KOMISJA
EUROPEJSKA

Bruksela, dnia 13.3.2024 r.
C(2024) 1532 final

ROZPORZĄDZENIE DELEGOWANE KOMISJI (UE) …/…

z dnia 13.3.2024 r.

uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 w odniesieniu do regulacyjnych standardów technicznych określających narzędzia, metody, procesy i polityki zarządzania ryzykiem związanym z ICT oraz uproszczone ramy zarządzania ryzykiem związanym z ICT

(Tekst mający znaczenie dla EOG)

UZASADNIENIE

1. KONTEKST AKTU DELEGOWANEGO

Jednym z celów rozporządzenia (UE) 2022/2554 w sprawie operacyjnej odporności cyfrowej sektora finansowego (DORA) jest ustanowienie jednolitych wymogów dotyczących bezpieczeństwa sieci i systemów informatycznych przedsiębiorstw i organizacji działających w sektorze finansowym. Tworzy ono zatem ramy regulacyjne w zakresie operacyjnej odporności cyfrowej, zgodnie z którymi wszystkie podmioty finansowe muszą upewnić się, że są w stanie przetrwać wszelkiego rodzaju zakłócenia i zagrożenia związane z technologiami informacyjno-komunikacyjnymi (ICT), reagować na nie i odzyskiwać sprawność po ich wystąpieniu. Wymogi te są jednolite w całej UE, a ich celem jest zapobieganie cyberzagrożeniom i łagodzenie ich skutków.

W związku z tym zgodnie z art. 15 akapit czwarty DORA „EUN, za pośrednictwem Wspólnego Komitetu i w porozumieniu z ENISA, opracowują wspólne projekty regulacyjnych standardów technicznych" w celu zapewnienia dalszej harmonizacji narzędzi, metod, procesów i polityk zarządzania ryzykiem związanym z ICT oraz, zgodnie z art. 16, opracowania uproszczonych ram zarządzania ryzykiem związanym z ICT w odniesieniu do niektórych podmiotów finansowych. ENISA wchodzi zatem w skład Podkomitetu ds. Operacyjnej Odporności Cyfrowej funkcjonującego w ramach Wspólnego Komitetu Europejskich Urzędów Nadzoru (JC SC DOR).

Niniejsze rozporządzenie delegowane odpowiada temu mandatowi i zostało przekazane Komisji 17 stycznia 2024 r.

2. KONSULTACJE PRZEPROWADZONE PRZED PRZYJĘCIEM AKTU

W ramach opracowywania standardów określonych w niniejszym projekcie rozporządzenia 19 czerwca 2023 r. EUN opublikowały projekt regulacyjnych standardów technicznych na potrzeby trzymiesięcznego okresu konsultacji, który zakończył się 11 września 2023 r. EUN otrzymały 120 odpowiedzi od różnych uczestników rynku z całego sektora finansowego. Sprawozdanie końcowe EUN zawiera pełny przegląd odpowiedzi udzielonych przez zainteresowane strony[1].

Respondenci biorący udział w konsultacjach publicznych przedstawili uwagi na temat następujących aspektów proponowanego projektu regulacyjnych standardów technicznych:

- wezwania do przedłużenia terminu wdrożenia;
- wezwania do zapewnienia większej proporcjonalności (np. proporcjonalności w obu kierunkach, tj. uwzględnienia zarówno zwiększonej, jak i ograniczonej złożoności oraz zwiększonego i ograniczonego ryzyka); bardziej sektorowego podejścia uwzględniającego większą proporcjonalność np. w odniesieniu do zakładów ubezpieczeń, ...);
- wezwania do wyłączenia z projektu regulacyjnych standardów technicznych aspektów związanych z zarządzaniem, ponieważ wydają się one wykraczać poza mandat; oraz

[1] Europejskie Urzędy Nadzoru (2024 r.), „Sprawozdanie końcowe w sprawie projektów regulacyjnych standardów technicznych w celu dalszej harmonizacji narzędzi, metod, procesów i polityk zarządzania ryzykiem związanym z ICT zgodnie z art. 15 i 16 ust. 3 rozporządzenia (UE) 2022/2554".

- wezwania do nieuwzględniania dodatkowych środków dotyczących zasobów chmury obliczeniowej.

W świetle otrzymanych uwag EUN wprowadziły zmiany do projektu regulacyjnych standardów technicznych. Zmiany te dotyczyły m.in. wprowadzenia większej proporcjonalności, usunięcia artykułu dotyczącego zarządzania z ogólnych wymogów systemowych oraz doprecyzowania przepisów, zwłaszcza tych zawartych w artykułach dotyczących bezpieczeństwa sieci, szyfrowania, kontroli dostępu i aspektów ciągłości działania. EUN opowiedziały się przeciwko włączeniu elementów dotyczących chmury obliczeniowej w celu zapewnienia zgodności z zasadą neutralności technologicznej. Zamiast tego EUN zdecydowały się rozszerzyć zakres rozpatrywanych wymogów tak, aby obejmowały one ogólnie zasoby ICT lub usługi ICT świadczone przez zewnętrznych dostawców usług ICT. W odniesieniu do terminów wdrożenia EUN nie rozważyły jednak żadnych zmian, ponieważ są one określone na poziomie 1 DORA.

3. ASPEKTY PRAWNE AKTU DELEGOWANEGO

W tytule I rozdział I ustanowiono główne zasady i elementy, które należy uwzględnić przy opracowywaniu i wdrażaniu polityk, procedur, protokołów i narzędzi w zakresie bezpieczeństwa ICT (art. 1).

W tytule II rozdział II określono warunki dalszej harmonizacji narzędzi, metod, procesów i polityk zarządzania ryzykiem związanym z ICT przez ustanowienie: ogólnych elementów polityk, procedur, protokołów i narzędzi w zakresie bezpieczeństwa ICT (sekcja 1); szczegółowych elementów polityk, procedur, protokołów i narzędzi w zakresie bezpieczeństwa ICT (sekcja 2); poziomu tolerancji ryzyka, metod przeprowadzania oceny ryzyka związanego z ICT, środków traktowania ryzyka związanego z ICT; polityki zarządzania zasobami ICT (sekcja 3); polityki w zakresie mechanizmów kontroli szyfrowania i kryptograficznej (sekcja 4); polityki bezpieczeństwa operacji ICT (sekcja 5); polityki zarządzania bezpieczeństwem sieci (sekcja 6); polityki zarządzania projektami ICT (sekcja 7); polityki bezpieczeństwa fizycznego i środowiskowego mająca na celu zachowanie dostępności, autentyczności, integralności i poufności danych (sekcja 8). W rozdziale II określono wszystkie elementy bezpieczeństwa ICT, które podmioty finansowe powinny uwzględnić przy opracowywaniu swoich polityk w zakresie zasobów ludzkich i kontroli dostępu. W rozdziale III określono wszystkie elementy polityki wykrywania incydentów związanych z ICT i reagowania na nie, które podmioty finansowe powinny opracować i wdrożyć. W rozdziale IV określono treść i format sprawozdania z przeglądu ram zarządzania ryzykiem związanym z ICT, które podmioty finansowe mają obowiązek sporządzić i przedłożyć.

W tytule III określono uproszczone ramy zarządzania ryzykiem związanym z ICT koncentrując się na ustanowieniu ram zarządzania i kontroli (rozdział I); ustanowieniu mechanizmu dostępu i kontroli oraz wymogów w tym zakresie (rozdział II); ustanowieniu planu ciągłości działania w zakresie ICT (rozdział III); oraz określeniu treści i formatu sprawozdania z przeglądu ram zarządzania ryzykiem związanym z ICT, które podmioty finansowe mają obowiązek sporządzić i przedłożyć (rozdział IV).

Tytuł IV zawiera przepisy końcowe dotyczące wejścia w życie (art. 42).

ROZPORZĄDZENIE DELEGOWANE KOMISJI (UE) …/…

z dnia 13.3.2024 r.

uzupełniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 w odniesieniu do regulacyjnych standardów technicznych określających narzędzia, metody, procesy i polityki zarządzania ryzykiem związanym z ICT oraz uproszczone ramy zarządzania ryzykiem związanym z ICT

(Tekst mający znaczenie dla EOG)

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając 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[2], w szczególności jego art. 15 akapit czwarty, i art. 16 ust. 3 akapit czwarty,

a także mając na uwadze, co następuje:

(1) Rozporządzenie (UE) 2022/2554 obejmuje szeroki zakres podmiotów finansowych, które różnią się pod względem wielkości, struktury, organizacji wewnętrznej oraz charakteru i stopnia złożoności realizowanych przez nie działań, w związku z czym charakteryzują się większymi lub mniejszymi elementami złożoności lub ryzyka. Aby zapewnić należyte uwzględnienie tej różnorodności, wszelkie wymogi dotyczące polityk, procedur, protokołów i narzędzi w zakresie bezpieczeństwa ICT oraz uproszczonych ram zarządzania ryzykiem związanym z ICT powinny być proporcjonalne do wielkości, struktury, organizacji wewnętrznej, charakteru i złożoności tych podmiotów finansowych oraz do odpowiadających im ryzyk.

(2) Z tego samego powodu podmioty finansowe objęte rozporządzeniem (UE) 2022/2554 powinny mieć pewną elastyczność pod względem sposobu, w jaki spełniają wszelkie wymogi dotyczące polityk, procedur, protokołów i narzędzi w zakresie bezpieczeństwa ICT oraz wszelkich uproszczonych ram zarządzania ryzykiem związanym z ICT. W związku z tym podmioty finansowe powinny mieć możliwość korzystania z posiadanej już dokumentacji w celu spełnienia wszelkich wymogów dotyczących dokumentacji wynikających z wyżej wymienionych wymogów. Wynika z tego, że opracowanie, udokumentowanie i wdrożenie określonych polityk w zakresie bezpieczeństwa ICT powinno być wymagane tylko w odniesieniu do niektórych istotnych elementów, z uwzględnieniem między innymi wiodących praktyk i standardów branżowych. Należy ponadto opracować, udokumentować i wdrożyć

[2] 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 (Dz.U. L 333 z 27.12.2022, s. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

procedury bezpieczeństwa ICT w celu uwzględnienia konkretnych technicznych aspektów wdrażania, w tym zarządzania pojemnością i wydajnością, zarządzania podatnościami i poprawkami, bezpieczeństwa danych i systemów oraz rejestrowania.

(3) W celu zapewnienia prawidłowego wdrożenia w czasie polityk, procedur, protokołów i narzędzi w zakresie bezpieczeństwa ICT, o których mowa w tytule II rozdział I niniejszego rozporządzenia, ważne jest, aby podmioty finansowe prawidłowo przypisywały i utrzymywały wszelkie zadania i obowiązki związane z bezpieczeństwem ICT oraz aby określiły konsekwencje nieprzestrzegania polityk lub procedur w zakresie bezpieczeństwa ICT.

(4) Aby ograniczyć ryzyko konfliktu interesów, podmioty finansowe powinny zapewnić podział obowiązków przy przydzielaniu zadań i obowiązków w zakresie ICT.

(5) Aby zapewnić elastyczność i uprościć ramy kontroli podmiotów finansowych, nie należy wymagać od podmiotów finansowych opracowywania szczegółowych przepisów dotyczących konsekwencji nieprzestrzegania polityk, procedur i protokołów w zakresie bezpieczeństwa ICT, o których mowa w tytule II rozdział I niniejszego rozporządzenia, w przypadku gdy takie przepisy są już określone w innej polityce lub procedurze.

(6) W dynamicznym środowisku, w którym ryzyko związane z ICT stale się zmienia, ważne jest, aby podmioty finansowe opracowały swój zestaw polityk w zakresie bezpieczeństwa ICT w oparciu o wiodące praktyki oraz, w stosownych przypadkach, normy w rozumieniu art. 2 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1025/2012[3]. Dzięki temu podmioty finansowe, o których mowa w tytule II niniejszego rozporządzenia, będą miały dostęp do aktualnych informacji i będą przygotowane na zmieniające się okoliczności.

(7) Aby zapewnić operacyjną odporność cyfrową, podmioty finansowe, o których mowa w tytule II niniejszego rozporządzenia, powinny – w ramach swoich polityk, procedur, protokołów i narzędzi w zakresie bezpieczeństwa ICT – opracować i wdrożyć politykę zarządzania zasobami ICT, procedury zarządzania pojemnością i wydajnością oraz polityki i procedury dotyczące operacji ICT. Te polityki i procedury są niezbędne do zapewnienia monitorowania stanu zasobów ICT przez cały ich cykl życia, tak aby aktywa te były efektywnie wykorzystywane i utrzymywane (zarządzanie zasobami ICT). Te polityki i procedury powinny również zapewniać optymalizację działania systemów ICT oraz zgodność wyników systemów ICT i ich zdolności z ustalonymi celami biznesowymi i celami w zakresie bezpieczeństwa informacji (zarządzanie pojemnością i wydajnością). Ponadto te polityki i procedury powinny zapewniać skuteczne i sprawne codzienne zarządzanie systemami ICT oraz ich działanie (operacje ICT), co pozwoli zminimalizować ryzyko utraty poufności, integralności i dostępności danych. Te polityki i procedury są zatem niezbędne do zapewnienia bezpieczeństwa sieci oraz odpowiednich zabezpieczeń przed włamaniami i wykorzystaniem danych niezgodnie z przeznaczeniem, a także do zachowania dostępności, autentyczności, integralności i poufności danych.

---

[3] Rozporządzenie (UE) nr 1025/2012 Parlamentu Europejskiego i Rady (UE) z dnia 25 października 2012 r. w sprawie normalizacji europejskiej, zmieniające dyrektywy Rady 89/686/EWG i 93/15/EWG oraz dyrektywy Parlamentu Europejskiego i Rady 94/9/WE, 94/25/WE, 95/16/WE, 97/23/WE, 98/34/WE, 2004/22/WE, 2007/23/WE, 2009/23/WE i 2009/105/WE oraz uchylające decyzję Rady 87/95/EWG i decyzję Parlamentu Europejskiego i Rady nr 1673/2006/WE (Dz.U. L 316 z 14.11.2012, s. 12, ELI: https://eur-lex.europa.eu/eli/reg/2012/1025/oj?locale=pl).

(8) Aby zapewnić właściwe zarządzanie ryzykiem związanym z dotychczasowymi systemami ICT, podmioty finansowe powinny rejestrować i monitorować daty końcowe usług wsparcia świadczonych przez strony trzecie w zakresie ICT. Ze względu na potencjalny wpływ, jaki może mieć utrata poufności, integralności i dostępności danych, przy rejestrowaniu i monitorowaniu tych dat końcowych podmioty finansowe powinny skupić się na tych zasobach lub systemach ICT, które mają kluczowe znaczenie dla działalności gospodarczej.

(9) Mechanizmy kontroli kryptograficznej mogą zapewnić dostępność, autentyczność, integralność i poufność danych. Podmioty finansowe, o których mowa w tytule II niniejszego rozporządzenia, powinny zatem określać i wdrażać takie kontrole, stosując podejście oparte na analizie ryzyka. W tym celu podmioty finansowe powinny szyfrować odpowiednie dane, gdy są przechowywane, przesyłane lub, w stosownych przypadkach, wykorzystywane, na podstawie wyników dwutorowego procesu, obejmującego klasyfikację danych i kompleksową ocenę ryzyka związanego z ICT. Biorąc pod uwagę złożony charakter szyfrowania danych wykorzystywanych, podmioty finansowe, o których mowa w tytule II niniejszego rozporządzenia, powinny szyfrować wykorzystywane dane tylko wtedy, gdy jest to właściwe w kontekście wyników oceny ryzyka związanego z ICT. Podmioty finansowe, o których mowa w tytule II niniejszego rozporządzenia, powinny jednak mieć możliwość, w przypadku gdy szyfrowanie danych wykorzystywanych nie jest wykonalne lub jest zbyt skomplikowane, ochrony poufności, integralności i dostępności danych za pomocą innych środków w zakresie bezpieczeństwa ICT. Biorąc pod uwagę szybki rozwój technologiczny w dziedzinie technik kryptograficznych, podmioty finansowe, o których mowa w tytule II niniejszego rozporządzenia, powinny na bieżąco śledzić istotne zmiany w obszarze analizy kryptograficznej oraz uwzględniać wiodące praktyki i normy. Podmioty finansowe, o których mowa w tytule II niniejszego rozporządzenia, powinny zatem stosować elastyczne podejście oparte na ograniczaniu i monitorowaniu ryzyka, aby radzić sobie z dynamicznym krajobrazem zagrożeń kryptograficznych, w tym zagrożeń wynikających z postępów informatyki kwantowej.

