



12 października 2010 r.

Poziom zastosowania: Wszystkie instytucje

Wytyczne dotyczące zarządzania ryzykiem operacyjnym w działalności związanej z rynkiem

1. Wprowadzenie

1. Zgodnie z Art. 22 dyrektywy 2006/48/WE (CRD), *“właściwe organy Państwa Członkowskiego pochodzenia wymagają, aby każda instytucja kredytowa posiadała solidne zasady zarządzania obejmujące jasną strukturę organizacyjną z dobrze określonymi, przejrzystymi i konsekwentnymi zakresami odpowiedzialności, skuteczne procesy mające na celu rozpoznawanie ryzyka, na które jest lub może być narażona instytucja kredytowa, zarządzanie nim, monitorowanie i sprawozdawczość związane z ryzykiem oraz odpowiednie mechanizmy kontroli wewnętrznej obejmujące prawidłowe procedury w zakresie administracji i rachunkowości. Powyższe zasady, procesy i mechanizmy powinny być kompleksowe i adekwatne co do charakteru, skali i złożoności działalności danej instytucji kredytowej.*
2. Tak jak w przypadku każdego rodzaju działalności, odpowiednie mechanizmy ładu korporacyjnego oraz systemów kontroli wewnętrznej są kluczowe dla zarządzania ryzykiem, zapobiegania zdarzeniom ryzyka operacyjnego w ramach działań związanych z rynkiem oraz łagodzenia ich wpływu na instytucje. Zdarzenia ryzyka operacyjnego w działalności związanej z rynkiem są często powiązane z transakcjami spekulacyjnymi, działaniami nieautoryzowanymi lub operacjami z wykorzystaniem dźwigni finansowej, złożonymi instrumentami, nowymi produktami, modelem ryzyka i szybkim wzrostem liczby operacji. Niektóre instytucje skupiły się głównie na ryzyku rynkowym i nie uznały w wystarczającym stopniu znaczenia odpowiedniego zarządzania ryzykiem operacyjnym.
3. Przypadki z przeszłości oraz niedawne wydarzenia pokazują, że gdy instytucje nie przestrzegają podstawowych zasad dobrego nadzoru wewnętrznego, nasilenie zdarzeń ryzyka operacyjnego w działalności związanej z rynkiem może być bardzo wysokie, co stwarza zagrożenie dla zarobków instytucji, istnienia danego obszaru działalności lub całej instytucji.
4. W tym kontekście, zasady ogólne dotyczące zarządzania wewnętrznego określone w Sekcji 2 „Wytyczne CEBS w sprawie zastosowania procesu nadzoru w ramach Filaru 2” (dokument CEBS wydany w styczniu 2006 r.), „Rozwiązania ogólne dotyczące zarządzania ryzykiem” (dokument CEBS

wydany w lutym 2010 r.) oraz „Zasady ogólne dotyczące polityki wynagrodzeń” (dokument CEBS wydany w kwietniu 2009 r.)¹ są podstawowym narzędziem odniesienia, które instytucje powinny rozważyć na poziomie ogólnym w zakresie zarządzania i kontroli ryzyka, uwzględniając zapobieganie i łagodzenie ryzyka operacyjnego w działalności związanej z rynkiem.

5. Celem niniejszego dokumentu jest uzupełnienie ram ogólnych wytycznych bardziej szczegółowymi zasadami oraz środkami wykonawczymi dotyczącymi identyfikacji, oceny, kontroli oraz monitorowania ryzyka operacyjnego w działalności związanej z rynkiem.
6. W szczególności dokument ten ma na celu podkreślenie oczekiwań nadzorczych w odniesieniu do szczególnych ustaleń, procedur, mechanizmów i systemów w obszarach handlowych, które mogą zapobiec lub ograniczyć występowanie zdarzeń ryzyka operacyjnego. Temat został opracowany z trzech różnych punktów widzenia, opisanych w następujących sekcjach – Mechanizmy zarządzania (Sekcja 2), Kontrole wewnętrzne (Sekcja 3) oraz Wewnętrzny system raportowania (Sekcja 4).
7. Ludzie, procesy, systemy oraz zdarzenia zewnętrzne są czynnikami ryzyka operacyjnego. Wysiłki zarządcze oraz działania mające na celu zapobieganie lub ograniczanie ryzyka operacyjnego w działalności związanej z rynkiem są skierowane do tych czynników, podczas gdy w tym samym czasie czynniki te są stosowane do zarządzania pozycją ryzyka rynkowego. Ze względu na te powiązania, niektóre zasady mogą być rozumiane jako skierowane na ryzyko rynkowe lub nawet zarządzanie ryzykiem kredytowym.
8. Jednakże, niniejszy dokument koncentruje się na zarządzaniu ryzykiem operacyjnym w działaniach związanych z rynkiem i nie skupia się na kwestiach dotyczących zarządzania innymi rodzajami ryzyka, które zazwyczaj charakteryzują tego rodzaju działalność². Wytyczne w sprawie zakresu ryzyka operacyjnego oraz strat z tytułu ryzyka operacyjnego (dokument CEBS opublikowany we wrześniu 2009r., oznaczony jako „Kompedium”³), zawierające szczegółowe wytyczne dotyczące granic pomiędzy ryzykiem operacyjnym a ryzykiem rynkowym, mogą przyczynić się do wyjaśnienia zagadnień ryzyka operacyjnego w działaniach związanych z rynkiem, w tym

¹ Wytyczne dotyczące procesu kontroli nadzorczej (GL03), Rozwiązania ogólne dotyczące zarządzania ryzykiem oraz Zasady ogólne dotyczące polityki wynagradzania można pobrać ze strony: <http://www.c-eps.org/getdoc/00ec6db3-bb41-467c-acb9-8e271f617675/GL03.aspx>, <http://www.c-eps.org/documents/Publications/Standards---Guidelines/2010/Risk-management/HighLevelprinciplesonriskmanagement.aspx> i <http://www.c-eps.org/getdoc/34beb2e0-bdff-4b8e-979a-5115a482a7ba/High-level-principles-for-remuneration-policies.aspx>

² Na przykład, podstawowe zasady zarządzania ryzykiem rynkowym wymagają od firm ustalenia odpowiednich limitów na ich pozycjach netto oraz ścisłego monitorowania, wykorzystywania oraz zgodności z tymi limitami. Elementy wewnętrznego zarządzania oraz potrzeby wynikające z tych zasad (np. definicja odpowiednich systemów monitoringu i kontroli ryzyka) wykraczają poza zakres tego dokumentu.

