EBA/GL/2024/14

14 listopada 2024 r.

Wytyczne

w sprawie wewnętrznych polityk, procedur i mechanizmów kontroli mających na celu zapewnienie wdrożenia unijnych i krajowych środków ograniczających

1. Zgodność i obowiązki sprawozdawcze

Status niniejszych wytycznych

1. Niniejszy dokument zawiera wytyczne wydane na podstawie art. 16 rozporządzenia (UE) nr 1093/2010[1]. Zgodnie z art. 16 ust. 3 rozporządzenia (UE) nr 1093/2010 właściwe organy i instytucje finansowe muszą dołożyć wszelkich starań, aby zastosować się do niniejszych wytycznych.

2. W wytycznych przedstawiono stanowisko EUNB w sprawie odpowiednich praktyk nadzoru w ramach Europejskiego Systemu Nadzoru Finansowego lub tego, jak należy stosować prawo Unii w konkretnym obszarze. Właściwe organy w rozumieniu art. 4 ust. 2 rozporządzenia (UE) nr 1093/2010, do których wytyczne mają zastosowanie, powinny stosować się do wytycznych poprzez odpowiednie włączenie ich do swoich praktyk (np. poprzez zmianę swoich ram prawnych lub procesów nadzorczych), również gdy wytyczne są skierowane przede wszystkim do instytucji.

Wymogi w zakresie sprawozdawczości

3. Zgodnie z art. 16 ust. 3 rozporządzenia (UE) nr 1093/2010 właściwe organy muszą do dnia 11.04.2025 r. powiadomić EUNB, czy stosują się lub zamierzają zastosować się do niniejszych wytycznych, albo podać powody niestosowania się do nich. W przypadku braku powiadomienia w tym terminie EUNB uzna, że właściwe organy nie stosują się do niniejszych wytycznych. Powiadomienia należy przekazać poprzez wysłanie formularza dostępnego na stronie internetowej EUNB z dopiskiem „EBA/GL/2024/14”. Powiadomienia powinny przekazać osoby odpowiednio upoważnione do przekazywania informacji o stosowaniu się do wytycznych w imieniu właściwych organów. EUNB należy również zgłaszać wszelkie zmiany dotyczące stosowania się do wytycznych.

4. Zgodnie z art. 16 ust. 3 powiadomienia zostaną opublikowane na stronie internetowej EUNB.

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1093/2010 z dnia 24 listopada 2010 r. w sprawie ustanowienia Europejskiego Urzędu Nadzoru (Europejskiego Urzędu Nadzoru Bankowego), zmiany decyzji nr 716/2009/WE oraz uchylenia decyzji Komisji 2009/78/WE (Dz.U. L 331 z 15.12.2010, s. 12).

2. Przedmiot, zakres stosowania i definicje

Przedmiot i zakres stosowania

5. Niniejsze wytyczne określają wewnętrzne polityki, procedury i mechanizmy kontroli, które instytucje finansowe podlegające regulacji i nadzorowi zgodnie z dyrektywą 2013/36/UE, dyrektywą (UE) 2015/2366 i dyrektywą 2009/110/WE powinny wprowadzić zgodnie z art. 74 ust. 1 dyrektywy 2013/36/UE, art. 11 ust. 4 dyrektywy (UE) 2015/2366 i art. 3 ust. 1 dyrektywy 2009/110/WE w celu zapewnienia skutecznego wdrożenia unijnych i krajowych środków ograniczających.

Adresaci

6. Niniejsze wytyczne skierowane są do:

   (i) właściwych organów określonych w aktach prawnych, o których mowa w art. 4 pkt 2 ppkt (i) rozporządzenia (UE) nr 1093/2010;

   (ii) właściwych organów określonych w art. 4 pkt 2 ppkt (vi) rozporządzenia (UE) nr 1093/2010 w odniesieniu do dyrektywy (UE) 2015/2366 i dyrektywy 2009/110/WE;

   (iii) instytucji finansowych, które podlegają regulacji i nadzorowi zgodnie z dyrektywą 2013/36/UE, dyrektywą (UE) 2015/2366 i dyrektywą 2009/110/WE.

7. Właściwe organy, które są odpowiedzialne za ocenę wewnętrznych polityk, procedur i mechanizmów kontroli przyjętych przez instytucje finansowe w celu zapewnienia wdrożenia unijnych i krajowych środków ograniczających, zgodnie z krajowymi ramami prawnymi, mogą odnieść się do niniejszych wytycznych podczas oceny takich wewnętrznych polityk, procedur i mechanizmów kontroli.

Definicja

O ile nie określono inaczej, pojęcia stosowane i zdefiniowane w dyrektywie 2013/36/UE, dyrektywie (UE) 2015/2366 i dyrektywie 2009/110/UE mają w niniejszych wytycznych takie samo znaczenie. Ponadto do celów niniejszych wytycznych stosuje się następującą definicję:

Środki ograniczające	oznaczają unijne środki ograniczające zdefiniowane w art. 2 pkt 1 dyrektywy (UE) 2024/1226 oraz krajowe środki ograniczające przyjęte przez państwa członkowskie zgodnie z ich krajowym porządkiem prawnym (w zakresie, w jakim mają one zastosowanie do instytucji finansowych).

3. Wykonanie

Data rozpoczęcia stosowania

8. Niniejsze wytyczne stosuje się od dnia 30 grudnia 2025 r.

4. Wytyczne w sprawie wewnętrznych polityk, procedur i mechanizmów kontroli mających na celu zapewnienie wdrożenia unijnych i krajowych środków ograniczających

Przepisy ogólne

1. Instytucje finansowe powinny określić i ocenić, które obszary ich działalności są szczególnie podatne lub narażone na naruszenie i obchodzenie środków ograniczających. Na tej podstawie powinny wprowadzić, wdrożyć i utrzymywać aktualne polityki, procedury i mechanizmy kontroli, aby zapewnić skuteczne stosowanie systemów środków ograniczających.

2. Te polityki, procedury i mechanizmy kontroli powinny być skuteczne i proporcjonalne do wielkości, charakteru i złożoności instytucji finansowej, a także do stopnia narażenia na naruszenie środków ograniczających.

4.1 Ramy zarządzania i rola organu zarządzającego

3. Instytucje finansowe powinny wprowadzić ramy zarządzania w celu zapewnienia, aby polityki, procedury i mechanizmy kontroli służące wdrażaniu środków ograniczających były adekwatne i skutecznie wdrażane.

4. Organ zarządzający instytucji finansowej powinien być odpowiedzialny za zatwierdzanie strategii instytucji finansowej w zakresie zapewnienia zgodności ze środkami ograniczającymi oraz za nadzorowanie jej wdrażania za pomocą polityk, procedur i mechanizmów kontroli niezbędnych do zapewnienia wdrażania środków ograniczających. Wszyscy członkowie organu zarządzającego powinni być świadomi narażenia instytucji finansowej na naruszenie środków ograniczających oraz jej podatności na obchodzenie środków ograniczających.

5. W przypadku gdy działalnością instytucji finansowej kieruje jedna osoba, może ona wyznaczyć członka kadry kierowniczej wyższego szczebla do pełnienia funkcji organu zarządzającego zgodnie z pkt 4.

6. W przypadku gdy instytucja finansowa jest jednostką dominującą grupy zgodnie z definicją zawartą w art. 2 pkt 9 i pkt 11 dyrektywy 2013/34/UE [2], organ zarządzający jednostki dominującej powinien zapewnić, aby każdy organ zarządzający, linia biznesowa i jednostka wewnętrzna, w tym każda jednostka kontroli wewnętrznej jednostek zależnych grupy, posiadała odpowiednie informacje umożliwiające zapewnienie zgodności ze środkami ograniczającymi. Ostateczna odpowiedzialność za zapewnienie zgodności ze środkami ograniczającymi spoczywa na każdym podmiocie należącym do grupy.

7. W przypadku gdy instytucja finansowa jest jednostką dominującą grupy, organ zarządzający jednostki dominującej powinien zapewnić, aby jednostki zależne grupy przeprowadzały własną ocenę narażenia na naruszenie środków ograniczających jak określono w sekcji 4.2, w sposób skoordynowany i zgodnie ze wspólną metodyką, odzwierciedlającą specyfikę grupy.

4.1.1 Rola organu zarządzającego pełniącego funkcję nadzorczą

8. Organ zarządzający pełniący funkcję nadzorczą powinien odpowiadać za nadzorowanie i monitorowanie mechanizmów kontroli wewnętrznej i ram zarządzania wdrożonych przez instytucję finansową w celu zapewnienia zgodności ze środkami ograniczającymi, aby zagwarantować ich skuteczność, zgodnie z sekcją 4.3.

