ryzyku powinno bazować na ocenie zagrożeń. Jest to prawdziwe przy każdym zastosowaniu podejścia opartego na ryzyku na jakimkolwiek poziomie czy to przez kraje, czy poszczególne MSB. Podejście kraju powinno być kształtowane przez działania zmierzające do osiągnięcia zrozumienia zagrożeń istniejących w danym kraju. Można to uznać za „krajową ocenę ryzyka”.

75. Krajowa ocena ryzyka powinna być uważana za opis podstawowych ogólnych informacji pomocnych dla nadzorujących, organów ścigania, jednostek wywiadu finansowego, aby zapewnić, że decyzje o alokacji obowiązków i źródeł na poziomie krajowym są oparte o praktyczną, pełną i aktualną wiedzę o zagrożeniach.

76. Krajowa ocena ryzyka powinna być dopasowana do sytuacji panującej w danym kraju, zarówno w zakresie sposobu jej przeprowadzenia, jak i jej wniosków. Czynniki mogące mieć wpływ na ryzyko prania pieniędzy i finansowania terroryzmu w kraju mogą obejmować:

- Środowisko polityczne.
- Środowisko prawne.
- Struktura gospodarcza kraju.
- Czynniki kulturowe oraz charakter społeczeństwa.
- Źródła, lokalizacja i koncentracja działalności przestępczej.
- Wielkość branży usług finansowych.
- Skład branży usług finansowych.
- Struktura własności MSB.
- Wielkość i charakter działalności prowadzonej przez MSB, które nie są zarejestrowane albo nie posiadają licencji.
- Zasady ładu korporacyjnego w odniesieniu do MSB oraz szeroko pojętej gospodarki.
- Charakter systemów płatności oraz dominacja transakcji gotówkowych.
- Rozprzestrzenienie geograficzne działalności instytucji finansowych i klientów.

- Rodzaje produktów i usług oferowanych przez sektor usług finansowych.
- Rodzaje klientów obsługiwanych przez branżę usług finansowych.
- Rodzaje przestępstw bazowych.
- Kwoty pieniędzy pozyskiwane z nielegalnej działalności w kraju.
- Kwoty pieniędzy pozyskiwane z nielegalnej działalności za granicą i pranych w kraju.
- Główne kanały lub instrumenty wykorzystane do prania pieniędzy i finansowania terroryzmu.
- Dotknięte sektory legalnej gospodarki.
- Podziemne obszary gospodarki.

77. Państwa powinny także rozważyć, jak wiedza o zagrożeniach praniem pieniędzy i finansowaniem terroryzmu może być najlepiej osiągnięta na poziomie krajowym. Który organ lub organy będą odpowiedzialne za wkład w taką ocenę? Jak formalna powinna być ocena? Czy pogląd uprawnionego organu powinien być upubliczniony? Są to pytania do rozważenia przez uprawniony organ.

78. Pożądanym rezultatem jest sytuacja, w której decyzje dotyczące przydzielenia obowiązków i środków na poziomie krajowym są oparte o pełną i aktualną wiedzę na temat zagrożeń. Aby osiągnąć ten pożądany rezultat, uprawnione organy powinny stworzyć i wdrożyć działania minimalizujące zidentyfikowane zagrożenia.

79. Stworzenie i stosowanie podejścia opartego na ryzyku wiąże się z dokonywaniem ocen. Ważne jest, żeby te oceny były oparte na wiedzy. Wynika z tego, że, aby było skuteczne, podejście oparte na ryzyku powinno być oparte o informacje i obejmować w miarę potrzeb wywiad. Należy dołożyć starań, żeby zapewnić, że ocena ryzyka jest oparta o świeże i dokładne informacje. Państwa, we współpracy z organami ścigania, jednostkami wywiadu finansowego, organami regulacyjnymi są w dobrej pozycji, żeby podzielić się swoją wiedzą i doświadczeniem w celu opracowania podejścia opartego na ryzyku odpowiedniego dla danego kraju. Ich oceny nie będą statyczne: będą się one zmieniać w miarę upływu czasu, w zależności od rozwoju sytuacji i ewolucji zagrożeń. Zatem państwa powinny ułatwiać wymianę informacji między różnymi organami, aby nie istniały przeszkody instytucjonalne w rozpowszechnianiu informacji.

80. Bez względu na formę, krajowa ocena ryzyka, wraz z działaniami mającymi na celu minimalizację tego ryzyka, mogą nadawać kształt temu, jak środki są wykorzystywane do zwalczania prania pieniędzy i finansowania terroryzmu, biorąc pod uwagę inne istotne cele polityczne. Może to również wskazywać na sposób najskuteczniejszego przypisania tych środków do różnych organów publicznych oraz na to, jak te organy wykorzystają te środki w sposób efektywny.

81. Oprócz pomocy uprawnionym organom w podejmowaniu decyzji dotyczących alokacji środków w związku ze zwalczaniem prania pieniędzy i finansowania terroryzmu, krajowa ocena ryzyka może także dostarczyć informacji decydentom w zakresie relacji pomiędzy reżimem nadzorującym/regulacyjnym a zidentyfikowanymi zagrożeniami. Zbyt gorliwe wysiłki zamierzone na przeciwdziałanie zagrożeniom mogą być szkodliwe i dać przeciwny efekt, poprzez nałożenie nadmiernych obciążeń na branżę i działanie wbrew interesom społeczeństwa poprzez ograniczanie dostępu do usług finansowych dla niektórych segmentów populacji. Z drugiej strony, mniej agresywne wysiłki mogą nie być wystarczające, żeby ochronić społeczeństwa przed zagrożeniami stwarzanymi przez przestępców i terrorystów. Dogłębne zrozumienie zagrożeń na poziomie krajowym może pomóc w usunięciu tego niebezpieczeństwa.

## **Nadzór regulacyjny – Zasady ogólne**

### *Definiowanie dopuszczalnego poziomu ryzyka*

82. Poziom zagrożenia praniem pieniędzy i finansowaniem terroryzmu będzie generalnie kształtowany przez wewnętrzne i zewnętrzne czynniki ryzyka. Przykładowo, poziomy ryzyka mogą się zwiększać dzięki czynnikom wewnętrznym, takim jak niskie nakłady na zapewnienie przestrzegania norm, nieadekwatne kontrole ryzyka czy niewystarczające zaangażowanie wyższych kadr kierowniczych. Zagrożenia zewnętrzne mogą wynikać z takich czynników jak działalność stron trzecich i/lub zmiany polityczne i społeczne.

83. Jak opisano w Części Pierwszej, wszelka działalność posiada pewien element ryzyka. Uprawnione organy nie powinny powstrzymywać MSB przed prowadzeniem działalności z klientami wysokiego ryzyka, o ile funkcjonują odpowiednie polityki, procedury i procesy zarządzania istniejącym ryzykiem. Tylko w szczególnych przypadkach, na przykład gdy uzasadnia to walka z terroryzmem, przestępczością lub wdrażanie międzynarodowych zobowiązań, wyznaczonym osobom, podmiotom prawnym, organizacjom lub krajom kategorycznie odmawia się dostępu do usług.

84. Jednak nie wyklucza to potrzeby wdrożenia minimalnych podstawowych wymagań. Na przykład Zalecenie 5 FATF określa, że „jeśli instytucja finansowa nie jest w stanie postępować zgodnie z (wymogami zachowania należytej staranności w stosunkach z klientem), nie powinna zawierać umowy rachunku bankowego ani nawiązywać stosunków gospodarczych i dokonywać transakcji danego klienta; jeżeli doszło już do zawarcia umowy lub prowadzenia przedsięwzięcia powinna doprowadzić do ich zakończenia i rozważyć możliwość sporządzenia raportu o podejrzanym transakcji przeprowadzanej przez tego klienta.” Zatem poziom ryzyka powinien znajdować się gdzieś pośrodku między skrajnościami nieakceptowania klientów a prowadzeniem działalności przy nieakceptowanym lub niezmnieszonym ryzyku.

85. Uprawnione organy oczekują od MSB wprowadzenia w życie skutecznych polityk, programów i systemów minimalizowania zagrożeń, przy równoczesnym uznaniu, że nawet przy skutecznych systemach nie każda podejrzana transakcja będzie mogła być wykryta. Powinni oni także zapewnić, że te polityki, programy i systemy będą stosowane skutecznie w celu zapobiegania temu, żeby MSB stały się kanałami przesyłania nielegalnych zysków i zapewnienia, że prowadzić będą one ewidencję i sporządzać raporty użyteczne dla władz krajowych w zwalczaniu prania pieniędzy i finansowania terroryzmu. Skuteczne polityki i procedury będą obniżały poziom ryzyka, ale małe są szanse, że je całkowicie wyeliminują. Ocena ryzyka prania pieniędzy i finansowania terroryzmu wymaga dokonywania subiektywnych ocen i nie jest nauką ścisłą. Monitorowanie ma na celu wykrycie niecodziennych lub podejrzanym transakcji wśród niezwykle dużej liczby zgodnych z prawem transakcji, a dodatkowo odróżnienie tego, co jest niecodzienne, może być czasami trudne, ponieważ to, co „zwyczajowe”, może różnić się w zależności od rodzaju działalności klientów. Dlatego stworzenie dokładnego profilu klienta jest ważne w zarządzaniu systemem opartym na ryzyku. Co więcej, procedury i kontrole są często oparte o typologie uprzednich spraw, a przestępcy szybko adaptują swoje techniki zmniejszając użyteczność takich typologii.

86. Dodatkowo, nie wszystkie sytuacje wskazujące na wysokie ryzyko są identyczne i dlatego nie zawsze wymagają zachowania dokładnie takiego samego poziomu wzmożonej należytej staranności. W rezultacie wyznaczone organy nadzorujące będą oczekiwać od MSB identyfikacji kategorii wysokiego ryzyka i stosowania konkretnych i odpowiednich środków minimalizacji ryzyka. Przykładowo niektóre kategorie mogą obejmować:

- Klientów niebędących rezydentami (pozyskanie informacji dlatego chcą prowadzić przedsięwzięcie w innym kraju).

- Osoby na eksponowanych stanowiskach politycznych (aby zastosować odpowiednią politykę).
- Spółki posiadające pakiety akcji na okaziciela (aby zwrócić szczególną uwagę na identyfikację i weryfikację rzeczywistego beneficjenta).
- Dalsze informacje z zakresu identyfikacji konkretnych kategorii ryzyka znaleźć można w Części Trzeciej, „Wskazówki dla sektora prywatnego”.

*Proporcjonalne działania nadzorujące wspierające podejście oparte na ryzyku*

87. Organy nadzorujące powinny starać się zidentyfikować słabe punkty poprzez skuteczny program nadzoru zarówno na miejscu, jak „zza biurka”<sup>9</sup>, a także poprzez analizę informacji wewnętrznych i innych dostępnych informacji.

88. W trakcie przeprowadzania kontroli organy nadzorujące powinny sprawdzać ocenę ryzyka w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu MSB, jak również jego polityki, procedury i systemy kontroli, aby opracować całościową ocenę profilu ryzyka podmiotu gospodarczego oraz adekwatności jego działań mających na celu minimalizację ryzyka. W miarę dostępności, oceny przeprowadzone przez lub dla podmiotu gospodarczego mogą być użytecznym źródłem informacji. Ocena powinna obejmować wrywkowe sprawdzanie transakcji klienta, w celu sprawdzenia oceny. Przeprowadzona przez organ nadzorujący ocena zdolności zarządzania i chęci podejmowania koniecznych działań naprawczych jest także niezmiernie ważnym czynnikiem determinującym. Organy nadzorujące powinny podejmować współmierne działania, aby zapewnić właściwe i terminowe naprawienie niedociągnięć przy uwzględnieniu faktu, że zidentyfikowane słabe obszary mogą mieć szersze konsekwencje. Ogólnie rzecz ujmując, załamania systemu lub nieadekwatne kontrole doprowadzą do maksymalnego zaostrzenia nadzoru.

89. Tym niemniej, może się zdarzyć, że niewykrycie pojedynczej transakcji wysokiego ryzyka lub transakcji pojedynczego klienta wysokiego ryzyka będzie znaczące samo w sobie, na przykład, gdy przy znaczących kwotach, lub gdy typologia prania pieniędzy i finansowania terroryzmu jest dobrze znana, lub gdy schemat pozostawał niewykryty przez długi czas. Taki przypadek może wskazywać na nagromadzenie złych praktyk zarządzania ryzykiem lub naruszeń przepisów dotyczących identyfikacji poważnych zagrożeń, monitorowania, szkolenia pracowników i kontroli wewnętrznych, dlatego może sam uzasadnić wprowadzenie działań zapewniających przestrzeganie wymagań związanych z przeciwdziałaniem praniu pieniędzy i finansowaniu terroryzmu.