³ Wytyczne opublikowano w ramach „Kompedium” pod następującym linkiem: http://www.c-eps.org/getdoc/0448297d-3f85-4f7d-9fa6-c6ba5f80895a/CEBS-2009_161_rev1_Compedium.aspx

zakresu strat z tytułu ryzyka operacyjnego⁴, a zatem stanowią kontekst dla zakresu niniejszego dokumentu.

9. Ogólnie rzecz biorąc, instytucje muszą odpowiednio zarządzać wszystkimi rodzajami ryzyka. W rezultacie zarządzanie ryzykiem operacyjnym jest niekiedy podejmowane przez pracowników jednostek biznesowych, podczas gdy odpowiedzialność za wdrażanie odpowiednich ram zarządzania ryzykiem operacyjnym spoczywa na organie zarządczym lub na funkcjach kontroli i wsparcia (zob. pkt 12 poniżej), w szczególności w zakresie funkcji zarządzania ryzykiem operacyjnym.
10. Ponieważ niniejsze wytyczne odnoszą się do wszystkich instytucji, przy ich stosowaniu⁵ powinna być brana pod uwagę zasada proporcjonalności. Tym samym poziom złożoności mechanizmów ładu korporacyjnego, kontroli wewnętrznej i systemu raportowania w zakresie zarządzania ryzykiem operacyjnym w działalności związanej z rynkiem powinien być proporcjonalny do złożoności i skali tych działań w danej instytucji.
11. CEBS oczekuje od swoich członków wdrożenia wytycznych w sprawie zarządzania ryzykiem operacyjnym w działalności związanej z rynkiem do dnia 30 czerwca 2011 roku. CEBS jest świadom, że ich realizacja będzie obejmować nie tylko zmiany wytycznych krajowych, ale także procesów nadzorczych.

2. Mechanizmy zarządzania

Zasada 1. Organ zarządzający⁶ powinien być świadom ryzyka operacyjnego, rzeczywistego i potencjalnego, wpływającego na działalność związaną z rynkiem. Powinien rozwijać i utrzymywać struktury organizacyjne, kontrolę wewnętrzną oraz system raportowania odpowiednie do celów identyfikacji, oceny, kontroli oraz monitorowania ryzyka operacyjnego w działalności związanej z rynkiem.

12. Zgodnie z ustępem 602 CEBS GL10, organ zarządzający może, w razie potrzeby, ustanowić odpowiednie Komitety i przekazać im

⁴W odniesieniu do interakcji pomiędzy ryzykiem operacyjnym a innymi rodzajami ryzyka w ramach Filaru 1, dla instytucji stosujących zaawansowaną metodę pomiaru (AMA), CRD wskazuje granice pomiędzy ryzykiem operacyjnym a ryzykiem kredytowym oraz ryzykiem rynkowym, traktując te granice w odmienny sposób. Podczas gdy straty z tytułu ryzyka operacyjnego powiązane z kredytami są wyłączone z wymogu kapitałowego z tytułu ryzyka operacyjnego (o ile są traktowane jako straty z tytułu ryzyka kredytowego dla celów obliczania minimalnego kapitału regulacyjnego), wydarzenia na granicy ryzyka operacyjnego i ryzyka rynkowego są objęte zakresem ryzyka operacyjnego dla kalkulacji kapitału regulacyjnego.

⁵Zgodnie z zasadą proporcjonalności, wytyczne dla instytucji oraz organów nadzoru winny być stosowane w sposób proporcjonalny, aby odzwierciedlić charakter, skalę oraz złożoność działalności instytucji (zobacz Wytyczne CEBS w sprawie zastosowania procesu nadzoru w ramach Filaru 2).

⁶Termin „organ zarządzający”, który reprezentuje najwyższy poziom zarządzania instytucją, jest stosowany w niniejszym dokumencie w znaczeniu obejmującym różne struktury, takie jak systemy monistyczne i dualistyczne (patrz wyżej wspomniany dokument GL03).

pewne obszary w ramach zarządzania ryzykiem operacyjnym w działalności związanej z rynkiem. Komitety te powinny posiadać:

- zasoby materialne i ludzkie niezbędne do realizacji wymaganych zadań. W szczególności pracownicy „funkcji kontroli i wsparcia” (patrz ustęp 13 poniżej) powinni odgrywać zasadniczą rolę w tych Komitetach – ze względu na liczbę ich przedstawicieli lub ze względu na ich role w komitetach – tak aby być w stanie skutecznie kontrolować działania podejmowane przez jednostki organizacyjne mające bezpośredni kontakt z klientem;
 - szeroko zakrojony zakres kompetencji umożliwiający uwzględnienie wszystkich kwestii istotnych dla zapewnienia skuteczności zarządzania ryzykiem operacyjnym w działalności związanej z rynkiem. Zakres ten powinien obejmować badanie stosowanych w instytucji zasad odnoszących się do rekrutacji, zadań, norm etyki oraz odszkodowań – z uwzględnieniem premii;
 - dostęp do wyników systemów sprawozdawczych oraz kontroli wewnętrznej, w tym informacji przekazywanych do organów nadzoru; oraz
 - odpowiedzialność za wspieranie organu zarządzającego w swoich decyzjach dotyczących identyfikacji, oceny, kontroli oraz monitorowania ryzyka operacyjnego.
13. Struktura organizacyjna powinna zapewniać odpowiedni podział obowiązków pomiędzy obsługą klienta a funkcjami w zakresie wsparcia, weryfikacji oraz monitorowania transakcji (np. operacje, rozliczenia, wsparcie prawne, finanse, kontrola ryzyka, zgodność oraz audyt wewnętrzny i zewnętrzny, zwane dalej „funkcjami kontroli i wsparcia”). Instytucje powinny rozważyć, czy odpowiednie fizyczne rozdzielanie funkcji wsparcia wdrożenie zasad dotyczących podziału obowiązków (np. pracownicy obsługi klienta nie powinni posiadać fizycznego dostępu do zaplecza informatycznego, drukarek oraz dokumentacji w przypadku nieobecności pracowników obsługi zaplecza). Obowiązki powinny być przydzielane w odpowiedni sposób do funkcji kontroli i wsparcia oraz do poszczególnych osób. Należy upewnić się, że w zakresie obsługi transakcji handlowych działania mogące powodować konflikt interesów są podejmowane przez różne osoby.
14. Instytucje powinny starannie rozważyć w jaki sposób funkcje kontroli i wsparcia są zorganizowane w stosunku do obszarów, które kontrolują i weryfikują. Jeżeli funkcje kontroli i wsparcia są podzielone pomiędzy kilka jednostek, to należy je odpowiednio zrównoważyć, aby kontrola była skuteczna, przejrzysta i obejmowała wszystkie istotne działania. Instytucje powinny rozważyć następujące kwestie:
- integracja lub współpraca w zakresie funkcji kontroli i wsparcia, w szczególności obejmujące kontrolę finansów oraz kontrolę ryzyka, mogą zwiększyć poziom nadzoru oraz kontroli nad działalnością handlową i przyczynić się do stworzenia całościowego spojrzenia na takie działania;
 - zbliżenie funkcji kontroli i wsparcia do linii biznesowych może prowadzić do powstania wątpliwych praktyk (np. w obszarach procesu potwierdzania oraz depozytów zabezpieczających), które mogłyby być lepiej kontrolowane, gdyby zostały powierzone szerszej jednostce. Jednakże, w tym drugim przypadku należy przypisać i sformalizować odpowiedzialność w sposób zapewniający

uniknięcie luk w systemie kontroli. Przeprowadzane powinny być odpowiednie weryfikacje (np. w ramach audytu wewnętrznego) w celu zapewnienia, że różne funkcje kontroli i wsparcia obejmują wszystkie znaczące działania oraz że wdrożone zostały wydajne procesy; oraz