(10) Bezpieczeństwo operacji ICT oraz polityki, procedury, protokoły i narzędzia operacyjne są niezbędne do zapewnienia poufności, integralności i dostępności danych. Jednym z kluczowych aspektów jest bezwzględne oddzielenie środowisk produkcyjnych ICT od środowisk, w których systemy ICT są opracowywane i testowane, lub od innych środowisk niezwiązanych z produkcją. Takie oddzielenie powinno służyć jako ważny środek bezpieczeństwa ICT zapobiegający niezamierzonemu i nieuprawnionemu dostępowi do danych oraz ich modyfikowaniu i usuwaniu w środowisku produkcyjnym, co mogłoby skutkować poważnymi zakłóceniami w działalności podmiotów finansowych, o których mowa w tytule II niniejszego rozporządzenia. Biorąc jednak pod uwagę obecne praktyki w zakresie opracowywania systemów ICT, w wyjątkowych okolicznościach podmioty finansowe powinny mieć możliwość testowania w środowiskach produkcyjnych, pod warunkiem że uzasadnią takie testy i uzyskają wymagane zatwierdzenie.

(11) Szybko zmieniający się charakter krajobrazów ICT, podatności w obszarze ICT oraz cyberzagrożeń wymaga proaktywnego i kompleksowego podejścia do identyfikowania, oceny i eliminowania podatności w zakresie ICT. Bez takiego podejścia podmioty finansowe, ich klienci, użytkownicy lub kontrahenci mogą być poważnie narażeni na ryzyko zagrażające ich operacyjnej odporności cyfrowej, bezpieczeństwu ich sieci oraz dostępności, autentyczności, integralności i poufności danych, które polityka i procedury w zakresie bezpieczeństwa ICT powinny chronić.

Podmioty finansowe, o których mowa w tytule II niniejszego rozporządzenia, powinny zatem identyfikować i usuwać podatności w swoim środowisku ICT, a zarówno podmioty finansowe, jak i ich zewnętrzni dostawcy usług ICT powinni przestrzegać spójnych, przejrzystych i odpowiedzialnych ram zarządzania podatnościami. Z tego samego powodu podmioty finansowe powinny monitorować podatności w obszarze ICT przy użyciu wiarygodnych zasobów i zautomatyzowanych narzędzi poprzez sprawdzanie, czy zewnętrzni dostawcy usług ICT zapewniają szybkie działania wobec podatności w obszarze świadczonych usług ICT.

(12) Zarządzanie poprawkami powinno być istotnym elementem tych polityk i procedur w zakresie bezpieczeństwa ICT, które poprzez testowanie i wdrażanie w kontrolowanym środowisku mają na celu usunięcie stwierdzonych podatności i zapobieganie zakłóceniom wynikającym z instalacji poprawek.

(13) Aby zapewnić terminowe i przejrzyste informacje o potencjalnych zagrożeniach bezpieczeństwa, które mogą mieć wpływ na podmiot finansowy i jego interesariuszy, podmioty finansowe powinny ustanowić procedury odpowiedzialnego ujawniania podatności w obszarze ICT klientom, kontrahentom i ogółowi społeczeństwa. Przy ustanawianiu tych procedur podmioty finansowe powinny uwzględniać czynniki, w tym wagę podatności, potencjalny wpływ takiej podatności na interesariuszy oraz gotowość do wprowadzenia środków naprawczych lub łagodzących.

(14) Aby umożliwić przydzielanie praw dostępu użytkowników, podmioty finansowe, o których mowa w tytule II niniejszego rozporządzenia, powinny ustanowić solidne środki służące zapewnieniu jednoznacznej identyfikacji osób i systemów, które będą miały dostęp do informacji podmiotu finansowego. Niezastosowanie się do tego wymogu naraziłoby podmioty finansowe na potencjalny nieuprawniony dostęp, naruszenie danych i nieuczciwe działania, co z kolei stanowiłoby zagrożenie dla poufności, integralności i dostępności wrażliwych danych finansowych. Chociaż korzystanie z kont generycznych lub współdzielonych powinno być wyjątkowo dozwolone w okolicznościach określonych przez podmioty finansowe, podmioty finansowe powinny zapewnić, aby odpowiedzialność za działania podejmowane za pośrednictwem tych kont była zachowana. Bez takiego zabezpieczenia potencjalni złośliwi użytkownicy mogliby utrudniać działania dochodzeniowe i naprawcze, przez co podmioty finansowe byłyby narażone na zagrożenia związane z niewykrytymi złośliwymi działaniami lub na kary za nieprzestrzeganie przepisów.

(15) Aby przygotować się na gwałtowne zmiany w środowiskach ICT, podmioty finansowe, o których mowa w tytule II niniejszego rozporządzenia, powinny wdrożyć solidne polityki i procedury zarządzania projektami ICT służące utrzymaniu dostępności, autentyczności, integralności i poufności danych. W tych politykach i procedurach zarządzania projektami ICT należy określić elementy niezbędne do skutecznego zarządzania projektami ICT, w tym zmianami, pozyskiwaniem, utrzymaniem i rozwojem systemów ICT danego podmiotu finansowego, niezależnie od metodyki zarządzania projektami ICT wybranej przez ten podmiot finansowy. W kontekście tych polityk i procedur podmioty finansowe powinny przyjąć praktyki i metody testowania, które odpowiadają ich potrzebom, a jednocześnie stosować podejście oparte na analizie ryzyka i zapewniać utrzymanie bezpiecznego, niezawodnego i odpornego środowiska ICT. W celu zagwarantowania bezpiecznego wdrożenia projektu ICT podmioty finansowe powinny zapewnić, aby pracownicy reprezentujący określone sektory biznesowe lub funkcje, na które dany projekt ICT ma wpływ, mogli zapewniać niezbędne informacje i wiedzę specjalistyczną. Aby zapewnić skuteczny nadzór, organowi zarządzającemu należy przedkładać

sprawozdania dotyczące projektów ICT, w szczególności projektów, które mają wpływ na krytyczne lub istotne funkcje oraz na temat związanego z nimi ryzyka. Podmioty finansowe powinny dostosować częstotliwość i stopień szczegółowości systematycznych i bieżących przeglądów i sprawozdań do znaczenia i wielkości odnośnych projektów ICT.

(16) Konieczne jest zapewnienie, aby pakiety oprogramowania pozyskiwane i opracowywane przez podmioty finansowe, o których mowa w tytule II niniejszego rozporządzenia, były skutecznie i bezpiecznie integrowane z istniejącym środowiskiem ICT, zgodnie z ustalonymi celami biznesowymi i celami w zakresie bezpieczeństwa informacji. Podmioty finansowe powinny zatem szczegółowo oceniać takie pakiety oprogramowania. W tym celu oraz w celu zidentyfikowania podatności i potencjalnych luk w zakresie bezpieczeństwa zarówno w pakietach oprogramowania, jak i w szerszych systemach ICT podmioty finansowe powinny przeprowadzać testy bezpieczeństwa ICT. Aby ocenić integralność oprogramowania i upewnić się, że korzystanie z tego oprogramowania nie wiąże się z ryzykiem dla bezpieczeństwa ICT, podmioty finansowe powinny również dokonywać przeglądu kodów źródłowych pozyskanego oprogramowania, w tym, w miarę możliwości, oprogramowania zamkniętego dostarczonego przez zewnętrznych dostawców usług ICT, przy użyciu zarówno statycznych, jak i dynamicznych metod testowania.

(17) Zmiany, niezależnie od ich skali, wiążą się z nieodłącznym ryzykiem i mogą stwarzać znaczące ryzyko utraty poufności, integralności i dostępności danych, a tym samym mogą prowadzić do poważnych zakłóceń działalności gospodarczej. Aby zabezpieczyć podmioty finansowe przed potencjalnymi podatnościami i słabościami w obszarze ICT, które mogłyby narazić je na znaczne ryzyko, konieczny jest rygorystyczny proces weryfikacji w celu potwierdzenia, że wszystkie zmiany spełniają niezbędne wymogi bezpieczeństwa ICT. Podmioty finansowe, o których mowa w tytule II niniejszego rozporządzenia, powinny zatem, jako zasadniczy element swoich polityk i procedur w zakresie bezpieczeństwa ICT, wdrożyć solidne polityki i procedury zarządzania zmianą w systemach ICT. Aby utrzymać obiektywność i skuteczność procesu zarządzania zmianą w systemach ICT, zapobiegać konfliktom interesów oraz zapewnić obiektywną ocenę zmian w systemach ICT, konieczne jest oddzielenie funkcji odpowiedzialnych za zatwierdzanie tych zmian od funkcji odpowiedzialnych za wnioskowanie o te zmiany i ich wdrażanie. Aby osiągnąć skuteczne przemiany, kontrolowane wdrażanie zmian w systemach ICT i minimalne zakłócenia w działaniu systemów ICT, podmioty finansowe powinny przypisać jasne zadania i obowiązki, które zapewnią, aby zmiany w systemach ICT były planowane i odpowiednio testowane oraz aby zagwarantowana była ich jakość. Aby zapewnić dalsze skuteczne działanie systemów ICT oraz mechanizmy zabezpieczające dla podmiotów finansowych, powinny one również opracować i wdrożyć procedury awaryjne. Podmioty finansowe powinny jasno określić te procedury awaryjne i przypisać obowiązki, aby zapewnić szybkie i skuteczne reagowanie w przypadku nieudanych zmian ICT.

(18) Aby wykrywać incydenty związane z ICT, zarządzać nimi i je zgłaszać, podmioty finansowe, o których mowa w tytule II niniejszego rozporządzenia, powinny ustanowić politykę dotyczącą incydentów związanych z ICT obejmującą elementy procesu zarządzania incydentami związanymi z ICT. W tym celu podmioty finansowe powinny określić wszystkie odpowiednie osoby kontaktowe wewnątrz organizacji i poza nią, które mogą ułatwić prawidłową koordynację i realizację różnych etapów tego procesu. Aby zoptymalizować wykrywanie incydentów związanych z ICT

i reagowanie na nie, a także aby określić tendencje związane z tymi incydentami, które są cennym źródłem informacji umożliwiającym podmiotom finansowym określenie podstawowych przyczyn i problemów oraz zajęcie się nimi w skuteczny sposób, podmioty finansowe powinny w szczególności szczegółowo przeanalizować incydenty związane z ICT, które uważają za najbardziej znaczące, między innymi ze względu na ich regularne powtarzanie się.

(19) Aby zagwarantować wczesne i skuteczne wykrywanie nietypowych działań, podmioty finansowe, o których mowa w tytule II niniejszego rozporządzenia, powinny gromadzić, monitorować i analizować różne źródła informacji oraz przydzielać związane z tym zadania i obowiązki. Jeżeli chodzi o wewnętrzne źródła informacji, rejestry są niezwykle istotnym źródłem, ale podmioty finansowe nie powinny opierać się wyłącznie na rejestrach. Zamiast tego podmioty finansowe powinny uwzględniać szerszy zakres informacji, w tym informacje zgłaszane w ramach innych funkcji wewnętrznych, ponieważ funkcje te są często cennym źródłem istotnych informacji. Z tego samego powodu podmioty finansowe powinny analizować i monitorować informacje gromadzone ze źródeł zewnętrznych, w tym informacje dostarczane przez zewnętrznych dostawców usług ICT na temat incydentów mających wpływ na ich systemy i sieci, a także z innych źródeł informacji, które podmioty finansowe uznają za istotne. W zakresie, w jakim takie informacje stanowią dane osobowe, zastosowanie mają unijne przepisy o ochronie danych. Dane osobowe powinny być ograniczone do tego, co jest niezbędne do wykrywania incydentów.

(20) Aby ułatwić wykrywanie incydentów związanych z ICT, podmioty finansowe powinny przechowywać dowody dotyczące takich incydentów. Aby zapewnić, z jednej strony, przechowywanie takich dowodów przez wystarczająco długi czas, a z drugiej strony uniknąć nadmiernego obciążenia regulacyjnego, podmioty finansowe powinny określić okres przechowywania, biorąc pod uwagę, między innymi, krytyczność danych i wymogi dotyczące przechowywania wynikające z prawa Unii.

(21) Aby zapewnić terminowe wykrywanie incydentów związanych z ICT, podmioty finansowe, o których mowa w tytule II niniejszego rozporządzenia, powinny traktować określone kryteria służące uruchamianiu procesów wykrywania incydentów związanych z ICT i reagowania na nie jako niewyczerpujące. Ponadto, chociaż podmioty finansowe powinny brać pod uwagę wszystkie te kryteria, okoliczności opisane w kryteriach nie muszą występować jednocześnie, a znaczenie usług ICT, na które incydenty mają wpływ, powinno być odpowiednio uwzględniane w celu uruchomienia procesów wykrywania incydentów związanych z ICT i reagowania na nie.

(22) Przy opracowywaniu strategii na rzecz ciągłości działania w zakresie ICT podmioty finansowe, o których mowa w tytule II niniejszego rozporządzenia, powinny uwzględniać podstawowe elementy zarządzania ryzykiem związanym z ICT, w tym strategie zarządzania incydentami związanymi z ICT i informowania o nich, proces zarządzania zmianą w systemach ICT oraz ryzyko związane z zewnętrznymi dostawcami usług ICT.

(23) Konieczne jest określenie zestawu scenariuszy, które podmioty finansowe, o których mowa w tytule II niniejszego rozporządzenia, powinny uwzględnić zarówno przy wdrażaniu planów reagowania i przywracania sprawności ICT, jak i przy testowaniu planów ciągłości działania w zakresie ICT. Scenariusze te powinny służyć podmiotom finansowym jako punkt wyjścia do analizy zarówno istotności i prawdopodobieństwa

wystąpienia poszczególnych scenariuszy, jak i potrzeby opracowania scenariuszy alternatywnych. Podmioty finansowe powinny skupić się na tych scenariuszach, w przypadku których inwestycje w środki zwiększające odporność mogłyby być bardziej wydajne i skuteczne. Poprzez testowanie przełączania się z głównej infrastruktury ICT na nadmiarowe zdolności w zakresie ICT, kopie zapasowe i urządzenia redundantne instytucje finansowe powinny ocenić, czy te zdolności, kopie zapasowe i urządzenia funkcjonują skutecznie przez wystarczający okres, oraz zapewnić przywrócenie normalnego funkcjonowania podstawowej infrastruktury ICT zgodnie z celami związanymi z przywracaniem sprawności.

(24) Konieczne jest ustanowienie wymogów dotyczących ryzyka operacyjnego, a w szczególności wymogów dotyczących zarządzania projektami ICT i zmianą w systemach ICT oraz zarządzania ciągłością działania w zakresie ICT w oparciu o wymogi, które mają już zastosowanie do kontrahentów centralnych, centralnych depozytów papierów wartościowych i systemów obrotu na mocy, odpowiednio, rozporządzeń Parlamentu Europejskiego i Rady (UE) nr 648/2012[4], (UE) nr 600/2014[5] i (UE) nr 909/2014[6].

(25) W art. 6 ust. 5 rozporządzenia (UE) 2022/2554 nałożono na podmioty finansowe obowiązek dokonania przeglądu swoich ram zarządzania ryzykiem związanym z ICT oraz przedstawienia właściwemu organowi sprawozdania z tego przeglądu. Aby umożliwić właściwym organom łatwe przetwarzanie informacji zawartych w tych sprawozdaniach oraz zagwarantować odpowiednie przekazywanie tych informacji, podmioty finansowe powinny przekazywać te zgłoszenia w formacie elektronicznym umożliwiającym wyszukiwanie.

(26) Wymogi dotyczące podmiotów finansowych podlegających uproszczonym ramom zarządzania ryzykiem związanym z ICT, o których mowa w art. 16 rozporządzenia (UE) 2022/2554, powinny koncentrować się na tych kluczowych obszarach i elementach, które w świetle skali, ryzyka, wielkości i stopnia złożoności tych podmiotów finansowych stanowią niezbędne minimum do zapewnienia poufności, integralności, dostępności i autentyczności danych i usług tych podmiotów finansowych. W tym kontekście te podmioty finansowe powinny posiadać ramy zarządzania wewnętrznego i kontroli, w których określone zostaną jasne obowiązki, aby umożliwić stosowanie skutecznych i należytych ram zarządzania ryzykiem. Ponadto, aby zmniejszyć obciążenie administracyjne i operacyjne, te podmioty finansowe powinny opracować i udokumentować tylko jedną politykę, tj. politykę bezpieczeństwa informacji, określającą ogólne zasady i przepisy niezbędne do ochrony poufności, integralności, dostępności i autentyczności danych i usług świadczonych przez te podmioty finansowe.