90. Organy nadzorujące powinny mieć możliwość porównania czynników ryzyka i procedur zastosowanych przez podobne MSB. Może to być pomocne dla organów nadzorujących w lepszym zrozumieniu tego, w jaki sposób MSB tworzą i wdrażają podejście oparte na ryzyku oraz w identyfikacji możliwych niedociągnięć. Podobnie organy nadzorujące mogą i powinny korzystać ze swojej wiedzy o zagrożeniach związanych z produktami, usługami, klientami oraz lokalizacjami geograficznymi, aby pomóc MSB w ocenie ich oceny ryzyka związanego z praniem pieniędzy i finansowaniem terroryzmu, należy jednak pamiętać, że mogą one posiadać informacje nieudostępnione dla MSB, dlatego samo MSB nie byłoby w stanie wziąć takich informacji pod uwagę przy opracowywaniu i wdrażaniu podejścia opartego na ryzyku. Organy nadzorujące (i inne zainteresowane strony) są zachęcane do wykorzystywania tej wiedzy przy wydawaniu wskazówek pomagających MSB w zarządzaniu ich ryzykiem. Gdy MSB mogą określić zakres działań związanych z zachowaniem należytej staranności wobec klientów w sposób uwzględniający ryzyko, powinien on być spójny ze wskazówkami

<sup>9</sup> Metodologia FATF, kryteria 29.2

wydanymi przez uprawnione organy<sup>10</sup>. Ocena podejścia opartego na ryzyku pomoże na przykład zidentyfikować przypadki, gdy podmioty gospodarcze wykorzystują bardzo wąskie kategorie ryzyka, które nie ujmuje wszystkich istniejących rodzajów ryzyka, albo przyjmują kryteria, które prowadzą do identyfikacji dużej liczby partnerów biznesowych wysokiego ryzyka, ale nie uwzględniają adekwatnych dodatkowych działań z zakresu należytej staranności.

91. W kontekście podejścia opartego na ryzyku, podstawowym zadaniem organów nadzorujących powinno być określenie, czy program przestrzegania zasad przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu i zarządzania ryzykiem MSB jest adekwatny dla: (a) spełnienia minimalnych wymogów regulacyjnych oraz (b) odpowiedniego i skutecznego minimalizowania zagrożeń. Celem nadzorowania nie jest zapobieganie działalności wysokiego ryzyka, ale zapewnienie, że MSB posiadają adekwatne i skutecznie wdrożone strategie minimalizacji ryzyka.

92. Zgodnie z 29 Zaleceniem FATF, osoby odpowiedzialne za nadzór powinny nakładać adekwatne sankcje za nieprzestrzeganie wymogów ustawowych lub regulacyjnych związanych ze zwalczaniem prania pieniędzy i finansowania terroryzmu. Skuteczny nadzór prania pieniędzy i finansowania terroryzmu wymaga, by osoba odpowiedzialna za nadzór posiadała odpowiedni zakres narzędzi nadzoru do zastosowania w sytuacji, w której, w ocenie osoby odpowiedzialnej za nadzór, instytucja finansowa nie działa zgodnie z prawem, regulacjami lub decyzją osoby odpowiedzialnej za nadzór. Narzędzia te obejmują zdolność wymagania od MSB, by podjęło natychmiastowe działania naprawcze i możliwość nałożenia kar. W praktyce zakres narzędzi jest stosowany zgodnie z powagą sytuacji.

93. Grzywny i/lub kary nie są odpowiednie we wszystkich działaniach regulacyjnych poprawiających lub naprawiających niedociągnięcia w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu. Jednak osoby odpowiedzialne za nadzór muszą mieć uprawnienia i chęć stosowania grzywien i/lub kar w przypadkach, gdy istnieją znaczące niedociągnięcia. Często działania mogą także przyjąć postać programu naprawczego poprzez normalne procesy nadzorujące.

94. Z uwagi na powyższe czynniki staje się jasne, że współmierna regulacja będzie wsparta dwoma centralnymi cechami:

#### a) Przejrzystość regulacyjna

95. Przejrzystość regulacyjna będzie miała pierwszorzędne znaczenie przy wdrażaniu współmiernych działań. Osoby odpowiedzialne za nadzór są świadome, że MSB, poszukując swobody operacyjnej do dokonywania własnych ocen ryzyka, będą także potrzebowały wskazówek w zakresie wypełniania zobowiązań regulacyjnych. Zatem organ regulacyjny o obowiązkach nadzorczych w zakresie monitorowania przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu powinien starać się przejrzysto określać swoje oczekiwania od instytucji podlegających regulacji, a także będzie musiał rozważyć odpowiednie mechanizmy przekazywania tych wiadomości. Przykładowo, może to przyjąć formę ogólnych wymogów opartych na pożądanym rezultacie, a nie szczegółowego procesu.

96. Bez względu na to, jaka konkretna procedura zostanie przyjęta, podstawową zasadą powinno być zapewnienie, że MSB jest świadome obowiązków prawnych i oczekiwań regulacyjnych. Wobec braku przejrzystości istnieje ryzyko, że nadzorowanie działań może być postrzegane jako albo nieproporcjonalne, albo nieprzewidywalne, co może podważyć najbardziej nawet efektywne zastosowanie podejścia opartego na ryzyku przez MSB.

---

<sup>10</sup> Zalecenia FATF nr 5 i 25, Metodologia Podstawowe Kryteria 25.1 i 5.12

b) Szkolenia pracowników organów nadzorujących i pracowników organów ścigania

97. W kontekście podejścia opartego na ryzyku nie jest możliwe dokładne określenie, co MSB musi zrobić, we wszystkich przypadkach, żeby spełnić dotyczące jej obowiązki regulacyjne. Zatem podstawowym zmartwieniem będzie to, jak najlepiej zapewnić spójne wdrażanie wykonalnych i współmiernych działań nadzorujących. Skuteczność szkoleń w zakresie nadzoru będzie zatem ważna dla skutecznej realizacji proporcjonalnych działań nadzorujących.

98. Szkolenie powinno mieć na celu pozwolenie osobie odpowiedzialnej za nadzór na stworzenie solidnych porównawczych ocen systemów i kontroli w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu przez MSB. Ważne jest przy przeprowadzaniu ocen, żeby osoby odpowiedzialne za nadzór miały zdolność dokonywania ocen dotyczących kontroli zarządzania w świetle ryzyka przyjętego przez podmioty gospodarcze oraz uwzględniając dostępne praktyki branżowe. Osoby odpowiedzialne za nadzór mogą także uznać za użyteczne przedsięwzięcie ocen porównawczych, tak aby dokonać ocen względnych silnych i słabych punktów różnych podmiotów.

99. Szkolenia powinny obejmować pouczenie osób odpowiedzialnych za nadzór o tym, jak ocenić, czy pracownicy wyższego szczebla kierowniczego wdrożyli adekwatne działania z zakresu zarządzania ryzykiem oraz określić, czy istnieją konieczne procedury i kontrole. Szkolenie powinno także obejmować odniesienie do konkretnych wskazówek, gdy będą one dostępne. Należy zauważyć, że "proces nadzorujący powinien obejmować nie tylko weryfikację polityk i procedur, ale również weryfikację plików klienta i przykładowych kont"<sup>11</sup>. Osoba odpowiedzialna na za nadzór może ocenić czy procesy te są adekwatne, a jeżeli stwierdzi, że procesy zarządzania ryzykiem nie są adekwatne jest upoważniona to wymagania od grupy biznesowej usprawnienia procesów. Osoby odpowiedzialne za nadzór powinny także być zapewnione o dostępności wystarczających środków dla zapewnienia wdrożenia skutecznego zarządzania ryzykiem.

100. Aby wypełnić te zobowiązania, szkolenie powinno umożliwić osobom odpowiedzialnym za nadzór adekwatnie ocenić:

- i. Jakość procedur wewnętrznych, włączając program ustawicznego szkolenia pracowników i audytu wewnętrznego, przestrzeganie przepisów i funkcje zarządzania ryzykiem.
- ii. Czy polityki i procesy zarządzania ryzykiem są odpowiednie w świetle profilu ryzyka MSB oraz okresowo dostosowywane w świetle zmieniających się profili ryzyka.
- iii. Uczestnictwo pracowników wyższego szczebla kierowniczego, aby zapewnić, że przedsięwzięli adekwatne zarządzanie ryzykiem, oraz że istnieją konieczne procedury i kontrole.

Poniższa lista nie jest wyczerpująca, jednak lista tematów oceny na miejscu może zawierać następujące elementy:

- Zastosowanie polityki szerokiej grupy.
- Ocena ryzyka związanego z każdą linią biznesu.
- Zakres, w jakim oceny zostały formalnie udokumentowane i podzielone na produkty, kanały dostaw, rodzaje klientów i lokalizacje geograficzne klientów.
- Zakres procedur należytej staranności w tym identyfikacja nowych klientów, profilowanie klientów i gromadzenie informacji „Poznaj swojego klienta”.
- Podejmowana jest dodatkowa należyta staranność w odniesieniu do klientów i podmiotów

<sup>11</sup> Zob. Z. 29 i *Zachowanie należytej staranności wobec klienta dla banków*, ust. 61.

gospodarczych wysokiego ryzyka, np. osoby o dużym kapitale własnym, osoby na eksponowanych stanowiskach politycznych.

- Posiadane procedury monitorowania transakcji i weryfikacji sytuacji alarmowych.
- Polityki określające to w jaki sposób i na jakich podstawach istniejące pliki klientów mogą być aktualizowane.
- Jakość systemów i kontroli wewnętrznych w tym procesów służących identyfikacji i zgłaszania dużych transakcji gotówkowych i transakcji podejrzanych.
- Polityki dotyczące prowadzenia rejestru i łatwości odzyskiwania zapisów ustalania tożsamości lub transakcji.
- Zakres, częstotliwość i odbiorcy szkoleń z zakresu prania pieniędzy i finansowania terroryzmu oraz ocena skuteczności.
- Odpowiednie wyrywkowe badania.

**Nie istnieje zestaw “właściwych odpowiedzi” na te zagadnienia. Kluczową sprawą do rozważenia jest to, że (a) podmioty świadczące usługi pieniężne spełniają wszelkie minimalne wymagania regulacyjne (b) podmioty świadczące usługi pieniężne zidentyfikowały swoje ryzyka prania pieniędzy i finansowania terroryzmu, wypracowały najlepszą metodę zarządzania ryzykiem i przeznaczyły odpowiednie środki na to zadanie; oraz że (c) wyższa kadra kierownicza we właściwy sposób odpowiada za kontrole związane z praniem pieniędzy i finansowaniem terroryzmu.**

# **CZĘŚĆ TRZECIA: WSKAZÓWKI DLA PODMIOTÓW ŚWIADCZĄCYCH USŁUGI PIENIĘŻNE (MSB) W ZAKRESIE WDRAŻANIA PODEJŚCIA OPARTEGO NA RYZYKU**

## **Preambuła**

101. Specyfika procesu opartego na ryzyku MSB służącego zarządzaniu i minimalizowaniu ryzyka związanego z praniem pieniędzy i finansowaniem terroryzmu powinna być określona na podstawie działalności danego podmiotu gospodarczego, w tym wielkości, oferowanych produktów i usług, i zasięgu geograficznego operacji.

Tam gdzie ma to zastosowanie i jest wykonalne polityki i procedury ustalające sposób, w jaki MSB będzie zarządzało i minimalizowało ryzyka związane z praniem pieniędzy i finansowaniem terroryzmu powinny być przedstawione w całej firmie lub grupie. Zauważa się jednak, że charakterystyka finansowania terroryzmu różni się od prania pieniędzy, a zatem powiązane ryzyko może być trudne do oceny bez bardziej całościowego zestawu wskaźników metod i technik wykorzystywanych do finansowania terroryzmu (zob. ust. 40 do 44). Ponieważ nie istnieją wyraźne znaki ostrzegawcze do wykrywania działalności związanej z finansowaniem terroryzmu, i ponieważ metody finansowania terroryzmu mogą być takie same lub podobne do prania pieniędzy identyfikacja samego finansowania terroryzmu może być trudnym procesem. Odpowiednio zaprojektowane podejście oparte na ryzyku zapewnia środki, dzięki którym MSB identyfikuje kryteria oceny potencjalnego ryzyka prania pieniędzy/finansowania terroryzmu. W sytuacji, gdy MSB występują w zintegrowanej grupie powinny być w pełni zintegrowane i stosować spójne podejście oparte na ryzyku do wszystkich swoich operacji. Żadnego rodzaju przeszkody nie powinny blokować przekazywania informacji pomiędzy różnymi pośrednikami grupy, oraz powinno być przeprowadzane badanie zgodności z politykami na skalę grupową. Takie badania zgodności mogłyby być również przeglądane przez zewnętrznych audytorów lub nadzorców. Jednym z komponentów odpowiednio zaprojektowanego podejścia opartego na ryzyku jest ocena ryzyka geograficznego, która może pomóc w identyfikacji lokalizacji geograficznych, które mogą wykazywać zwiększone ryzyko tj. kraje podlegające sankcjom rządowym. Odpowiednio wdrożony proces oparty na ryzyku zapewnia ramy dla identyfikacji stopnia potencjalnego ryzyka prania pieniędzy i finansowania terroryzmu związanego z klientami i transakcjami oraz pozwala podmiotowi gospodarczemu skupić się na tych klientach i transakcjach, którzy potencjalnie wykazują większe ryzyko prania pieniędzy i finansowania terroryzmu. Aby dalej zwalczać zagrożenie systemów MSB, które mogą być używane do finansowania terroryzmu transakcje klienta powinny być sprawdzane pod kątem odpowiednich list rządowych.