9. Oprócz przepisów określonych w wytycznych EBA/GL/2021/05[3] organ zarządzający instytucji finansowej w ramach swojej funkcji nadzorczej powinien:

    a. być informowany o wynikach najnowszej oceny narażenia na naruszenie środków ograniczających, zgodnie z sekcją 4.2;
    b. nadzorować i monitorować, za pośrednictwem funkcji kontroli wewnętrznej, zakres, w jakim polityki i procedury dotyczące środków ograniczających są odpowiednie i skuteczne, zgodnie z sekcją 4.3, w świetle narażenia na naruszenie środków ograniczających i ryzyka obchodzenia środków ograniczających, na które narażona jest instytucja finansowa, a także podejmować odpowiednie działania w celu zapewnienia podjęcia środków naprawczych, gdy jest to konieczne;
    c. co najmniej raz w roku oceniać skuteczność funkcjonowania komórki ds. zgodności ze środkami ograniczającymi, m. in. wewnętrznych polityk, procedur i mechanizmów kontroli, w tym adekwatność zasobów ludzkich i technicznych przydzielonych do zapewnienia zgodności ze środkami ograniczającymi.

[2] Dyrektywa Parlamentu Europejskiego i Rady 2013/34/UE z dnia 26 czerwca 2013 r. w sprawie rocznych sprawozdań finansowych, skonsolidowanych sprawozdań finansowych i powiązanych sprawozdań niektórych rodzajów jednostek, zmieniająca dyrektywę Parlamentu Europejskiego i Rady 2006/43/WE oraz uchylająca dyrektywy Rady 78/660/EWG i 83/349/EWG.

[3] Wytyczne EBA/GL/2021/05 w sprawie zarządzania wewnętrznego na podstawie dyrektywy 2013/36/UE.

10. W przypadku gdy instytucja finansowa jest jednostką dominującą grupy, organ zarządzający jednostki dominującej powinien również wykonywać wszystkie zadania, o których mowa w pkt 9, na poziomie grupy. Ostateczna odpowiedzialność za zapewnienie zgodności ze środkami ograniczającymi spoczywa na każdym podmiocie należącym do grupy.

4.1.2 Rola organu zarządzającego pełniącego funkcję zarządzającą

11. Oprócz przepisów określonych w wytycznych EBA/GL/2021/05 organ zarządzający instytucji finansowej w ramach swojej funkcji nadzorczej powinien:

    a. upewnić się, że został poinformowany o wynikach najnowszej oceny narażenia na naruszenie środków ograniczających, zgodnie z sekcją 4.2;
    b. przyjąć odpowiednie ramy zarządzania ryzykiem i system kontroli wewnętrznej, które są wystarczająco niezależne od działalności, którą kontroluje;
    c. zatwierdzać polityki, procedury i mechanizmy kontroli, które są proporcjonalne do stopnia narażenia instytucji finansowej na naruszenie środków ograniczających i odpowiednie do zapewnienia zgodności instytucji finansowej ze środkami ograniczającymi;
    d. zapewniać skuteczne wdrażanie procesów instytucji finansowej w celu zapewnienia zgodności ze środkami ograniczającymi;
    e. wdrożyć strukturę organizacyjną i operacyjną niezbędną do skutecznego stosowania strategii w zakresie zapewnienia zgodności ze środkami ograniczającymi, przyjętej przez organ zarządzający;
    f. zapewnić, aby zasoby ludzkie i techniczne przydzielone do zapewnienia zgodności ze środkami ograniczającymi były odpowiednie i współmierne do narażenia instytucji na naruszenie środków ograniczających;
    g. jeżeli funkcje operacyjne dotyczące zgodności ze środkami ograniczającymi są przedmiotem outsourcingu, zapewnić zgodność tych rozwiązań z wytycznymi EBA/GL/2019/02[4] oraz otrzymywać od dostawcy usług regularne sprawozdania na temat skuteczności systemu w celu przekazywania informacji organowi zarządzającemu.

12. W przypadku gdy instytucja finansowa jest jednostką dominującą grupy, organ zarządzający tej jednostki dominującej powinien zapewnić, aby wszystkie zadania, o których mowa w pkt 11, były również wykonywane na poziomie jednostek zależnych oraz aby wprowadzone polityki i procedury były dostosowane do procedur i polityk grupy, w zakresie dozwolonym przez obowiązujące prawo krajowe.

[4] Wytyczne EBA/GL/2019/02 w sprawie outsourcingu, które zostaną zastąpione Wytycznymi EBA/GL/XXX/XX w sprawie należytego zarządzania ryzykiem osób trzecich.

4.1.3 Rola pracownika wyższego szczebla odpowiedzialnego za zgodność ze środkami ograniczającymi

4.1.3.1 Wyznaczenie pracownika wyższego szczebla

13. Instytucje finansowe powinny wyznaczyć pracownika wyższego szczebla odpowiedzialnego za wykonywanie funkcji i zadań określonych w pkt 19–21. Organ zarządzający powinien zapewnić, aby pracownik wyższego szczebla posiadał wiedzę i zrozumienie w zakresie środków ograniczających niezbędne do skutecznego pełnienia swoich funkcji.

14. Organ zarządzający może powierzyć tę funkcję pracownikowi wyższego szczebla, który pełni już inne obowiązki lub funkcje w ramach instytucji finansowej (np. pracownika ds. zgodności z przepisami AML/CFT lub dyrektora ds. zgodności z przepisami), pod warunkiem że:

    a. jest to uzasadnione wielkością i złożonością instytucji finansowej oraz wynikami oceny narażenia na naruszenie środków ograniczających;
    b. nie ma to wpływu na zdolność tego pracownika wyższego szczebla do skutecznego wypełniania swoich obowiązków lub funkcji; oraz
    c. takie połączenie zadań nie powoduje żadnych konfliktów interesów, takich jak konflikty między zadaniami operacyjnymi i kontrolnymi przypisanymi temu pracownikowi.

15. Organ zarządzający powinien umożliwić pracownikowi wyższego szczebla przydzielanie i delegowanie zadań określonych w pkt 19–21 innym pracownikom działającym pod kierownictwem i nadzorem pracownika wyższego szczebla, pod warunkiem że ostateczna odpowiedzialność za skuteczne wykonywanie tych zadań spoczywa na pracowniku wyższego szczebla.

16. Niezależnie od rozwiązań instytucjonalnych instytucje finansowe powinny zapewnić, aby:

    a. pracownik wyższego szczebla może skutecznie koordynować i współpracować z jednostkami kontroli wewnętrznej; oraz
    b. pracownik wyższego szczebla może składać sprawozdania i ma bezpośredni dostęp do organu zarządzającego pełniącego funkcję zarządczą i nadzorczą.

17. W przypadku gdy instytucja finansowa jest częścią grupy, organ zarządzający dominującej instytucji finansowej powinien wyznaczyć pracownika wyższego szczebla na poziomie grupy.

4.1.3.2 Rola pracownika wyższego szczebla

18. Pracownik wyższego szczebla powinien opracować, wdrożyć i utrzymywać polityki, procedury i mechanizmy kontroli odpowiednie do zapewnienia zgodności instytucji finansowej ze środkami ograniczającymi i proporcjonalne do poziomu narażenia instytucji finansowej na naruszenie środków ograniczających.

19. Pracownik wyższego szczebla powinien:

a. podejmować działania niezbędne do zapewnienia zgodności z sekcją 4.2 w zakresie oceny narażenia na naruszenie środków ograniczających;
b. podejmować działania niezbędne do zapewnienia zgodności z sekcją 4.3 w zakresie skutecznych polityk i procedur dotyczących środków ograniczających;
c. udzielać organowi zarządzającemu regularnych i odpowiednich informacji umożliwiające mu wykonywanie funkcji określonych w sekcji 4.1.1 i sekcji 4.1.2. Informacje zarządcze powinny obejmować co najmniej:
    i) zmiany dotyczące narażenia instytucji finansowej na naruszenie środków ograniczających oraz wynik oceny narażenia instytucji finansowej na naruszenie środków ograniczających;
    ii) zmiany w systemach środków ograniczających i ich wpływ na instytucję finansową;
    iii) dane statystyczne i informacje dotyczące:

- liczby wygenerowanych alertów;
- liczby alertów oczekujących na analizę;
- liczby sprawozdań przekazanych odpowiedniemu organowi krajowemu właściwemu do wdrażania środków ograniczających[5] lub właściwemu organowi nadzorczemu zgodnie z wymogami obowiązujących przepisów prawa;
- średni czas między potwierdzonym dopasowaniem a sprawozdaniem przedłożonym odpowiedniemu organowi krajowemu właściwemu do wdrażania środków ograniczających lub właściwemu organowi nadzorczemu zgodnie z wymogami obowiązujących przepisów prawa;
- wartość zamrożonych środków finansowych, zamrożonych zasobów gospodarczych[6] i charakter tych środków przechowywanych w instytucji finansowej;

    iv) informacje na temat zasobów ludzkich i technicznych oraz adekwatności tych zasobów w świetle narażenia instytucji finansowej na naruszenie środków ograniczających;
    v) braki lub uchybienia stwierdzone w związku z polityką, procedurami i mechanizmami kontroli instytucji finansowej w zakresie środków ograniczających, w tym uwagi przekazane przez właściwe organy do celów nadzoru nad politykami, procedurami i mechanizmami kontroli w zakresie wdrażania środków ograniczających;
    vi) przypadki naruszenia i obejścia środków ograniczających oraz przyczyny takiego naruszenia i obejścia;
    vii) propozycje dotyczące sposobu uwzględnienia wszelkich zmian w wymogach regulacyjnych lub w narażeniu na naruszenie środków ograniczających lub wszelkich braków lub uchybień w politykach, procedurach lub mechanizmach kontroli dotyczących środków ograniczających w instytucji finansowej, które

[5] https://finance.ec.europa.eu/eu-and-world/sanctions-restrictive-measures/overview-sanctions-and-related-resources_en#contact.