- prawidłowa organizacja głównych procesów po zakończeniu transakcji, zwłaszcza w obszarach zaplecza oraz księgowości, ma zasadnicze znaczenie dla wdrożenia odpowiednich kontroli.

Zasada 2. Organ zarządzający powinien promować, zwłaszcza w obszarze obsługi klienta, kulturę mającą na celu ograniczanie ryzyka operacyjnego w działalności związanej z rynkiem.

15. Wysokie standardy zawodowe oraz odpowiednia kultura ryzyka powinny być promowane w szczególności w obszarze obsługi klienta w sposób wspierający profesjonalne i odpowiedzialne zachowanie. Działanie takie powinno obejmować (ale nie ograniczać się do) opracowania i wdrożenia odpowiednich zasad oraz procedur ustalających standardy (często w formie „kodeksu postępowania”) w stosunkach pomiędzy handlowcami⁷ i ich kontrahentami oraz procedur szkoleniowych.
16. Odpowiednie polityki oraz procedury odnoszące się do świadczeń urlopowych oraz zmian kadrowych powinny być rozwijane, wdrażane i regularnie monitorowane. W szczególności:
 - polityka ustanawiająca wymagania dotyczące minimalnej nieobecności handlowców przez okres co najmniej dwóch kolejnych tygodni (wakacje, święta lub inne nieobecności w biurze lub przerwy w działalności handlowej, z uwzględnieniem zakazu korzystania z urządzeń mobilnych w celu uzyskania dostępu do systemów handlowych) jest dobrą praktyką, fizycznie uniemożliwiającą handlowcom oznaczanie lub wycenę wartości księgowych, poprzez przeniesienie odpowiedzialności w tym okresie na inne osoby; oraz
 - zapewniona powinna być odpowiednia kontrola w przypadku zmian stanowisk pomiędzy bezpośrednią obsługą klienta, obsługą administracyjną oraz zapleczem lub informatyką. Potencjalne zagrożenia wynikające ze zmiany stanowiska, zwłaszcza w ramach tej samej działalności lub linii produktowej, powinny być zrównoważone przez odpowiednie procedury kontrolne.

Zasada 3. Kierownictwo wyższego szczebla⁸ powinno zapewnić odpowiednie

⁷Termin „handlowiec” odnosi się również do innych pracowników zaangażowanych w obsługę klienta w działalności związanej z rynkiem, takich jak „osoby zajmujące się finansowaniem strukturyzowanym ” („structuring”) oraz „dealerzy”.

⁸Zgodnie z ustępem 413 Wytycznych w zakresie walidacji (<http://www.c-eps.org/getdoc/5b3ff026-4232-4644-b593-d652fa6ed1ec/GL10.aspx>) organ zarządzający reprezentuje ściśle kierownictwo danej instytucji, zaś kierownictwo najwyższego szczebla (które nie zostało zdefiniowane w CRD) należy rozumieć jako kadre kierowniczą podlegającą organowi zarządzającemu.

rozumienie, umiejętności, uprawnienia oraz motywację do sprawowania efektywnej kontroli działalności handlowej, zarówno przez jego członków, jak i pracowników funkcji kontroli i wsparcia.

17. Kierownictwo wyższego szczebla powinno nabywać, utrzymywać i pogłębiać wiedzę oraz umiejętności w celu wypełniania swoich obowiązków. Dotyczy to również posiadania dobrego zrozumienia potencjalnego i rzeczywistego ryzyka operacyjnego w ramach działalności związanej z rynkiem, w tym ekspozycji na ryzyko operacyjne wynikające z obsługi klienta, w procesach rozliczeniowych oraz z nowych produktów i procesów.
18. Aby wspierać efektywne wdrażanie procesów oraz procedur kontrolnych, pracownicy odpowiedzialni za funkcje kontroli i wsparcia powinni być odpowiednio wykwalifikowani. Dotyczy to właściwej polityki rekrutacyjnej oraz środków podejmowanych w celu utrzymania wykwalifikowanego personelu w zakresie funkcji kontrolnych, jak również zapewnienia odpowiednich szkoleń.
19. Należy rozważyć możliwość wprowadzenia mechanizmów motywacyjnych na poziomie funkcji kontroli i wsparcia, aby nagradzać należyte pełnienie tych funkcji. Pracownicy sprawujący funkcje kontrolne są niezależni w stosunku do nadzorowanych przez siebie jednostek, w związku z czym powinni być wynagradzani za osiągnięcie celów wynikających z pełnionych przez nich funkcji, bez względu na wyniki uzyskiwane przez kontrolowane przez nich obszary działalności.

Zasada 4. Ryzyko operacyjne powinno być brane pod uwagę przy ustalaniu celów dotyczących wydajności poszczególnych osób lub jednostek biznesowych w działalności związanej z rynkiem oraz przy ocenie dokonywanej w tym zakresie.

20. Instytucje powinny znaleźć właściwą równowagę między czynnikami rentowności i kulturą ryzyka operacyjnego lub tolerancją ryzyka na różnych szczeblach hierarchii, począwszy od obszaru obsługi klienta.
21. Na przykład, instytucje mogą ustalić cele dla menedżerów oraz handlowców lub jednostek biznesowych w zakresie maksymalnego dopuszczalnego poziomu ryzyka operacyjnego i/lub brać pod uwagę poziom ryzyka operacyjnego podczas przypisywania im wynagrodzenia zmiennego. Można tego dokonać poprzez uwzględnianie obserwowanego poziomu strat spowodowanych ryzykiem operacyjnym lub poprzez ustanowienie limitów ryzyka operacyjnego w oparciu o kluczowe wskaźniki ryzyka, karty wyników, poziomy ostrzegania itp. Cele i limity powinny być zgodne ze strategią ryzyka oraz całkowitym apetytem na ryzyko.