102. Sektor MSB składa się z bardzo zróżnicowanych grup organizacji. MSB może być małą organizacją z punktami zbytu takimi jak sklep spożywczy, apteka, sklep chemiczny lub sklepik wielobranżowy. Może również obejmować regionalne sieci urzędów pocztowych lub banków lub innych MSB, które mogą być oddziałami lub pośrednikami. Rozważając sposób wdrożenia podejścia opartego na ryzyku w sektorze MSB, władze publiczne mogą wziąć pod uwagę uproszczoną wersję niniejszych wskazówek dla mniejszych i mniej złożonych MSB. W zależności od jurysdykcji i struktury udzielania licencji/rejestracji, sektor MSB może być regulowany jako instytucja finansowa, która oferuje podobne usługi. Wymaga się, by MSB monitorowały i zgłaszały podejrzane działania oraz, jeżeli jest to wymagane prawem krajowym, duże transakcje, oraz by gromadziły wymaganą identyfikację klienta przy

określonych progach pieniężnych i aby prowadziły rejestry zgodnie z odpowiednimi regulacjami. Niniejsze Wskazówki dotyczą głównie przekazu środków pieniężnych i wartości majątkowych oraz wymiany pieniędzy i walut obsługiwanej przez MSB. W niektórych przypadkach MSB utrzymuje relacje rachunkowe z klientami. W większości przypadków MSB działa w środowisku opartym na transakcjach.

103. Przeprowadzanie oceny ryzyka jest podstawą podejścia opartego na ryzyku. Intencją oceny ryzyka jest identyfikacja produktów, usług, lokalizacji geograficznej i punktów interakcji z klientem, które są najbardziej podatne na działania związane z praniem pieniędzy i finansowaniem terroryzmu. Ocena ryzyka służy również zaznaczeniu pozostałych obszarów, które są zagrożone, i które powinny być wzięte pod uwagę po zastosowaniu reżimu kontroli wewnętrznych pod względem prania pieniędzy i finansowania terroryzmu. Ocena ryzyka może obejmować wiele różnych czynników w zależności od konkretnych okoliczności w tym, lecz nie wyłącznie:

- Charakteru, skali i złożoności działalności podmiotu gospodarczego, w tym różnorodności geograficznej.
- Wstępnego lub bieżącego zachowania staranności lub monitorowania prowadzonego w lokalizacjach pośredników podmiotu gospodarczego.
- Klienta, produktu i profilu działalności podmiotu gospodarczego.
- Charakteru przedsięwzięcia (tj. okazjonalne vs. trwałe relacje).
- Użytych kanałów dystrybucji.
- Systemów elektronicznych lub użytych platform do transmisji danych.
- Wykonywanego monitorowania transakcji.
- Wartości i rozmiaru transakcji.
- Zakresu, w jakim podmiot gospodarczy obsługuje bezpośrednio klienta lub obsługuje go przez pośredników, osoby trzecie lub w transakcji bez fizycznego udziału klienta.

104. Aby zapewnić odpowiednie podejście oparte na ryzyku MSB musi gromadzić informacje. Skuteczność podejścia opartego na ryzyku mogłaby się zwiększyć gdyby MSB mogły dzielić się informacjami z innymi MSB bez przeszkód formalnych, z innymi stronami transakcji niezależnie od tego czy obie są częścią grupy finansowej, a zwłaszcza jeżeli inne MSB jest zlokalizowane w innym kraju.

## **Rozdział pierwszy: Kategorie ryzyka**

105. Aby wdrożyć podejście oparte na ryzyku, MSB powinny zidentyfikować kryteria oceny potencjalnych zagrożeń związanych z praniem pieniędzy i finansowaniem terroryzmu. Identyfikacja zagrożeń związanych z praniem pieniędzy i finansowaniem terroryzmu, w stopniu, w którym zagrożenia te mogą zostać zidentyfikowane, związane z klientami lub kategoriami klientów, produktów, usług, obszarów geograficznych i transakcji pozwoli MSB określić i wdrożyć proporcjonalne działania i kontrole w celu minimalizacji tych zagrożeń. W odniesieniu do oceny ryzyka dla klasy lub rodzaju klienta warto zauważyć, że podczas gdy powinno to zawsze być przeprowadzane na początku kontaktów z klientem, w przypadku niektórych klientów czynniki ryzyka mogą stać się widoczne dopiero w trakcie prowadzenia transakcji z klientem, poprzez monitoring transakcji klienta i bieżące weryfikacje czyli podstawowy element rozsądnie zaprojektowanego podejścia opartego na ryzyku. MSB może również musieć dostosować swoją ocenę ryzyka w oparciu o informacje otrzymane od uprawnionych organów.

106. Ryzyko prania pieniędzy i finansowania terroryzmu może być mierzone przy użyciu różnych kategorii. Zastosowanie kategorii ryzyka umożliwia zarządzanie potencjalnymi zagrożeniami poprzez umożliwienie MSB podporządkowanie klientów proporcjonalnym

kontrolom i nadzorowi. Najpowszechniej stosowanymi kryteriami ryzyka są: ryzyko związane z krajem lub obszarem geograficznym; ryzyko związane z klientem; ryzyko związane z produktem/usługami. Waga przyznana tym kategoriom ryzyka (pojedynczo lub w połączeniach) przy ocenie całościowego ryzyka potencjalnego prania pieniędzy i finansowania terroryzmu może różnić się między poszczególnymi instytucjami, w zależności od ich konkretnych sytuacji. W konsekwencji MSB będą musiały podejmować swoje własne decyzje dotyczące wag poszczególnych rodzajów ryzyka, jednak parametry określone przez prawo lub regulacje mogą ograniczać dowolność podmiotów gospodarczych.

107. Mimo że nie istnieje zgoda, co do zbioru kategorii ryzyka przykłady dostarczone w niniejszym opracowaniu są najpowszechniej identyfikowanymi kategoriami ryzyka. Nie istnieje jedna metodologia stosowania tych kategorii ryzyka, a ich zastosowanie ma na celu pomoc w projektowaniu skutecznej strategii zarządzania potencjalnym ryzykiem.

### ***Ryzyko związane z krajem/obszarem geograficznym***

108. Nie istnieje definicja ogólnie przyjęta przez uprawnione organy lub MSB przesądzająca o tym, czy konkretny kraj lub obszar geograficzny (włączając kraje/obszary, w których działa dany MSB) jest krajem lub obszarem wysokiego ryzyka.

Ryzyko związane z krajem/obszarem, w połączeniu z innymi czynnikami ryzyka, dostarcza użytecznych informacji na temat potencjalnego zagrożenia praniem pieniędzy i finansowaniem terroryzmu. Czynniki, które mogą decydować o tym, że kraj określany jest jako kraj wysokiego ryzyka obejmują:

- Kraje zidentyfikowane w Oświadczeniach FATF jako posiadające słabe reżimy zapobiegania praniu pieniędzy i finansowaniu terroryzmu, i na które instytucje finansowe powinny zwrócić szczególną uwagę w trakcie prowadzenia przedsięwzięć i transakcji.
- Kraje podlegające sankcjom, embargom lub podobnym działaniom nałożonym przez np. Narody Zjednoczone („NZ”). Ponadto w niektórych okolicznościach kraje podlegające sankcjom lub działaniom podobnym do tych nałożonych przez organy takie jak NZ, ale które nie mogą być powszechnie uznawane, mogą otrzymać kredyt zaufania od MSB, ze względu na pozycję nakładającego i charakter działania.
- Kraje/obszary zidentyfikowane przez wiarygodne źródła<sup>12</sup> jako nieposiadające odpowiedniego prawa, regulacji lub innych działań zapobiegających praniu pieniędzy i finansowaniu terroryzmu.
  - Kraje/obszary zidentyfikowane przez wiarygodne źródła jako dostarczające finansowanie lub wsparcie dla działalności terrorystycznej lub które wyznaczyły organizacje terrorystyczne do współdziałania z nimi.
- Kraje/obszary zidentyfikowane przez wiarygodne źródła jako posiadające znaczący poziom korupcji lub innej działalności przestępczej w tym kraje/obszary źródłowe lub przepływowe dla trwającej działalności przestępczej tj. handel i przemysł nielegalnych narkotyków, ludzi, systematyczne oszustwa i nielegalny hazard.

---

<sup>12</sup> „Wiarygodne źródła” odnoszą się do informacji, które są dostarczane przez dobrze znane organy, które są ogólnie uważane za wiarygodne, i które udostępniają takie informacje wszystkim zainteresowanym osobom. Oprócz FATF oraz ciał regionalnych FATF, takie źródła mogą obejmować, ale nie ograniczają się do organów ponadnarodowych lub międzynarodowych takich jak Międzynarodowy Fundusz Walutowy, czy Grupa Egmont skupiająca Jednostki Wywiadu Finansowego, jak również inne właściwe krajowe organy rządowe i organizacje pozarządowe. Informacje dostarczone przez te wiarygodne źródła nie mają skutku regulacji prawnych i nie powinny być postrzegane jako automatyczne określenie, że coś reprezentuje wysokie ryzyko, ale zapewniają bardzo znaczące wskaźniki stopnia ryzyka geograficznego.

109. W zależności od oferowanych produktów lub usług MSB powinno rozważyć ryzyko geograficzne związane z prowadzoną transakcją. Ryzyko to może obejmować, ale nie wyłącznie, poniższe elementy:

- Przekaz pieniężny przesłany do lub otrzymany z jurysdykcji/obszaru wysokiego ryzyka.
- Klient przeprowadzający transakcję wymiany walut, a następnie wysyłający kwotę do jurysdykcji wysokiego ryzyka.

### **Ryzyko związane z klientem**

110. Określanie potencjalnego ryzyka prania pieniędzy i finansowania terroryzmu w zakresie jakim ryzyko finansowania terroryzmu może być zidentyfikowane ma zasadnicze znaczenie dla stworzenia całościowej ramy ryzyka. W oparciu o własne kryteria MSB powinno określić czy dany klient stwarza wyższe ryzyko i potencjalny wpływ czynników minimalizujących na tę ocenę. Zastosowanie czynników ryzyka może zminimalizować lub pogorszyć ocenę ryzyka.

Kategorie klientów, których działania mogą wskazywać na podwyższone ryzyko obejmują:

- Klientów, którzy prowadzą swoje przedsięwzięcia lub transakcje w niezwykłych okolicznościach tj.:
  - Klient, który podróżuje z niewyjaśnionych przyczyn do miejsc, w których prowadzi transakcje.
  - Przekaz bez widocznego celu biznesowego lub legalnego.
  - Niezwykła działalność pojedyncza lub kilkudniowa.
  - Większa skala lub częstotliwość transakcji wysłanych lub otrzymanych bez żadnego logicznego lub widocznego powodu.
  - Sieci klientów; tj. zdefiniowane grupy osób prowadzących transakcje w jednym lub kilku miejscach zbytu lub świadczących różne usługi.
  - Klient oferujący łapówkę lub napiwek w miejscu innym niż tam, gdzie dawanie napiwku jest zachowanie zwyczajowym.
- Klient, będący osobą na eksponowanym stanowisku politycznym.
- Transakcja bez fizycznego udziału klienta.
- Klient dzieli swoje transakcje (dzieli kwoty, aby uniknąć zgłoszenia lub rejestrowania).
- Klient przesyła pieniądze na internetowe strony hazardowe.
- Klient przesyła pieniądze do jurysdykcji wysokiego ryzyka.
- Klient, który wykorzystuje pośredników lub wspólników, kiedy charakter przedsięwzięcia lub transakcji utrudnia identyfikację rzeczywistego beneficjenta funduszy.
- Klient wie niewiele o beneficjencie lub niechętnie ujawnia szczegóły dotyczące beneficjenta (adres/informacje kontaktowe itd.).
- Klient lub osoba zaangażowana w transakcje nie ma widocznych powiązań z krajem przeznaczenia.
- Podejrzenie, że klient działa w imieniu strony trzeciej, ale nie ujawnia takiej informacji.
- Transakcja związane z organizacjami charytatywnymi i innymi organizacjami typu non-profit, które podlegają monitoringowi lub nadzorowi (zwłaszcza te, które działają w sposób transgraniczny).
- Klient, który był przedmiotem śledztwa organów ścigania, o którym MSB wiedziało.
- Klient, który przedstawia fałszywą tożsamość, co jest widoczne na podstawie dokumentów, na podstawie tego, że nie istnieje związek pomiędzy klientem a dokumentem, lub w porównaniu z innymi dokumentami (np. użycie dokumentu tożsamości wydanego przez inne państwo).
- Klient, który przedstawia różną tożsamość lub różne dane potwierdzające tożsamości (takie

jak numer telefonu lub adres) w różnych okolicznościach.

- Klient, który jest odbiorcą transakcji zgodnych z modelem postępowania przestępcy np. od osób starszych z szerokiego obszaru geograficznego w kworach zgodnych z oszustwem na loterii.
- Klient, który jest odbiorcą przekazów w sposób sezonowy zgodny z modelem postępowania przestępcy np. w sezonie zbiorów marihuany, nielegalnej imigracji.