---

[4] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 z dnia 4 lipca 2012 r. w sprawie instrumentów pochodnych będących przedmiotem obrotu poza rynkiem regulowanym, kontrahentów centralnych i repozytoriów transakcji (Dz.U. L 201 z 27.7.2012, s. 1, ELI: http://data.europa.eu/eli/reg/2012/648/oj).

[5] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 600/2014 z dnia 15 maja 2014 r. w sprawie rynków instrumentów finansowych oraz zmieniające rozporządzenie (UE) nr 648/2012 (Dz.U. L 173 z 12.6.2014, s. 84, ELI: http://data.europa.eu/eli/reg/2014/600/oj).

[6] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 909/2014 z dnia 23 lipca 2014 r. w sprawie usprawnienia rozrachunku papierów wartościowych w Unii Europejskiej i w sprawie centralnych depozytów papierów wartościowych, zmieniające dyrektywy 98/26/WE i 2014/65/UE oraz rozporządzenie (UE) nr 236/2012 (Dz.U. L 257 z 28.8.2014, s. 1, ELI: http://data.europa.eu/eli/reg/2014/909/oj).

(27) Przepisy niniejszego rozporządzenia odnoszą się do obszaru ram zarządzania ryzykiem związanym z ICT, określając szczegółowe elementy mające zastosowanie do podmiotów finansowych zgodnie z art. 15 rozporządzenia (UE) 2022/2554 oraz opracowując uproszczone ramy zarządzania ryzykiem związanym z ICT dla podmiotów finansowych określone w art. 16 ust. 1 tego rozporządzenia. Aby zapewnić spójność między zwykłymi i uproszczonymi ramami zarządzania ryzykiem związanym z ICT oraz biorąc pod uwagę, że przepisy te powinny mieć zastosowanie w tym samym czasie, należy włączyć te przepisy do jednego aktu ustawodawczego.

(28) Podstawę niniejszego rozporządzenia stanowi projekt regulacyjnych standardów technicznych przekazany Komisji przez Europejski Urząd Nadzoru Bankowego, Europejski Urząd Nadzoru Ubezpieczeń i Pracowniczych Programów Emerytalnych oraz Europejski Urząd Nadzoru Giełd i Papierów Wartościowych („europejskie urzędy nadzoru") po konsultacji z Agencją Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA).

(29) Wspólny Komitet Europejskich Urzędów Nadzoru, o którym mowa w art. 54 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1093/2010[7], w art. 54 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1094/2010[8] i w art. 54 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1095/2010[9], przeprowadził otwarte konsultacje publiczne na temat projektu regulacyjnych standardów technicznych, który stanowi podstawę niniejszego rozporządzenia, dokonał analizy potencjalnych powiązanych kosztów i korzyści proponowanych standardów oraz zwrócił się o opinię do Bankowej Grupy Interesariuszy powołanej zgodnie z art. 37 rozporządzenia (UE) nr 1093/2010, do Grupy Interesariuszy z Sektora Ubezpieczeń i Reasekuracji i Grupy Interesariuszy z Sektora Pracowniczych Programów Emerytalnych powołanych zgodnie z art. 37 rozporządzenia (UE) nr 1094/2010 oraz do Grupy Interesariuszy z Sektora Giełd i Papierów Wartościowych powołanej zgodnie z art. 37 rozporządzenia (UE) nr 1095/2010.

(30) W zakresie, w jakim przetwarzanie danych osobowych jest wymagane do wypełnienia obowiązków określonych w niniejszym akcie, zastosowanie w pełni mają rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. i rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. Na przykład w przypadku gromadzenia danych osobowych w celu zapewnienia odpowiedniego wykrywania incydentów należy przestrzegać zasady minimalizacji danych. W sprawie projektu niniejszego aktu skonsultowano się również z Europejskim Inspektorem Ochrony Danych,

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

---

[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, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

[8] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1094/2010 z dnia 24 listopada 2010 r. w sprawie ustanowienia Europejskiego Urzędu Nadzoru (Europejskiego Urzędu Nadzoru Ubezpieczeń i Pracowniczych Programów Emerytalnych), zmiany decyzji nr 716/2009/WE i uchylenia decyzji Komisji 2009/79/WE (Dz.U. L 331 z 15.12.2010, s. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

[9] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1095/2010 z dnia 24 listopada 2010 r. w sprawie ustanowienia Europejskiego Urzędu Nadzoru (Europejskiego Urzędu Nadzoru Giełd i Papierów Wartościowych), zmiany decyzji nr 716/2009/WE i uchylenia decyzji Komisji 2009/77/WE (Dz.U. L 331 z 15.12.2010, s. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

TYTUŁ I
ZASADA OGÓLNA

Artykuł 1
Ogólny profil ryzyka i stopień złożoności

Przy opracowywaniu i wdrażaniu polityk, procedur, protokołów i narzędzi w zakresie bezpieczeństwa ICT, o których mowa w tytule II, oraz uproszczonych ram zarządzania ryzykiem związanym z ICT, o których mowa w tytule III, uwzględnia się wielkość i ogólny profil ryzyka podmiotu finansowego oraz charakter, skalę i elementy zwiększonego lub zmniejszonego stopnia złożoności realizowanych usług, działań i operacji, w tym elementy związane z:

a) szyfrowaniem i kryptografią;

b) bezpieczeństwem operacji ICT;

c) bezpieczeństwem sieci;

d) zarządzaniem projektami ICT i zmianą w systemach ICT;

e) potencjalnym wpływem ryzyka związanego z ICT na poufność, integralność i dostępność danych oraz zakłóceń na ciągłość i dostępność działań podmiotu finansowego.

TYTUŁ II
DALSZA HARMONIZACJA NARZĘDZI, METOD, PROCESÓW I POLITYK ZARZĄDZANIA RYZYKIEM ZWIĄZANYM Z ICT ZGODNIE Z ART. 15 ROZPORZĄDZENIA (UE) 2022/2554

ROZDZIAŁ I
POLITYKI, PROCEDURY, PROTOKOŁY I NARZĘDZIA W ZAKRESIE BEZPIECZEŃSTWA ICT

SEKCJA 1

Artykuł 2
Ogólne elementy polityk, procedur, protokołów i narzędzi w zakresie bezpieczeństwa ICT

1. Podmioty finansowe zapewniają, aby ich polityki w zakresie bezpieczeństwa ICT, bezpieczeństwo informacji oraz powiązane procedury, protokoły i narzędzia, o których mowa w art. 9 ust. 2 rozporządzenia (UE) 2022/2554, zostały włączone do ich ram zarządzania ryzykiem związanym z ICT. Podmioty finansowe ustanawiają polityki, procedury, protokoły i narzędzia w zakresie bezpieczeństwa ICT określone w niniejszym rozdziale, które:

   a) zapewniają bezpieczeństwo sieci;

   b) zawierają zabezpieczenia przed włamaniami i wykorzystaniem danych niezgodnie z przeznaczeniem;

   c) zachowują dostępność, autentyczność, integralność i poufność danych, w tym za pomocą technik kryptograficznych;

   d) gwarantują dokładne i niezwłoczne przekazywanie danych bez poważnych zakłóceń i nieuzasadnionych opóźnień.

2. Podmioty finansowe zapewniają, aby polityki bezpieczeństwa ICT, o których mowa w ust. 1:

   a) były dostosowane do celów podmiotu finansowego w zakresie bezpieczeństwa informacji zawartych w strategii operacyjnej odporności cyfrowej, o której mowa w art. 6 ust. 8 rozporządzenia (UE) 2022/2554;

   b) wskazywały datę formalnego zatwierdzenia polityki bezpieczeństwa ICT przez organ zarządzający;

   c) zawierały wskaźniki i środki na potrzeby:

      (i) monitorowania wdrażania polityk, procedur, protokołów i narzędzi w zakresie bezpieczeństwa ICT;

      (ii) odnotowywania wyjątków od tego wdrażania;

      (iii) zapewnienia operacyjnej odporności cyfrowej podmiotu finansowego w przypadku wyjątków, o których mowa w pkt (ii);

d) zawierały informacje na temat obowiązków pracowników na wszystkich szczeblach w celu zapewnienia bezpieczeństwa ICT podmiotu finansowego;

e) określały konsekwencje nieprzestrzegania polityki bezpieczeństwa ICT przez pracowników podmiotu finansowego w przypadku, gdy przepisy w tym zakresie nie zostały określone w innych politykach podmiotu finansowego;

f) zawierały wykaz dokumentacji, która ma być przechowywana;

g) określały podział ustaleń dotyczących obowiązków w kontekście modelu trzech linii obrony lub innego wewnętrznego modelu zarządzania ryzykiem i kontroli, w stosownych przypadkach, w celu uniknięcia konfliktu interesów;

h) uwzględniały wiodące praktyki i, w stosownych przypadkach, normy w rozumieniu art. 2 pkt 1 rozporządzenia (UE) nr 1025/2012;

i) zawierały szczegółowo określone role i obowiązki w zakresie opracowywania, wdrażania i utrzymywania polityk, procedur, protokołów i narzędzi w zakresie bezpieczeństwa ICT;

j) były poddawane przeglądowi zgodnie z art. 6 ust. 5 rozporządzenia (UE) 2022/2554;

k) uwzględniały istotne zmiany dotyczące podmiotu finansowego, w tym istotne zmiany w działaniach lub procesach podmiotu finansowego, w krajobrazie cyberzagrożeń lub mających zastosowanie obowiązkach prawnych.

SEKCJA 2

Artykuł 3
Zarządzanie ryzykiem związanym z ICT

Podmioty finansowe opracowują, dokumentują i wdrażają polityki i procedury zarządzania ryzykiem związanym z ICT, które obejmują wszystkie następujące elementy:

a) wskazanie zatwierdzenia poziomu tolerancji ryzyka w odniesieniu do ryzyka związanego z ICT ustanowionego zgodnie z art. 6 ust. 8 lit. b) rozporządzenia (UE) 2022/2554;

b) procedurę i metodykę przeprowadzania oceny ryzyka związanego z ICT, określające:

(i) podatności i zagrożenia, które wpływają lub mogą wpływać na wspierane funkcje biznesowe, systemy ICT i zasoby ICT wspierające te funkcje;

(ii) wskaźniki ilościowe lub jakościowe służące do pomiaru wpływu i prawdopodobieństwa wystąpienia podatności i zagrożeń, o których mowa w pkt (i);

c) procedurę określania, wdrażania i dokumentowania środków traktowania ryzyka związanego z ICT w odniesieniu do zidentyfikowanego i ocenianego ryzyka związanego z ICT, w tym określenie środków przeciwdziałania ryzyku związanemu z ICT niezbędnych do sprowadzenia ryzyka związanego z ICT do poziomu tolerancji ryzyka, o którym mowa w lit. a);

d) w odniesieniu do rezydualnego ryzyka związanego z ICT, które nadal istnieje po wdrożeniu środków traktowania ryzyka związanego z ICT, o których mowa w lit. c):

(i) przepisy dotyczące identyfikacji tego rezydualnego ryzyka związanego z ICT;

(ii) podział ról i obowiązków w odniesieniu do:

1) akceptacji rezydualnego ryzyka związanego z ICT, które przekracza poziom tolerancji ryzyka podmiotu finansowego, o którym mowa w lit. a);

2) procesu przeglądu, o którym mowa w lit. d) pkt (iv);

(iii) opracowanie wykazu akceptowanego rezydualnego ryzyka związanego z ICT, w tym uzasadnienia jego akceptacji;

(iv) przepisy dotyczące przeglądu akceptowanego rezydualnego ryzyka związanego z ICT co najmniej raz w roku, w tym:

1) określenie wszelkich zmian rezydualnego ryzyka związanego z ICT;

2) ocenę dostępnych środków łagodzących;

3) ocenę, czy powody uzasadniające akceptację rezydualnego ryzyka związanego z ICT są nadal aktualne i mają zastosowanie w dniu przeglądu;

e) przepisy dotyczące monitorowania:

(i) wszelkich zmian ryzyka związanego z ICT i krajobrazu cyberzagrożeń;

(ii) podatności i zagrożeń o charakterze wewnętrznym i zewnętrznym:

(iii) ryzyka związanego z ICT danego podmiotu finansowego, które umożliwia szybkie wykrywanie zmian, które mogą mieć wpływ na jego profil ryzyka związanego z ICT;

f) przepisy dotyczące procesu zapewniającego uwzględnienie wszelkich zmian w strategii biznesowej i strategii operacyjnej odporności cyfrowej podmiotu finansowego.

Do celów akapitu pierwszego lit. c) procedura, o której mowa w tej literze, zapewnia:

a) monitorowanie skuteczności wdrożonych środków traktowania ryzyka związanego z ICT;

b) ocenę, czy osiągnięto ustalone poziomy tolerancji ryzyka podmiotu finansowego;

c) ocenę tego, czy podmiot finansowy podjął działania w celu skorygowania lub udoskonalenia tych środków w razie potrzeby.

SEKCJA 3
ZARZĄDZANIE ZASOBAMI ICT

Artykuł 4
Polityka zarządzania zasobami ICT

1. W ramach polityk, procedur, protokołów i narzędzi w zakresie bezpieczeństwa ICT, o których mowa w art. 9 ust. 2 rozporządzenia (UE) 2022/2554, podmioty finansowe opracowują, dokumentują i wdrażają politykę zarządzania zasobami ICT.

2. W polityce zarządzania zasobami ICT, o której mowa w ust. 1:

a) nakazuje się monitorowanie cyklu życia zasobów ICT zidentyfikowanych i sklasyfikowanych zgodnie z art. 8 ust. 1 rozporządzenia (UE) 2022/2554 oraz zarządzanie nim;

b) nakazuje się, aby podmiot finansowy prowadził ewidencję zawierającą wszystkie następujące elementy:

(i) niepowtarzalny identyfikator każdego zasobu ICT;

(ii) informacje o lokalizacji, fizycznej albo logicznej, wszystkich zasobów ICT;

(iii) klasyfikację wszystkich zasobów ICT, o której mowa w art. 8 ust. 1 rozporządzenia (UE) 2022/2254;

(iv) dane identyfikacyjne właścicieli zasobów ICT;

(v) funkcje lub usługi biznesowe wspierane przez zasoby ICT;

(vi) wymogi dotyczące ciągłości działania w zakresie ICT, w tym zakładany czas przywrócenia sprawności oraz akceptowalny poziom utraty danych;

(vii) informację o tym, czy zasoby ICT mogą być lub są narażone na działanie sieci zewnętrznych, w tym internetu;

(viii) powiązania i współzależności między zasobami ICT a funkcjami biznesowymi wykorzystującymi każdy zasób ICT;

(ix) w stosownych przypadkach, w odniesieniu do wszystkich zasobów ICT – daty końcowe regularnych, rozszerzonych i niestandardowych usług wsparcia świadczonych przez zewnętrznego dostawcę usług ICT, po których te zasoby ICT nie są już wspierane przez ich dostawcę lub przez zewnętrznego dostawcę usług ICT;

c) w przypadku podmiotów finansowych innych niż mikroprzedsiębiorstwa nakazuje się tym podmiotom finansowym prowadzenie ewidencji informacji niezbędnych do przeprowadzenia szczegółowej oceny ryzyka związanego z ICT w odniesieniu do wszystkich dotychczasowych systemów ICT, o których mowa w art. 8 ust. 7 rozporządzenia (UE) 2022/2554.

Artykuł 5
Procedura zarządzania zasobami ICT

1. Podmioty finansowe opracowują, dokumentują i wdrażają procedurę zarządzania zasobami ICT.

2. Procedura zarządzania zasobami ICT, o której mowa w ust. 1, określa kryteria przeprowadzania oceny krytyczności zasobów informacyjnych i zasobów ICT wspierających funkcje biznesowe. Ocena ta uwzględnia:

a) ryzyko związane z ICT dotyczące tych funkcji biznesowych i ich zależności od zasobów informacyjnych lub zasobów ICT;

b) sposób, w jaki utrata poufności, integralności i dostępności takich zasobów informacyjnych i zasobów ICT wpłynęłaby na procesy biznesowe i działania podmiotów finansowych.