Zasada 5. Proaktywne zachowania przeciwdziałające działaniom uważanym za nadużycie⁹ lub podejrzanym zachowaniom w zakresie działalności związanej z rynkiem powinny być kluczowym elementem systemów kontroli wewnętrznej oraz

⁹W zakresie tych wytycznych „oszustwo” obejmuje oszustwo wewnętrzne i oszustwo zewnętrzne zdefiniowane w Dyrektywie 2006/48/WE, Załącznik X, Część V. Obejmuje straty spowodowane działaniem polegającym na celowej defraudacji, sprzeniewierzeniu majątku, obejściach regulacji, przepisów prawa lub przepisów wewnętrznych przedsiębiorstwa, wyłączając straty wynikające z różnorodności lub dyskryminacji pracowników, które dotyczą co najmniej jednej strony wewnętrznej (oszustwo wewnętrzne) oraz straty spowodowane celowym działaniem polegającym na defraudacji, sprzeniewierzeniu majątku lub obejściu regulacji prawnych przez stronę trzecią (oszustwo zewnętrzne).

raportowania.

22. Instytucje powinny analizować potencjalne źródła nadużyć i określić środki zwalczania nadużyć finansowych, z uwzględnieniem ekspozycji na nadużycia wynikające z ich działalności związanej z rynkiem. W zależności od wielkości i rodzaju ekspozycji na nadużycia w ramach działalności związanej z rynkiem, niektóre działania mogą być częścią codziennych procesów kontrolnych w obszarze rynku, podczas gdy inne mogą być wykonywane rzadziej, ale w każdym przypadku regularnie.
23. Poniższe przykłady wykrywania oraz zapobiegania nadużyciom oraz podejrzanym działaniom odnoszącym się do działalności związanej z rynkiem mogą odnosić się oraz znaleźć zastosowanie w przypadku każdej działalności biznesowej instytucji:
- stosowanie scenariuszy w celu zwiększenia zrozumienia w jaki sposób nadużycie może wystąpić na różnych poziomach organizacji oraz zdolności instytucji do wykrywania oraz zarządzania wewnętrznymi i zewnętrznymi przypadkami nadużycia;
 - regularny przegląd oraz analiza przypadków nadużyć, na przykład poprzez zastosowanie procesu zdobywania doświadczeń i wyciągania wniosków w ramach badania przypadków nadużyć (np. łamanie haseł, inne naruszenia bezpieczeństwa informatycznego, przekraczanie limitów) oraz wdrożenie środków zapobiegawczych w celu zmniejszenia prawdopodobieństwa ich ponownego wystąpienia;
 - ramy umożliwiające testowanie włamań do infrastruktury firmy, obejmujące niewłaściwe użycie haseł, profili użytkowników oraz tworzenie fikcyjnych dokumentów lub księgowanie fałszywych pozycji;
 - specjalny program identyfikacji ryzyka nadużyć oraz rozwoju mapowania ryzyka nadużyć, który może być częścią zintegrowanych ram zarządzania ryzykiem, spójnego z oceną ryzyka stosowaną w odniesieniu do ryzyka operacyjnego;
 - środki mające na celu zwiększenie świadomości pracowników w zakresie nadużyć;
 - odpowiednie zdefiniowanie praw dostępu oraz infrastruktura zapewniająca właściwy poziom ochrony przed nieuprawnioną ingerencją w dane wykorzystywane w procesach realizowanych po zakończeniu transakcji (na przykład poprzez fizyczne lub logiczne oddzielenie infrastruktury wykorzystywanej w procesach handlowych oraz procesach realizowanych po zakończeniu transakcji); oraz
 - ustalenie sytuacji powodujących konieczność dokonania przeglądu ekspozycji na ryzyko operacyjne, w tym zintegrowanych i skutecznych systemów powiadomień/ostrzegania umożliwiających kadrze zarządzającej identyfikację oraz reagowanie w odpowiednim czasie na wszelkie nielegalne lub podejrzanе działania. W szczególności mechanizmami tymi należy pokryć wrażliwe procesy, działania biznesowe i linie produktowe.
24. Powinien zostać wprowadzony proces eskalacji mający na celu informowanie odpowiedniego szczebla kierownictwa o zdarzeniach, które przekraczają wcześniej ustalone poziomy tolerancji na ryzyko lub posiadają określone cechy, w tym związane z faktycznymi nadużyciami lub podejrzanymi działaniami.

25. Organ nadzoru powinien być informowany o przypadkach nadużyć lub podejrzanych działaniach przekraczających określony próg lub posiadających pewne cechy (na przykład z wykorzystaniem szablonów sporządzonych ad hoc w związku z wymogiem organu nadzoru, lub wykorzystując szablony COREP tam, gdzie zostały wdrożone).

3. Kontrole wewnętrzne

Zasada 6. Handlowcy powinni inicjować transakcje wyłącznie wtedy, gdy są one zgodne z ich ustalonym zakresem obowiązków. Należy stosować minimalne normy dotyczące rozpoczynania oraz zamykania transakcji.

26. Istnienie odpowiednich zakresów obowiązków określających działalność każdego handlowca lub ich grupy jest warunkiem koniecznym dla prawidłowego zarządzania operacjami rynkowymi. Pozwala to każdej z zaangażowanych stron – handlowcom, menedżerom wszystkich szczebli oraz funkcjom kontroli i wsparcia – na weryfikację, czy charakter, wolumen oraz ogólna wielkość rozpatrywanych transakcji każdego handlowca lub grupy handlowców mieszczą się w limitach oraz strategii określonych przez zarząd instytucji.
27. Jednym z celów ram autoryzowanej działalności handlowej dla obsługi klienta powinno być sformalizowanie przepisów dla handlowców, umożliwiające ich funkcjonowanie w jasno określonych warunkach. Przykłady efektów prac w tym zakresie mogą obejmować wykaz dopuszczonych produktów, limitów na ryzyko rynkowe oraz szczegółowych obowiązków (np. wytyczne nadzoru dla kierowników). Należy wprowadzić odpowiedni proces eskalacji oraz kontroli na potrzeby badania naruszeń w zakresie dopuszczonych działań lub limitów.
28. Transakcje niezgodne z warunkami rynkowymi (np. transakcje zawarte z zawarte z refinansowaniem historycznymi kursami) powinny generalnie być ograniczone pod względem liczby oraz wartości nominalnej i stosować się do przepisów wewnętrznych regulujących rodzaj, skalę oraz strukturę transakcji, a także charakterystykę kontrahentów oraz komunikację z nimi. Odchylenia od warunków rynkowych powinny być wyraźnie widoczne w dokumentacji oraz zgłaszane do odpowiednich funkcji kontroli i wsparcia, a w razie potrzeby kierownictwu wyższego szczebla.
29. Zakres obowiązków oraz minimalne standardy dotyczące rozpoczynania i realizacji transakcji powinny podlegać ścisłemu monitorowaniu przez funkcje kontroli. W szczególności, niezwłocznie po zawarciu transakcji, do funkcji kontroli i wsparcia powinny zostać przekazane odpowiednie dane oraz dokumenty w celu umożliwienia ich odpowiedniej weryfikacji, potwierdzenia, rozliczenia oraz uzgodnienia.
30. Rozmowy handlowców związane z transakcjami powinny być nagrywane, a nagrania przechowywane przez odpowiedni okres czasu.