### **Ryzyko związane z produktem/usługą**

111. Ogólna ocena ryzyka powinna także obejmować określenie potencjalnych zagrożeń wynikających z produktów i usług oferowanych przez MSB. MSB powinno być świadome ryzyka związanego z nowymi albo innowacyjnymi produktami lub usługami nieoferowanymi dokładnie przez MSB, ale które wykorzystują systemy MSB do dostarczania produktu lub świadczenia usługi. Badanie ryzyka związanego z produktami lub usługami powinno obejmować rozważenie następujących czynników:

- Produkty lub usługi, które mogą nierozłącznie wiązać się z pewnym stopniem anonimowości lub mogą bez trudu przekraczać granice międzynarodowe tj. przekazy pieniężne przeprowadzane online, karty z zakodowaną wartością (stored-value cards), przekazy bankowe i przekazy pieniężne przez telefony komórkowe.
- Produkty lub usługi, które mają bardzo wysoki limit transakcji albo transakcja nie ma limitu.
- Globalny zasięg produktu lub usługi.
- Produkt lub usługa, która umożliwia wymianę gotówki na negocjowalny instrument taki jak karta z zakodowaną wartością lub przekazy bankowe.

112. Ryzyko związane z transakcją może różnić się w zależności od tego czy MSB wysyła czy odbiera transakcję. Ogólna ocena ryzyka powinna obejmować weryfikację transakcji jako całość.

Powinno ona obejmować uwzględnienie takich czynników jak:

a) Transakcje wysyłane:

- Zachowanie klienta w miejscu pochodzenia:
  - Transakcja jest niepotrzebnie złożona jak na przedstawiony cel.
  - Przekazy są dokonywane w imieniu osób trzecich.
  - Transakcja jest niezgodna z sytuacją finansową lub zawodową, lub jest poza normalnym działaniem biznesowym dla klienta w świetle informacji dostarczonych przez klienta w trakcie przeprowadzania transakcji lub w trakcie dalszych kontaktów (takich jak rozmowa) z klientem.
  - Klient chce zapłacić niezwykle opłaty za przeprowadzenie transakcji.
  - Klient ma znikomą wiedzę na temat kwoty, jaka jest związane z transakcją.
  - Klient jest ślepy na fakt, że transakcja zdaje się być związana z praniem pieniędzy lub finansowaniem terroryzmu.
  - Klient zasięga informacji w celu uniknięcia zgłoszenia lub stara się przekonać personel do zaniechania zgłoszenia.
  - Klient wysyła pieniądze za granicę i stwierdza, że oczekuje otrzymania przekazu przychodzącego na tę samą kwotę.
  - Klient otrzymuje przekaz elektroniczny i natychmiast dokonuje przekazu na taką samą kwotę.
  - Niezwykle wysokie przekazy elektroniczne.
  - Klient wysyła często przekazy elektroniczne do obcych państw, ale nie wydaje się, by miał jakiegokolwiek powiązania z krajami przeznaczenia.

- Niezwykła wymiana waluty (np. waluta o małej denominacji za walutę o wysokiej denominacji).
- Działalność wykryta w trakcie monitoringu końcowego:
  - Przekazy do tej samej osoby od różnych osób lub do różnych osób od tej samej osoby.
  - Klient otrzymuje przekaz elektroniczny i natychmiast dokonuje przekazu na taką samą kwotę. - Niezwykle wysokie sumy przekazów elektronicznych.
  - Klient wykorzystuje pseudonimy i wiele podobnych, ale różnych adresów.
  - Sieć klientów wykorzystująca ten sam adres.

W wielu z tych przypadków działalność klienta może być widoczna zarówno w interakcji w punkcie sprzedaży, jak i w monitoringu końcowym transakcji.

b) Transakcje odbierane:

- Krajowym przekazom elektronicznym, otrzymanym przez MSB w wysokości 1 000 EUR/USD lub większe powinny towarzyszyć, w wiadomości lub formularzu zapłaty, numer rachunku inicjatora lub unikalny numer identyfikacyjny. Międzynarodowe przekazy elektroniczne w wysokości 1 000 EUR/USD lub większe powinny zawierać pełne informacje o inicjatorze (nazwę nadawcy, numer rachunku nadawcy lub unikalny numer referencyjny, adres nadawcy lub krajowy numer identyfikacyjny lub numer identyfikacyjny klienta lub datę i miejsce urodzenia).

Dlatego MSB powinny zwrócić szczególną uwagę na:

- Transakcje, którym nie towarzyszą pełne wymagane informacje o inicjatorze.
- Kiedy zażądano dodatkowych informacji od zlecającego MSB, ale i tak nie zostały przesłane.
- Klient, który jest odbiorcą transakcji zgodnych z modelem postępowania przestępcy np. od osób starszych z szerokiego obszaru geograficznego w kwotach zgodnych z oszustwem na loterii.
- Klient, który jest odbiorcą przekazów elektronicznych w sposób sezonowy zgodny z modelem postępowania przestępcy np. w sezonie zbiorów marihuany, nielegalnej imigracji.
- Duża liczba odebranych transakcji jednocześnie lub w pewnym okresie, które nie zdają się pasować do zwykłych potrzeb odbiorcy lub jego modelu odbioru transakcji.

## **Ryzyko związane z pośrednikami**

113. Ogólna ocena ryzyka powinna analizować szczególne czynniki, które wynikają z wykorzystania pewnych pośredników<sup>13</sup> w celu ułatwienia dostarczenia produktów lub świadczenia usług MSB. W niektórych przypadkach pośrednicy mogą również samodzielnie wykorzystywać produkty i usługi. Ocena ryzyka związanego z pośrednikiem jest bardziej złożona dla tych MSB, które są obecne na arenie międzynarodowej ze względu na wymogi weryfikacyjne jurysdykcji i logistykę nadzoru pośrednika. Analiza ryzyka związanego z pośrednikiem powinna obejmować takie czynniki jak poniższe w oparciu o zasadność i adekwatność czynnika w ramach modelu, systemów i kontroli biznesowych MSB:

- Pośrednicy prowadzący zazwyczaj wiele transakcji z innymi lokalizacjami pośredników zwłaszcza z pośrednikiem z obszaru geograficznego, który wymaga uwagi.

---

<sup>13</sup> Glosariusz FATF podaje następującą definicję pośrednika: „Dla celów Zalecenia Specjalnego nr 6 pośrednik to osoba, która świadczy usługi przekazu środków pieniężnych lub wartości majątkowych w ramach prowadzenia lub w ramach kontraktu z prawnie zarejestrowaną lub posiadającą licencję osobą zajmującą się przekazem pieniężnym (np. licencjobiorca, franczyzobiorca, koncesjonariusz).

- Wartość transakcji pośrednika albo ogólna, albo względem typowych wartości transakcji dokonywanych w przeszłości.
- Pośrednicy, do których odnosiły się inne departamenty MSB.
- Pośrednicy, którzy byli przedmiotem negatywnej uwagi wiarygodnych mediów lub śledztwa organów ścigania.
- Pośrednicy, którzy nie działają zgodnie z politykami wewnętrznymi i regulacjami zewnętrznymi tj. wymogami dot. zgodności, monitoringu, sprawozdawczości lub praktyki Poznaj swojego klienta.
- Pośrednicy, którzy nie chcą postępować zgodnie z zaleceniami dot. zgodności i dlatego podlegają nadzorowi, zawieszeniu lub rozwiązaniu.
- Pośrednicy, którzy nie dostarczają wymaganych informacji dotyczących na żądanie.
- Pośrednicy, których pobieranie danych jest nieściśle, niedbałe lub niespójne.
- Pośrednicy, chcący przyjąć fałszywe dane identyfikacyjne.
- Pośrednicy, chcący wprowadzić dane identyfikacyjne do rejestru, który zawiera fałszywe informacje, adresy, które nie istnieją, o których wiadomo, że nie istnieją dla osoby z tego obszaru, lub numery telefonu, które są używane jako wypełniacze.
- Pośrednicy z proporcjami wysłanych do odebranych transakcji, które są niezgodne z innymi pośrednikami w danej lokalizacji lub wskazują na udział w transakcjach o charakterze przestępczym.
- Pośrednicy, których sezonowe wahanie transakcji jest niezgodne z innymi pośrednikami w danej lokalizacji lub wskazuje na udział w transakcjach o charakterze przestępczym.
- Pośrednicy, których stosunek klientów, którzy są kwestionowani lub nietypowi do klientów, którzy nie mieszczą się w takiej grupie jest poza normą dla porównywalnych lokalizacji.
- Pośrednicy, których stosunek transakcji, które są kwestionowane lub nietypowe do transakcji, które nie mieszczą się w takiej grupie jest poza normą dla porównywalnych lokalizacji.

### **Czynniki mogące wpłynąć na ocenę ryzyka**

114. Metodologia podejścia opartego na ryzyku MSB może uwzględnić czynniki ryzyka odpowiednie dla danych kategorii klientów lub transakcji. Czynniki te mogą zwiększyć lub zmniejszyć dostrzegane ryzyko stwarzane przez konkretnego klienta lub transakcję i mogą obejmować:

- Cel transakcji: transakcje przeprowadzane głównie w celu ułatwienia tradycyjnych, nisko denominowanych transakcji klienta mogą stanowić niższe ryzyko niż transakcje prowadzone w celu ułatwienia przemieszczania dużych ilości gotówki.
- Rodzaj transakcji: transakcja wysłana przez osobę na rachunek firmowy może stanowić mniejsze ryzyko niż transakcja detaliczna przeprowadzana pomiędzy dwiema osobami.
- Metoda wysyłania lub odbioru transakcji: transakcja bez fizycznego udziału klienta może stanowić wyższe ryzyko niż transakcja przeprowadzana osobiście.
- Rodzaj klienta: przypadkowy klient może stanowić większe ryzyko niż znany klient z historią transakcji i długotrwałymi relacjami z MSB i/lub lokalizacją pośrednika.
- Poziom współpracy ze strony klienta w związku z prośbą o dostarczenie informacji osobowych związanych z charakterem transakcji: klienci, którzy współpracują i są gotowi podać rzetelne informacje dotyczące charakteru transakcji na wniosek mogą stanowić niższe ryzyko niż klienci, którzy stają się podirytowani lub defensywni lub nieświadomi informacji, których znajomości się od nich oczekuje w danych okolicznościach, kiedy je przedstawiają (np. numer telefonu osoby, do której przesyłany jest tysiąc dolarów).

- Częstotliwość powtarzania się sytuacji, w której MSB otrzymuje wniosek o konkretny rodzaj transakcji: rodzaje transakcji, o które się wnioskuje i pojawiające się rzadziej mogą stanowić wyższe ryzyko niż rodzaje transakcji prowadzone w sposób regularny. Transakcje, które wykraczają poza normę w świetle informacji dostarczonych przez klienta w czasie prowadzenia transakcji powinny być uznane za wykazujące wyższe ryzyko.

### **Kontrole w sytuacjach wysokiego ryzyka**

115. MSB powinny wdrożyć odpowiednie środki i kontrole w celu minimalizacji potencjalnego ryzyka prania pieniędzy i finansowania terroryzmu wobec tych sytuacji, którym przypisano wysoki stopień ryzyka w wyniku oceny ryzyka przeprowadzonej przez MSB. Te środki i kontrole mogą obejmować:

- Zwiększony poziom procedury poznaj swojego klienta (KYC) lub zwiększona należyta staranność tj. kontakt prowokacyjny z klientem w celu określenia powodu transakcji, relacji klienta z nadawcą lub odbiorcą i źródła funduszy.
- Zwiększony poziom kontroli i częstotliwości przeglądów relacji klienta.
- Zwiększony monitoring transakcji produktów, usług i kanałów wyższego ryzyka.
- Zwiększona świadomość podmiotu gospodarczego o klientach i transakcjach wyższego ryzyka.
- Zwiększone systematyczne kontrole i integralność danych w punkcie płatności, zwłaszcza w lokalizacjach pośredników o wyższym ryzyku.
- Skupienie działalności przez znanego lub nowego klienta.
- Te same środki i kontrole mogą często być skierowane do więcej niż jednego zidentyfikowanego kryterium i niekoniecznie oczekuje się, że podmiot gospodarczy ustanowi specjalne kontrole skupiające się na każdym kryterium ryzyka.

## **Rozdział drugi: Zastosowanie podejścia opartego na ryzyku**

### **Należyta staranność w kontaktach z klientami/poznaj swojego klienta**

116. Procedury: *Należyta staranność wobec klientów (CDD)* lub *Poznaj swojego klienta (KYC)* mają na celu umożliwienie MSB sformułowania uzasadnionego przekonania, że zna ono prawdziwą tożsamość każdego klienta w czasie, gdy klient prowadzi transakcje lub w czasie przeglądu końcowego modelu działalności klienta.