SEKCJA 4
SZYFROWANIE I KRYPTOGRAFIA

Artykuł 6
Mechanizmy kontroli szyfrowania i kryptograficznej

1. W ramach polityk, procedur, protokołów i narzędzi w zakresie bezpieczeństwa ICT, o których mowa w art. 9 ust. 2 rozporządzenia (UE) 2022/2554, podmioty finansowe opracowują, dokumentują i wdrażają politykę dotyczącą mechanizmów kontroli szyfrowania i kryptograficznej.

2. Podmioty finansowe opracowują politykę dotyczącą mechanizmów kontroli szyfrowania i kryptograficznej, o której mowa w ust. 1, na podstawie wyników zatwierdzonej klasyfikacji danych i oceny ryzyka związanego z ICT. Polityka ta zawiera zasady dotyczące wszystkich następujących elementów:

   a) szyfrowania danych przechowywanych i przesyłanych;

   b) w stosownych przypadkach, szyfrowania danych wykorzystywanych;

   c) szyfrowania wewnętrznych połączeń sieciowych i ruchu w sieci z udziałem podmiotów zewnętrznych;

   d) zarządzania kluczami kryptograficznymi, o którym mowa w art. 7, określając zasady prawidłowego stosowania, ochrony i cyklu życia kluczy kryptograficznych.

   Do celów lit. b), jeżeli szyfrowanie wykorzystywanych danych nie jest możliwe, podmioty finansowe przetwarzają dane wykorzystywane w oddzielonym i chronionym środowisku lub wprowadzają równoważne środki w celu zapewnienia poufności, integralności, autentyczności i dostępności danych.

3. Podmioty finansowe uwzględniają w polityce dotyczącej mechanizmów kontroli szyfrowania i kryptograficznej, o której mowa w ust. 1, kryteria wyboru technik kryptograficznych i praktyk stosowania, z uwzględnieniem wiodących praktyk i norm w rozumieniu art. 2 pkt 1 rozporządzenia (UE) nr 1025/2012 oraz klasyfikacji odpowiednich zasobów ICT ustanowionej zgodnie z art. 8 ust. 1 rozporządzenia (UE) 2022/2554. Podmioty finansowe, które nie są w stanie przestrzegać wiodących praktyk lub standardów ani stosować najbardziej wiarygodnych technik, przyjmują środki łagodzące i środki monitorowania zapewniające odporność na cyberzagrożenia.

4. Podmioty finansowe uwzględniają w polityce dotyczącej mechanizmów kontroli szyfrowania i kryptograficznej, o której mowa w ust. 1, przepisy dotyczące aktualizacji lub zmiany, w razie potrzeby, technologii kryptograficznej w oparciu o rozwój kryptoanalizy. Te aktualizacje lub zmiany zapewniają, aby technologia kryptograficzna pozostała odporna na cyberzagrożenia, zgodnie z wymogami art. 10 ust. 2 lit. a). Podmioty finansowe, które nie są w stanie zaktualizować lub zmienić technologii kryptograficznej, przyjmują środki łagodzące i środki monitorowania zapewniające odporność na cyberzagrożenia.

5. Podmioty finansowe uwzględniają w polityce dotyczącej mechanizmów kontroli szyfrowania i kryptograficznej, o której mowa w ust. 1, wymóg rejestrowania przypadków przyjęcia środków łagodzących i środków monitorowania zgodnie z ust. 3 i 4 oraz przedstawienia uzasadnionego wyjaśnienia tego faktu.

Artykuł 7
Zarządzanie kluczami kryptograficznymi

1. Podmioty finansowe uwzględniają w polityce zarządzania kluczami kryptograficznymi, o której mowa w art. 6 ust. 2 lit. d), wymogi dotyczące zarządzania kluczami kryptograficznymi w całym ich cyklu życia, z uwzględnieniem generowania, odnawiania, przechowywania, tworzenia kopii zapasowych, archiwizowania, pobierania, przesyłania, utraty ważności, cofania i niszczenia tych kluczy kryptograficznych.

2. Podmioty finansowe określają i wdrażają kontrole w celu ochrony kluczy kryptograficznych w całym ich cyklu życia przed utratą, nieuprawnionym dostępem, ujawnieniem i modyfikacją. Podmioty finansowe opracowują te kontrole na podstawie wyników zatwierdzonej klasyfikacji danych i oceny ryzyka związanego z ICT.

3. Podmioty finansowe opracowują i wdrażają metody zastępowania kluczy kryptograficznych w przypadku ich utraty lub gdy klucze te zostaną naruszone lub uszkodzone.

4. Podmioty finansowe tworzą i prowadzą rejestr wszystkich certyfikatów i urządzeń do przechowywania certyfikatów w odniesieniu do co najmniej zasobów ICT wspierających krytyczne lub istotne funkcje. Podmioty finansowe aktualizują ten rejestr.

5. Podmioty finansowe zapewniają niezwłoczne odnowienie certyfikatów przed ich wygaśnięciem.

SEKCJA 5
BEZPIECZEŃSTWO OPERACJI ICT

Artykuł 8
Polityki i procedury dotyczące operacji ICT

1. W ramach polityk, procedur, protokołów i narzędzi w zakresie bezpieczeństwa ICT, o których mowa w art. 9 ust. 2 rozporządzenia (UE) 2022/2554, podmioty finansowe opracowują, dokumentują i wdrażają polityki i procedury zarządzania operacjami ICT. Wspomniane polityki i procedury określają sposób, w jaki podmioty finansowe obsługują, monitorują, kontrolują i przywracają swoje zasoby ICT, w tym dokumentację operacji ICT.

2. Polityki i procedury dotyczące operacji ICT, o których mowa w ust. 1, zawierają wszystkie następujące elementy:

   a) opis zasobów ICT, zawierający wszystkie poniższe informacje:

      (i) wymogi dotyczące bezpiecznej instalacji, konserwacji, konfiguracji i demontażu systemu ICT;

      (ii) wymogi dotyczące zarządzania zasobami informacyjnymi wykorzystywanymi przez zasoby ICT, w tym ich przetwarzania i obsługi, zarówno w sposób zautomatyzowany, jak i ręczny;

      (iii) wymogi dotyczące identyfikacji i kontroli dotychczasowych systemów ICT;

b) kontrole i monitorowanie systemów ICT, uwzględniające wszystkie poniższe elementy:

(i) wymogi dotyczące tworzenia kopii zapasowych i przywracania systemów ICT;

(ii) wymogi dotyczące ustalania harmonogramu, z uwzględnieniem współzależności między systemami ICT;

(iii) protokoły dotyczące ścieżki audytu i informacje zawarte w dzienniku sieciowym;

(iv) wymogi mające na celu zapewnienie, aby przeprowadzanie audytu wewnętrznego i innych testów minimalizowało zakłócenia w działalności gospodarczej;

(v) wymogi dotyczące oddzielenia środowisk produkcyjnych ICT od środowisk rozwojowych, testowych i innych środowisk nieprodukcyjnych;

(vi) wymogi prowadzenia działań z zakresu rozwoju i testowania w środowiskach, które są oddzielone od środowiska produkcyjnego;

(vii) wymogi prowadzenia działań z zakresu rozwoju i testowania w środowiskach produkcyjnych;

c) obsługę błędów dotyczących systemów ICT, z uwzględnieniem wszystkich poniższych elementów:

(i) procedury i protokoły obsługi błędów;

(ii) kontakty do celów wsparcia i na wypadek eskalacji, w tym kontakty wsparcia zewnętrznego w przypadku nieoczekiwanych problemów operacyjnych lub technicznych;

(iii) procedury ponownego uruchomienia, powrotu do poprzedniej konfiguracji i przywracania sprawności systemu ICT do stosowania w przypadku zakłócenia funkcjonowania systemu ICT.

Do celów lit. b) pkt (v) oddzielenie uwzględnia wszystkie elementy środowiska, w tym konta, dane lub połączenia, zgodnie z wymogami art. 13 ust. 1 lit. a).

Do celów lit. b) pkt (vii) w politykach i procedurach, o których mowa w ust. 1, przewiduje się, że przypadki, w których testy są przeprowadzane w środowisku produkcyjnym, są jasno określone, uzasadnione, trwają przez ograniczony czas i zostają zatwierdzone przez odpowiednią funkcję zgodnie z art. 16 ust. 6. Podmioty finansowe zapewniają dostępność, poufność, integralność i autentyczność systemów ICT i danych dotyczących produkcji podczas działań rozwojowych i testowych w środowisku produkcyjnym.

Artykuł 9
Zarządzanie pojemnością i wydajnością

1. W ramach polityk, procedur, protokołów i narzędzi w zakresie bezpieczeństwa ICT, o których mowa w art. 9 ust. 2 rozporządzenia (UE) 2022/2554, podmioty finansowe opracowują, dokumentują i wdrażają procedury zarządzania pojemnością i wydajnością dotyczące:

a) określenia wymogów w zakresie pojemności ich systemów ICT;

b) stosowania optymalizacji zasobów;

c) procedur monitorowania w celu utrzymania i poprawy:

(i) dostępności danych i systemów ICT;

(ii) efektywności systemów ICT;

(iii) zapobiegania niedoborom pojemności w zakresie ICT.

2. Procedury zarządzania pojemnością i wydajnością, o których mowa w ust. 1, zapewniają, aby podmioty finansowe wdrażały środki, które należycie odpowiadają specyfice systemów ICT, w przypadku których procesy udzielania zamówień lub zatwierdzania są długie lub złożone, lub systemów ICT, które wymagają wielu zasobów.

Artykuł 10
Zarządzanie podatnościami i poprawkami

1. W ramach polityk, procedur, protokołów i narzędzi w zakresie bezpieczeństwa ICT, o których mowa w art. 9 ust. 2 rozporządzenia (UE) 2022/2554, podmioty finansowe opracowują, dokumentują i wdrażają procedury zarządzania podatnościami.

2. Procedury zarządzania podatnościami, o których mowa w ust. 1, obejmują:

a) określanie i aktualizowanie odpowiednich i wiarygodnych zasobów informacyjnych w celu budowania i utrzymywania świadomości na temat podatności;

b) zapewnienie przeprowadzania automatycznego skanowania pod kątem podatności i ocen dotyczących zasobów ICT, przy czym częstotliwość i zakres tych działań muszą być współmierne do klasyfikacji ustanowionej zgodnie z art. 8 ust. 1 rozporządzenia (UE) 2022/2554 oraz do ogólnego profilu ryzyka zasobów ICT;

c) sprawdzanie, czy:

(i) zewnętrzni dostawcy usług ICT reagują na podatności związane z usługami ICT świadczonymi na rzecz podmiotu finansowego;

(ii) zewnętrzni dostawcy usług ICT w odpowiednim czasie zgłaszają podmiotowi finansowemu co najmniej krytyczne podatności oraz statystyki i tendencje;

d) monitorowanie wykorzystania:

(i) bibliotek zewnętrznych, w tym bibliotek open source, stosowanych w ramach usług ICT wspierających krytyczne lub istotne funkcje;

(ii) usług ICT opracowanych samodzielnie przez podmiot finansowy bądź specjalnie dostosowanych lub opracowanych na potrzeby podmiotu finansowego przez zewnętrznego dostawcę usług ICT;

e) ustanowienie procedur odpowiedzialnego ujawniania podatności klientom, kontrahentom i opinii publicznej;

f) priorytetowe traktowanie wdrażania poprawek i innych środków łagodzących w celu wyeliminowania zidentyfikowanych podatności;

g) monitorowanie i weryfikowanie eliminowania podatności;

h) wymóg rejestrowania wszelkich wykrytych podatności mających wpływ na systemy ICT oraz monitorowania ich usuwania.

Do celów lit. b) podmioty finansowe co najmniej raz w tygodniu przeprowadzają zautomatyzowane skanowanie pod kątem podatności oraz oceny podatności zasobów ICT w odniesieniu do zasobów ICT wspierających krytyczne lub istotne funkcje.

Do celów lit. c) podmioty finansowe zwracają się do zewnętrznych dostawców usług ICT o zbadanie odpowiednich podatności, określenie ich podstawowych przyczyn oraz wdrożenie odpowiednich działań łagodzących.

Do celów lit. d) podmioty finansowe, w stosownych przypadkach we współpracy z zewnętrznym dostawcą usług ICT, monitorują wersję i ewentualne aktualizacje bibliotek zewnętrznych. W przypadku gotowych do użytku zasobów ICT lub komponentów zasobów ICT pozyskanych i wykorzystywanych do świadczenia usług ICT, które nie wspierają krytycznych lub istotnych funkcji, podmioty finansowe monitorują korzystanie w miarę możliwości z bibliotek zewnętrznych, w tym bibliotek open source.

Do celów lit. f) podmioty finansowe uwzględniają krytyczność podatności, klasyfikację ustanowioną zgodnie z art. 8 ust. 1 rozporządzenia (UE) 2022/2554, a także profil ryzyka zasobów ICT, w przypadku których stwierdzono podatności.

3. W ramach polityk, procedur, protokołów i narzędzi w zakresie bezpieczeństwa ICT, o których mowa w art. 9 ust. 2 rozporządzenia (UE) 2022/2554, podmioty finansowe opracowują, dokumentują i wdrażają procedury zarządzania poprawkami.

4. Procedury zarządzania poprawkami, o których mowa w ust. 3, obejmują:

a) w miarę możliwości identyfikację i ocenę dostępnych poprawek i aktualizacji oprogramowania i sprzętu komputerowego przy użyciu zautomatyzowanych narzędzi;

b) określenie procedur awaryjnych dotyczących wdrażania poprawek i aktualizowania zasobów ICT;

c) testowanie i wdrażanie poprawek oprogramowania i sprzętu komputerowego oraz aktualizacji, o których mowa w art. 8 ust. 2 lit. b) pkt (v), (vi) i (vii);

d) określenie terminów instalacji poprawek oprogramowania i sprzętu komputerowego oraz aktualizacji i eskalacji w przypadku, gdy terminów tych nie można dotrzymać.

Artykuł 11
Bezpieczeństwo danych i systemów

1. W ramach polityk, procedur, protokołów i narzędzi w zakresie bezpieczeństwa ICT, o których mowa w art. 9 ust. 2 rozporządzenia (UE) 2022/2554, podmioty finansowe opracowują, dokumentują i wdrażają procedurę bezpieczeństwa danych i systemów.

2. Procedura bezpieczeństwa danych i systemów, o której mowa w ust. 1, obejmuje wszystkie następujące elementy związane z bezpieczeństwem danych i systemów ICT, zgodnie z klasyfikacją ustanowioną zgodnie z art. 8 ust. 1 rozporządzenia (UE) 2022/2554:

a) ograniczenia dostępu, o których mowa w art. 21 niniejszego rozporządzenia, ułatwiające spełnienie wymogów w zakresie ochrony w odniesieniu do każdego poziomu klauzuli tajności;

b) określenie bezpiecznego poziomu bazowego konfiguracji zasobów ICT, który minimalizuje narażenie tych zasobów ICT na cyberzagrożenia, oraz środków umożliwiających regularną weryfikację, czy te poziomy bazowe są skutecznie wdrażane;

c) określenie środków bezpieczeństwa w celu zapewnienia, aby w systemach ICT i urządzeniach końcowych instalowano wyłącznie zatwierdzone oprogramowanie;

d) określenie środków bezpieczeństwa przeciwko kodom złośliwym;

e) określenie środków bezpieczeństwa w celu zapewnienia, aby do przekazywania i przechowywania danych podmiotu finansowego wykorzystywano tylko zatwierdzone nośniki danych, systemy i urządzenia końcowe;

f) następujące wymogi mające na celu zapewnienie korzystania z przenośnych urządzeń końcowych i prywatnych nieprzenośnych urządzeń końcowych:

   (i) wymóg stosowania rozwiązania w zakresie zarządzania umożliwiającego zdalne zarządzanie urządzeniami końcowymi i zdalne wyczyszczenie danych podmiotu finansowego;

   (ii) wymóg korzystania z mechanizmów bezpieczeństwa, których pracownicy ani zewnętrzni dostawcy usług ICT nie mogą w sposób nieuprawniony zmienić, usunąć ani ominąć;

   (iii) wymóg korzystania z przenośnych urządzeń do przechowywania danych wyłącznie w przypadku, gdy rezydualne ryzyko związane z ICT pozostaje w granicach poziomu tolerancji ryzyka podmiotu finansowego, o którym to poziomie mowa w art. 3 ust. 1 lit. a);

g) proces bezpiecznego usuwania danych znajdujących się w obiektach podmiotu finansowego lub przechowywanych na zewnątrz, których podmiot finansowy nie musi już gromadzić ani przechowywać;

h) proces bezpiecznego pozbywania się lub wycofywania z eksploatacji urządzeń do przechowywania danych znajdujących się w obiektach podmiotu finansowego lub przechowywanych na zewnątrz, zawierających informacje poufne;

i) identyfikacja i wdrożenie środków bezpieczeństwa zapobiegających utracie i wyciekowi danych w systemach i urządzeniach końcowych;

j) wdrożenie środków bezpieczeństwa w celu zapewnienia, aby telepraca i korzystanie z prywatnych urządzeń końcowych nie miały negatywnego wpływu na bezpieczeństwo ICT podmiotu finansowego;

k) w przypadku zasobów lub usług ICT obsługiwanych przez zewnętrznego dostawcę usług ICT – określenie i wdrożenie wymogów w celu utrzymania operacyjnej odporności cyfrowej, zgodnie z wynikami klasyfikacji danych i oceny ryzyka związanego z ICT.