Zasada 7. Wymagania dotyczące dokumentacji działalności handlowej powinny być właściwie określone. Wątpliwości prawne powinny być ograniczone do minimum tak, aby kontrakty były egzekwowalne w możliwie najszerszym zakresie.

31. Instytucje powinny określić swoje wymagania dotyczące dokumentacji przed rozpoczęciem działań handlowych. W szczególności, jeżeli kontrahent wymaga specjalnych uzgodnień – na przykład dotyczących płatności strony trzeciej lub usług w pośrednictwie zleceń giełdowych – ustalenia te powinny zostać uzgodnione i udokumentowane z możliwie dużym wyprzedzeniem w stosunku do momentu rozpoczęcia transakcji.
32. W przypadku zawierania umowy ramowej z kontrahentem, w miarę możliwości należy zamieścić w niej prawnie egzekwowalne przepisy dotyczące potrąceń związanych z „kompensowaniem upadłościowym” („closeout netting”) oraz kompensacją zobowiązań.

Zasada 8. Zgodnie z ogólną zasadą transakcje powinny być inicjowane oraz zawierane w pomieszczeniach do tego przeznaczonych oraz w godzinach urzędowania.

33. Transakcje realizowane poza siedzibą przedsiębiorstwa (na przykład przy użyciu urządzeń mobilnych) powinny być dozwolone wyłącznie w ramach przepisów wewnętrznych określających uprawnione osoby, zakres dopuszczalnych transakcji oraz rejestrowanie transakcji. Zasady te powinny uwzględniać ryzyko operacyjne wynikające z prowadzenia transakcji poza siedzibą prowadzenia działalności. Transakcje takie powinny być identyfikowane oraz zgłaszane tak szybko jak to możliwe do oceny przez odpowiednie funkcje kontroli.
34. Transakcje zawierane po zakończeniu sesji (transakcje po zamknięciu) powinny zostać oznaczone i ujęte w pozycjach danego dnia (z uwzględnieniem późniejszych rozliczeń), jeżeli powodują one istotne zmiany. Dane dotyczące transakcji oraz dokumentacja związana z transakcjami po zamknięciu powinny być natychmiast zgłaszane do odpowiednich funkcji kontroli.

Zasada 9. Wszystkie istotne pozycje, przepływy pieniężne oraz kalkulacje związane z transakcją (np. pozycje portfela handlowego, zyski i straty oraz warunkowe przepływy pieniężne) powinny być wyraźnie odnotowane w systemie informatycznym instytucji z udokumentowaną ścieżką kontrolną.

35. Ścieżki kontrolne są istotne dla kontroli w instytucji po zakończeniu transakcji. Kontrole te powinny być przeprowadzane regularnie przez funkcje kontroli i wsparcia (np. menedżerów do spraw ryzyka operacyjnego, kontrole ryzyka, finanse, wewnętrznych i zewnętrznych audytorów). Są one również istotne dla uzgadniania transakcji. Ponadto, księgowanie transakcji i przepływów pieniężnych wymaga ścisłego monitorowania oraz kontroli wewnętrznej.
36. Ścieżki kontrolne powinny umożliwić identyfikację przepływów pieniężnych od źródła płatności do odbiorcy końcowego i odwrotnie, na dostatecznie szczegółowym poziomie (np. handlowcy, księgi rachunkowe, produkty oraz portfele).
37. Ścieżka kontrolna, w idealnej sytuacji, powinna rozpoczynać się od handlowca, który zainicjował transakcję i przechodzić całą drogę do kontrahenta, który otrzymał należność lub zapłacił za transakcję. Jednakże, zautomatyzowana ścieżka kontrolna „front-to-end” (odpowiadająca łatwo dostępnej ścieżce kontrolnej „push button”) może nie być wymagana, o ile ścieżka kontrolna wystarczająco dokumentuje dane wejściowe oraz zmiany danych dotyczących transakcji (w tym rozliczenia), pozycji,

wyceny oraz innych istotnych kwestii, a także umożliwia powstanie pełnej ścieżki kontrolnej

(uwzględniającej odpowiedzialnego menedżera lub handlowców), która może być tworzona na żądanie lub w dopuszczalnym terminie.

Zasada 10. Instytucje powinny zapewnić odpowiednie ramy kontroli nad stosunkami pomiędzy handlowcami a ich kontrahentami.

38. Instytucje powinny określić i wdrożyć odpowiednie mechanizmy kontroli oraz procedury od momentu nawiązania relacji do dalszych bieżących działań oraz monitorowania handlowców oraz powiązanych kontrahentów, jak również transakcji wewnętrznych¹⁰, uśpionych portfeli (tj. portfeli, które nie są już kontrolowane przez obsługę klienta) oraz nieaktywnych kontrahentów (oczekujących na przydział).
39. Powinny być również brane pod uwagę relacje i powiązania pomiędzy branżowymi klientami oraz uprawnionymi kontrahentami, a także obsługą klienta. Instytucje powinny monitorować te relacje (uwzględniając zgodność ze standardami oraz „kodeksem postępowania” <jak wspomniano w ustępie 15> np. kontrolując płatności ex-gratia <bez zobowiązań>, wszystkie inne znaczące płatności dokonane lub otrzymane poza zakresem ustaleń kontraktowych) oraz to, w jaki sposób zdarzenia ryzyka operacyjnego są traktowane przez obsługę klienta. W szczególności fakt, że relacja jest zarządzana przez obsługę klienta może oznaczać, że instytucje nie będą reagować z niezbędną starannością na przychodzące ostrzeżenia, na przykład pochodzące z zaplecza operacyjnego oraz administracyjnego kontrahentów. Kwestie dotyczące cen, zagadnień prawnych, handlowych oraz zapytania dotyczące rozliczeń, jak również błędy i roszczenia powinny być kierowane i rozpatrywane przez funkcje kontroli i wsparcia oraz wyznaczony zespół pracowników niezależnych od funkcji handlowych w ramach nadzoru nad funkcjami kontrolnymi.