[6] Zob. art. 2 pkt 5 i 6 dyrektywy (UE) 2024/1226.

zostały zidentyfikowane, oraz przypadki naruszenia i obejścia środków ograniczających, które zostały zidentyfikowane.

d. zgłaszać wszelkie naruszenia środków ograniczających odpowiednim organom krajowym właściwym do wdrażania środków ograniczających lub właściwemu organowi nadzorczemu zgodnie z wymogami obowiązujących przepisów prawa**;**
e. skutecznie i konstruktywnie współpracować z odpowiednimi organami krajowymi właściwymi do wdrażania środków ograniczających oraz z właściwym organem nadzorczym, zgodnie z wymogami obowiązujących przepisów prawa**;**

20. W przypadku gdy instytucja finansowa jest częścią grupy, pracownik wyższego szczebla na poziomie grupy powinien, w stosownych przypadkach, ocenić skuteczność polityk, procedur i mechanizmów kontroli pod kątem zgodności z odpowiednimi środkami ograniczającymi w oddziałach, jednostkach zależnych, u pośredników, dystrybutorów i agentów. Ostateczna odpowiedzialność za zgodność ze środkami ograniczającymi spoczywa na każdym podmiocie należącym do grupy.

21. Pracownik wyższego szczebla powinien nadzorować przygotowanie i realizację programu szkoleniowego, o którym mowa w sekcji 4.4.

4.2 Przeprowadzanie oceny narażenia na naruszenie środków ograniczających

22. Wewnętrzne procedury instytucji finansowych powinny obejmować ocenę narażenia na naruszenie środków ograniczających w celu zrozumienia w jakim stopniu każdy obszar ich działalności jest narażony na naruszenie środków ograniczających i podatny na obchodzenie środków ograniczających.

23. Ocena narażenia na naruszenie środków ograniczających powinna umożliwiać instytucjom finansowym określenie i ocenę:

a. które systemy środków ograniczających mają do nich zastosowanie;
b. prawdopodobieństwo niewdrożenia środków ograniczających;
c. prawdopodobieństwo obejścia środków ograniczających;
d. skutki wszelkich naruszeń środków ograniczających; oraz
e. następujące czynniki ryzyka:
a) ryzyko geograficzne, w tym:

i. gdzie instytucja finansowa prowadzi swoją działalność, tj. jurysdykcje i terytoria, w których instytucja finansowa ma siedzibę lub prowadzi działalność;
ii. zakres, w jakim te jurysdykcje i terytoria są narażone na środki ograniczające lub o których wiadomo, że są wykorzystywane do obchodzenia środków ograniczających;
iii. pochodzenie i przeznaczenie transakcji.

b) ryzyko dotyczące klienta, w tym:

   i. powiązania klientów oraz, w stosownych przypadkach, ich beneficjentów rzeczywistych i akcjonariuszy większościowych, z krajami, w odniesieniu do których obowiązują środki ograniczające ze względu na sytuację dotyczącą tego kraju lub o których wiadomo, że są wykorzystywane do obchodzenia środków ograniczających;
   ii. liczbę klientów, rodzaj klientów i złożoność tych klientów, takie jak problemy z identyfikacją beneficjenta rzeczywistego;
   iii. działalność bazy klientów i złożoność działalności, w tym wszelkie powiązania z branżami lub sektorami, które mogą podlegać środkom ekonomicznym lub innym środkom ograniczającym, a także częstotliwość i rodzaje transakcji.

c) ryzyko związane z produktami i usługami, w tym:

   i. charakter produktów i usług instytucji finansowej;
   ii. zakres, w jakim dostarczanie tych produktów i świadczenie usług naraża instytucję finansową na ryzyko naruszenia środków ograniczających i obejścia środków ograniczających.

d) ryzyko związane z kanałami dostaw, w tym informacje na temat tego, czy korzystanie z pośredników, agentów, osób trzecich, relacji w ramach bankowości korespondenckiej lub innych kanałów dostaw stwarza zagrożenia, m. in. poprzez:

   i. ograniczenie instytucji finansowej możliwości identyfikacji zaangażowanych stron;
   ii. uzależnianie instytucji finansowej od procesów kontroli stron trzecich;
   iii. zwiększenie narażenia instytucji finansowej na ryzyko geograficzne, ponieważ prowadzi ona działalność lub ma siedzibę w państwach objętych środkami ograniczającymi lub w państwach, o których wiadomo, że są wykorzystywane do obchodzenia środków ograniczających.

24. Ocena, o której mowa w pkt 22, powinna opierać się na wystarczająco zróżnicowanych źródłach informacji, w tym co najmniej następujących:

   a. informacje uzyskane w ramach stosowania przez instytucję finansową środków należytej staranności wobec klienta, zgodnie z przepisami art. 13 dyrektywy (UE) 2015/849;
   b. informacje od organów międzynarodowych, rządów, właściwych organów krajowych, w tym organów nadzoru AML/CFT, jednostek analityki finansowej (FIU) oraz organów ścigania, takie jak aktualne typologie obchodzenia środków ograniczających;
   c. informacje z wiarygodnych i rzetelnych źródeł otwartych, takich jak raporty z wiarygodnych gazet i innych wiarygodnych mediów;

d. informacje od wiarygodnych i rzetelnych organizacji handlowych, takie jak sprawozdania z oceny ryzyka;
e. w miarę możliwości, analiza wcześniejszych ostrzeżeń o środkach ograniczających dotyczących potwierdzonych dopasowań i fałszywie pozytywnych dopasowań w celu zidentyfikowania sytuacji, w których występowanie potwierdzonych dopasowań jest najbardziej prawdopodobne.

25. Przeprowadzając ocenę narażenia na naruszenie środków ograniczających, instytucje finansowe powinny rozważyć, czy screening bazy danych klientów i rejestrów transakcji obejmujący dane historyczne mógłby być przydatny i proporcjonalny. Może się tak zdarzyć, gdy instytucja finansowa stwierdzi lub ma uzasadnione podstawy podejrzewać, że jej poprzedni system wykorzystywany do screeningu był niewystarczający lub nieskuteczny.

26. Instytucje finansowe powinny zapewnić, aby ich ocena narażenia na naruszenie środków ograniczających była aktualna i odpowiednia. Aby to osiągnąć, instytucje finansowe powinny dokonywać jej przeglądu co najmniej raz w roku oraz, w razie potrzeby, aktualizować ją. Ponadto, w razie konieczności, instytucje finansowe powinny dokonać przeglądu oceny narażenia na naruszenie środków ograniczających w następujących sytuacjach:

    a. przyjęcie nowych środków ograniczających i wprowadzenie istotnych zmian do istniejących środków ograniczających;
    b. przed udostępnieniem nowych produktów, oferowaniem nowych kanałów dostawy produktów, obsługą nowych grup klientów, wejściem na nowe obszary geograficzne;
    c. istotne zmiany profilu działalności instytucji, jej bazy klientów, struktury organizacyjnej lub modelu biznesowego;
    d. identyfikacja niewdrożenia środków ograniczających i obchodzenia środków ograniczających, co wskazuje że ocena narażenia na naruszenie środków ograniczających została przeprowadzona nierzetelnie;
    e. braki w ocenie narażenia na naruszenie środków ograniczających, zidentyfikowane przez instytucję finansową lub właściwy organ odpowiedzialny za nadzór nad wewnętrznymi politykami, procedurami i mechanizmami kontroli w celu zapewnienia wdrożenia unijnych i krajowych środków ograniczających.

27. Instytucje finansowe powinny udokumentować swoją metodykę przeprowadzania i przeglądu oceny narażenia na naruszenie środków ograniczających oraz wyniki tej oceny i udostępnić je właściwemu organowi na żądanie.

28. W przypadku gdy instytucja finansowa jest jednostką dominującą grupy, organ zarządzający grupy powinien zapewnić, aby jednostki zależne grupy przeprowadzają własną ocenę narażenia na naruszenie środków ograniczających w sposób skoordynowany i w oparciu o wspólną metodykę, przy jednoczesnym uwzględnieniu własnej specyfiki.

4.3 Zapewnienie skuteczności polityk, procedur i mechanizmów kontroli w zakresie wdrażania środków ograniczających.

29. Aby polityki, procedury i mechanizmy kontroli instytucji finansowej w zakresie wdrażania środków ograniczających były skuteczne, instytucja ta powinna niezwłocznie umożliwić pełne i prawidłowe wdrożenie wszystkich mających zastosowanie środków ograniczających.