Do celów lit. b) przy określaniu bezpiecznego poziomu bazowego konfiguracji, o którym mowa w tej literze, uwzględnia się wiodące praktyki i odpowiednie techniki określone w normach w rozumieniu art. 2 pkt 1 rozporządzenia (UE) nr 1025/2012.

Do celów lit. k) podmioty finansowe uwzględniają następujące elementy:

a) wdrożenie zalecanych przez dostawcę ustawień elementów obsługiwanych przez podmiot finansowy;

b) jasny podział ról i obowiązków w zakresie bezpieczeństwa informacji między podmiotem finansowym a zewnętrznym dostawcą usług ICT, zgodnie z zasadą pełnej odpowiedzialności podmiotu finansowego względem jego zewnętrznego dostawcy usług ICT, o której mowa w art. 28 ust. 1 lit. a) rozporządzenia (UE) 2022/2554, oraz zgodnie z polityką podmiotu finansowego dotyczącą korzystania z usług ICT wspierających krytyczne lub istotne funkcje w przypadku podmiotów finansowych, o których mowa w art. 28 ust. 2 tego rozporządzenia;

c) potrzebę zapewnienia i utrzymania odpowiednich kompetencji podmiotu finansowego w zakresie zarządzania i bezpieczeństwa wykorzystywanej usługi;

d) środki techniczne i organizacyjne mające na celu zminimalizowanie ryzyka związanego z infrastrukturą wykorzystywaną przez zewnętrznego dostawcę usług ICT do celów świadczonych przez niego usług ICT, z uwzględnieniem wiodących praktyk i norm w rozumieniu art. 2 pkt 1 rozporządzenia (UE) nr 1025/2012.

Artykuł 12
Rejestrowanie

1. Przy wprowadzaniu zabezpieczeń przed włamaniami i wykorzystaniem danych niezgodnie z przeznaczeniem podmioty finansowe opracowują, dokumentują i wdrażają procedury, protokoły i narzędzia rejestrowania.

2. Procedury, protokoły i narzędzia rejestrowania, o których mowa w ust. 1, obejmują wszystkie następujące elementy:

a) identyfikację zdarzeń, które mają być rejestrowane, okres zatrzymywania rejestrów oraz środki służące zabezpieczeniu i przetwarzaniu danych z rejestru, z uwzględnieniem celu, w jakim rejestry zostały utworzone;

b) dostosowanie poziomu szczegółowości rejestrów do ich celu i wykorzystania, tak aby umożliwić skuteczne wykrywanie nietypowych działań, o których mowa w art. 24;

c) wymóg rejestrowania zdarzeń dotyczących wszystkich poniższych elementów:

(i) logicznej i fizycznej kontroli dostępu, o której mowa w art. 21, oraz zarządzania tożsamością;

(ii) zarządzania pojemnością;

(iii) zarządzania zmianą;

(iv) operacji ICT, w tym działań związanych z systemem ICT;

(v) działań związanych z ruchem w sieci, w tym wydajności sieci ICT;

d) środki mające na celu ochronę systemów rejestrowania i informacji o rejestrach przed manipulacją, usuwaniem i nieuprawnionym dostępem, gdy są one przechowywane, przesyłane oraz, w stosownych przypadkach, wykorzystywane;

e) środki umożliwiające wykrywanie awarii systemów rejestrowania;

f) bez uszczerbku dla wszelkich wymogów regulacyjnych mających zastosowanie na mocy prawa Unii lub prawa krajowego – synchronizację zegarów każdego z systemów ICT podmiotu finansowego zgodnie z udokumentowanym wiarygodnym źródłem czasu referencyjnego.

Do celów lit. a) podmioty finansowe określają okres zatrzymywania, uwzględniając cele biznesowe i cele w zakresie bezpieczeństwa informacji, powód zarejestrowania zdarzenia w rejestrach oraz wyniki oceny ryzyka związanego z ICT.

SEKCJA 6
BEZPIECZEŃSTWO SIECI

Artykuł 13
Zarządzanie bezpieczeństwem sieci

1. Przy wprowadzaniu zabezpieczeń zapewniających ochronę sieci przed włamaniami i wykorzystaniem danych niezgodnie z przeznaczeniem podmioty finansowe opracowują, dokumentują i wdrażają polityki, procedury, protokoły i narzędzia w zakresie zarządzania bezpieczeństwem sieci obejmujące wszystkie następujące elementy:

   a) segregację i segmentację systemów i sieci ICT z uwzględnieniem:

      (i) krytyczności lub istotności funkcji, którą te systemy i sieci ICT wspierają;

      (ii) klasyfikacji ustanowionej zgodnie z art. 8 ust. 1 rozporządzenia (UE) 2022/2554;

      (iii) ogólnego profilu ryzyka związanego z zasobami ICT wykorzystującymi te systemy i sieci ICT;

   b) dokumentację wszystkich połączeń sieciowych i przepływów danych podmiotu finansowego;

   c) wykorzystanie odrębnej i wyspecjalizowanej sieci do administrowania zasobami ICT;

   d) określenie i wdrożenie kontroli dostępu do sieci w celu zapobiegania podłączaniu do sieci podmiotu finansowego za pomocą jakiegokolwiek nieuprawnionego urządzenia lub systemu lub jakiegokolwiek punktu końcowego niespełniającego wymogów bezpieczeństwa podmiotu finansowego oraz wykrywania takich przypadków;

   e) szyfrowanie połączeń sieciowych przechodzących przez sieci korporacyjne, sieci publiczne, sieci krajowe, sieci podmiotów zewnętrznych i sieci bezprzewodowe do celów wykorzystywanych protokołów komunikacyjnych, z uwzględnieniem wyników zatwierdzonej klasyfikacji danych, wyników oceny ryzyka związanego z ICT oraz szyfrowania połączeń sieciowych, o których mowa w art. 6 ust. 2;

   f) projektowanie sieci zgodnie z wymogami bezpieczeństwa ICT ustanowionymi przez podmiot finansowy, z uwzględnieniem wiodących praktyk w celu zapewnienia poufności, integralności i dostępności sieci;

g) zabezpieczenie ruchu w sieci między sieciami wewnętrznymi a internetem i innymi połączeniami zewnętrznymi;

h) określenie ról i obowiązków oraz etapów specyfikacji, wdrożenia, zatwierdzenia, zmiany i przeglądu reguł zapory sieciowej i filtrów połączeń;

i) przeprowadzanie przeglądów architektury sieci i struktury bezpieczeństwa sieci raz w roku, a w przypadku mikroprzedsiębiorstw – okresowo, w celu zidentyfikowania potencjalnych podatności;

j) środki tymczasowego izolowania, w razie potrzeby, podsieci oraz elementów i urządzeń sieci;

k) wdrożenie bezpiecznego poziomu bazowego konfiguracji wszystkich elementów sieci oraz umacnianie sieci i urządzeń sieciowych zgodnie z wszelkimi instrukcjami dostawcy, w stosownych przypadkach, normami w rozumieniu art. 2 pkt 1 rozporządzenia (UE) nr 1025/2012 oraz wiodącymi praktykami;

l) procedury ograniczania, blokowania i zamykania systemu oraz sesji zdalnych po upływie określonego okresu braku aktywności;

m) w odniesieniu do umów o świadczenie usług sieciowych:

(i) identyfikację i specyfikację środków bezpieczeństwa ICT i informacji, poziomów usług i wymogów w zakresie zarządzania w odniesieniu do wszystkich usług sieciowych;

(ii) wskazanie, czy usługi te są świadczone przez dostawcę usług ICT wewnątrz grupy czy przez zewnętrznych dostawców usług ICT.

Do celów lit. h) podmioty finansowe regularnie przeprowadzają przegląd reguł zapory sieciowej i filtrów połączeń zgodnie z klasyfikacją ustanowioną zgodnie z art. 8 ust. 1 rozporządzenia (UE) 2022/2554 oraz ogólnym profilem ryzyka odpowiednich systemów ICT. W przypadku systemów ICT, które wspierają krytyczne lub istotne funkcje, podmioty finansowe weryfikują adekwatność obowiązujących reguł zapory sieciowej i filtrów połączeń co najmniej raz na sześć miesięcy.

Artykuł 14
Zabezpieczenie przesyłanych informacji

1. Przy wprowadzaniu zabezpieczeń służących zapewnieniu dostępności, autentyczności, integralności i poufności danych podmioty finansowe opracowują, dokumentują i wdrażają polityki, procedury, protokoły i narzędzia w zakresie ochrony przesyłanych informacji. W szczególności podmioty finansowe zapewniają wszystkie następujące elementy:

a) dostępność, autentyczność, integralność i poufność danych podczas ich przesyłania w sieci, a także ustanowienie procedur oceny zgodności z tymi wymogami;

b) zapobieganie wyciekom danych i ich wykrywanie oraz bezpieczne przekazywanie informacji między podmiotem finansowym a podmiotami zewnętrznymi;

c) wdrażanie, dokumentowanie i regularne przeglądanie wymogów dotyczących poufności lub umów o zachowaniu poufności odzwierciedlających potrzeby

podmiotu finansowego w zakresie ochrony informacji w odniesieniu do zarówno pracowników podmiotu finansowego, jak i pracowników osób trzecich.

2. Podmioty finansowe opracowują polityki, procedury, protokoły i narzędzia służące ochronie przesyłanych informacji, o których mowa w ust. 1, na podstawie wyników zatwierdzonej klasyfikacji danych i oceny ryzyka związanego z ICT.

SEKCJA 7
ZARZĄDZANIE PROJEKTAMI ICT I ZMIANĄ W SYSTEMACH ICT

Artykuł 15
Zarządzanie projektami ICT

1. Przy wprowadzaniu zabezpieczeń służących zapewnieniu dostępności, autentyczności, integralności i poufności danych podmioty finansowe opracowują, dokumentują i wdrażają politykę zarządzania projektami ICT.

2. W polityce zarządzania projektami ICT, o której mowa w ust. 1, określa się elementy, które zapewniają skuteczne zarządzanie projektami ICT związanymi z pozyskiwaniem, utrzymaniem i, w stosownych przypadkach, rozwojem systemów ICT podmiotu finansowego.

3. W polityce zarządzania projektami ICT, o której mowa w ust. 1, określa się wszystkie następujące elementy:

   a) cele projektu ICT;

   b) zarządzanie projektem ICT, w tym role i obowiązki;

   c) planowanie projektu ICT, ramy czasowe i etapy;

   d) ocenę ryzyka projektu ICT;

   e) odpowiednie etapy pośrednie;

   f) wymogi dotyczące zarządzania zmianą;

   g) testowanie pod kątem wszystkich wymogów, w tym wymogów bezpieczeństwa, oraz odpowiedni proces zatwierdzania przy wdrażaniu systemu ICT w środowisku produkcyjnym.

4. Polityka zarządzania projektami ICT, o której mowa w ust. 1, zapewnia bezpieczną realizację projektu ICT dzięki dostarczeniu niezbędnych informacji i wiedzy fachowej z obszaru działalności lub funkcji, na które dany projekt ICT ma wpływ.

5. Zgodnie z oceną ryzyka projektu ICT, o której mowa w ust. 3 lit. d), w polityce zarządzania projektami ICT, o której mowa w ust. 1, przewiduje się konieczność informowania organu zarządzającego o ustanowieniu i postępach w realizacji projektów ICT mających wpływ na krytyczne lub istotne funkcje podmiotu finansowego oraz o związanym z nimi ryzyku w następujący sposób:

   a) indywidualnie lub zbiorczo, w zależności od znaczenia i wielkości projektów ICT;

   b) okresowo oraz, w razie potrzeby, doraźnie w związku z określonymi zdarzeniami.

Artykuł 16

Pozyskiwanie, rozwój i utrzymanie systemów ICT

1. Przy wprowadzaniu zabezpieczeń służących zapewnieniu dostępności, autentyczności, integralności i poufności danych podmioty finansowe opracowują, dokumentują i wdrażają politykę regulującą pozyskiwanie, rozwój i utrzymanie systemów ICT. W polityce tej:

   a) określa się praktyki i metody w zakresie bezpieczeństwa związane z pozyskiwaniem, rozwojem i utrzymaniem systemów ICT;

   b) ustanawia się wymóg identyfikacji:

      (i) specyfikacji technicznych i specyfikacji technicznych TIK w rozumieniu art. 2 pkt 4 i 5 rozporządzenia (UE) nr 1025/2012;

      (ii) wymogów dotyczących pozyskiwania, rozwoju i utrzymania systemów ICT, ze szczególnym uwzględnieniem wymogów bezpieczeństwa ICT oraz ich zatwierdzania przez odpowiednią funkcję biznesową i właściciela zasobów ICT zgodnie z ustaleniami podmiotu finansowego dotyczącymi zarządzania wewnętrznego;

   c) określa się środki ograniczające ryzyko niezamierzonych zmian lub zamierzonej manipulacji systemami ICT podczas rozwoju, utrzymywania i wdrażania tych systemów ICT w środowisku produkcyjnym.

2. Podmioty finansowe opracowują, dokumentują i wdrażają procedurę pozyskiwania, rozwoju i utrzymania systemów ICT na potrzeby testowania i zatwierdzania wszystkich systemów ICT przed ich wykorzystaniem i po zakończeniu ich utrzymywania, zgodnie z art. 8 ust. 2 lit. b) pkt (v), (vi) i (vii). Poziom testów musi być proporcjonalny do krytyczności odnośnych procedur biznesowych i zasobów ICT. Testy projektuje się w taki sposób, aby można było zweryfikować, czy nowe systemy ICT są odpowiednie do działania zgodnie z przeznaczeniem, z uwzględnieniem jakości wewnętrznie opracowywanego oprogramowania.

   W stosownych przypadkach, oprócz wymogów określonych w akapicie pierwszym, kontrahenci centralni angażują następujące podmioty w proces opracowywania i przeprowadzania testów, o których mowa w akapicie pierwszym:

   a) członków rozliczających i klientów;

   b) interoperacyjnych kontrahentów centralnych;

   c) inne zainteresowane strony.

   W stosownych przypadkach, oprócz wymogów określonych w akapicie pierwszym, centralne depozyty papierów wartościowych angażują następujące podmioty w proces opracowywania i przeprowadzania testów, o których mowa w akapicie pierwszym:

   a) użytkowników;

   b) dostawców najważniejszych mediów i usług;

   c) inne centralne depozyty papierów wartościowych;

   d) inne infrastruktury rynkowe;

e) wszelkie inne instytucje, które centralne depozyty papierów wartościowych wskazały jako powiązane z nimi współzależnościami w swoich strategiach na rzecz ciągłości działania.

3. Procedura, o której mowa w ust. 2, obejmuje przeprowadzanie przeglądów kodu źródłowego, w tym zarówno testy statyczne, jak i dynamiczne. Testy te obejmują testowanie bezpieczeństwa systemów i aplikacji internetowych zgodnie z art. 8 ust. 2 lit. b) pkt (v), (vi) i (vii). Podmioty finansowe:

a) identyfikują i analizują podatności i nieprawidłowości w kodzie źródłowym;

b) przyjmują plan działania w celu wyeliminowania tych podatności i nieprawidłowości;

c) monitorują realizację tego planu działania.