Zasada 11. Procesy potwierdzania, rozliczania oraz uzgadniania powinny być odpowiednio zaprojektowane i należycie wykonywane.

40. W celu zapobieżenia występowaniu luk oraz słabych punktów, a także wspomoczenia identyfikacji i rozwiązywania naruszeń, zdefiniowane powinny być procesy potwierdzania, rozliczania oraz uzgadniania. Stosowność tych procesów powinna być regularnie oceniana.
41. Funkcje kontroli i wsparcia powinny pozostawać odpowiedzialne za procesy potwierdzania, rozliczania oraz uzgadniania. Podczas wykonywania stosownych działań kontrolnych funkcje te mogą wymagać dodatkowych informacji od obsługi klienta (np. w celu wyjaśnienia kwestii oraz uzyskiwania dodatkowych danych lub informacji).
42. Instytucje powinny posiadać rygorystyczny i niezawodny proces potwierdzania zasad i warunków transakcji z zewnętrznymi kontrahentami w odpowiednim

¹⁰Transakcje wewnętrzne odnoszą się zarówno do transakcji pomiędzy podmiotami prawnymi należącymi do tej samej grupy (transakcje międzyzakładowe), jak i pomiędzy księgami/działami tego samego podmiotu prawnego.

czasie i w jednoznaczny sposób¹¹, tak aby uniknąć nagromadzenia nierozliczonych transakcji, które stanowią główne źródło ryzyka. Mogą to być systemy automatycznego uzgadniania, o ile zapewniają ten sam poziom pewności.

43. W przypadkach, gdy tworzenie kompletnej dokumentacji oraz procesy potwierdzające są w toku, powinno zostać rozważane wykorzystanie procesów potwierdzających, w celu zapobieżenia wystąpieniu ryzyka operacyjnego – w szczególności ryzyka nadużyć finansowych – które potwierdzałyby istnienie transakcji (np. dodatkowe deklaracje telefoniczne pomiędzy funkcjami kontroli i wsparcia instytucji zaangażowanych w transakcję). Niepotwierdzone i niezatwierdzone transakcje powinny być zgłaszane w odpowiedni sposób.
44. Zgodnie z ogólną zasadą, potwierdzenia powinny być wymieniane z odpowiednimi funkcjami kontroli i/lub wsparcia kontrahentów oraz powinny być dopasowane do wszystkich transakcji rynkowych, uwzględniając te, które będą kompensowane oraz które zostaną przeprowadzone za pośrednictwem porad stron trzecich, takich jak rejestry Reuter's, dowody transakcji EBS oraz porady głosowe brokerów. Odejście od tej zasady powinno być możliwe tylko w wyjątkowych sytuacjach (np. w przypadku pewnych kontrahentów lub szczególnych transakcji), które powinny w każdym przypadku zostać jasno określone, w pełni udokumentowane, zgłoszone oraz odpowiednio ocenione przez funkcje kontroli.
45. W celu skutecznego ograniczenia ryzyka operacyjnego związanego z rozliczaniem transakcji, zdefiniowane oraz stosowane powinny być odpowiednie procesy i procedury w tym zakresie. Instytucje mogą między innymi rozważyć następujące elementy, które mogą znaleźć zastosowanie:
 - autoryzacja danych wejściowych przez obsługę zaplecza;
 - płatności/rozliczenia prowadzone w zamian za niezależne dokumenty;
 - uzgodnienie między systemami obsługi klienta oraz zaplecza; oraz
 - procedury uzgadniania niezależne od funkcji przetwarzania.
46. Kontrole powinny obejmować codzienne rozliczanie pozycji i znanych przepływów pieniężnych w ramach systemów własnych (obsługa klienta, ryzyko, rozliczenia oraz księgi główne) oraz z podmiotami zewnętrznymi. Uzgodnienia te powinny obejmować wszystkie zdarzenia związane z transakcjami, w tym zmiany, anulacje, wykonania, reset oraz wygaśnięcia.
47. Transakcje wewnętrzne (patrz przypis 10) powinny być uzależnione od warunków i kontroli, tworząc ten sam poziom pewności, który obowiązuje w odniesieniu do transakcji z kontrahentami zewnętrznymi. W szczególności, gdy nie podlegają depozytowi gwarancyjnemu lub rozliczeniom fizycznym, obie strony transakcji powinny być uzgadniane codziennie w oparciu o ich kluczowe cechy.
48. W przypadku transakcji pozagiełdowych (OTC) szczególną uwagę należy zwrócić na następujące kwestie:

¹¹Można to osiągnąć na przykład odwołując się do standardowych formularzy potwierdzeń lub poprzez elektroniczne dopasowywanie potwierdzeń.

- korzystanie z kontraktów, które są możliwie najbardziej standardowe, na przykład stosowanie szablonów kontraktów opracowanych przez stowarzyszenia branżowe;
- dostępność dedykowanego procesu wewnątrz każdej instytucji, który powodowałby interwencję odpowiedniej jednostki spoza obsługi klienta w przypadku, gdy zapisy kontraktowe różniłyby się od zapisów w szablonach lub jeżeli stosowane byłyby niezmienione szablony kontraktów w przypadku transakcji indywidualnych.
- przydzielenie odpowiedniego personelu do sprawdzenia, czy kontrakty są zgodne z pierwotnie uzgodnionymi warunkami, a także czy warunki te zostały spisane oraz zatwierdzone. Wszelkie zmiany, anulacje lub reakcje ze strony kontrahentów powinny prowadzić do odpowiednich procesów weryfikacji. Dotyczy to w szczególności nowacji, które wymagają ingerencji stron trzecich niebędących stronami pierwotnego kontraktu;
- bezpieczne przechowywanie dokumentacji (np. poprzez wykorzystanie repozytorium zdolnego do przechowywania kopii każdego kontraktu, w celu umożliwienia stwierdzenia jego autentyczności w przypadku postępowania sądowego);
- częsta weryfikacja liczby oraz czasu trwania nieudanych, modyfikowanych oraz anulowanych transakcji, a także ustanowienie procesu mającego na celu zapewnienie, że transakcje zostały potwierdzone w odpowiednim terminie. Szczególną uwagę należy zwrócić na niektóre niepotwierdzone transakcje pozagiełdowe, które charakteryzują się większym ryzykiem (takie jak transakcje pozagiełdowe nieuwzględniające w najbliższym czasie przepływów pieniężnych z kontrahentami, z którymi nie uzgodniono zabezpieczeń);
- dostosowane do działalności instytucji raportowanie wykazu transakcji, w których rozliczenia nie doszły do skutku, wraz z systemem ostrzegania powiadamiającym odpowiednie funkcje kontroli i wsparcia o osobach bezpośrednio zaangażowanych w przebieg transakcji; oraz
- raportowanie do odpowiednich funkcji kontroli wszelkich odchyień od normy oraz zdarzeń związanych z wystąpieniem ryzyka operacyjnego w ramach transakcji pozagiełdowych, powstałych wewnątrz instytucji lub wynikających z działań stron zewnętrznych/zewnętrznych dostawców usług.