30. Polityki, procedury i mechanizmy kontroli powinny obejmować co najmniej:

    a. procesy zapewniające instytucjom finansowym posiadanie wszystkich aktualnych informacji dotyczących obowiązujących środków ograniczających;
    b. procesy zapewniające aktualizację wykazów i wymogów dotyczących obowiązujących środków ograniczających niezwłocznie po ich wejściu w życie;
    c. procesy zapewniające adekwatność i aktualność oceny narażenia na naruszenie środków ograniczających;
    d. procesy zapewniające proporcjonalność polityk, procedur i mechanizmów kontroli do oceny narażenia na naruszenie środków ograniczających;
    e. procesy zapewniające, aby polityki i procedury dotyczące środków ograniczających były:
        i. regularnie poddawane przeglądowi;
        ii. regularnie zmieniane i aktualizowane w razie potrzeby;
        iii. skutecznie wdrażane; oraz
        iv. opracowane w taki sposób, aby po zidentyfikowaniu uchybień uruchamiane były niezbędne działania.
    f. procedury niezwłocznego rozpoczęcia badania wszystkich potencjalnych dopasowań;
    g. w przypadku wystąpienia potwierdzonych dopasowań – procedury, które uruchamiają działania następcze w celu zapewnienia zgodności z obowiązującymi środkami ograniczającymi, w tym natychmiastowe odrzucenie, zawieszenie lub zamrożenie, oraz składanie sprawozdań odpowiednim organom krajowym właściwym do wdrożenia środków ograniczających lub właściwemu organowi nadzorczemu zgodnie z mającymi zastosowanie przepisami w terminach określonych przez te organy lub aktach prawnych wprowadzających stosowanie środków ograniczających;
    h. udokumentowaną organizację wewnętrzną, która jasno określa zadania i obowiązki w odniesieniu do środków ograniczających, m. in. w przypadku outsourcingu;
    i. inne aspekty określone w Wytycznych EBA/GL/2024/15 w sprawie wewnętrznych polityk, procedur i mechanizmów kontroli mających na celu zapewnienie wdrożenia środków ograniczających na mocy rozporządzenia (UE) 2023/1113.

4.4 Szkolenia

31. Instytucje finansowe powinny regularnie organizować szkolenia dla swoich pracowników, aby zapewnić, aby posiadali oni wiedzę w zakresie:

    a. obowiązujących środków ograniczających;
    b. wyników oceny narażenia na naruszenie środków ograniczających; oraz
    c. polityk, procedur i mechanizmów kontroli mających na celu zapewnienie zgodności z obowiązującymi środkami ograniczającymi.

32. Szkolenia powinny być dostosowane do pracowników i ich konkretnej roli. Powinny one być organizowane we właściwym terminie i w odpowiedni sposób, tak aby umożliwić instytucji finansowej zapewnienie zgodności ze środkami ograniczającymi. W ramach grupy szkolenia takie mogą być organizowane – w całości lub częściowo – przez jednostkę dominującą.

33. Instytucje finansowe powinny dokumentować swój plan szkolenia i na żądanie właściwego organu być w stanie wykazać, że ich szkolenie jest odpowiednie i skuteczne.

EBA/GL/2024/15

14 listopada 2024 r.

Wytyczne

w sprawie wewnętrznych polityk, procedur i mechanizmów kontroli mających na celu zapewnienie wdrożenia unijnych i krajowych środków ograniczających na podstawie rozporządzenia (UE) 2023/1113

1. Zgodność i obowiązki sprawozdawcze

Status niniejszych wytycznych

1. Niniejszy dokument zawiera wytyczne wydane na podstawie art. 16 rozporządzenia (UE) nr 1093/2010 [7]. Zgodnie z art. 16 ust. 3 rozporządzenia (UE) nr 1093/2010 właściwe organy, dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów muszą dołożyć wszelkich starań, aby zastosować się do niniejszych wytycznych.

2. W wytycznych przedstawiono stanowisko EUNB w sprawie odpowiednich praktyk nadzoru w ramach Europejskiego Systemu Nadzoru Finansowego lub tego, jak należy stosować prawo Unii w konkretnym obszarze. Właściwe organy, określone w art. 4 ust. 2 rozporządzenia (UE) nr 1093/2010, do których niniejsze wytyczne mają zastosowanie, powinny stosować się do wytycznych poprzez odpowiednie włączenie ich do swoich praktyk (np. poprzez zmianę swoich ram prawnych lub procesów nadzorczych), również gdy wytyczne są skierowane przede wszystkim do instytucji.

Wymogi w zakresie sprawozdawczości

3. Zgodnie z art. 16 ust. 3 rozporządzenia (UE) nr 1093/2010 właściwe organy muszą do dnia 11.04.2025 r. powiadomić EUNB, czy stosują się lub zamierzają zastosować się do niniejszych wytycznych, albo podać powody niestosowania się do nich. W przypadku braku powiadomienia w tym terminie EUNB uzna, że właściwe organy nie stosują się do niniejszych wytycznych. Powiadomienia należy przekazać poprzez wysłanie formularza dostępnego na stronie internetowej EUNB z dopiskiem „EBA/GL/2024/15”. Powiadomienia powinny przekazać osoby odpowiednio upoważnione do przekazywania informacji o stosowaniu się do wytycznych w imieniu właściwych organów. EUNB należy również zgłaszać wszelkie zmiany dotyczące stosowania się do wytycznych.

4. Zgodnie z art. 16 ust. 3 powiadomienia zostaną opublikowane na stronie internetowej EUNB.

[7] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1093/2010 z dnia 24 listopada 2010 r. w sprawie ustanowienia Europejskiego Urzędu Nadzoru (Europejskiego Urzędu Nadzoru Bankowego), zmiany decyzji nr 716/2009/WE oraz uchylenia decyzji Komisji 2009/78/WE (Dz.U. L 331 z 15.12.2010, s. 12).

2. Przedmiot, zakres stosowania i definicje

Przedmiot i zakres stosowania

5. Niniejsze wytyczne określają wewnętrzne polityki, procedury i mechanizmy kontroli, które dostawcy usług płatniczych (PSP) i dostawcy usług w zakresie kryptoaktywów (CASP) powinni wprowadzić w celu zapewnienia skutecznego wdrożenia unijnych i krajowych środków ograniczających przy wykonywaniu transferów środków pieniężnych i kryptoaktywów, o których mowa w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2023/1113[8].

Adresaci

6. Niniejsze wytyczne skierowane są do:

   a. właściwych organów odpowiedzialnych za nadzór nad dostawcami usług płatniczych i dostawcami usług w zakresie kryptoaktywów pod względem wypełniania przez nich obowiązków wynikających z rozporządzenia (UE) 2023/1113.

   b. instytucji finansowych, o których mowa w art. 4 pkt 1 rozporządzenia (UE) nr 1093/2010, które są dostawcami usług płatniczych zdefiniowanymi w art. 3 pkt 5 rozporządzenia (UE) 2023/1113 oraz dostawcami usług w zakresie kryptoaktywów zdefiniowanymi w art. 3 pkt 15 rozporządzenia (UE) 2023/1113.

Definicje

7. Terminy stosowane i zdefiniowane w rozporządzeniu (UE) 2023/1113 mają takie samo znaczenie w niniejszych wytycznych. Ponadto do celów niniejszych wytycznych stosuje się następujące definicje:

Sektorowe środki ograniczające	oznaczają środki ograniczające, takie jak embargo na broń i sprzęt pokrewny lub środki gospodarcze i finansowe (np. ograniczenia przywozowe i wywozowe oraz ograniczenia w świadczeniu niektórych usług, takich jak usługi bankowe).

[8] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1113 z dnia 31 maja 2023 r. w sprawie informacji towarzyszących transferom środków pieniężnych i niektórych kryptoaktywów oraz zmiany dyrektywy (UE) 2015/849 (wersja przekształcona)(Dz.U. L 150 z 9.6.2023, s. 1).

Środki ograniczające	oznaczają unijne środki ograniczające zdefiniowane w art. 2 pkt 1 dyrektywy (UE) 2024/1226 oraz krajowe środki ograniczające przyjęte przez państwa członkowskie zgodnie z ich krajowym porządkiem prawnym (w zakresie, w jakim mają one zastosowanie do instytucji finansowych).
Ukierunkowane sankcje finansowe	oznaczają zarówno zamrożenie środków, jak i zakazy bezpośredniego lub pośredniego udostępniania środków finansowych lub innych aktywów na rzecz wskazanych osób i podmiotów zgodnie z decyzjami Rady przyjętymi na podstawie art. 29 TUE i rozporządzeniami Rady przyjętymi na podstawie art. 215 TFUE.