4. Procedura, o której mowa w ust. 2, zakłada przeprowadzenie testów bezpieczeństwa pakietów oprogramowania nie później niż na etapie integracji, zgodnie z art. 8 ust. 2 lit. b) pkt (v), (vi) i (vii).

5. W procedurze, o której mowa w ust. 2, przewiduje się, że:

a) dane dotyczące produkcji mogą być przechowywane w środowiskach nieprodukcyjnych wyłącznie w postaci zanonimizowanej, pseudonimizowanej lub randomizowanej;

b) podmioty finansowe muszą chronić integralność i poufność danych w środowiskach nieprodukcyjnych.

6. Na zasadzie odstępstwa od ust. 5 procedura, o której mowa w ust. 2, może stanowić, że dane dotyczące produkcji przechowuje się wyłącznie na potrzeby konkretnych testów, przez ograniczony czas oraz po zatwierdzeniu przez odpowiednią funkcję i zgłoszeniu takich przypadków funkcji zarządzania ryzykiem związanym z ICT.

7. Procedura, o której mowa w ust. 2, obejmuje wdrożenie kontroli mających na celu ochronę integralności kodu źródłowego systemów ICT, które są opracowywane wewnętrznie lub przez zewnętrznego dostawcę usług ICT i dostarczane podmiotowi finansowemu przez zewnętrznego dostawcę usług ICT.

8. W procedurze, o której mowa w ust. 2, przewiduje się, że oprogramowanie zamknięte oraz, w miarę możliwości, kod źródłowy dostarczony przez zewnętrznych dostawców usług ICT lub pozyskany w ramach projektów open source, muszą być analizowane i testowane zgodnie z ust. 3 przed ich wdrożeniem w środowisku produkcyjnym.

9. Ust. 1–8 niniejszego artykułu mają również zastosowanie do systemów ICT opracowywanych lub zarządzanych przez użytkowników niezwiązanych z funkcją ICT, z zastosowaniem podejścia opartego na analizie ryzyka.

Artykuł 17
Zarządzanie zmianą w systemach ICT

1. Przy wprowadzaniu zabezpieczeń służących zapewnieniu dostępności, autentyczności, integralności i poufności danych podmioty finansowe uwzględniają w procedurach zarządzania zmianą w systemach ICT, o których mowa w art. 9 ust. 4 lit. e) rozporządzenia (UE) 2022/2554, w odniesieniu do wszystkich zmian w oprogramowaniu, sprzęcie komputerowym, komponentach oprogramowania

sprzętowego, parametrach systemowych lub parametrach bezpieczeństwa, wszystkie następujące elementy:

a) weryfikację, czy spełniono wymogi bezpieczeństwa ICT;

b) mechanizmy zapewniające niezależność funkcji zatwierdzających zmiany oraz funkcji odpowiedzialnych za żądanie wprowadzenia tych zmian i ich wdrażanie;

c) jasny opis ról i obowiązków w celu zapewnienia, aby:

   (i) określono i zaplanowano zmiany;

   (ii) przewidziano odpowiedni okres przejściowy;

   (iii) zmiany były poddawane testom i finalizowane w sposób kontrolowany;

   (iv) prowadzono skuteczne zapewnianie jakości;

d) dokumentację i przekazywanie szczegółowych informacji na temat zmiany, w tym:

   (i) celu i zakresu zmiany;

   (ii) ram czasowych wdrażania zmiany;

   (iii) oczekiwanych wyników;

e) identyfikacja procedur awaryjnych i związanych z nimi obowiązków, w tym procedur i obowiązków związanych z przerywaniem zmian lub przywracaniem stanu sprzed zmian, które nie zostały pomyślnie wdrożone;

f) procedury, protokoły i narzędzia do zarządzania zmianami awaryjnymi, zapewniające odpowiednie zabezpieczenia;

g) procedury dokumentowania, ponownej oceny, oceny i zatwierdzania zmian awaryjnych po ich wdrożeniu, z uwzględnieniem obejść i poprawek;

h) określenie potencjalnego wpływu zmiany na istniejące środki bezpieczeństwa ICT wraz z oceną, czy taka zmiana wymaga przyjęcia dodatkowych środków bezpieczeństwa ICT.

2. Po wprowadzeniu znaczących zmian w swoich systemach ICT kontrahenci centralni i centralne depozyty papierów wartościowych poddają te systemy rygorystycznym testom, symulując warunki skrajne.

W stosownych przypadkach kontrahenci centralni angażują następujące podmioty w proces opracowywania i przeprowadzania testów, o których mowa w akapicie pierwszym:

a) członków rozliczających i klientów;

b) interoperacyjnych kontrahentów centralnych;

c) inne zainteresowane strony.

W stosownych przypadkach centralne depozyty papierów wartościowych angażują następujące podmioty w proces opracowywania i przeprowadzania testów, o którym mowa w akapicie pierwszym:

a) użytkowników;

b) dostawców najważniejszych mediów i usług;

c) inne centralne depozyty papierów wartościowych;

d) inne infrastruktury rynkowe;

e) wszelkie inne instytucje, które centralne depozyty papierów wartościowych wskazały jako powiązane z nimi współzależnościami w swoich strategiach na rzecz ciągłości działania w zakresie ICT.

SEKCJA 8

Artykuł 18
Bezpieczeństwo fizyczne i środowiskowe

1. Przy wprowadzaniu zabezpieczeń służących zapewnieniu dostępności, autentyczności, integralności i poufności danych podmioty finansowe określają, dokumentują i wdrażają politykę bezpieczeństwa fizycznego i środowiskowego. Podmioty finansowe opracowują tę politykę, biorąc pod uwagę aktualny krajobraz cyberzagrożeń i opierając się na klasyfikacji ustanowionej zgodnie z art. 8 ust. 1 rozporządzenia (UE) 2022/2554, a także uwzględniając ogólny profil ryzyka zasobów ICT i dostępnych zasobów informacyjnych.

2. Polityka bezpieczeństwa fizycznego i środowiskowego, o której mowa w ust. 1, musi zawierać wszystkie następujące elementy:

   a) odniesienie do sekcji polityki dotyczącej kontroli praw zarządzania dostępem, o której mowa w art. 21 akapit pierwszy lit. g);

   b) środki mające na celu ochronę wskazanych przez podmiot finansowy obiektów, ośrodków przetwarzania danych i wyznaczonych obszarów wrażliwych, gdzie znajdują się zasoby ICT i zasoby informacyjne, przed atakami, wypadkami oraz zagrożeniami środowiskowymi;

   c) środki mające na celu zabezpieczenie zasobów ICT, zarówno w obiektach podmiotu finansowego, jak i poza tymi obiektami, z uwzględnieniem wyników oceny ryzyka związanego z ICT towarzyszącego odpowiednim zasobom ICT;

   d) środki mające na celu zagwarantowanie dostępności, autentyczności, integralności i poufności zasobów ICT, zasobów informacyjnych oraz urządzeń fizycznej kontroli dostępu podmiotu finansowego poprzez zapewnienie odpowiedniego utrzymania;

   e) środki mające na celu zachowanie dostępności, autentyczności, integralności i poufności danych, w tym:

      (i) polityka „czystego biurka” w odniesieniu do dokumentów w formie papierowej;

      (ii) polityka „czystego ekranu” w odniesieniu do obiektów zajmujących się przetwarzaniem danych.

   Do celów lit. b) środki służące zapewnieniu ochrony przed zagrożeniami środowiskowymi muszą być współmierne do znaczenia obiektów, ośrodków przetwarzania danych i wyznaczonych obszarów wrażliwych oraz do krytyczności prowadzonych w nich operacji lub znajdujących się w nich systemów ICT.

   Do celów lit. c) polityka bezpieczeństwa fizycznego i środowiskowego, o której mowa w ust. 1, musi zawierać środki gwarantujące odpowiednią ochronę zasobów ICT pozostawionych bez dozoru.

Rozdział II
POLITYKA KADROWA I KONTROLA DOSTĘPU

Artykuł 19
Polityka kadrowa

Podmioty finansowe uwzględniają w swojej polityce kadrowej lub innych odpowiednich politykach wszystkie następujące elementy związane z bezpieczeństwem ICT:

a) określenie i powierzenie wszelkich szczególnych obowiązków w zakresie bezpieczeństwa ICT;

b) zobowiązanie pracowników podmiotu finansowego i zewnętrznych dostawców usług ICT korzystających z zasobów ICT podmiotu finansowego lub uzyskujących dostęp do tych zasobów do:

   (i) zaznajomienia się z politykami, procedurami i protokołami podmiotu finansowego w zakresie bezpieczeństwa ICT i przestrzegania tych polityk, procedur i protokołów;

   (ii) dysponowania wiedzą na temat kanałów dokonywania zgłoszeń ustanowionych przez podmiot finansowy na potrzeby wykrywania nietypowych zachowań, uwzględniając, w stosownych przypadkach, kanały dokonywania zgłoszeń ustanowione zgodnie z dyrektywą Parlamentu Europejskiego i Rady (UE) 2019/1937[10];

   (iii) w przypadku pracowników, po rozwiązaniu stosunku pracy – zwrócenia podmiotowi finansowemu wszystkich zasobów ICT oraz materialnych zasobów informacyjnych znajdujących się w ich posiadaniu i będących własnością podmiotu finansowego.

Artykuł 20
Zarządzanie tożsamością

1. W ramach kontroli praw zarządzania dostępem podmioty finansowe opracowują, dokumentują i wdrażają polityki i procedury zarządzania tożsamością zapewniające możliwość jednoznacznego zidentyfikowania i uwierzytelnienia osób fizycznych i systemów uzyskujących dostęp do informacji podmiotów finansowych w celu przyznania im praw dostępu użytkowników zgodnie z art. 21.

2. Polityki i procedury zarządzania tożsamością, o których mowa w ust. 1, obejmują wszystkie następujące elementy:

   a) bez uszczerbku dla art. 21 akapit pierwszy lit. c), każdemu pracownikowi podmiotu finansowego lub pracownikowi zewnętrznego dostawcy usług ICT uzyskującemu dostęp do zasobów informacyjnych i zasobów ICT podmiotu finansowego przydziela się unikalną tożsamość odpowiadającą unikalnemu kontu użytkownika;

[10] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1937 z dnia 23 października 2019 r. w sprawie ochrony osób zgłaszających naruszenia prawa Unii (Dz.U. L 305 z 26.11.2019, s. 17, ELI: http://data.europa.eu/eli/dir/2019/1937/oj).

b) proces zarządzania cyklem życia tożsamości i kont umożliwiający zarządzanie tworzeniem wszystkich kont, wprowadzaniem w nich zmian i dokonywaniem ich przeglądu, a także ich aktualizowaniem, tymczasową dezaktywacją i usuwaniem.

Do celów lit. a) podmioty finansowe prowadzą rejestr wszystkich przydzielonych tożsamości. Rejestr ten przechowuje się po dokonaniu reorganizacji podmiotu finansowego lub po rozwiązaniu stosunku umownego, bez uszczerbku dla wymogów dotyczących zatrzymywania danych przewidzianych w obowiązujących przepisach unijnych i krajowych.

Do celów lit. b) podmioty finansowe wprowadzają – w miarę możliwości i w stosownych przypadkach – zautomatyzowane rozwiązania na potrzeby procesu zarządzania cyklem życia tożsamości.

Artykuł 21
Kontrola dostępu

W ramach przeprowadzanej przez siebie kontroli praw zarządzania dostępem podmioty finansowe opracowują, dokumentują i wdrażają politykę obejmującą wszystkie poniższe elementy:

a) przyznawanie praw dostępu do zasobów ICT zgodnie z zasadami wiedzy koniecznej, potrzeby koniecznej i minimalizacji uprawnień, w tym również w kontekście dostępu zdalnego i dostępu awaryjnego;

b) podział obowiązków w taki sposób, aby zapobiegać nieuprawnionemu dostępowi do danych krytycznych lub przeciwdziałać przyznawaniu praw dostępu, których połączenie może umożliwiać obchodzenie kontroli;

c) uregulowanie kwestii rozliczalności użytkowników poprzez jak największe ograniczenie możliwości korzystania z generycznych i współdzielonych kont użytkownika oraz umożliwienie każdorazowego przyporządkowania działań podejmowanych w systemach ICT do konkretnych użytkowników;

d) uregulowanie kwestii ograniczeń dostępu do zasobów ICT oraz ustanowienie kontroli i narzędzi służących zapobieganiu nieuprawnionemu dostępowi;

e) procedury zarządzania kontem umożliwiające udzielanie, zmianę lub cofanie praw dostępu do kont użytkownika i kont generycznych, uwzględniając generyczne konta administratora, a także regulujące wszystkie poniższe kwestie:

   (i) podział ról i obowiązków w zakresie przyznawania, przeglądu i cofania praw dostępu;

   (ii) udzielanie dostępu uprzywilejowanego, dostępu awaryjnego i dostępu administratora do wszystkich systemów ICT na zasadzie potrzeby koniecznej lub na zasadzie *ad hoc*;

   (iii) niezwłoczne cofanie praw dostępu po rozwiązaniu stosunku pracy lub po ustaniu okoliczności uzasadniających przyznanie dostępu;

   (iv) aktualizowanie praw dostępu w przypadku konieczności wprowadzenia zmian i przynajmniej raz do roku w odniesieniu do wszystkich systemów ICT niebędących systemami ICT obsługującymi krytyczne lub istotne funkcje, a w odniesieniu do systemów ICT wspierających krytyczne lub istotne funkcje – przynajmniej raz na 6 miesięcy;

f) metody uwierzytelniania, w tym wszystkie poniższe elementy:

(i) stosowanie metod uwierzytelniania współmiernych do klasyfikacji ustanowionej zgodnie z art. 8 ust. 1 rozporządzenia (UE) 2022/2554 i do ogólnego profilu ryzyka zasobów ICT, przy należytym uwzględnieniu wiodących praktyk branżowych;

(ii) stosowanie solidnych metod uwierzytelniania zgodnie z wiodącymi praktykami i technikami branżowymi w zakresie zdalnego dostępu do sieci podmiotu finansowego, dostępu uprzywilejowanego, a także dostępu do zasobów ICT wspierających krytyczne lub istotne funkcje bądź publicznie dostępnych zasobów ICT;

g) środki kontroli dostępu fizycznego, w tym:

(i) identyfikowanie i rejestrowanie osób fizycznych uprawnionych do uzyskania dostępu do wskazanych przez podmiot finansowy obiektów, ośrodków przetwarzania danych i wyznaczonych obszarów wrażliwych, gdzie znajdują się zasoby ICT i zasoby informacyjne;

(ii) przyznawanie praw dostępu fizycznego do krytycznych zasobów ICT wyłącznie upoważnionym osobom, zgodnie z zasadami wiedzy koniecznej i minimalizacji uprawnień i na zasadzie *ad hoc*;

(iii) monitorowanie dostępu fizycznego do wskazanych przez podmiot finansowy obiektów, ośrodków przetwarzania danych i wyznaczonych obszarów wrażliwych, gdzie znajdują się zasoby ICT albo zasoby informacyjne, bądź zarówno zasoby ICT, jak i zasoby informacyjne;

(iv) dokonywanie przeglądu praw dostępu fizycznego, aby zapewnić niezwłoczne cofanie zbędnych praw dostępu.

Do celów lit. e) pkt (i) podmioty finansowe określają okres zatrzymywania, uwzględniając cele biznesowe i cele w zakresie bezpieczeństwa informacji, powody zarejestrowania zdarzenia w rejestrach oraz wyniki oceny ryzyka związanego z ICT.

Do celów lit. e) pkt (ii) podmioty finansowe korzystają w miarę możliwości ze specjalnych kont do wykonywania zadań administracyjnych w ramach systemów ICT. W miarę możliwości i w stosownych przypadkach podmioty finansowe wprowadzają zautomatyzowane rozwiązania na potrzeby procesu zarządzania dostępem uprzywilejowanym.

Do celów lit. g) pkt (i) działania w zakresie identyfikowania i rejestrowania muszą być współmierne do znaczenia obiektów, ośrodków przetwarzania danych i wyznaczonych obszarów wrażliwych oraz do krytyczności prowadzonych w nich operacji lub znajdujących się w nich systemów ICT.

Do celów lit. g) pkt (iii) monitorowanie musi być współmierne do klasyfikacji ustanowionej zgodnie z art. 8 ust. 1 rozporządzenia (UE) 2022/2554 i krytyczności obszaru, do którego uzyskuje się dostęp.