Zasada 12. Instytucje powinny zapewnić, że ich procesy związane z depozytami gwarancyjnymi działają poprawnie oraz że wszelkie zmiany są uzgadniane z odpowiednimi pozycjami w ich księgach.

49. W przypadku dużych pozycji wymagane są duże depozyty lub zabezpieczenia. W związku z tym, instytucje powinny uzgadniać depozyt oraz zabezpieczenia w taki sposób, aby zapewnić odpowiednie depozyty zabezpieczające, a także prawidłowe zapisy w księgach. Instytucje powinny wdrożyć odpowiednie mechanizmy kontroli, w tym procedury alarmowe, w celu zapewnienia, że zabezpieczenie oraz zabezpieczone ryzyka kontrahenta zostaną prawidłowo wykonane. W przypadku zidentyfikowania odchyień od normy, instytucje powinny mieć możliwość śledzenia danej kwestii do poziomu transakcji oraz handlowca.
50. O ile to możliwe, instytucje powinny posiadać systemy kredytowe czasu rzeczywistego zdolne do obliczania linii kredytowych oraz informacji o ich wykorzystaniu po rozpoczęciu transakcji.

Instytucje muszą być zdolne do dokonania globalnej agregacji ekspozycji wszystkich stanowisk handlowych oraz dokładnego odzwierciedlenia efektu kompensowanych transakcji.

51. W obrocie instrumentami pochodnymi, istotne zmiany na pozycjach są zazwyczaj wykonywane poprzez produkty notowane lub zabezpieczone kontrakty pozagiełdowe OTC. Wszelkie istotne rozbieżności między kwotami i/lub kierunkiem wyceny rynkowej a depozytami zabezpieczającymi („collateral calls”) transakcji pozagiełdowych mogą być zatem oznaką niewłaściwego zarządzania lub utrzymywania portfela handlowego. Konieczna jest ścisła współpraca pomiędzy funkcją kontroli (odpowiedzialną za rachunek zysków i strat oraz niezależną weryfikację cen) a funkcją zarządzania zabezpieczeniami.

Zasada 13. Źródła ryzyka operacyjnego w działalności związanej z rynkiem powinny być właściwie identyfikowane i monitorowane na odpowiednim poziomie dogłębności, intensywności i terminowości.

52. Instytucje powinny rozumieć, jakie aspekty prowadzą do rachunku zysków i strat generowanego w obszarze handlu. Rachunek zysków i strat powinien być wiarygodny w kontekście upoważnienia do obrotu oraz rozwoju rynku. Główne wpisy w ramach rachunku zysków i strat, co do których zasadne są wątpliwości w zakresie ich wiarygodności, powinny być dalej analizowane w celu sprawdzenia, czy są one spowodowane przez zdarzenia związane z wystąpieniem ryzyka operacyjnego. W szczególności monitorowanie anomalii – takich jak anulacje, zmiany, transakcje zawierane po zakończeniu sesji lub pozagiełdowe – powinno zostać włączone do dziennych oraz miesięcznych procesów analizy rachunku zysków i strat. Istotne zmiany w handlu powinny być oficjalnie zgłaszane do funkcji obrotu i/lub funkcji kontroli ryzyka. Przypisania w zakresie rachunku zysków i strat („attribution”) są kluczem do zrozumienia ryzyka występującego w działalności handlowej, zwłaszcza w przypadku handlu złożonymi produktami oraz ryzykiem bazowym („basis risk”). Ponadto, instytucje powinny zapewnić, że wszelkie duże pozycje oraz wartości w rachunku zysków i strat są odpowiednio analizowane od pierwszego dnia, z uwzględnieniem tych, które zostały anulowane lub zmienione.
53. Transakcje nietypowe i wyjątkowe, nieprawidłowości w procesach potwierdzania oraz uzgadniania, błędy w zapisie, przetwarzaniu oraz rozliczaniu transakcji, wraz z anulacjami, zmianami, transakcjami zawieranymi po zakończeniu sesji oraz stopami pozarynkowymi powinny być monitorowane na odpowiednim poziomie szczegółowości przez właściwe funkcje kontroli i wsparcia oraz zgłaszane na odpowiednich szczeblach hierarchii. Procedury monitorowania i ich skuteczność powinny być okresowo weryfikowane.
54. Korzystanie z kont technicznych (np. rachunków przejściowych) powinno być przeanalizowane i zrozumiałe dla obsługi administracyjnej i zaplecza oraz kwestionowane w przypadku nieprawidłowego wykorzystania przez obsługę klienta. Podejrzane działania na tych kontach powinny być eskalowane i rozpatrywane przez kierownictwo wyższego szczebla.
55. Ponadto instytucje powinny dokonywać przeglądu kont wrażliwych (np. kont nierozliczonych) i wdrożyć odpowiednie kontrole w celu zapewnienia, że ich obsługa jest prawidłowa. Instytucje powinny określić odpowiednią częstotliwość monitorowania działalności związanej z rynkiem, w zależności od przedmiotu kontroli (np. handlowcy lub grupy handlowców, księgi, produkty, portfele oraz procesy) oraz profilu ich ryzyka.

56. Aby kontrole miały charakter odstraszający oraz umożliwiały szybkie podjęcie działań naprawczych, w każdym przypadku monitoring powinien być przeprowadzany z częstotliwością konieczną do wykrycia niewłaściwych działań lub nietypowych zachowań w jak najkrótszym czasie. Wprowadzenie jedynie miesięcznych kontroli ksiąg handlowych (np. alokacja kosztów finansowania, wewnętrzne oraz międzyzakładowe uzgodnienia transakcji, kontrola kont przejściowych oraz raportowanie) może prowadzić do nieuzasadnionej zwłoki w wykrywaniu nieprawidłowości.

Zasada 14. Wartość nominalna transakcji/pozycji powinna pozostawać pod ścisłą kontrolą, mającą na celu monitorowanie ryzyka operacyjnego oraz kontrahenta poprzez określenie istotnych ograniczeń i/lub uczestnictwo w inicjatywach na rzecz nowacji kontraktów.