3. Wykonanie

Data rozpoczęcia stosowania

8. Niniejsze wytyczne stosuje się od dnia 30 grudnia 2025 r.

4. Wytyczne w sprawie wewnętrznych polityk, procedur i mechanizmów kontroli mających na celu zapewnienie wdrożenia unijnych i krajowych środków ograniczających na podstawie rozporządzenia (UE) 2023/1113

Przepisy ogólne

1. Dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów powinni wprowadzić polityki, procedury i mechanizmy kontroli umożliwiające im zapewnienie zgodności ze środkami ograniczającymi. Takie polityki, procedury i mechanizmy kontroli powinny być zgodne z wytycznymi EBA/GL/2024/14 w sprawie wewnętrznych polityk, procedur i mechanizmów kontroli mających na celu zapewnienie wdrożenia unijnych i krajowych środków ograniczających.

2. Polityki, procedury i mechanizmy kontroli powinny umożliwiać dostawcom usług płatniczych i dostawcom usług w zakresie kryptoaktywów identyfikację podmiotów objętych środkami ograniczającymi. Powinny one również umożliwiać dostawcom usług płatniczych i dostawcom usług w zakresie kryptoaktywów wprowadzanie środków niezbędnych do zapewnienia, że nie udostępniają oni żadnych środków pieniężnych ani kryptoaktywów tym podmiotom, nie realizują transakcji finansowych ani nie świadczą usług objętych zakazem nałożonym środkami ograniczającymi oraz zarządzają ryzykiem obchodzenia środków ograniczających.

4.1 Screening w zakresie środków ograniczających

3. Dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów powinni wprowadzić skuteczny system wykorzystywany do screeningu w celu wiarygodnego zidentyfikowania celów objętych środkami ograniczającymi jak określono szczegółowo w sekcji 4.4.

4.1.1 Wybór systemu wykorzystywanego do screeningu

4. Dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów powinni wykorzystać swoją ocenę narażenia na naruszenie środków ograniczających, w celu podjęcia decyzji, który system wykorzystywany do screeningu będą stosować, lub aby zatwierdzić stosowany przez siebie system wykorzystywany do screeningu w celu zapewnienia zgodności z obowiązującymi

środkami ograniczającymi. System wykorzystywany do screeningu powinien być dostosowany do wielkości, charakteru i złożoności działalności dostawców usług płatniczych i dostawców usług w zakresie kryptoaktywów oraz narażenia ich na naruszenie środków ograniczających.

5. Podejmując decyzję w sprawie swojego systemu wykorzystywanego do screeningu, dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów powinni rozważyć, czy mają dostęp do zasobów niezbędnych do efektywnego korzystania z wybranego przez siebie systemu.

6. Dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów powinni regularnie dokonywać przeglądu działania systemu stosowanego do screeningu, aby upewnić się, że jest on skuteczny i w dalszym ciągu niezawodnie identyfikuje cele objęte środkami restrykcyjnymi. Dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów powinni przeprowadzać przegląd skuteczności stosowanego systemu wykorzystywanego do screeningu co najmniej raz w roku oraz niezwłocznie, jeżeli mają powody do obaw, że system ten może nie być adekwatny do zakładanych celów.

7. Zgodnie z art. 8 rozporządzenia (UE) 2022/2554 dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów powinni znać i udokumentować możliwości i ograniczenia systemu wykorzystywanego do screeningu. Dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów powinni być w stanie wykazać właściwemu organowi, któremu podlegają, że ich system wykorzystywany do screeningu jest odpowiedni.

4.1.2 Zarządzanie listami

8. Dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów powinni określić w swoich politykach i procedurach środki ograniczające, które muszą stosować.

9. Dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów powinni dysponować politykami i procedurami w celu:

    a. określania, kiedy przyjęty został nowy zestaw środków ograniczających lub czy istniejący środek ograniczający został zaktualizowany lub zniesiony;
    b. aktualizowania swoich wewnętrznych zbiorów danych w celu poddania ich weryfikacji zgodnie z sekcją 4.1.3 niezwłocznie po wejściu w życie nowego środka ograniczającego lub po aktualizacji lub zniesieniu istniejącego środka ograniczającego.

4.1.3 Określenie zestawu danych, które należy poddać screeningowi

10. Dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów powinni określić w swoich politykach i procedurach rodzaje danych, które będą poddane weryfikacji w przypadku każdego rodzaju środka ograniczającego, biorąc pod uwagę wynik ich oceny narażenia na naruszenie środków ograniczających i zakres środków ograniczających, które muszą stosować.

11. Podejmując decyzję o zestawie danych podlegających kontroli screeningowi pod kątem rodzaju obowiązującego środka ograniczającego, dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów powinni wziąć pod uwagę wszystkie dane, jakie posiadają na temat swoich klientów, w tym informacje uzyskane:

    a. w czasie stosowania środków należytej staranności wobec klienta na podstawie prawa Unii i prawa krajowego transponującego prawo Unii; oraz
    b. zgodnie z rozporządzeniem (UE) 2023/1113.

12. Zgodnie z wymogami rozporządzenia (UE) 2023/1113 dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów powinni ocenić, czy posiadane przez nich dane są wystarczająco dokładne, aktualne i szczegółowe, aby umożliwić im ustalenie, czy strona transferu, ich beneficjent rzeczywisty lub jakakolwiek osoba, która twierdzi, że działa w ich imieniu, lub która jest upoważniona do działania w ich imieniu, podlega środkom ograniczającym.

13. Aby uniknąć powtarzających się fałszywych alertów dotyczących osób fizycznych lub prawnych, podmiotów lub organów, które nie podlegają środkom ograniczającym, ale zostały błędnie zidentyfikowane jako takie przez istniejący system wykorzystywany do screeningu, dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów mogą podjąć decyzję o umieszczeniu takich osób na określonej wewnętrznej liście („białej liście”). Uzasadnienie takiej decyzji musi być udokumentowane. Dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów powinni dokonać przeglądu takiej listy niezwłocznie po wejściu w życie nowego lub zmienionego środka ograniczającego lub w przypadku zmiany informacji o kliencie.

4.1.4 Screening bazy klientów

14. Dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów powinni określić w swoich politykach i procedurach, w jaki sposób będą poddawać screenigowi swoją bazę klientów.

15. Dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów powinni regularnie poddawać screenigowi całą bazę danych klientów i określać częstotliwość kontroli klienta na podstawie ich oceny narażenia na naruszenie środków ograniczających.

16. Dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów powinni określić w decyzji wewnętrznej zdarzenia inicjujące decyzję, w jakich przypadkach należy zawsze dokonywać weryfikacji swoich klientów i aktualizować takie decyzje. Zdarzenia inicjujące powinny obejmować co najmniej:

    a. zmianę któregokolwiek z istniejących wykazów lub środków ograniczających, wejście w życie nowego wykazu lub środka ograniczającego;
    b. przed nawiązaniem lub w czasie nawiązywania stosunków gospodarczych z klientem;

c. przypadki wystąpienia istotnych zmian w danych uzyskanych w ramach środków należytej staranności wobec istniejącego klienta, takich jak zmiana nazwiska, miejsca zamieszkania, obywatelstwa lub zmiana działalności gospodarczej;
d. przypadki istnienia uzasadnionych podstaw aby podejrzewać, że klient, jakakolwiek osoba, która twierdzi, że działa w imieniu klienta, lub która jest upoważniona do działania w imieniu klienta podejmuje próbę obejścia środków ograniczających.

17. Zgodnie z obowiązującymi środkami ograniczającymi dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów powinni dokonywać screeningu co najmniej następujących informacji o klientach:

    a. w przypadku osoby fizycznej:
        a. imię i nazwisko, w oryginale lub transliteracja takich danych; oraz
        b. datę urodzenia.
    b. w przypadku osoby prawnej: nazwę osoby prawnej, w oryginale lub transliteracja takich danych;
    c. w przypadku osoby fizycznej, osoby prawnej, organu lub podmiotu: wszelkie inne imiona i nazwiska, pseudonimy, nazwy handlowe, adresy portfeli, jeżeli są one dostępne w odpowiednich wykazach środków ograniczających. Dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów powinni należycie uzasadnić za pomocą oceny narażenia na naruszenie środków ograniczających decyzję o niedokonywaniu kontroli takich informacji, jeżeli są dostępne.

18. Podczas dokonywania screeningu klientów będących osobami prawnymi, osobami fizycznymi, organami lub podmiotami, dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów powinni, w zakresie, w jakim informacje te są dostępne, również weryfikować:

    a. beneficjentów rzeczywistych poprzez udział własnościowy;
    b. beneficjentów rzeczywistych poprzez kontrolę;
    c. każdą osobę, która twierdzi, że działa w imieniu klienta, lub która jest upoważniona do działania w imieniu klienta.

4.1.5 Screening transferów środków pieniężnych i kryptoaktywów

19. Z wyjątkiem przypadków objętych art. 5d rozporządzenia (UE) nr 260/2012 dostawcy usług płatniczych powinni dokonywać screeningu transferów środków pieniężnych przed udostępnieniem środków odbiorcy, a dostawcy usług w zakresie kryptoaktywów powinni dokonywać weryfikacji wszystkich transferów kryptoaktywów przed udostępnieniem kryptoaktywów beneficjentowi, niezależnie od tego, czy są one realizowane w ramach stosunków gospodarczych, czy w ramach jednorazowej transakcji.

20. Dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów powinni dokonywać weryfikacji wszystkich stron transferów środków pieniężnych lub kryptoaktywów pod kątem obowiązujących środków ograniczających. W swojej ocenie narażenia na naruszenie środków ograniczających dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów

powinni zwracać szczególną uwagę na rzetelność i wiarygodność polityk i procedur dotyczących środków ograniczających wprowadzonych przez dostawców usług płatniczych i dostawców usług w zakresie kryptoaktywów, z którymi posiadają stosunki gospodarcze , aby zapewnić zgodność ze środkami ograniczającymi.

21. Wszystkie dane, które mogą być istotne dla oceny, czy obowiązujące środki ograniczające mogą mieć wpływ na transakcję, należy poddać weryfikacji pod kątem obowiązujących środków ograniczających. Dane, które mają być poddane weryfikacji, powinny obejmować co najmniej:
    a. informacje o płatniku i odbiorcy płatności zgodnie z art. 4 rozporządzenia (UE) 2023/1113;
    b. informacje o inicjatorze i beneficjencie zgodnie z art. 14 rozporządzenia (UE) 2023/1113;
    c. cel transferu środków pieniężnych lub kryptoaktywów oraz, jeśli informacje są dostępne i podlegają ocenie narażenia na naruszenie środków ograniczających, inne pola tekstowe, które zawierają dalsze informacje na temat faktycznego nadawcy/odbiorcy środków pieniężnych lub kryptoaktywów;
    d. szczegółowe informacje na temat dostawców usług płatniczych i dostawców usług w zakresie kryptoaktywów uczestniczących w transferze środków pieniężnych lub kryptoaktywów, w tym instytucji pośredniczących, korespondentów, wraz z kontrolą kodów identyfikacyjnych, takich jak BIC, SWIFT i inne;
    e. inne szczegóły transferu środków pieniężnych lub kryptoaktywów, w zależności od charakteru, rodzaju operacji, otrzymanej dokumentacji uzupełniającej, jeśli informacje są dostępne i podlegają ocenie narażenia na naruszenie środków ograniczających;
    f. adresy portfeli inicjatora i beneficjenta transferu kryptoaktywów, w zakresie, w jakim informacje te są dostępne w oficjalnych wykazach adresów portfeli powiązanych ze środkami ograniczającymi.

22. Zgodnie z postanowieniami sekcji 4.6 Wytycznych EBA/GL/2024/11 dotyczących wymogów informacyjnych w odniesieniu do transferów środków pieniężnych i transferów niektórych kryptoaktywów wydane na podstawie rozporządzenia (UE) 2023/1113 („wytyczne dotyczące reguły podróży (ang. travel rule)”) wszelkie nowe informacje uzyskane później, przed wykonaniem lub po wykonaniu transferu, również powinny zostać poddane weryfikacji.

23. W stosownych przypadkach, w zależności od wielkości i liczby transferów kryptoaktywów, dostawcy usług w zakresie kryptoaktywów powinni rozważyć włączenie do istniejących ram analizy łańcucha bloków na potrzeby monitorowania transakcji.

4.1.6 Kalibracja

24. Dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów powinni określić sposób kalibrowania ustawień automatycznego systemu wykorzystywanego do screeningu w celu zmaksymalizowania jakości alertów, co umożliwi jednoznaczną identyfikację przy jednoczesnym zapewnieniu zgodności ze środkami ograniczającymi. Na podstawie swojej oceny

narażenia na naruszenie środków ograniczających i regularnych testów dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów powinni co najmniej:

a. określić, dla każdego obowiązującego środka ograniczającego, odpowiednie parametry dopasowania, które będą w stanie wygenerować uzasadniony alert umożliwiający dostawcom usług płatniczych i dostawcom usług w zakresie kryptoaktywów wypełnienie ich obowiązku stosowania środków ograniczających, poprzez sprawdzenie progów potwierdzonych trafień związanych z różnymi wartościami procentowymi dopasowania. Kalibracja nie powinna być ani zbyt czuła, powodując dużą liczbę fałszywie pozytywnych dopasowań, ani niewystarczająco czuła, powodując, że wskazane osoby, podmioty i organy nie zostaną wykryte lub informacje w dowolnym formacie nie zostaną wykorzystane do innych środków ograniczających;
b. stosować system wykorzystywany do screeningu, który umożliwia zastosowanie techniki opartej na algorytmie, która może dopasować jedną nazwę lub ciąg słów, w przypadku gdy treść informacji poddanych weryfikacji nie jest identyczna, ale ich pisownia, wzór lub dźwięk są bliskie treści zawartej w zbiorze danych stosowanym do screeningu („techniki dopasowania rozmytego") i skalibrować procent „dopasowania rozmytego" w swoim systemie wykorzystywanym do screeningu.

25. Dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów powinni decydować o kalibracji zarówno przed opracowaniem nowego systemu wykorzystywanego do screeningu, jak i okresowo, zgodnie ze swoją oceną narażenia na naruszenie środków ograniczających. Powinni oni dokumentować swoje uzasadnienie i udostępniać je właściwym organom na ich żądanie.

4.1.7 Korzystanie z usług osób trzecich i outsourcingu

26. Dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów powinni określić w swoich politykach i procedurach działania, które będą podejmowane przez dostawców usług płatniczych, dostawców usług w zakresie kryptoaktywów lub dostawców usług zleconych na zasadzie outsourcingu w celu zapewnienia zgodności z obowiązującymi środkami ograniczającymi. W przypadku outsourcingu usług dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów, biorąc pod uwagę wytyczne EBA/GL/2019/02 w stosownych przypadkach[9], powinni stosować następujące kluczowe zasady:

a. ostateczna odpowiedzialność za zgodność ze środkami ograniczającymi, niezależnie od tego, czy konkretne funkcje są zlecane w ramach outsourcingu, spoczywa na dostawcach usług płatniczych i dostawcach usług w zakresie kryptoaktywów;
b. prawa i obowiązki dostawców usług płatniczych i dostawców usług w zakresie kryptoaktywów oraz dostawcy usług powinny być w sposób jasny rozdzielone i określone w pisemnej umowie;

[9] Wytyczne EBA/GL/2019/02 w sprawie outsourcingu.

c. dostawcy usług płatniczych lub dostawcy usług w zakresie kryptoaktywów, korzystający z umowy outsourcingowej, powinni nadal być odpowiedzialni za monitorowanie i nadzorowanie jakości usługi świadczonej przez dostawcę usług;
d. outsourcing wewnątrz grupy powinien podlegać tym samym ramom regulacyjnym co zlecanie zadań w ramach outsourcingu dostawcom usług spoza grupy.

27. Dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów powinni wdrożyć i stosować niezbędne mechanizmy kontroli, aby zagwarantować, że korzystanie z usług zewnętrznych dostawców usług nie narazi ich na ryzyko naruszenia środków ograniczających, a także udokumentować te mechanizmy kontroli w umowie outsourcingowej.

28. W przypadku gdy dostawcy usług powinni zaktualizować dane, które mają być wykorzystywane przez dostawców usług płatniczych i dostawców usług w zakresie kryptoaktywów w odniesieniu do osób fizycznych, osób prawnych, podmiotów i organów, które podlegają obowiązującym środkom ograniczającym, dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów powinni zapewnić, aby umowa o świadczenie usług minimalizowała ryzyko naruszenia środków ograniczających przez dostawców usług płatniczych lub dostawców usług w zakresie kryptoakywów.

29. W przypadku zawarcia umów outsourcingowych dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów powinni przeprowadzać regularną kontrolę przestrzegania przez dostawcę usług obowiązków wynikających z umowy, oceniać skuteczność usług objętych umową i podejmować wszelkie niezbędne środki ograniczania ryzyka, w tym renegocjację umowy.

30. Przepisy niniejszej sekcji nie mają wpływu na obowiązki i zadania dostawców usług płatniczych i dostawców usług w zakresie kryptoaktywów w zakresie operacyjnej odporności cyfrowej określonej w rozporządzeniu (UE) 2022/2554[10].

4.2 Środki należytej staranności i środki weryfikacji w odniesieniu do analizy alertów

4.2.1 Polityki i procedury dotyczące analizy alertów i zarządzania nimi

31. Dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów powinni wdrożyć polityki i procedury umożliwiające badanie alertów dotyczących środków ograniczających. Te polityki i procedury powinny umożliwiać dostawcom usług płatniczych i dostawcom usług w zakresie kryptoaktywów potwierdzenie, czy alert jest potwierdzonym dopasowaniem, a jeżeli tak, określenie działań niezbędnych do zastosowania się do obowiązującego środka ograniczającego.

[10] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Tekst mający znaczenie dla EOG) (Dz.U. L 333 z 27.12.2022, s. 1).