Procedury Należyta staranność wobec klientów lub Poznaj swojego klienta dla MSB różnią się od procesów instytucji finansowych takich jak bank lub firmy brokerskie, w nich MSB zazwyczaj świadczy okazjonalne, oparte na transakcjach usługi dla przypadkowych klientów i na ogół nie otwiera ani nie prowadzi rachunków. Jednak MSB czasem również wprowadzają systemy lojalnościowe dla klientów i narzędzia zarządzania kontaktami takie jak karty członkowskie. Procedury te są w dużym stopniu powiązane z jego zdolnością monitorowania i analizowania transakcji po jej wykonaniu. MSB powinno posiadać procedury, które są skutecznie wdrożone i stosowane do:

a) Identyfikacji i weryfikacji tożsamości (a) każdego klienta prowadzącego lub próbującego przeprowadzić transakcję osiągającą próg albo powyżej ustawowego progu kwotowego<sup>14</sup>; (b) każdego klienta, który prowadzi przedsięwzięcie związane z licznymi transakcjami przez określony czas z wykorzystaniem MSB, poprzez fizyczne sprawdzanie dokumentów tożsamości klienta w czasie przeprowadzania transakcji lub w czasie ustanawiania relacji biznesowych, oraz

b) W sytuacji gdy transakcja jest przekazem elektronicznym<sup>15</sup> na kwotę wyższą niż 1 000 EUR/USD tożsamość klienta powinna obejmować następujące informacje zwane „pełnymi informacjami o inicjatorze”: nazwa nadawcy, numer rachunku nadawcy lub unikalny numer referencyjny, adres klienta lub krajowy numer identyfikacyjny lub numer identyfikacyjny klienta lub datę i miejsce urodzenia, informacje te powinny być zawarte w wiadomości lub na formularzy zapłaty, który towarzyszy przekazowi elektronicznemu. W przypadku przekazów elektronicznych krajowych, zlecający MSB może zawrzeć pełne informacje o nadawcy lub tylko numer rachunku nadawcy lub unikalny numer identyfikacyjny, zakładając, że pełna informacja inicjatorze będzie dostępna dla instytucji finansowej beneficjenta i dla uprawnionego organu w ciągu 3 dni roboczych.

c) MSB powinno również:

zidentyfikować rzeczywistego beneficjenta i podjąć rozsądne działania mające na celu weryfikację jego tożsamości. Działania, które muszą być podjęte w celu zweryfikowania tożsamości rzeczywistego beneficjenta będą różniły się w zależności od ryzyka.

d) W przypadku transakcji wyższego ryzyka lub klienta, należy pozyskać właściwe informacje dodatkowe w celu poznania okoliczności i działalności związanych z klientem w tym oczekiwany charakter i poziom transakcji. O ile to wskazane, należy pozyskać dalsze właściwe informacje dodatkowe w celu poznania okoliczności związanych z klientem w tym relacje z nadawcą lub odbiorcą i źródło funduszy.

e) Należy okresowo aktualizować odpowiednie informacje dotyczące należytej staranności wraz z oceną ryzyka klienta.

f) O ile to wskazane i ma zastosowanie w trakcie weryfikacji końcowej działalności klienta, należy pozyskać dalsze właściwe informacje dodatkowe w celu poznania okoliczności związanych z klientem w tym charakter transakcji, relacje z nadawcą lub odbiorcą i źródło funduszy.

117. Punktem wyjściowym dla MSB jest ocena ryzyka, które mogą stanowić niektóre kategorie lub rodzaje klientów biorąc pod uwagę wszelkie odpowiednie zmienne ryzyka przed podjęciem końcowej decyzji. W związku z tym MSB może również uwzględnić użyteczne przykłady ryzyka wyższego lub niższego, które mogą być przedstawione przez krajowe organy regulacyjne. MSB określi wymogi dotyczące należytej staranności odpowiednie dla każdego klienta.

---

<sup>14</sup> FATF wymaga, by prób krajowy nie był wyższy od 15 000 USD/EUR dla transakcji okazjonalnych (innych niż przekazy elektroniczne), w tym sytuacji, w których transakcja jest przeprowadzana w ramach jednej operacji lub w kilku operacjach, które wydają się być powiązane. Zob. Uwagi interpretacyjne do Zaleceń 5, 12 i 16.

W przypadku transgranicznych przekazów elektronicznych przekraczających 1 000 USD/EUR instytucja inicjująca powinna załączyć „pełne informacje o inicjatorze”, które obejmują nazwę inicjatora i numer rachunku, o ile istnieje, lub w przypadku braku rachunku unikalny numer referencyjny; albo adres inicjatora, albo krajowy numer identyfikacyjny, numer identyfikacyjny klienta, lub datę albo miejsce urodzenia. W przypadku krajowego przekazu elektronicznego przekraczającego próg, jeżeli pełne informacje o inicjatorze mogą być udostępnione instytucjom finansowym i odpowiednim organom inną drogą, instytucja inicjująca musi załączyć jedynie nazwę i numer rachunku lub unikalny identyfikator. Zob. Uwagi interpretacyjne do SR VII. Należy zauważyć, że w niektórych krajach lub jurysdykcjach obowiązek załączania informacji o inicjatorze w przekazach funduszy może mieć zastosowanie niezależnie od progów.

<sup>15</sup> Termin przekaz elektroniczny odnosi się do każdej transakcji przeprowadzanej w imieniu inicjatora (osoby prawnej lub fizycznej) przez instytucję finansową drogą elektroniczną, mającej na celu udostępnienie kwoty pieniędzy beneficjentowi w innej instytucji finansowej. Inicjator i beneficjent mogą być tą samą osobą.

Mogą one obejmować:

- Standardowy poziom należytej staranności stosowany do wszystkich klientów, zwłaszcza stosowana identyfikacja klienta przy odpowiednim progu kwotowym wymagana przez prawo, regulacje lub inne wymogi krajowe lub politykę wewnętrzną i stosowane regulaminy.
- Standardowy poziom należytej staranności ograniczony przy wystąpieniu ustalonych okoliczności niższego ryzyka tj. przeprowadzanie transakcja dla:
  - Firm notowane na giełdzie podlegających regulacyjnym wymogom jawności.
  - Innych instytucji finansowych (krajowe lub zagraniczne) podlegających reżimowi przeciwdziałania praniu pieniędzy i finansowania terroryzmu zgodnemu z Zaleceniami FATF. Jednakże dla wszystkich przekazów pieniężnych przekraczających próg 1000 EUR/USD MSB powinny przynajmniej uzyskać informacje o inicjatorze, jak zostało wskazane powyżej, oraz starać się zidentyfikować rzeczywistego beneficjenta transakcji.
- Zwiększony poziom należytej staranności powinien być zastosowany względem klientów określonych jako stwarzających wysokie ryzyko tj.:
  - Transakcja bez fizycznego udziału klienta.
  - Klienci przeprowadzający duże transakcje finansowe, albo w trakcie pojedynczego działania albo w trakcie kilku działań, które wdają się być ze sobą powiązane.
  - Klienci prowadzący działalność na dużą skalę lub o dużej częstotliwości.
  - Klienci wysyłający lub odbierający transakcje z jurysdykcji wyższego ryzyka.
  - Klienci zlokalizowani w jurysdykcji wyższego ryzyka.
  - Klienci, którzy są osobami zajmującymi eksponowane stanowiska polityczne.
  - Klienci, których okoliczności są opisane w ust. 110 powyżej.

### ***Monitoring klientów i transakcji***

118. Stopień i charakter monitorowania przez MSB będzie zależał od rozmiaru MSB, ryzyka prania pieniędzy i finansowania terroryzmu, które wykazuje podmiot gospodarczy, używanej metody monitorowania (ręcznej, zautomatyzowanej lub połączenie obu) i rodzaju nadzorowanej działalności. Przy zastosowaniu podejścia opartego na ryzyku do monitoringu MSB i osoby odpowiedzialne za nadzór regulacyjny muszą uznać, że nie wszystkie transakcje, rachunki lub klienci będą monitorowani w ten sam sposób. Stopień monitorowania będzie oparty o dostrzegane ryzyko powiązane z klientem, produktami lub usługami używanymi przez klienta, lokalizacji klienta i charakteru transakcji. Metodologie monitorowania i procesy również muszą uwzględniać zasoby MSB. Na przykład mniejsze MSB nie musi wdrażać technologicznie zaawansowanych systemów monitorowania transakcji o ile używane metody do przeprowadzania monitoringu adekwatnie odzwierciedlają ryzyko działalności MSB.

119. Głównym celem monitoringu w ramach systemu opartego na ryzyku jest odpowiadanie na kwestie związane z całym przedsiębiorstwem w oparciu o analizę głównych zagrożeń każdego MSB. Organy regulacyjne powinny zatem pamiętać i zwrócić odpowiednią uwagę na oceny dokonane przez MSB, zakładając, że te oceny są zgodne z wymogami legislacyjnymi lub regulacyjnymi i są rozsądnie i adekwatnie udokumentowane.

120. Monitorowanie w ramach podejścia opartego na ryzyku pozwala MSB na tworzenie progów pieniężnych lub innych w celu określenia, które z działalności będą sprawdzane. Zdefiniowane sytuacje i progi stosowane w tym celu powinny być regularnie kontrolowane w celu stwierdzenia ich adekwatności dla ustalonych poziomów ryzyka. MSB powinny również oceniać adekwatność i integralność systemów i procesów w sposób okresowy. Rezultaty monitoringu powinny być dokumentowane albo automatycznie, albo ręcznie (lub przez

połączenie dwóch opcji) w celu utworzenia całościowego audytu, a także powinno być przechowywane zgodnie ze stosownymi wymogami dotyczącymi prowadzenia rejestrów.

121. Prawo krajowe powinno zakładać, że dla wszystkich przekazów elektronicznych w wysokości 1 000 EUR/USD lub więcej, instytucja beneficjenta powinna przyjąć skuteczne procedury podejścia opartego na ryzyku w celu identyfikacji i obsługi przekazów elektronicznych, którym nie towarzyszą pełne informacje o inicjatorze. Brak pełnych informacji o inicjatorze może być uznane za czynnik w ocenie czy przekaz elektroniczny czy też powiązane transakcje są podejrzane i, o ile ma to konieczne, czy powinny być zgłoszone do jednostki wywiadu finansowego lub innego uprawnionego organu.

### ***Raportowanie transakcji podejrzanych***

122. Zgłaszanie podejrzanych transakcji lub działalności jest znaczące dla zdolności kraju do wykorzystania informacji finansowej do zwalczania prania pieniędzy i finansowania terroryzmu i innych przestępstw finansowych. Reżimy zgłaszania transakcji podejrzanych w poszczególnych państwach są opisane w prawie krajowym, i wymagają by instytucje dokonywały zgłoszeń kiedy osiągnięto poziom podejrzania.

123. W sytuacji kiedy konieczne jest zgłoszenie podejrzanej transakcji podejście oparte na ryzyku nie ma zastosowania. Jednakże pojawiają się wyzwania dla tych MSB, które są zlokalizowane w różnych jurysdykcjach. W celu uniknięcia sankcji regulacyjnych należy zwrócić uwagę na odpowiedni format, czas zgłoszenia i stosowane wymogi dotyczące prowadzenia rejestrów, ponieważ wymogi mogą różnić się w zależności od jurysdykcji.

124. Podejście oparte na ryzyku jest jednak odpowiednie w celu identyfikacji podejrzanej działalności np. poprzez kierowanie dodatkowych środków do tych obszarów, w których MSB zidentyfikowało wyższe ryzyko tj. niektóre produkty lub usługi lub pośrednicy lub niektóre modele przeprowadzania transakcji. W ramach podejścia opartego na ryzyku prawdopodobne jest, że MSB wykorzysta informacje dostarczone przez uprawnione organy w celu nakierowanie jego podejścia w celu zidentyfikowania podejrzanej działalności. MSB powinno również okresowo oceniać adekwatność i integralność swoich systemów do identyfikacji i zgłaszania podejrzanych transakcji. Decyzje dotyczące zgłoszenia czy zaniechania zgłoszenia powinny być dokumentowane albo automatycznie, albo ręcznie (lub przez połączenie dwóch opcji) w celu utworzenia całościowego audytu, a także powinny być przechowywane zgodnie ze stosownymi wymogami dotyczącymi prowadzenia rejestrów.

### ***Szkolenie i zwiększanie świadomości***

125. Zgodnie z Zaleceniem 15 wymaga się, by MSB zapewniły dla swoich pracowników szkolenia w zakresie prania pieniędzy i finansowania terroryzmu i ważne jest, by pracownicy MSB otrzymali odpowiednie i proporcjonalne szkolenie dotyczące prania pieniędzy i finansowania terroryzmu. Zobowiązanie MSB zakładające przeprowadzanie i utrzymywanie skutecznych kontroli polega zarówno na szkoleniu jak i zwiększaniu świadomości. Wymaga to wysiłku na skalę całego przedsiębiorstwa w celu przekazania wszystkim odpowiednim pracownikom co najmniej ogólnych informacji dotyczących prawa, regulacji i polityki wewnętrznej dotyczących przeciwdziałaniu prania pieniędzy i finansowania terroryzmu.

126. Zastosowanie podejścia opartego na ryzyku do różnych metod dostępnych dla szkolenia daje każdemu MSB dodatkową elastyczność dotyczącą częstotliwości, mechanizmów przeprowadzenia i kluczowych punktów szkolenia. Szkolenie powinno być udokumentowane, a dokumentacja powinna zawierać nazwiska uczestników, daty uczestnictwa, metodę

przeprowadzenia i treść. Rejestry spotkań powinny być przechowywane zgodnie z odpowiednimi wymogami dotyczącymi prowadzenia rejestru. MSB powinien dokonywać przeglądu swojej liczby zatrudnionych i dostępnych środków oraz wdrażać programy szkoleniowe, które dostarczają odpowiednie informacje z zakresu prania pieniędzy i finansowania terroryzmu tzn.:

- Dostosowane do odpowiednich obowiązków personelu (np. zarządzanie, personel niższego szczebla posiadający bezpośredni kontakt z klientem lub obsługa).
- Na odpowiednim poziomie uszczegółowienia (np. personel niższego szczebla, skomplikowane produkty lub produkty zarządzane przez klienta).
- W częstotliwości związanej z poziomem ryzyka linii biznesowej i związanej obrotem personelu poziomem ryzyka związanego z pośrednikiem.
- Przeprowadzane wstępnie dla nowego personelu i w kolejnych okresach dla personelu istniejącego w celu ponownego przypomnienia o bieżących zagrożeniach związanych praniem pieniędzy i finansowaniem terroryzmu i wprowadzenia nowych.
- Zakończone testem w celu sprawdzenia i upewnienia się że wiedza personelu jest współmierna ze szczegółami dostarczonych informacji.