57. Tradycyjna kontrola ryzyka rynkowego pozycji/transakcji netto (np. limity kwot netto ustalane na handlowców, księgi, produkty oraz poziomy portfeli) powinny w razie potrzeby być uzupełniane kontrolą wartości nominalnej transakcji/pozycji, ponieważ wartości netto nie zawsze identyfikują ryzyko operacyjne lub ryzyko kontrahenta leżące u podstaw tych transakcji/pozycji. Tego typu kontrole mogą obejmować procedury ostrzegania, nadzór nad transakcjami o wysokim wolumenie lub nietypowymi operacjami handlowymi oraz kontrole oparte na wolumenach lub limitach. Odstępstwa od tej zasady powinny być możliwe tylko w wyjątkowych sytuacjach, które powinny w każdym przypadku zostać jasno określone, w pełni udokumentowane oraz odpowiednio ocenione przez funkcje kontroli.
58. Niezależnie od charakteru transakcji (tj. wewnętrznej lub zewnętrznej), limity na łączną wartość nominalną transakcji/pozycji na wymaganym poziomie szczegółowości (np. handlowcy, księgi handlowe, produkty i portfele) powinny być odpowiednio ustalone, aktualizowane w odpowiednim czasie i okresowo weryfikowane. Funkcje kontroli i wsparcia powinny monitorować przestrzeganie limitów przez obsługę klienta.
59. W niektórych systemach prawnych, udział w programach dla nowacji lub zrywania kontraktów może być przydatny w zmniejszaniu pozycji nominalnej, a także ekspozycji instytucji na ryzyko kontrahenta i operacyjne bez istotnej zmiany jej pozycji w odniesieniu do ryzyka rynkowego.

Zasada 15. Systemy informatyczne w obszarach handlowych powinny być odpowiednio zaprojektowane, wdrożone i utrzymywane, w celu zapewnienia wysokiego poziomu ochrony w działaniach związanych z rynkiem¹².

60. Ogólnie rzecz biorąc, dostęp do zasobów informacyjnych powinien być kontrolowany przez procedurę oficjalnie zatwierdzoną przez kierownictwo wyższego szczebla. Procedura ta powinna obejmować okresowe przeglądy wymagań dotyczących dostępu i powinna być aktualizowana tak często, jak jest to niezbędne w związku z postępem

¹²Zarządzania ryzykiem operacyjnym w kontekście systemów informatycznych jest obszarem, który może być częścią przyszłych prac CEBS.

w technologiach systemów informatycznych stosowanych przez instytucję. Przestrzeganie tych zasad powinno zapewnić, że przyznany dostęp jest zgodny z wyznaczonymi funkcjami, a także uniemożliwić dostęp do systemów informatycznych w nielegalnych celach.

61. Poziom bezpieczeństwa tych systemów powinien być systematycznie testowany i monitorowany w celu zapobiegania nieupoważnionemu dostępowi.

4. Wewnętrzny system raportowania¹³

Zasada 16. System sprawozdawczości ryzyka operacyjnego dla działań związanych z rynkiem powinien być zaprojektowany tak, aby generować odpowiednie ostrzeżenia oraz informować kadrę zarządzającą w przypadku wykrycia podejrzanych operacji lub istotnych zdarzeń.

62. Systemy zarządzania ryzykiem operacyjnym powinny określać kryteria, wskaźniki i progi umożliwiające identyfikację istotnych zdarzeń wykrytych przez wewnętrzne procedury kontroli. Elementy te powinny być dostosowane do działalności instytucji i powinny obejmować potencjalne straty, nawet przed ich materializacją. Istotne zdarzenia powinny być zgłaszane bezzwłocznie kadrze zarządzającej. Warunkiem umożliwiającym powyższe jest śledzenie przez instytucje istotnych strat wynikających z ryzyka operacyjnego w działaniach związanych z rynkiem oraz analizowanie tych strat w odniesieniu do możliwych powiązań (tj. strat wywołane przez jedno zdarzenie lub przyczynę źródłową).
63. Zgłaszanie nieprawidłowości i monitorowanie ostrzeżeń mogą pomóc w wykrywaniu nieprawidłowych wzorców handlowych oraz w prowadzeniu dochodzeń dotyczących zdarzeń wykrytych przez system kontroli wewnętrznej. Powinno to obejmować również eskalację ostrzeżeń i obaw wyrażanych przez giełdę, brokerów, agentów i opiekunów oraz procedury zapewniające, że wszystkie pytania od podmiotów zewnętrznych są dokładnie zbadane.

Zasada 17. Instytucje powinny zapewnić jakość oraz spójność wewnętrznych raportów, a także ich adekwatność do potrzeb odbiorców, dla których są przeznaczone.

64. Na różnych szczeblach zarządzania i/lub kontroli występują potrzeby informacyjne, które różnią się zarówno w aspekcie treści, jak i częstotliwości. Jednostki biznesowe powinny tworzyć dokumenty służące zaspokojeniu ich własnych potrzeb zarządczych oraz kontrolnych, jak również na potrzeby sprawozdawczości dla innych jednostek. Dokumenty te mogą być zestandaryzowane lub mogą odpowiadać na specyficzne potrzeby, które zmieniają się z upływem czasu. Dostarczone informacje muszą być wystarczające do tego, aby służyć zgodnie z przeznaczeniem.
65. Instytucje powinny zapewnić wystarczającą jakość i odpowiednie wyjaśnienia w wewnętrznych raportach przesyłanych na różnych szczeblach

¹³Niniejszy rozdział, dotyczący działalności związanej z rynkiem, obowiązuje w odniesieniu do wszystkich innych obszarów działalności firmy.

hierarchii, aby uczynić je kluczowym elementem solidnego systemu kontroli wewnętrznej. Na przykład raporty, których celem jest wykrycie ryzyka operacyjnego w działalności związanej z rynkiem powinny być tworzone pod nadzorem funkcji kontrolnych. Jeżeli raport jest tworzony poza nadzorem funkcji kontrolnych, powinny one określać jego format i zawartość oraz zapewniać odpowiednią kontrolę nad przestrzeganiem wymogów dotyczących sprawozdawczości. Ponadto, raporty te powinny korzystać w możliwie najszerszym zakresie z alternatywnych danych wejściowych oraz źródeł przyjętych przez obsługę klienta w zakresie rozpoczęcia oraz zakończenia transakcji.

66. Istotne jest, aby informacje przepływające pomiędzy różnymi działami były – zwłaszcza w złożonych organizacjach – dobrze ustrukturyzowane, w celu uniknięcia opóźnień lub zmian w trakcie przekazywania istotnych informacji, które mogą być spowodowane filtrowaniem ich przez szczeble pośrednie.
67. Raporty powinny być zrozumiałe i powinny zawierać wyraźnie określone oraz właściwe działania naprawcze, które mają zostać wdrożone na wszystkich szczeblach organizacji. Wdrożenie działań naprawczych powinno być śledzone w odpowiedni sposób. Działania naprawcze, jak również efektywność ram sprawozdawczych, powinny znajdować się w zakresie audytów wewnętrznych.