ROZDZIAŁ III
WYKRYWANIE INCYDENTÓW ZWIĄZANYCH Z ICT I REAGOWANIE NA NIE

Artykuł 22
Polityka zarządzania incydentami związanymi z ICT

W ramach mechanizmów służących do wykrywania nietypowych działań, w tym problemów związanych z wydajnością sieci ICT i incydentów związanych z ICT, podmioty finansowe opracowują, dokumentują i wdrażają politykę dotyczącą incydentów związanych z ICT, za pośrednictwem której:

a) dokumentują proces zarządzania incydentami związanymi z ICT, o którym mowa w art. 17 rozporządzenia (UE) 2022/2554;

b) sporządzają wykaz odpowiednich osób wyznaczonych do kontaktów pełniących funkcje wewnętrzne oraz interesariuszy zewnętrznych bezpośrednio zaangażowanych w kwestie związane z bezpieczeństwem operacji ICT, w tym:

   (i) wykrywanie i monitorowanie cyberzagrożeń;

   (ii) wykrywanie nietypowych działań;

   (iii) zarządzanie podatnościami;

c) ustanawiają, wdrażają i obsługują mechanizmy techniczne, organizacyjne i operacyjne służące wspieraniu procesu zarządzania incydentami związanymi z ICT, uwzględniając mechanizmy umożliwiające szybkie wykrywanie nietypowych działań i zachowań zgodnie z art. 23 niniejszego rozporządzenia;

d) zatrzymują wszystkie dowody dotyczące incydentów związanych z ICT przez okres nie dłuższy niż okres konieczny do realizacji celów, dla których zgromadzono te dane, współmiernie do krytyczności funkcji biznesowych, procesów wspierających oraz zasobów ICT i zasobów informacyjnych, których dotyczy dany incydent, zgodnie z [art. 15 rozporządzenia delegowanego Komisji (UE) [...]/[...] [rozporządzenie delegowane Komisji w sprawie klasyfikacji incydentów związanych z ICT][11] i z wszelkimi obowiązującymi wymogami w zakresie zatrzymywania danych przewidzianymi w prawie Unii;

e) ustanawiają i wdrażają mechanizmy analizy znaczących lub powtarzających się incydentów i wzorców związanych z ICT pod względem liczby i występowania incydentów związanych z ICT.

Do celów lit. d) podmioty finansowe przechowują dowody, o których mowa w tej literze, w bezpieczny sposób.

[11] (UP: Proszę wstawić [odniesienie do niniejszego rozporządzenia i jego tytuł])

Artykuł 23

Wykrywanie nietypowych działań i kryteria wykrywania incydentów związanych z ICT oraz reagowania na nie

1. Podmioty finansowe jasno określają role i obowiązki w celu skutecznego wykrywania incydentów związanych z ICT i nietypowych działań oraz reagowania na nie.

2. Mechanizm pozwalający na szybkie wykrywanie nietypowych działań, w tym problemów związanych z wydajnością sieci ICT i incydentów związanych z ICT, o którym mowa w art. 10 ust. 1 rozporządzenia (UE) 2022/2554, umożliwia podmiotom finansowym:

   a) gromadzenie, monitorowanie i analizowanie wszystkich poniższych elementów:

      (i) czynników wewnętrznych i zewnętrznych, w tym co najmniej rejestrów zgromadzonych zgodnie z art. 12 niniejszego rozporządzenia, informacji pochodzących z funkcji biznesowych i funkcji ICT oraz wszelkich problemów zgłaszanych przez użytkowników podmiotu finansowego;

      (ii) potencjalnych wewnętrznych i zewnętrznych cyberzagrożeń, z uwzględnieniem scenariuszy powszechnie stosowanych przez agresorów oraz scenariuszy opartych na analizie zagrożeń;

      (iii) powiadomień o incydentach związanych z ICT od zewnętrznego dostawcy usług ICT podmiotu finansowego wykrytych w systemach i sieciach ICT zewnętrznego dostawcy usług ICT, które mogą mieć wpływ na podmiot finansowy;

   b) identyfikowanie nietypowych działań i zachowań oraz wdrożenie narzędzi generujących ostrzeżenia o nietypowych działaniach i zachowaniach, przynajmniej w odniesieniu do zasobów ICT i zasobów informacyjnych wspierających krytyczne lub istotne funkcje;

   c) priorytetowe traktowanie ostrzeżeń, o których mowa w lit. b), aby umożliwić zarządzanie wykrytymi incydentami związanymi z ICT w oczekiwanym czasie rozwiązania określonym przez podmioty finansowe, zarówno w godzinach pracy, jak i poza nimi;

   d) rejestrowanie, analizowanie i ocenę wszelkich istotnych informacji na temat wszystkich nietypowych działań i zachowań – automatycznie lub ręcznie.

   Do celów lit. b) narzędzia, o których mowa w tej literze, obejmują narzędzia zapewniające automatyczne ostrzeżenia oparte na wcześniej określonych zasadach w celu identyfikacji nieprawidłowości mających wpływ na kompletność i integralność źródeł danych lub gromadzenia rejestrów.

3. Podmioty finansowe chronią wszelkie zapisy dotyczące nietypowych działań przed manipulacją i nieuprawnionym dostępem, gdy są one przechowywane, przesyłane oraz, w stosownych przypadkach, wykorzystywane.

4. Podmioty finansowe rejestrują wszystkie istotne informacje dotyczące każdego wykrytego nietypowego działania, umożliwiające:

   a) określenie daty i godziny wystąpienia nietypowego działania;

   b) określenie daty i godziny wykrycia nietypowego działania;

c) określenie rodzaju nietypowego działania.

5. Aby uruchomić procesy wykrywania incydentów związanych z ICT i reagowania na nie, o których to procesach mowa w art. 10 ust. 2 rozporządzenia (UE) 2022/2554, podmioty finansowe uwzględniają wszystkie poniższe kryteria:

a) przesłanki świadczące o tym, że w systemie lub sieci ICT mogło dojść do złośliwego działania lub że taki system lub taka sieć ICT mogły zostać zagrożone;

b) utrata danych wykryta w odniesieniu do dostępności, autentyczności, integralności i poufności danych;

c) wykryty niekorzystny wpływ na transakcje i operacje podmiotu finansowego;

d) niedostępność systemów i sieci ICT.

6. Do celów ust. 5 podmioty finansowe biorą również pod uwagę krytyczność usług, których dotyczy incydent.

ROZDZIAŁ IV
ZARZĄDZANIE CIĄGŁOŚCIĄ DZIAŁANIA W ZAKRESIE ICT

Artykuł 24
Elementy strategii na rzecz ciągłości działania w zakresie ICT

1. Podmioty finansowe uwzględniają w swojej strategii na rzecz ciągłości działania w zakresie ICT, o której mowa w art. 11 ust. 1 rozporządzenia (UE) 2022/2554, wszystkie następujące elementy:

a) opis:

(i) celów strategii na rzecz ciągłości działania w zakresie ICT, w tym wzajemnych powiązań między ICT a ogólną ciągłością działania, z uwzględnieniem wyników analizy wpływu na działalność (BIA), o której mowa w art. 11 ust. 5 rozporządzenia (UE) 2022/2554;

(ii) zakresu ustaleń, planów, procedur i mechanizmów zapewniających ciągłość działania w zakresie ICT, w tym ograniczeń i wyłączeń;

(iii) ram czasowych, które mają być objęte ustaleniami, planami, procedurami i mechanizmami zapewniającymi ciągłość działania w zakresie ICT;

(iv) kryteriów uruchamiania i dezaktywowania planów ciągłości działania w zakresie ICT, planów reagowania i przywracania sprawności ICT oraz planów działań informacyjnych na wypadek wystąpienia sytuacji kryzysowej;

b) przepisy dotyczące:

(i) zarządzania i organizacji na potrzeby wdrażania strategii na rzecz ciągłości działania w zakresie ICT, w tym ról, obowiązków i procedur eskalacji zapewniających dostępność wystarczających zasobów;

(ii) dostosowania między planami ciągłości działania w zakresie ICT a ogólnymi planami ciągłości działania, w odniesieniu do co najmniej wszystkich poniższych elementów:

1) potencjalnych scenariuszy awarii, w tym scenariuszy, o których mowa w art. 26 ust. 2 niniejszego rozporządzenia;

2) celów związanych z przywracaniem sprawności, określających, że podmiot finansowy musi być w stanie przywrócić funkcjonowanie swoich krytycznych lub istotnych funkcji po zakłóceniach w ramach zakładanego czasu przywrócenia sprawności oraz akceptowalnego poziomu utraty danych;

(iii) opracowywania planów ciągłości działania w zakresie ICT w przypadku poważnych zakłóceń działalności gospodarczej w ramach tych planów oraz określania hierarchii środków na rzecz ciągłości działania w zakresie ICT z zastosowaniem podejścia opartego na analizie ryzyka;

(iv) opracowywania, testowania i przeglądu planów reagowania i przywracania sprawności ICT, zgodnie z art. 25 i 26 niniejszego rozporządzenia;

(v) przeglądu skuteczności wdrożonych ustaleń, planów, procedur i mechanizmów zapewniających ciągłość działania w zakresie ICT, zgodnie z art. 26 niniejszego rozporządzenia;

(vi) dostosowania strategii na rzecz ciągłości działania w zakresie ICT do:

1) polityki komunikacyjnej, o której mowa w art. 14 ust. 2 rozporządzenia (UE) 2022/2554;

2) działań w zakresie komunikacji i zarządzania kryzysowego, o których mowa w art. 11 ust. 2 lit. e) rozporządzenia (UE) 2022/2554.

2. Oprócz wymogów, o których mowa w ust. 1, kontrahenci centralni zapewniają, aby ich strategia na rzecz ciągłości działania w zakresie ICT:

a) obejmowała maksymalny czas przywrócenia sprawności ich funkcji krytycznych nie dłuższy niż 2 godziny;

b) uwzględniała zewnętrzne powiązania i współzależności w obrębie infrastruktur finansowych, w tym systemów obrotu rozliczanych przez kontrahenta centralnego, systemów rozrachunku papierów wartościowych i płatności oraz instytucji kredytowych wykorzystywanych przez kontrahenta centralnego lub powiązanego kontrahenta centralnego;

c) zawierała wymóg wprowadzenia ustaleń mających na celu:

(i) zapewnienie ciągłości krytycznych lub istotnych funkcji kontrahenta centralnego w oparciu o scenariusze wystąpienia sytuacji nadzwyczajnej;

(ii) utrzymywanie zapasowej lokalizacji przetwarzania danych, która jest w stanie zapewnić ciągłość krytycznych lub istotnych funkcji kontrahenta centralnego, identycznej z głównym miejscem przetwarzania danych;

(iii) utrzymywanie zapasowej lokalizacji przetwarzania danych lub posiadanie natychmiastowego dostępu do niej, aby umożliwić pracownikom zapewnienie ciągłości świadczenia usług, jeżeli główne miejsce przetwarzania danych nie jest dostępne;

(iv) rozważenie konieczności posiadania dodatkowych lokalizacji przetwarzania danych, zwłaszcza jeżeli profile ryzyka głównej i zapasowej lokalizacji nie są na tyle zróżnicowane, aby z wystarczającą pewnością zagwarantować, że wszystkie cele kontrahenta centralnego z zakresu ciągłości działania zostaną zrealizowane we wszystkich scenariuszach.

Do celów lit. a) kontrahenci centralni realizują procedury i płatności na koniec dnia w wymaganym terminie i dniu w każdych okolicznościach.

Do celów lit. c) pkt (i) ustalenia, o których mowa w tej literze, dotyczą dostępności odpowiednich zasobów ludzkich, maksymalnej przerwy w świadczeniu funkcji krytycznych oraz pracy awaryjnej i przywrócenia sprawności funkcji przez systemy znajdujące się w lokalizacji zapasowej.

Do celów lit. c) pkt (ii) zapasowa lokalizacja przetwarzania danych, o której mowa w tej literze, musi mieć geograficzny profil ryzyka, który różni się od geograficznego profilu ryzyka głównego miejsca przetwarzania.

3. Oprócz wymogów, o których mowa w ust. 1, centralne depozyty papierów wartościowych zapewniają, aby ich strategia na rzecz ciągłości działania w zakresie ICT:

a) uwzględniała wszelkie powiązania i współzależności z użytkownikami, dostawcami najważniejszych mediów i usług, innymi centralnymi depozytami papierów wartościowych i innymi infrastrukturami rynkowymi;

b) zawierała wymóg, zgodnie z którym ustalenia dotyczące ciągłości działania w zakresie ICT muszą zapewniać, by zakładany czas przywrócenia sprawności krytycznych lub istotnych funkcji nie był dłuższy niż 2 godziny.

4. Oprócz wymogów, o których mowa w ust. 1, systemy obrotu zapewniają, aby ich strategia na rzecz ciągłości działania w zakresie ICT zapewniała, by:

a) obrót mógł zostać wznowiony w ciągu dwóch godzin lub blisko dwóch godzin od wystąpienia incydentu zakłócającego;

b) maksymalna ilość danych, które mogą zostać utracone w ramach jakiejkolwiek usługi informatycznej systemu obrotu w wyniku wystąpienia incydentu zakłócającego, była bliska zeru.

Artykuł 25

Testowanie planów ciągłości działania w zakresie ICT

1. Testując plany ciągłości działania w zakresie ICT zgodnie z art. 11 ust. 6 rozporządzenia (UE) 2022/2554, podmioty finansowe uwzględniają analizę wpływu na działalność (BIA) podmiotu finansowego oraz ocenę ryzyka związanego z ICT, o której mowa w art. 3 akapit pierwszy lit. b) niniejszego rozporządzenia.

2. Testując swoje plany ciągłości działania w zakresie ICT, o których mowa w ust. 1, podmioty finansowe oceniają, czy są w stanie zapewnić ciągłość krytycznych lub istotnych funkcji podmiotu finansowego. Testowanie to powinno:

a) być przeprowadzane na podstawie scenariuszy testowych, które symulują potencjalne zakłócenia, w tym odpowiedniego zestawu pesymistycznych, ale prawdopodobnych scenariuszy;

b) w stosownych przypadkach obejmować testowanie usług ICT świadczonych przez zewnętrznych dostawców usług ICT;

c) w przypadku podmiotów finansowych innych niż mikroprzedsiębiorstwa, o których mowa w art. 11 ust. 6 akapit drugi rozporządzenia (UE) 2022/2554 – obejmować scenariusze przełączania się z głównej infrastruktury ICT na nadmiarowe zdolności, kopie zapasowe i urządzenia redundantne;

d) być zaprojektowane tak, aby kwestionować założenia, na których opierają się plany ciągłości działania, w tym rozwiązania w zakresie zarządzania i plany działań informacyjnych na wypadek wystąpienia sytuacji kryzysowej;

e) obejmować procedury służące weryfikacji zdolności personelu podmiotów finansowych, zewnętrznych dostawców usług ICT, systemów ICT i usług ICT do odpowiedniego reagowania na scenariusze należycie uwzględnione zgodnie z art. 26 ust. 2.

Do celów lit. a) podmioty finansowe zawsze uwzględniają w ramach testowania scenariusze brane pod uwagę przy opracowywaniu planów ciągłości działania.

Do celów lit. b) podmioty finansowe należycie uwzględniają scenariusze związane z niewypłacalnością lub awariami zewnętrznych dostawców usług ICT lub z ryzykiem politycznym w jurysdykcjach zewnętrznych dostawców usług ICT, w stosownych przypadkach.

Do celów lit. c) w ramach testowania sprawdza się, czy co najmniej krytyczne lub istotne funkcje mogą być prawidłowo obsługiwane przez wystarczający czas oraz czy można przywrócić normalne funkcjonowanie.

3. Oprócz wymogów, o których mowa w ust. 2, kontrahenci centralni angażują w testowanie swoich planów ciągłości działania w zakresie ICT, o których mowa w ust. 1:

a) członków rozliczających;

b) usługodawców zewnętrznych;

c) odpowiednie instytucje w infrastrukturze finansowej, które kontrahenci centralny wskazali jako powiązane z nimi współzależnościami w swoich strategiach na rzecz ciągłości działania.

4. Oprócz wymogów, o których mowa w ust. 2, centralne depozyty papierów wartościowych angażują w testowanie swoich planów ciągłości działania w zakresie ICT, o których mowa w ust. 1, w stosownych przypadkach:

a) użytkowników centralnych depozytów papierów wartościowych;

b) dostawców najważniejszych mediów i usług;

c) inne centralne depozyty papierów wartościowych;

d) inne infrastruktury rynkowe;

e) wszelkie inne instytucje, które centralne depozyty papierów wartościowych wskazały jako powiązane z nimi współzależnościami w swoich strategiach na rzecz ciągłości działania.