127. W zależności od wymogów regulacyjnych i/lub polityk wewnętrznych w tym wymogów zgodności z przeciwdziałaniem prania pieniędzy lub najlepszymi praktykami w branży MASB musi również wymagać od swoich pośredników, aby przeszli oni odpowiednie szkolenie w zakresie zapobiegania praniu pieniędzy i finansowaniu terroryzmu. Szkolenie pośredników może również być oparte na ryzyku, ale na ogół może obejmować szkolenie wstępne na miejscu i "zza biurka" (tj. po aktywacji) i trwające szkolenie przez programy oparte na sieci, okresowe maile lub newslettery, strony internetowe chronione hasłem lub wyskakujące komunikaty w miejscu siedziby. Szkolenie to powinno przekazać im informacje na temat wszelkich nowych osiągnięć w tym informacje na temat bieżących technik prania pieniędzy i finansowania terroryzmu, metod i trendów, a także informacje na temat wszelkich aspektów prawa i obowiązków związanych z zapobieganiem praniu pieniędzy i finansowaniu terroryzmu. W połączeniu lub jako dodatek do takiego szkolenia MSB może zapewnić okresowe programy kontroli zgodności związane z całościową oceną zgodności pośrednika z wewnętrznymi i zewnętrznymi wymogami regulacyjnymi w sprawie zapobiegania praniu pieniędzy i finansowaniu terroryzmu.

### ***Należyta staranność w kontaktach z pośrednikiem/poznaj swojego pośrednika***

128. Działania realizujące zasadę „należyta staranność w kontaktach z pośrednikiem/poznaj swojego pośrednika” mają na celu umożliwienie MSB osiągnięcie uzasadnionego przekonania, że zna strukturę prawną i własnościową swoich pośredników oraz że będzie prowadzić przedsięwzięcia z legalnymi i rzeczywistymi pośrednikami, którzy w sposób rzetelny będą wdrażać lub stosować się do (w zależności od lokalnych przepisów) wymogów dotyczących zapobiegania praniu pieniędzy i finansowaniu terroryzmu, obowiązków, polityk i procedur.

Procedury MSB powinny obejmować takie czynniki jak:

- Po zastosowaniu, należy zidentyfikować pośrednika i wykonać niezbędne podstawowe sprawdzenie oraz procedury należytej staranności, takie jak ostatnie zmiany od innego dostawcy produktu/usługi, czas pracy w podmiocie gospodarczym, struktura własności, zdolność kredytowa, płynność finansowa, rodzaj handlu lub branży, struktura licencyjna i regulacyjna i inne licencje regulacyjne lub rejestracje, którym MSB może podlegać (np. jako inkasent czeków).

- Należy pozyskać odpowiednie dodatkowe informacje, aby zrozumieć działalność aplikanta tj. oferowanie innych usług MSB, wcześniejsze zapisy zgodności prawnej i regulacyjnej Pośrednika, oczekiwany charakter i poziom transakcji i działalność klientów oraz ryzyko geograficzne.
- Po zatwierdzeniu należy przeprowadzić szkolenie z zakresu zapobiegania praniu pieniędzy dla nowego pośrednika obejmujące stosowne wymogi dot. zapobiegania praniu pieniędzy i finansowaniu terroryzmu, obowiązku dotyczące zgodności z programem zapobiegania praniu pieniędzy i wewnętrzne polityki i procedury MSB.
- Należy zapewnić materiały, narzędzia i szkolenie bieżące i okresowe dla pośredników w zakresie zgodności z programem zapobiegania praniu pieniędzy i finansowaniu terroryzmu.
- Należy wykorzystać podstawowe narzędzie oceny ryzyka, które monitoruje działalność pośrednika w celu sprawdzenia ryzyka związanego z transakcją lub identyfikacji pośrednika, który wykazuje zachowania ryzykowne takie jak transakcje strukturalnie powiązane, dzielenie się tożsamością klienta lub dzielenie się informacjami biograficznymi, większy zakres nadawców lub odbiorców, niezwykle lub niewytłumaczalne szybkie transakcje, proporcjonalne lub sezonowe wahania w wartości transakcji, wprowadzone podrzędne dane w miejscu nadania lub płatności, powiązana lub słabej jakości działalność STR/SAR, korytarze pośrednik-do-pośrednika o wyższej wartości, niezwykle zachowania pośrednika, lub niezwykle koncentracja produktów lub usług.
- Należy zapewnić natychmiastową uwagę lub naprawę zachowań ryzykownych na miejscu lub „zza biurka” kontaktując się z pośrednikiem, co może skutkować dalszym szkoleniem lub nadzorem, zawieszeniem lub rozwiązaniem umowy z pośrednikiem.
- Należy zapewnić wskazówki i pomoc dla pośrednika w celu oceny własnej zgodności z programem i przeprowadzenia własnej oceny ryzyka w oparciu o unikalne profile ryzyka dla jego produktów i usług, klientów, lokalizacji geograficznej i pod-pośredników oraz miejsc zbytu (jeśli ma to zastosowanie).
- Należy zapewnić zgodność z politykami wewnętrznymi i regulacjami zewnętrznymi tj. zgłaszanie podejrzanych lub zamierzonych jako podejrzane transakcje, dużych transakcji, monitorowanie zachowań ryzykownych opisanych powyżej zgłaszanie i prowadzenie rejestru poprzez okresowe przeglądy zgodności z programem zapobiegania praniu pieniędzy.

129. Punktem wyjściowym dla MSB jest ocena ryzyka, które może wykazywać pośrednik biorąc pod uwagę wszelkie odpowiednie czynniki ryzyka przez podjęciem ostatecznej decyzji. Ocena ryzyka związanego z pośrednikiem jest bardziej złożona dla tych MSB, które są obecne na arenie międzynarodowej ze względu na wymogi weryfikacyjne jurysdykcji i logistykę nadzoru pośrednika.

Analiza ryzyka związanego z pośrednikiem powinna zawierać:

- Standardowy poziom należytej staranności stosowany do wszystkich aplikantów tj. struktura prawna i własnościowa, solidność i zgodność z programem zapobiegania praniu pieniędzy i finansowaniu terroryzmu.
- Standardowy poziom ograniczony przy wystąpieniu okoliczności niższego ryzyka tj. prowadzenie transakcji dla:
  - Firmy notowanych na giełdzie podlegających regulacyjnym wymogom ujawniania informacji.
  - Innych MSB (krajowych lub zagranicznych) podlegające reżimowi zapobiegania praniu pieniędzy i finansowaniu terroryzmu zgodnemu z zaleceniami FATF i które są nadzorowane pod względem zgodności z tymi wymogami.
- Zwiększony poziom należytej staranności zastosowany względem podmiotów określonych jako stwarzających wysokie ryzyko tj.:
  - Pośrednicy zlokalizowani w jurysdykcji wyższego ryzyka.

- Kierownicy posiadający status osoby zajmującej eksponowane stanowisko polityczne.
- Pośrednicy, którzy w przeszłości nie działali zgodnie z regulacjami.
- Pośrednicy obsługujący klientów lub transakcje wysokiego ryzyka zgodnie z ust. 110 do 112 powyżej.

## **Monitorowanie pośredników**

130. Monitorowanie pośredników jest bardzo ważnym elementem w skutecznym programie zapobiegania praniu pieniędzy i finansowaniu terroryzmu MSB. Podczas gdy wszyscy pośrednicy wymagają podstawowego monitoringu w celu oceny i określenia ryzyka systemowego tj. nieadekwatne szkolenia, nowe lub zmieniające się produkty lub usługi, i słaba indywidualna ocena lub wydajność, podejście oparte na ryzyku wymaga wyższego poziomu monitorowania w celu zlokalizowania i wyeliminowania kilku pośredników, którzy świadomie lub przez zamierzony brak uwagi działają w sposób, który pozwala zataić ich relacje z klientami w trakcie rutynowego monitorowania. Stopień i charakter monitorowania pośredników będzie zależał od wartości transakcji i ogólnej wartości pośrednika, z którym MSB dzieli obowiązki skutecznego zapobiegania praniu pieniędzy i finansowaniu terroryzmu, używaną metodę monitorowania (ręcznej, zautomatyzowanej lub połączenie obu) i rodzaj nadzorowanej działalności. W trakcie stosowania podejścia opartego na ryzyku do monitorowania, stopień monitorowania będzie oparty o dostrzegane ryzyko zarówno zewnętrzne jak i wewnętrzne związane z pośrednikiem tj. produkty lub usługi świadczone przez pośrednika, lokalizacja pośrednika i charakter działalności.

131. Głównym celem monitorowania w ramach systemu opartego na ryzyku jest odpowiadanie na kwestie związane z całym przedsiębiorstwem w oparciu o analizę głównych zagrożeń każdego MSB. Organy regulacyjne powinny zatem pamiętać i zwrócić odpowiednią uwagę na oceny dokonane przez MSB, zakładając, że te oceny są zgodne z wymogami legislacyjnymi lub regulacyjnymi i są rozsądnie i adekwatnie udokumentowane.

132. Monitorowanie pośrednika w ramach podejścia opartego na ryzyku pozwala MSB na tworzenie progów kwotowych lub innych w celu określenia, które działalności będą sprawdzane. Zdefiniowane sytuacje i progi stosowane w tym celu powinny być regularnie kontrolowane w celu stwierdzenia ich adekwatności dla ustalonych poziomów ryzyka. MSB powinny również oceniać adekwatność i integralność systemów i procesów w sposób okresowy.

133. Monitorowanie pośrednika w ramach podejścia opartego na ryzyku powinno wykorzystywać podstawowe narzędzia oceny ryzyka, które monitorują działalność pośrednika w celu sprawdzenia ryzyka związanego z transakcją lub identyfikacji pośredników, którzy wykazują ryzykowne zachowania tj. opisane w ust. 113 powyżej, transakcje strukturalnie, dzielenie się tożsamością klienta lub dzielenie informacji biograficznych, większy zakres nadawców lub odbiorców, niezwykle lub niewytłumaczalne szybkie transakcje, wprowadzone podrzędne dane w miejscu nadania, powiązana działalność STR/SAR, korytarze pośrednik-do-pośrednika o wyższej wartości, niezwykle zachowania pośrednika, lub niezwykle koncentracja produktów lub usług. Należy natychmiast zwrócić uwagę lub skorygować zachowania ryzykowne przy użyciu odpowiednich środków tj. zwiększona kontrola historii transakcji pośrednika i integralność danych, poznanie i ocena wyjaśnień pośrednika, niejawne wyrwykowe sprawdzanie zakwestionowanych aspektów usług pośrednika lub kontakt na miejscu lub "zza biurka" z pośrednikiem, co może skutkować dalszym szkoleniem lub nadzorem, zawieszeniem lub rozwiązaniem umowy z pośrednikiem.

## **Szkolenie i zwiększanie świadomości**

134. MSB powinny zapewnić pośrednikom odpowiednie szkolenia w zakresie prania pieniędzy i finansowania terroryzmu. Zobowiązanie MSB zakładające przeprowadzanie i utrzymywanie skutecznych kontroli polega zarówno na szkoleniu jak i zwiększaniu świadomości. Wymaga to wysiłku na skalę całego przedsiębiorstwa w celu przekazania wszystkim odpowiednim pracownikom i pośrednikom co najmniej ogólnych informacji dotyczących prawa, regulacji i polityki wewnętrznej dotyczących przeciwdziałaniu praniu pieniędzy i finansowania terroryzmu.

135. Zastosowanie podejścia opartego na ryzyku do różnych metod dostępnych dla szkolenia daje każdemu MSB dodatkową elastyczność dotyczącą częstotliwości, mechanizmów przeprowadzenia i kluczowych punktów szkolenia. Szkolenia pośredników powinny być dokumentowane a rejestry ze szkoleń powinny być przechowywane zgodnie z odpowiednimi wymogami dotyczącymi prowadzenia rejestru. MSB powinien dokonywać przeglądu swojej bazy pośredników i dostępnych środków i wdrażać programy szkoleniowe, które dostarczają odpowiednie informacje z zakresu prania pieniędzy i finansowania terroryzmu na właściwym poziomie uszczegółowienia.

136. Szkolenie pośredników może obejmować szkolenie wstępne na miejscu i "zza biurka" (tj. po aktywacji) i trwające szkolenie przez programy oparte na sieci, okresowe maile lub newslettery, strony internetowe chronione hasłem lub wyskakujące komunikaty w miejscu siedziby. W połączeniu lub jako dodatek do takiego szkolenia MSB może zapewnić okresowe programy kontroli zgodności związane z całościową oceną zgodności pośrednika z wewnętrznymi i zewnętrznymi wymogami regulacyjnymi w sprawie zapobiegania praniu pieniędzy.