32. Tego rodzaju polityki i procedury powinny obejmować:

    a. działania mające na celu niezwłoczne rozpoczęcie badania wszystkich potencjalnych dopasowań w odniesieniu do każdego transferu środków pieniężnych lub transferu kryptoaktywów;
    b. zasady wynikające z ogólnej polityki prowadzenia rejestrów przez dostawców usług płatniczych i dostawców usług w zakresie kryptoaktywów dotyczące dokumentowania wszelkich decyzji podjętych w związku z alertami;
    c. środki zapewniające zgodność z sekcją 4.2.2 niniejszych wytycznych;
    d. różne poziomy weryfikacji przeprowadzane zgodnie z oceną narażenia na naruszenie środków ograniczających, poprzez wdrożenie przeglądu przeprowadzanego co najmniej przez dwie osoby w przypadku sytuacji wyższego ryzyka narażenia.

4.2.2 Środki należytej staranności w odniesieniu do analizy alertów

33. Alert wygenerowany przez system stosowany do screeningu powinien wskazywać dany środek ograniczający, do którego odnosi się alert. Alerty powinny być analizowane przez pracowników posiadających odpowiednią wiedzę specjalistyczną i odpowiednio przeszkolonych[11].

34. W razie wątpliwości co do prawdziwości dopasowania dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów powinni wykorzystać dodatkowe informacje, którymi dysponują lub które mogą uzyskać, aby wesprzeć analizę ostrzeżeń w zakresie, w jakim informacje te są dostępne, takie jak:

    a. dane identyfikacyjne osoby fizycznej, osoby prawnej, podmiotu lub organu, które nie zostały wykorzystane na etapie screeningu;
    b. informacje o miejscu zamieszkania osoby fizycznej oraz informacje o adresie siedziby osoby prawnej, podmiotu lub jednostki, niewykorzystywane na etapie screeningu;
    c. informacje na temat narodowości, obywatelstwa osób fizycznych, które nie są wykorzystywane na etapie screeningu;
    d. struktura reprezentacyjna, zarządcza i organizacyjna osób prawnych niewykorzystywana na etapie screeningu;
    e. dane kontaktowe niewykorzystywane na etapie screeningu.

35. Dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów powinni określić w swoich politykach i procedurach sposób postępowania w przypadkach, w których mimo dodatkowej należytej staranności nie można jednoznacznie ustalić, że dopasowanie jest potwierdzonym dopasowaniem, fałszywie pozytywnym dopasowaniem lub zbieżnością nazw. Dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów nie powinni świadczyć usług finansowych na rzecz strony transferu przed podjęciem świadomej decyzji.

[11] Zob. sekcja 4.4 wytycznych w sprawie wewnętrznych polityk, procedur i mechanizmów kontroli mających na celu zapewnienie wdrożenia unijnych i krajowych środków ograniczających.

4.2.3 Ocena, czy podmiot jest własnością wyznaczonej osoby lub jest przez nią kontrolowany

36. Dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów powinni określić w swoich politykach i procedurach sposób oceny, czy osoba prawna lub podmiot są własnością wskazanej osoby lub wskazanego podmiotu lub są przez nie kontrolowane.

37. Dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów powinni:

    a. stosować kryteria określone w wytycznych Rady UE w sprawie sankcji[12] oraz w rozdziale VIII najlepszych praktyk Rady UE w[13] celu ustalenia, czy podmiot prawny jest własnością innej osoby lub innego podmiotu lub jest przez niego kontrolowany;
    b. stosować kryteria wykorzystywane do identyfikacji beneficjenta rzeczywistego zgodnie z obowiązującymi przepisami[14];
    c. korzystać z dostępnych publicznych źródeł informacji, takich jak rejestry posiadanych i kontrolowanych podmiotów oraz rejestry beneficjentów rzeczywistych.

38. Jeżeli ocena pozostaje niejednoznaczna, dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów powinni rozważyć współpracę z organem krajowym właściwym do wdrażania środków ograniczających. Ostateczna odpowiedzialność za zastosowanie się do środków ograniczających spoczywa na dostawcach usług płatniczych i dostawcach usług w zakresie kryptoaktywów.

4.2.4 Mechanizmy kontroli i środki należytej staranności mające na celu zapewnienie zgodności z sektorowymi środkami ograniczającymi

39. Dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów powinni wziąć pod uwagę ocenę narażenia na naruszenie środków ograniczających przy określaniu rodzajów kontroli, które będą stosować w celu zapewnienia zgodności ze środkami ograniczającymi. W ramach tych działań dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów powinni określić, jakie dostępne informacje związane z transakcją będą poddane screeningowi.

40. Dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów powinni zwracać szczególną uwagę na sektorowe środki ograniczające, które są związane z określoną jurysdykcją lub terytorium. W ramach takich środków ograniczających dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów powinni sprawdzać wszystkie informacje bazowe związane z transferem środków pieniężnych lub kryptoaktywów do lub z tej konkretnej jurysdykcji lub terytorium bądź do transferów środków pieniężnych lub kryptoaktywów zainicjowanych przez klientów, o których wiadomo, że prowadzą działalność w tej konkretnej

[12] https://data.consilium.europa.eu/doc/document/ST-11618-2024-INIT/en/pdf, Bruksela, 2 lipca 2024 r., 11618/24 (aktualizacja).

[13] Aktualizacja najlepszych praktyk UE w zakresie skutecznego wprowadzania w życie środków ograniczających (dok. 11623/24).

[14] Artykuł 3 pkt 6 dyrektywy (UE) 2015/849.

jurysdykcji lub na tym konkretnym terytorium. W miarę możliwości, dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów powinni kontrolować:

a. informacje o kraju (krajach) obywatelstwa, miejscu urodzenia;
b. informacje o zwykłym miejscu zamieszkania lub głównym miejscu prowadzenia działalności gospodarczej pod innymi adresami, zgodnie z oceną narażenia na naruszenie środków ograniczających;
c. informacje o państwie, do którego lub z którego dokonywany jest transfer środków pieniężnych, w którym dokonywany jest transfer środków pieniężnych;
d. cel transferu środków pieniężnych lub kryptoaktywów i inne pola tekstowe zawierające dodatkowe informacje na temat towarów, statków, kraju przeznaczenia lub kraju pochodzenia towarów, za które dokonywana jest płatność, zgodnie z oceną narażenia na naruszenie środków ograniczających.

41. Jeżeli ocena na naruszenie środków ograniczających uzasadnia taką konieczność dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów powinni rozważyć włączenie do swojego systemu wykorzystywanego do screeningu narzędzi geolokalizacyjnych i narzędzi wykrywających korzystanie z usług proxy w celu identyfikacji i uniemożliwienia adresom IP pochodzącym z kraju, wobec którego zastosowano środki ograniczające z uwagi na sytuację mającą wpływ na ten kraj, dostępu do strony internetowej i usług dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów w celu prowadzenia działalności zakazanej na mocy reżimów środków ograniczających.

42. Zgodnie z oceną narażenia na naruszenie środków ograniczających dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów mogą rozważyć zastosowanie szczególnych mechanizmów kontroli, takich jak:

a. przy nawiązywaniu stosunków gospodarczych, pozyskiwanie odpowiednich informacji o rodzaju działalności klienta i krajach, w których klient prowadzi działalność;
b. żądanie od klienta dodatkowych informacji, takich jak opis towarów podwójnego zastosowania lub towarów podlegających sektorowym środkom ograniczającym, informacji o odpowiedniej licencji na obrót towarami podwójnego zastosowania, kraju pochodzenia towarów, informacji o użytkowniku końcowym towarów;
c. żądanie od klienta bardziej szczegółowych informacji na temat celu transferu środków pieniężnych lub kryptoaktywów;
d. wykorzystanie następujących danych: rejestrów statków, rejestrów nieruchomości i innych publicznie dostępnych zbiorów danych (jeżeli są dostępne).

43. W przypadku gdy dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów korzystają z funkcji automatycznego odczytu informacji z dokumentów związanych z transferem środków pieniężnych lub kryptoaktywów, takich jak algorytmy optycznego rozpoznawania znaków lub weryfikacje stref przeznaczonych do odczytu maszynowego, powinni podjąć działania niezbędne w celu zapewnienia, że narzędzia te wychwytują informacje w sposób dokładny i spójny.

4.2.5 Środki należytej staranności mające na celu wykrywanie prób obchodzenia środków ograniczających

44. Dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów powinni być na bieżąco informowani o typologii i tendencjach w zakresie obchodzenia środków ograniczających. Odpowiednie źródła informacji, do których dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów powinni zawsze się odnosić, obejmują co najmniej sprawozdania udostępniane przez:

    a. odpowiednie organy krajowe właściwe do wdrażania środków ograniczających[15] lub krajowe organy nadzoru;
    b. jednostki analityki finansowej i organy ścigania;
    c. odpowiednie partnerstwa publiczno-prywatne na szczeblu krajowym lub unijnym;
    d. organy UE[16].