## **Rozdział trzeci: Kontrole wewnętrzne**

137. Aby MSB posiadały skuteczne podejścia oparte na ryzyku, proces oparty na ryzyku musi być włączony do systemu kontroli wewnętrznej firmy. Kadra kierownicza wyższego szczebla jest odpowiedzialna za zapewnienie, że MSB utrzymuje skuteczną strukturę kontroli wewnętrznych w tym monitoring i zgłaszanie działalności podejrzanej. Silne przywództwo kierownictwa wyższego szczebla i zaangażowanie w zapobieganie praniu pieniędzy są ważnymi aspektami zastosowania podejścia opartego na ryzyku. Kierownictwo wyższego szczebla musi wprowadzić zasady zgodności zapewniając, że personel działa zgodnie z politykami, procedurami i procesami MSB mającymi na celu ograniczenie i kontrolę ryzyka.

138. Poza innego rodzaju kontrolą wewnętrzną zgodności, charakter i zakres kontroli przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu będzie zależał od różnych czynników w tym:

- Charakteru, skali i złożoności działalności MSB.
- Różnorodności operacji MSB w tym różnorodności geograficznej.
- Klienta, produktu i profilu działalności MSB.
- Użytych kanałów dystrybucji.
- Wartości i rozmiaru transakcji.
- Stopnia ryzyka związanego z każdym obszarem działania MSB.
- Integralności użytych systemów.
- Zakresu, w jakim MSB obsługuje bezpośrednio klientem lub obsługuje go przez pośredników, osoby trzecie lub w transakcji bez fizycznego udziału klienta.

139. Ramy kontroli wewnętrznej powinny:

- Skupiać się na działaniach MSB (produktach, usługach, klientach i lokalizacjach

geograficznych), które są bardziej podatne na nadużycia przez podmioty zaangażowane w pranie pieniędzy, osoby finansujące terrorystów i innych przestępców.

- Zapewniać regularną weryfikację oceny ryzyka i procesów zarządzania ryzykiem biorąc pod uwagę środowisko, w którym działa MSB i działalność na jego rynku.
- Wyznaczać osobę lub osoby na poziomie zarządu odpowiedzialne za zarządzanie zgodnością z programem zapobiegania praniu pieniędzy i finansowania terroryzmu.
- Zapewniać zgodność z programem zapobiegania praniu pieniędzy i finansowaniu terroryzmu i programu weryfikacji.
- Zapewniać, że adekwatne kontrole są przeprowadzane przed zaoferowaniem nowego produktu.
- Informować kadrę kierowniczą wyższego szczebla o inicjatywach związanych z zachowaniem zgodności, zidentyfikowanych niedociągnięciach w zgodności, podejmowanych działaniach naprawczych i polach zgłaszania działalności podejrzanej.
- Zapewniać ciągłość programu mimo zmian w zarządzie lub składzie pracowników lub struktury.
- Skupiać się na spełnieniu wszystkich wymogów regulacyjnych dotyczących prowadzenia rejestru i zgłaszania i zaleceń dotyczących zgodności z programem zapobiegania praniu pieniędzy i finansowaniu transakcji i zapewnienie terminowej aktualizacji w odpowiedzi na zmiany w regulacjach.
- Zapewniać adekwatne kontrole dla klientów wyższego ryzyka, transakcji i produktów, pośredników, o ile to konieczne, tj. kontrole limitów dla transakcji i zatwierdzenia kierownictwa.
- Umożliwiać terminową identyfikację transakcji podlegających zgłoszeniu i zapewniać dokładne przekazywanie wymaganych zgłoszeń.
- Zapewniać adekwatne zarządzanie i nadzór pośredników w tym wstępne szkolenie z zakresu poznaj swojego pośrednika, należytej staranności, zapobiegania praniu pieniędzy i finansowaniu terroryzmu i bieżący monitoring oparty na ryzyku.
- Zapewniać adekwatny nadzór pracowników, którzy obsługują transakcje, wypełniają zgłoszenie, udzielają zwolnień, monitorują działalność podejrzaną lub są zaangażowani w inną działalność, która stanowi część programu zapobiegania praniu pieniędzy i finansowaniu terroryzmu podmiotu gospodarczego.
- Stwarzać i wdrażać pisemne polityki, procedury i procesy dotyczące zapobiegania praniu pieniędzy i finansowaniu terroryzmu z okresową kontrolą wewnętrzną w celu zapewnienia przestrzegania przez personel obowiązków związanych z zapobieganiem praniu pieniędzy i finansowaniu terroryzmu.
- Zapewniać zgodność z programem zapobiegania praniu pieniędzy i finansowaniu terroryzmu do opisu zadań i przeprowadzenie ocen właściwego personelu.
- Zapewniać odpowiednie wstępne i ponowne szkolenie dla właściwego personelu.
- Zapewniać odpowiednie wstępne i ponowne szkolenie dla pośredników w odpowiednich odstępach czasu.

140. Kadra kierownicza wyższego szczebla będzie musiała posiadać środki niezależnego oceniania rozwoju i działania oceny ryzyka i procesów zarządzania i powiązanych kontroli wewnętrznych oraz pozyskiwania odpowiedniej pewności, że przyjęta metodologia oparta na ryzyku odzwierciedla profil ryzyka MSB. To niezależne badanie i zgłaszanie powinno być prowadzone przez np. departament audytu wewnętrznego, audytorów zewnętrznych, konsultantów specjalistów i inne wykwalifikowane osoby, które nie są zaangażowane we wdrożenie lub działanie zgodnie z programem zapobiegania praniu pieniędzy i finansowaniu terroryzmu. Badanie powinno być oparte na ryzyku (skupiając uwagę na klientach, lokalizacjach geograficznych, produktach i usługach, pośrednikach wyższego ryzyka);

powinno oceniać adekwatność ogólnego programu zapobiegania praniu pieniędzy i finansowaniu terroryzmu MSB; i jakości zarządzania ryzykiem dla działań MSB, departamentów i jednostek zależnych; powinno obejmować całościowe procedury i kontrole; i obejmować wszystkie działania.

## ZAŁĄCZNIK 1 ŹRÓDŁA DALSZYCH INFORMACJI

Istnieją różne źródła informacji, które mogą pomóc państwom i MSB w opracowywaniu podejścia opartego na ryzyku. Chociaż poniższa lista nie jest wyczerpująca, w poniższej części podany jest szereg użytecznych linków, z których państwa i MSB mogą skorzystać. Wskazują one dodatkowe źródła informacji, a dalszą pomoc w prowadzeniu ocen w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu można także uzyskać z innych źródeł informacji.

### A. Dokumenty FATF

Grupa Specjalna do spraw Przeciwdziałania Prania Pieniędzy (FATF) jest organem międzyrządowym, którego celem jest rozwój i promocja krajowych i międzynarodowych polityk zwalczania prania pieniędzy i finansowania terroryzmu. Kluczowe materiały obejmują 40 Zaleceń dotyczących prania pieniędzy i 9 Zaleceń Specjalnych dotyczących finansowania terroryzmu, Metodologia oceny przestrzegania Zaleceń FATF, Podręcznik dla krajów i oceniających, raporty o metodach i trendach (typologie) i raporty wzajemnej oceny.  
<http://www.fatf-gafi.org>

Raport z typologii FATF dot. alternatywnych dróg przekazu płatności (czerwiec 2005):  
<http://www.fatf-gafi.org/dataoecd/16/8/35003256.pdf>

### B. Akty prawne/wskazówki dot. podejścia opartego na ryzyku.

W niniejszej części zaprasza się delegacje do wskazania możliwych linków do stron związanych z aktami prawnymi/wskazówkami, które zostały stworzone odnośnie do podejścia opartego na ryzyku dla sektora MSB lub odnośnie do analizy oceny ryzyka.

**Australia:** <http://austrac.gov.au/courses.html>

**Belgia:** "Wskaźniki prania pieniędzy " wydane przez jednostkę wywiadu finansowego ([http://www.ctif-cfi.be/doc/en/typo\\_ctif\\_cfi/NL1175eENG.pdf](http://www.ctif-cfi.be/doc/en/typo_ctif_cfi/NL1175eENG.pdf)), i okólnik belgijskiego Urzędu Nadzoru (CBFA) w sprawie obowiązku zachowania należytej staranności wobec klienta i w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy i finansowania terroryzmu([http://www.cbfa.be/eng/wk/circ/wk\\_circ.asp](http://www.cbfa.be/eng/wk/circ/wk_circ.asp))

**Brazylia:** <http://www.bcb.gov.br/?RMCCIINORMS> (angielski) lub  
<http://www.bcb.gov.br/rex/rmcci/port/rmcci.asp> (portugalski)

**Kanada:** Wytyczne FINTRAC  
(<http://www.fintrac-canafe.gc.ca/publications/guide/Guide4/4-eng.asp#66>)

**Dania:** "Wskaźniki możliwego prania pieniędzy lub finansowania terroryzmu" wydane przez duńską jednostkę wywiadu finansowego  
(<http://www.dfsa.dk/sw41296.asp>)

**Norwegia:** Wskazówki do nowej ustawy o praniu pieniędzy i rozporządzenia w tym wskazówki dot. podejścia opartego na ryzyku:

([http://www.kredittilsynet.no/Global/Venstremeny/Rundskriv%20-%20vedlegg/23062009\\_Rundskriv\\_8\\_2009\\_Endelig.pdf](http://www.kredittilsynet.no/Global/Venstremeny/Rundskriv%20-%20vedlegg/23062009_Rundskriv_8_2009_Endelig.pdf)) (tylko norweski)

**Zjednoczone Królestwo:** Wskazówki wydane przez Urząd Skarbowy i Celny  
<http://www.hmrc.gov.uk/mlr/mlr8.pdf>

**Stany Zjednoczone:** W grudniu 2008, Sieć Ścigania Przepływów Finansowych (FinCEN) wydała podręcznik zawierający wskazówki dla urzędników kontrolujących firmy świadczące usługi pieniężne (MSB) pod względem zgodności z wymogami ustawy o tajemnicy bankowej (BSA). Poniżej znajduje się link do Podręcznika: [http://www.fincen.gov/news\\_room/rp/files/MSB\\_Exam\\_Manual.pdf](http://www.fincen.gov/news_room/rp/files/MSB_Exam_Manual.pdf)

Ogólne informacje o MSB są również dostępne przez stronę główną FinCEN; na stronie znajdują się odniesienia do wszystkich wskazówek dot. MSB i dodatkowe materiały edukacyjne dot. MSB.

[http://www.fincen.gov/financial\\_institutions/msb/](http://www.fincen.gov/financial_institutions/msb/).

### **C. Inne źródła informacji pomocnych instytucjom państwowym i finansowym w przeprowadzaniu oceny ryzyka kraju i działalności transgranicznej.**

Określając poziomy ryzyka związanego z konkretnym państwem lub działalnością transgraniczną, instytucje finansowe oraz rządy mogą korzystać z szeregu ogólnie dostępnych źródeł informacji, które obejmują raporty podające szczegóły przestrzegania międzynarodowych standardów i kodeksów, konkretne oceny ryzyka związane z nielegalną działalnością, badania dotyczące korupcji i poziomów współpracy międzynarodowej. Chociaż poniższa lista nie jest wyczerpująca, podaje ona często wykorzystywane źródła:

- Raporty Międzynarodowego Funduszu Walutowego i Banku Światowego o przestrzeganiu międzynarodowych standardów i kodeksów (Program Oceny Systemu Finansowego)

- Raporty Banku Światowego :

<http://www1.worldbank.org/finance/html/cntrynew2.html>,

- Międzynarodowy Fundusz Walutowy:

<http://www.imf.org/external/np/rosc/rosc.asp?sort=topic#RR>

- Oceny Centrów Finansowych Offshore (Offshore Financial Centres – OFCs) pracowników MFW:

[www.imf.org/external/np/ofca/ofca.asp](http://www.imf.org/external/np/ofca/ofca.asp).

- Raporty wzajemnej oceny wydawane przez ciała regionalne typu FATF:
  1. Azjatycka/Pacyficzna Grupa ds. Prania Pieniędzy (Asia/Pacific Group on Money Laundering – APG)

<http://www.apgml.org/documents/default.aspx?DocumentCategoryID=8>

2. Karaibska Finansowa Grupa Zadaniowa (Caribbean Financial Action Task Force – CFATF)

<http://www.cfatf.org/profiles/profiles.asp>

3. Specjalny Komitet Ekspertów ds. Oceny Środków Przeciwdziałania Praniu Pieniędzy (The Committee of Experts on the Evaluation of Anti-Money Laundering Measures) (MONEYVAL)

[http://www.coe.int/t/e/legal\\_affairs/legal\\_cooperation/combating\\_economic\\_crime/5\\_money\\_laundering/Evaluations/Reports\\_summaries\\_3.asp#TopOfPage](http://www.coe.int/t/e/legal_affairs/legal_cooperation/combating_economic_crime/5_money_laundering/Evaluations/Reports_summaries_3.asp#TopOfPage)

4. Grupa Euroazjatycka (Eurasian Group – EAG)

<http://www.eurasiangroup.org/index-7.htm>

5. Wschodnio- i Południowoafrykańska Grupa ds. Prania Pieniędzy (The Eastern and South African Anti Money Laundering Group – ESAAMLG)

<http://www.esaamlg.org/reports/me.php>

6. GAFISUD

<http://www.gafisud.org/actividades.asp>

7. Grupa międzyrządowa ds. prania pieniędzy w Afryce Zachodniej (GIABA)

<http://www.giaba.org/index.php?type=c&id=24&mod=2&men=1>

8. FATF Bliski Wschód i Afryka Północna (MENAFATF)

<http://www.menafatf.org/TopicList.asp?cType=train>

- Podgrupa OECD ds. Klasyfikacji Krajów Ryzyka (lista klasyfikacji krajów ryzyka publikowanych po każdym spotkaniu)

[http://www.oecd.org/document/49/0,2340,en\\_2649\\_34171\\_1901105\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/49/0,2340,en_2649_34171_1901105_1_1_1_1,00.html)

- Międzynarodowy Strategiczny Raport Kontrolny na temat Narkotyków (International Narcotics Control Strategy Report) (publikowany corocznie przez Departament Stanu USA)

<http://www.state.gov/p/inl/rls/nrcrpt/>

- Członkostwo w Grupie Egmont – Koalicji jednostek wywiadu finansowego, które uczestniczą w regularnej wymianie informacji oraz dzieleniu się dobrymi praktykami,

przyjęcie do Grupy Egmont oparte jest o formalną procedurę, jaką muszą przejść kraje, aby uznano, że spełniają definicję jednostki wywiadu finansowego Grupy Egmont.

<http://www.egmontgroup.org/>

- Sygnatariusz Konwencji Organizacji Narodów Zjednoczonych przeciw międzynarodowej przestępczości zorganizowanej

[http://www.unodc.org/unodc/crime\\_cicp\\_signatures\\_convention.html](http://www.unodc.org/unodc/crime_cicp_signatures_convention.html)

- Biuro ds. Kontroli Aktywów Zagranicznych (the Office of Foreign Assets Control – OFAC) Departamentu Skarbu USA, Programy sankcji gospodarczych i handlowych

<http://www.ustreas.gov/offices/enforcement/ofac/programs/index.shtml>

- Skonsolidowana lista osób, grup i podmiotów podlegających sankcjom finansowym UE

[http://ec.europa.eu/comm/external\\_relations/cfsp/sanctions/list/consol-list.htm](http://ec.europa.eu/comm/external_relations/cfsp/sanctions/list/consol-list.htm)

- Komitet ds. Sankcji Rady Bezpieczeństwa ONZ UN – Status kraju:

<http://www.un.org/sc/committees/>

- Transparency International – światowa organizacja cywilna walcząca z korupcją, łącząca ludzi w silną koalicję światową mającą na celu zakończenie szkodliwego wpływu korupcji na mężczyzn, kobiet i dzieci na całym świecie. Misją TI jest wprowadzenie zmian, aby świat był wolny od korupcji.

<http://www.transparency.org/>

## **ZAŁĄCZNIK 2 GLOSARIUSZ TERMINOLOGII**

### **Pośrednik**

Dla celów Specjalnej Rekomendacji VI pośrednik to osoba, która świadczy usługi przekazu środków pieniężnych lub wartości majątkowych w ramach prowadzenia lub w ramach kontraktu z prawnie zarejestrowaną lub posiadającą licencję osobą zajmującą się przekazem pieniężnym (np. licencjobiorca, franczyzobiorca, koncesjonariusz). (Definicja została sporządzona na podstawie Uwagi Interpretacyjnej do Specjalnej Rekomendacji VI. Jest używana w kryteriach w ramach SR VI ).

### **Przekaz seryjny**

Przekaz seryjny to przekaz, na który składa się wiele pojedynczych przekazów, które są wysyłane do tych samych instytucji finansowych, ale mogą/nie mogą być ostatecznie przeznaczone do różnych osób.

### **Rzeczywisty beneficjent**

Osoba (lub osoby) fizyczna, która jest rzeczywistym właścicielem, lub która sprawuje rzeczywistą kontrolę nad klientem i / lub osobą, w której imieniu przeprowadzana jest transakcja. Należą do nich także osoby sprawujące skuteczną kontrolę nad osobami prawnymi i jednostkami nieposiadającymi osobowości prawnej.

### **Uprawnione organy**

Uprawnione organy oznaczają wszystkie organy administracyjne i organy ścigania zajmujące się zwalczaniem prania pieniędzy i finansowania terroryzmu, włączając jednostki nadzoru finansowego i organy nadzorujące.

### **Zasady podstawowe**

Zasady podstawowe oznaczają zasady zawarte w następujących dokumentach: Zasady Podstawowe Efektywnego Nadzoru Bankowego” wydane przez Komitet Bazylejski ds. Nadzoru Bankowego, „Cele i zasady regulacji obrotu papierami wartościowymi” wydane przez Międzynarodową Organizację Komisji Papierów Wartościowych (IOSCO) oraz „Zasady nadzoru nad ubezpieczeniami” wydane przez Międzynarodowe Stowarzyszenie Nadzorów Ubezpieczeniowych”.

### **Przekaz transgraniczny**

Przekaz transgraniczny oznacza przekaz, w przypadku którego instytucje inicjatora i beneficjenta są zlokalizowane w różnych jurysdykcjach. Termin ten odnosi się również do łańcucha przekazów elektronicznych, który posiada przynajmniej jeden element transgraniczny.

### **Waluta**

Waluta odnosi się do banknotów i monet, które są w obrocie jako środek wymiany.

### **Wartość progowa**

Odnosi się do kwot określonych w „Uwagach interpretacyjnych” do Zaleceń FATF.

### **Przekaz krajowy**

Przekaz krajowy oznacza przekaz, w przypadku którego instytucje inicjatora i beneficjenta są zlokalizowane w tej samej jurysdykcji. Termin ten odnosi się zatem do łańcucha przekazów

elektronicznych, które odbywają się w całości w granicach jednej jurysdykcji, mimo że system użyty do przeprowadzenia przekazu może być zlokalizowany w innej jurysdykcji.

### **Zalecenia FATF**

Odnoszą się do 40 Zaleceń FATF oraz do 9 Specjalnych Rekomendacji FAFT w sprawie finansowania terroryzmu.

### **Instytucje finansowe**

Oznaczają osoby lub podmioty, których działalność wiąże się z podejmowaniem co najmniej jednego z wymienionych poniżej rodzajów działań w imieniu klienta:

1. Podejmowanie depozytów i innych środków pod tytułem zwrotnym od osób. [5]
2. Udzielanie kredytów. [6]
3. Leasing. [7]
4. Przekaz środków pieniężnych i wartości majątkowych. [8]
5. Emitowanie i zarządzanie środkami płatniczymi (np. karty kredytowe debetowe, czeki, czeki podróżne, przekazy bankowe, czeki bankierskie, pieniądź elektroniczny).
6. Gwarancje i zobowiązania finansowe.
7. Obrót na rynkach:
  - rynkowych instrumentów pieniężnych (czeki, weksle, certyfikaty depozytowe, instrumenty pochodne itp.).
  - wymiany walut obcych.
  - wymiany, stóp procentowych i instrumentów indeksowych.
  - zbywalnych papierów wartościowych.
  - kontraktów terminowych na dostawy towarów.
8. Udział w emisjach akcji oraz świadczenie usług finansowych związanych z taką emisją.
9. Indywidualne i zbiorowe zarządzanie portfelem.
10. Przechowywanie i dysponowanie gotówką lub płynnymi walorami w imieniu osób trzecich.
11. Inne sposoby inwestowania, dysponowania lub zarządzania funduszami lub środkami pieniężnymi w imieniu osób trzecich.
12. Poręczanie i zawieranie umów o ubezpieczenie na życie i innych umów ubezpieczeniowych związanych z inwestowaniem środków. [9]
13. Wymiana waluty krajowej i obcej.

Gdy dana operacja finansowa przeprowadzana jest przez osobę lub podmiot rzadko lub w bardzo ograniczonym zakresie (z punktu widzenia kryteriów ilościowych i obiektywnych) tak, że ryzyko uczestniczenia w praniu brudnych pieniędzy jest niewielkie, dane państwo może zdecydować o częściowym lub całkowitym uchyleniu obowiązku przestrzegania procedur wymierzonych przeciwko praniu brudnych pieniędzy.

W precyzyjnie określonych i uzasadnionych wypadkach, gdy istnieją dowody na małe ryzyko prania brudnych pieniędzy, dane państwo może zdecydować o niestosowaniu Czterdziestu Zaleceń w niektórych instytucjach finansowych, wymienionych powyżej.

### *Przypisy:*

5. *Dotyczy to również bankowości prywatnej.*
6. *Obejmuje to m.in. kredyt konsumencki; kredyt hipoteczny; factoring, z lub bez regresu; i finansowanie transakcji handlowych (w tym forfaiting).*
7. *Nie rozszerza się to na leasing finansowy w związku z produktami konsumenckimi.*
8. *Ma to zastosowanie do działalności finansowej zarówno w sektorze formalnym jak i nieformalnym np. alternatywne drogi przekazu płatności. Zob. Uwagę interpretacyjną do Specjalnej Rekomendacji VI. Nie ma to zastosowania do żadnej osoby fizycznej lub*

*prawnej, która dostarcza instytucjom finansowym wyłącznie wiadomości lub inne systemy wsparcia dla transmisji funduszy. Zob. Uwagę interpretacyjną dla Specjalnej Rekomendacji VII.*

9. *Ma to zastosowanie do przedsiębiorstw ubezpieczeniowych i pośredników ubezpieczeniowych (agentów i brokerów).*

### **Przekaz funduszy**

Termin przekaz funduszy odnosi się do każdej transakcji przeprowadzanej w imieniu inicjatora (osoby prawnej lub fizycznej) przez instytucję finansową drogą elektroniczną, mającej na celu udostępnienie kwoty pieniędzy beneficjentowi w innej instytucji finansowej. Inicjator i beneficjent mogą być tą samą osobą.

### **Porozumienie prawne**

Oznacza bezpośrednio ustanowione powiernictwo lub innego typu przedsięwzięcia. Przykładami innych podobnych jednostek (dla celów zapobiegania praniu pieniędzy i finansowaniu terroryzmu) są fidejucja, treuhand i fideicomiso.

### **Osoba prawna**

Odnosi się do osób prawnych, fundacji, zakładów, spółek, stowarzyszeń i innych tego typu organów, które mogą stać się stałym klientem instytucji finansowych lub posiadać majątek.

### **Inicjator**

Inicjator jest posiadaczem rachunku lub w przypadku gdy rachunek nie istnieje osobą (fizyczną lub prawną), która zleca instytucji finansowej wykonanie przekazu elektronicznego.

### **Osoba na eksponowanym stanowisku politycznym**

Osoby, które pełniły lub pełnią ważne funkcje publiczne w innych państwach, np. prezydent lub premier, emerytowani politycy, emerytowani wyżsi rangą urzędnicy administracji rządowej, wymiaru sprawiedliwości lub byli wysokiej rangi wojskowi, kierownictwo przedsiębiorstw państwowych, ważni przedstawiciele partii politycznych. Prowadzenie interesów z członkami rodziny lub osobami blisko związanymi z osobami na eksponowanych stanowiskach publicznych wiąże się z podobnym ryzykiem dla reputacji jak prowadzenie interesów bezpośrednio z tymi osobami. Definicja ta nie odnosi się do urzędników średniego i niższego szczebla.

### **Organy nadzorujące/regulacyjne**

Oznacza specjalnie wyznaczone uprawnione organy odpowiedzialne za zapewnienie przestrzegania przez instytucje finansowe wymogów mających na celu przeciwdziałanie praniu brudnych pieniędzy i finansowaniu terroryzmu.

### **Unikalny identyfikator**

Dla celów Specjalnej Rekomendacji VII unikalny identyfikator odnosi się do unikalnej kombinacji liter, cyfr lub symboli, które odnoszą się do konkretnego inicjatora.

### **Przekaz elektroniczny**

Dla celów Specjalnej Rekomendacji VII termin przekaz elektroniczny odnosi się do każdej transakcji przeprowadzanej w imieniu inicjatora (osoby prawnej lub fizycznej) przez instytucję finansową drogą elektroniczną, mającej na celu udostępnienie kwoty pieniędzy beneficjentowi w innej instytucji finansowej. Zleceniodawca i beneficjent mogą być tą samą osobą.

## **ZAŁĄCZNIK 3 CZŁONKOWIE ELEKTRONICZNEJ GRUPY DORADCZEJ**

Członkowie i obserwatorzy FATF

Argentyna, Belgia, Kanada, Francja, Portugalia, Hiszpania, UK, US, GIABA, MENAFATF, MONEYVAL, OGBS, NZ, Bank Światowy.

Sektor podmiotów świadczących usługi pieniężne (MSB)

### **Kanada**

Money Services Round Table  
Cash Money  
Custom House Ltd.  
Independent Financial Brokers  
Travelex Worldwide Money  
The Western Union Company

### **Niemcy**

GDV

### **Afryka Południowa**

Asisa  
Moneygram

### **USA**

Financial Service Centers of America (FiSCA)  
Howrey LLP  
Moneygram  
National Money Transmitters Association, Inc  
Optima Compliance & Consulting, Inc.  
The Western Union Company