45. Strategie i procedury w zakresie należytej staranności powinny umożliwiać dostawcom usług płatniczych i dostawcom usług w zakresie kryptoaktywów wykrywanie potencjalnych prób obchodzenia środków ograniczających, takich jak próby:

    a. pomijania, usuwania lub zmiany informacji w komunikatach płatniczych;
    b. transfery kanałowe za pośrednictwem osób powiązanych z klientem podlegającym środkom ograniczającym;
    c. strukturyzowania transferów środków pieniężnych lub kryptoaktywów w celu ukrycia udziału wyznaczonej strony;
    d. ukrywania własności rzeczywistej lub kontroli nad aktywami;
    e. wykorzystywania podrobionych lub fałszywych dokumentów do transferu środków pieniężnych lub kryptoaktywów.

46. Dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów, którzy są szczególnie narażeni na ryzyko wykorzystania ich do obchodzenia środków, powinni również rozważyć przeprowadzenie zbiorczej analizy przepływów płatności do lub z państw objętych środkami ograniczającymi oraz państw, o których wiadomo, że są wykorzystywane do obchodzenia środków ograniczających.

[15] https://finance.ec.europa.eu/eu-and-world/sanctions-restrictive-measures/overview-sanctions-and-related-resources_en#contact.

[16] Zob. na przykład: https://finance.ec.europa.eu/news/sanctions-commission-publishes-guidance-help-european-operators-assess-sanctions-circumvention-risks-2023-09-07_en.

4.3 Środki polegające na zamrożeniu aktywów i środki sprawozdawcze

4.3.1 Zawieszenie realizacji transferów środków pieniężnych i zamrożenie środków finansowych

47. Dostawcy usług płatniczych powinni wprowadzić polityki i procedury umożliwiające niezwłoczne zawieszanie operacji uruchamiających alert o możliwym powiązaniu z wyznaczoną osobą lub podmiotem, lub podmiotem będącym własnością wyznaczonej osoby lub podmiotu, posiadanym lub kontrolowanym przez wyznaczoną osobę lub podmiot, lub którego beneficjentem rzeczywistym jest wyznaczona osoba.

48. Jeśli wewnętrzna analiza takiego alertu przeprowadzona przez dostawców usług płatniczych potwierdzi, że potencjalnym podmiotem dopasowanym jest wyznaczona osoba lub podmiot, lub podmiot będący własnością wyznaczonej osoby lub podmiotu, posiadany lub kontrolowany przez wyznaczoną osobę lub podmiot, lub którego beneficjentem rzeczywistym jest wyznaczona osoba, dostawcy usług płatniczych powinni niezwłocznie:

    a. zamrozić odpowiednie środki;
    b. wstrzymać realizację transferu środków pieniężnych, który stanowiłby naruszenie środków ograniczających.

4.3.2 Zamrożenie transferów kryptoaktywów

49. Dostawcy usług w zakresie kryptoaktywów powinni wprowadzić polityki i procedury, które w przypadku gdy wewnętrzna analiza alertu potwierdzi, że potencjalnym podmiotem dopasowanym jest wyznaczona osoba lub podmiot, lub podmiot będący własnością wyznaczonej osoby lub podmiotu, posiadany lub kontrolowany przez wyznaczoną osobę lub podmiot, lub którego beneficjentem rzeczywistym jest wyznaczona osoba, w celu natychmiastowego zamrożenia i zablokowania środków na rachunku przejściowym do czasu, aż odpowiedni organ krajowy właściwy do wdrażania środków ograniczających poinstruuje dostawcę usług w zakresie kryptoaktywów, jakie działania należy podjąć w odniesieniu do tych środków. Ostateczną odpowiedzialność za zgodność ze środkami ograniczającymi ponosi dostawca usług w zakresie kryptoaktywów.

4.3.3 Środki sprawozdawcze

50. Zgodnie z mającymi zastosowanie wymogami unijnymi i krajowymi dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów powinni posiadać jasne procedury umożliwiające zgłaszanie, niezwłocznie lub w określonym terminie, odpowiedniemu organowi krajowemu właściwemu do wdrażania środków ograniczających lub właściwemu organowi nadzorczemu:

    a. wszelkich działań podjętych w odniesieniu do konkretnego transferu związanego ze środkiem ograniczającym;
    b. wykrycie naruszenia środków ograniczających; oraz

c. realizację wszelkich transferów środków pieniężnych lub kryptoaktywów, które naruszają obowiązujące środki ograniczające poprzez udzielenie informacji na temat okoliczności, takich jak incydent w funkcjonowaniu systemu wykorzystywanego do screeningu w odniesieniu do takiego transferu.

51. W przypadku podejrzenia możliwego obejścia środków ograniczających lub wykrycia próby transferu środków pieniężnych lub kryptoaktywów przez osobę fizyczną, osobę prawną podmiot lub organ albo do osoby fizycznej, osoby prawnej, podmiotu lub organu, dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów powinni:

    a. zgłosić je właściwemu organowi krajowemu odpowiedzialnemu za wdrażanie środków ograniczających, jeżeli jest to wyraźnie wymagane przez właściwe rozporządzenie UE w sprawie środków ograniczających;
    b. zgłosić podejrzaną transakcję, jeżeli jest to wymagane na mocy obowiązujących przepisów.

4.3.4 Procedury dotyczące wyłączeń lub zniesienia środków ograniczających

52. Dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów powinni posiadać polityki i procedury pozwalające ustalić, czy mają zastosowanie wyłączenia, systemy licencyjne lub odstępstwa, a jeśli mają zastosowanie, jak postępować, aby zachować zgodność z obowiązującym prawem Unii lub prawem krajowym. Dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów powinni określić w swoich politykach i procedurach, jakie informacje udostępnią klientom chcącym wystąpić o odstępstwo w celu wykorzystania zamrożonych środków, jeżeli takie odstępstwo jest dozwolone na mocy obowiązujących przepisów prawnych. Informacje te powinny obejmować informacje o prawach klienta w takiej sytuacji.

53. Dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów powinni wprowadzić polityki i procedury określające działania dotyczące środków i kryptoaktywów podlegających szczególnym środkom ograniczającym po zniesieniu takiego środka.

4.4 Zapewnienie skuteczności polityk, procedur i systemów wykorzystywanych do screeningu w zakresie środków ograniczających

54. Aby środki ograniczające stosowane przez dostawcę usług płatniczych i dostawcę usług w zakresie kryptoaktywów były skuteczne, polityki, procedury i systemy wykorzystywane do screeningu powinny umożliwiać:

    a. niezawodne wykrywanie potwierdzonych dopasowań;
    b. po potwierdzeniu dopasowań, bezzwłoczne zawieszenie realizacji wszelkich transferów środków, zablokowanie wszelkich nadchodzących transferów i zdeponowanie ich na rachunku przejściowym, zamrożenie środków lub kryptoaktywów oraz zgłoszenie

takich działań odpowiedniemu organowi krajowemu właściwemu do wdrażania środków ograniczających w celu uzyskania dalszych instrukcji;

c. zgłoszenie zamrożonych aktywów odpowiednim organom krajowym właściwym do wdrażania środków ograniczających lub właściwemu organowi nadzorczemu zgodnie z wymogami obowiązujących przepisów niezwłocznie lub w terminach określonych w obowiązujących przepisach prawa Unii lub prawa krajowego;
d. zgłoszenie podejrzenia obejścia środków ograniczających lub próby obejścia środków ograniczających odpowiedniemu organowi krajowemu właściwemu do wdrażania środków ograniczających lub krajowej jednostce analityki finansowej, jeżeli jest to wymagane na mocy obowiązujących przepisów prawa.

55. Dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów powinni regularnie sprawdzać ustawienia swoich systemów wykorzystywanych do screeningu w celu stwierdzenia, czy system pozostaje odpowiedni w świetle oceny narażenia dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów na naruszenie środków ograniczających oraz czy pozostaje skuteczny. Dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów powinni określić częstotliwość tych testów w oparciu o ocenę narażenia na naruszenie środków ograniczających i uwzględniać ją w swoich politykach i procedurach.

56. W ramach testowania swojego systemu wykorzystywanego do screeningu dostawcy usług płatniczych i dostawcy usług w zakresie kryptoaktywów powinni:

a. przetestować kalibrację systemu wykorzystywanego do screeningu zgodnie z sekcją 4.1.6;
b. ocenić dokładność zarządzania listą przy użyciu obowiązujących i aktualnych środków ograniczających;
c. ocenić, czy wszyscy klienci oraz transfery środków i kryptoaktywów są weryfikowane, gdy jest to wymagane;
d. ocenić adekwatność i przydatność pól informacyjnych wykorzystywanych w systemie wykorzystywanym do screeningu, takich jak zakres transferów środków pieniężnych lub kryptoaktywów wprowadzanych do systemu weryfikacji;
e. ocenić terminowość automatycznego zawieszenia operacji;
f. ocenić, czy procesy i zasoby dostępne na potrzeby analizy alertów umożliwiają szybkie zgłaszanie potwierdzonych dopasowań.

57. Dostawcy usług płatniczych i dostawcy usług zakresie kryptoaktywów powinni poinformować organ zarządzający o istotnych słabościach lub brakach w systemie wykorzystywanym do screeningu oraz niezwłocznie podjąć działania naprawcze.