5. Podmioty finansowe dokumentują wyniki testowania, o których mowa w ust. 1. Wszelkie niedoskonałości stwierdzone w ramach tego testowania powinny być analizowane, eliminowane i zgłaszane organowi zarządzającemu.

Artykuł 26
Plany reagowania i przywracania sprawności ICT

1. Opracowując plany reagowania i przywracania sprawności ICT, o których mowa w art. 11 ust. 3 rozporządzenia (UE) 2022/2554, podmioty finansowe uwzględniają wyniki przeprowadzonej przez podmiot finansowy analizy wpływu na działalność (BIA). Te plany reagowania i przywracania sprawności ICT powinny:

   a) określać warunki powodujące ich uruchamianie lub dezaktywowanie oraz wszelkie wyjątki dotyczące takiego uruchamiania lub dezaktywowania;

   b) zawierać opis, jakie działania należy podjąć w celu zapewnienia dostępności, integralności, ciągłości i przywrócenia sprawności co najmniej systemów i usług ICT wspierających krytyczne lub istotne funkcje podmiotu finansowego;

   c) być zaprojektowane z myślą o osiągnięciu celów związanych z przywracaniem sprawności podmiotów finansowych;

   d) być dokumentowane i udostępniane pracownikom zaangażowanym w realizację planów reagowania i przywracania sprawności ICT oraz być łatwo dostępne w sytuacjach awaryjnych;

   e) zapewniać zarówno krótko-, jak i długoterminowe warianty przywracania sprawności, w tym częściowe przywracanie sprawności systemów;

   f) określać cele planów reagowania i przywracania sprawności ICT oraz warunki uznania pomyślnego wykonania tych planów.

   Do celów lit. d) podmioty finansowe jasno określają role i obowiązki.

2. W planach reagowania i przywracania sprawności ICT, o których mowa w ust. 1, określa się odpowiednie scenariusze, w tym scenariusze poważnych zakłóceń działalności gospodarczej i zwiększonego prawdopodobieństwa wystąpienia zakłóceń. W planach tych opracowuje się scenariusze oparte na aktualnych informacjach na temat zagrożeń oraz na wnioskach wyciągniętych z wcześniejszych przypadków zakłóceń działalności gospodarczej. Podmioty finansowe należycie uwzględniają wszystkie następujące scenariusze:

   a) cyberataki i pracę awaryjną w trakcie przełączania się z głównej infrastruktury ICT na nadmiarowe zdolności, kopie zapasowe i urządzenia redundantne;

   b) scenariusze, w których jakość pełnienia krytycznej lub istotnej funkcji pogarsza się do niedopuszczalnego poziomu lub funkcja ta przestaje być pełniona, a także należycie uwzględniają potencjalny wpływ niewypłacalności lub innych rodzajów awarii któregokolwiek z odnośnych zewnętrznych dostawców usług ICT;

   c) częściowe lub całkowite awarie obiektów, w tym obiektów biurowych i lokali przedsiębiorstwa, oraz ośrodków przetwarzania danych;

   d) poważną awarię zasobów ICT lub infrastruktury łączności;

   e) niedostępność krytycznej liczby pracowników lub członków personelu odpowiedzialnych za zagwarantowanie ciągłości operacji;

   f) wpływ zdarzeń związanych ze zmianą klimatu i degradacją środowiska, klęsk żywiołowych, pandemii i ataków fizycznych, w tym włamań i ataków terrorystycznych;

g) ataki wewnętrzne;

h) niestabilność polityczną i społeczną, w tym, w stosownych przypadkach, w jurysdykcji zewnętrznego dostawcy usług ICT oraz w lokalizacji, w której dane są przechowywane i przetwarzane;

i) przerwy w dostawie energii elektrycznej na szeroką skalę.

3. W przypadku gdy podstawowe środki przywracania sprawności mogą nie być wykonalne w perspektywie krótkoterminowej ze względu na koszty, ryzyko, logistykę lub nieprzewidziane okoliczności, w planach reagowania i przywracania sprawności ICT, o których mowa w ust. 1, bierze się pod uwagę alternatywne warianty.

4. W ramach planów reagowania i przywracania sprawności ICT, o których mowa w ust. 1, podmioty finansowe rozważają i wdrażają środki zapewniające ciągłość w celu ograniczenia awarii zewnętrznych dostawców usług ICT wspierających krytyczne lub istotne funkcje podmiotu finansowego.

ROZDZIAŁ V
SPRAWOZDANIE Z PRZEGLĄDU RAM ZARZĄDZANIA RYZYKIEM ZWIĄZANYM Z ICT

Artykuł 27

Format i treść sprawozdania z przeglądu ram zarządzania ryzykiem związanym z ICT

1. Podmioty finansowe przedkładają sprawozdanie z przeglądu ram zarządzania ryzykiem związanym z ICT, o którym mowa w art. 6 ust. 5 rozporządzenia (UE) 2022/2554, w formacie elektronicznym umożliwiającym wyszukiwanie.

2. Podmioty finansowe uwzględniają wszystkie poniższe informacje w sprawozdaniu, o którym mowa w ust. 1:

a) część wprowadzającą, która:

(i) zawiera wyraźne określenie podmiotu finansowego, który jest przedmiotem sprawozdania, oraz, w stosownych przypadkach, opis jego struktury grupy;

(ii) zawiera opis kontekstu sprawozdania pod względem charakteru, skali i stopnia złożoności usług, działań i operacji podmiotu finansowego, jego organizacji, zidentyfikowanych funkcji krytycznych, strategii, dużych bieżących projektów lub działań, relacji i jego zależności od wewnętrznych i zleconych usług i systemów ICT lub skutków, jakie całkowita utrata lub poważna degradacja takich systemów miałaby pod względem krytycznych lub istotnych funkcji oraz efektywności rynku;

(iii) zawiera podsumowanie istotnych zmian w ramach zarządzania ryzykiem związanym z ICT od czasu poprzedniego sprawozdania;

(iv) zawiera na poziomie wykonawczym podsumowanie obecnego i krótkoterminowego profilu ryzyka związanego z ICT, krajobrazu zagrożeń, ocenionej skuteczności kontroli oraz poziomu cyberbezpieczeństwa podmiotu finansowego;

b) datę zatwierdzenia sprawozdania przez organ zarządzający podmiotu finansowego;

c) opis przyczyny przeglądu ram zarządzania ryzykiem związanym z ICT zgodnie z art. 6 ust. 5 rozporządzenia (UE) 2022/2554;

d) daty rozpoczęcia i zakończenia okresu objętego przeglądem;

e) wskazanie funkcji odpowiedzialnej za przegląd;

f) opis istotnych zmian i ulepszeń ram zarządzania ryzykiem związanym z ICT od czasu poprzedniego przeglądu;

g) podsumowanie ustaleń z przeglądu oraz szczegółową analizę i ocenę wagi słabości i niedoskonałości ram zarządzania ryzykiem związanym z ICT oraz luk w tych ramach w okresie objętym przeglądem;

h) opis środków mających na celu wyeliminowanie stwierdzonych słabości, niedoskonałości i luk, w tym wszystkie poniższe elementy:

   (i) podsumowanie środków wdrożonych w celu wyeliminowania stwierdzonych słabości, niedoskonałości i luk;

   (ii) przewidywaną datę wdrożenia środków i terminy związane z kontrolą wewnętrzną wdrażania, w tym informacje na temat stanu zaawansowania wdrażania tych środków w dniu sporządzenia sprawozdania, wraz z wyjaśnieniem, w stosownych przypadkach, czy istnieje ryzyko, że terminy mogą nie zostać dotrzymane;

   (iii) narzędzia, które mają zostać wykorzystane, oraz określenie funkcji odpowiedzialnej za wdrożenie środków, ze wskazaniem, czy narzędzia i funkcje mają charakter wewnętrzny czy zewnętrzny;

   (iv) opis wpływu planowanych zmian środków na zasoby budżetowe, ludzkie i materialne podmiotu finansowego, w tym zasoby przeznaczone na wdrożenie wszelkich środków naprawczych;

   (v) w stosownych przypadkach informacje na temat procesu informowania właściwego organu;

   (vi) w przypadku gdy stwierdzone słabości, niedoskonałości lub luki nie są objęte środkami naprawczymi – szczegółowe wyjaśnienie kryteriów zastosowanych do analizy wpływu tych słabości, niedoskonałości lub luk, w celu oceny powiązanego rezydualnego ryzyka związanego z ICT, oraz kryteriów zastosowanych przy akceptacji powiązanego ryzyka rezydualnego;

i) informacje na temat planowanych dalszych zmian ram zarządzania ryzykiem związanym z ICT;

j) wnioski płynące z przeglądu ram zarządzania ryzykiem związanym z ICT;

k) informacje na temat poprzednich przeglądów, w tym:

   (i) wykaz dotychczasowych przeglądów;

   (ii) w stosownych przypadkach – stan wdrożenia środków naprawczych określonych w ostatnim sprawozdaniu;

   (iii) w przypadku gdy środki naprawcze zaproponowane w ramach poprzednich przeglądów okazały się nieskuteczne lub spowodowały pojawienie się nieoczekiwanych wyzwań – opis sposobu, w jaki można ulepszyć te środki naprawcze, lub opis tych nieoczekiwanych wyzwań;

l) źródła informacji wykorzystane do przygotowania sprawozdania, w tym wszystkie następujące elementy:

(i) w przypadku podmiotów finansowych innych niż mikroprzedsiębiorstwa, o których mowa w art. 6 ust. 6 rozporządzenia (UE) 2022/2554 – wyniki audytów wewnętrznych;

(ii) wyniki ocen zgodności;

(iii) wyniki testów operacyjnej odporności cyfrowej oraz, w stosownych przypadkach, wyniki zaawansowanych testów, opartych na testach penetracyjnych pod kątem wyszukiwania zagrożeń (TLPT), narzędzi, systemów i procesów ICT;

(iv) źródła zewnętrzne.

Do celów lit. c), w przypadku gdy przegląd wszczęto zgodnie z instrukcjami nadzorczymi lub wnioskami wynikającymi z odpowiednich testów lub procesów audytu operacyjnej odporności cyfrowej, sprawozdanie zawiera wyraźne odniesienia do takich instrukcji lub wniosków, umożliwiające określenie przyczyny wszczęcia przeglądu. W przypadku wszczęcia przeglądu w następstwie incydentów związanych z ICT sprawozdanie zawiera wykaz wszystkich incydentów związanych z ICT wraz z analizą przyczyn incydentów.

Do celów lit. f) opis zawiera analizę wpływu zmian na strategię podmiotu finansowego w zakresie operacyjnej odporności cyfrowej, na ramy kontroli wewnętrznej podmiotu finansowego w zakresie ICT oraz na zarządzanie ryzykiem związanym z ICT przez podmiot finansowy.

TYTUŁ III – UPROSZCZONE RAMY ZARZĄDZANIA RYZYKIEM ZWIĄZANYM Z ICT DOTYCZĄCE PODMIOTÓW FINANSOWYCH, O KTÓRYCH MOWA W ART. 16 UST. 1 ROZPORZĄDZENIA (UE) 2022/2554

ROZDZIAŁ I
UPROSZCZONE RAMY ZARZĄDZANIA RYZYKIEM ZWIĄZANYM Z ICT

Artykuł 28
Zarządzanie i organizacja

1. Podmioty finansowe, o których mowa w art. 16 ust. 1 rozporządzenia (UE) 2022/2554, posiadają ramy zarządzania wewnętrznego i kontroli, które zapewniają skuteczne i ostrożne zarządzanie ryzykiem związanym z ICT w celu osiągnięcia wysokiego poziomu operacyjnej odporności cyfrowej.

2. Podmioty finansowe, o których mowa w ust. 1, w ramach swoich uproszczonych ram zarządzania ryzykiem związanym z ICT zapewniają, aby ich organ zarządzający:

   a) ponosił ogólną odpowiedzialność za zapewnienie, aby uproszczone ramy zarządzania ryzykiem związanym z ICT umożliwiały realizację strategii biznesowej podmiotu finansowego zgodnie ze skłonnością tego podmiotu finansowego do podejmowania ryzyka, oraz zapewniały uwzględnienie ryzyka związanego z ICT w tym kontekście;

   b) określał jasne role i obowiązki w odniesieniu do wszystkich zadań związanych z ICT;

   c) określał cele w zakresie bezpieczeństwa informacji i wymogi dotyczące ICT;

   d) zatwierdzał następujące elementy, nadzorował je i okresowo poddawał je przeglądowi:

      (i) klasyfikację zasobów informacyjnych podmiotu finansowego, o której mowa w art. 30 ust. 1 niniejszego rozporządzenia, wykaz najważniejszych zidentyfikowanych rodzajów ryzyka oraz analiza wpływu na działalność i powiązane polityki;

      (ii) plany ciągłości działania podmiotu finansowego oraz środki reagowania i przywracania sprawności, o których mowa w art. 16 ust. 1 lit. f) rozporządzenia (UE) 2022/2554;

   e) przydzielał budżet niezbędny do zaspokojenia potrzeb podmiotu finansowego w zakresie operacyjnej odporności cyfrowej w odniesieniu do wszystkich rodzajów zasobów, w tym odpowiednich programów zwiększania świadomości w zakresie bezpieczeństwa ICT oraz szkoleń w zakresie operacyjnej odporności cyfrowej i umiejętności ICT dla wszystkich pracowników, i przynajmniej raz w roku dokonywał przeglądu tego budżetu;

   f) określał i wdrażał polityki i środki zawarte w rozdziałach I, II i III niniejszego tytułu w celu identyfikacji i oceny ryzyka związanego z ICT, na które narażony jest podmiot finansowy, oraz zarządzania tym ryzykiem;

g) identyfikował i wdrażał procedury, protokoły i narzędzia ICT, które są niezbędne do ochrony wszystkich zasobów informacyjnych i zasobów ICT;

h) zapewniał, aby pracownicy podmiotu finansowego posiadali aktualną wiedzę i umiejętności wystarczające do zrozumienia i oceny ryzyka związanego z ICT i jego wpływu na działalność podmiotu finansowego, współmiernie do ryzyka związanego z ICT będącego przedmiotem zarządzania;

i) określał ustalenia w zakresie sprawozdawczości, w tym częstotliwość, formę i treść sprawozdań dla organu zarządzającego w zakresie bezpieczeństwa informacji i operacyjnej odporności cyfrowej.

3. Podmioty finansowe, o których mowa w ust. 1, mogą, zgodnie z unijnym i krajowym prawem sektorowym, zlecić zadania dotyczące weryfikacji zgodności z wymogami w zakresie zarządzania ryzykiem związanym z ICT dostawcom usług ICT wewnątrz grupy lub zewnętrznym dostawcom usług ICT. W przypadku takiego outsourcingu podmioty finansowe pozostają w pełni odpowiedzialne za sprawdzanie zgodności z wymogami dotyczącymi zarządzania ryzykiem związanym z ICT.

4. Podmioty finansowe, o których mowa w ust. 1, zapewniają odpowiednie rozdzielenie i niezależność funkcji kontroli i funkcji audytu wewnętrznego.

5. Podmioty finansowe, o których mowa w ust. 1, zapewniają, aby ich uproszczone ramy zarządzania ryzykiem związanym z ICT podlegały audytowi wewnętrznemu przeprowadzanemu przez audytorów zgodnie z planami tych podmiotów finansowych dotyczącymi audytów. Audytorzy posiadają wystarczającą wiedzę, umiejętności i wiedzę fachową w zakresie ryzyka związanego z ICT oraz są niezależni. Częstotliwość i przedmiot audytów ICT są współmierne do ryzyka związanego z ICT danego podmiotu finansowego.

6. Na podstawie wyników audytu, o którym mowa w ust. 5, podmioty finansowe, o których mowa w ust. 1, zapewniają terminową weryfikację i wdrożenie środków zaradczych w następstwie krytycznych ustaleń audytu ICT.

Artykuł 29
Polityka i środki bezpieczeństwa informacji

1. Podmioty finansowe, o których mowa w art. 16 ust. 1 rozporządzenia (UE) 2022/2554, opracowują, dokumentują i wdrażają politykę bezpieczeństwa informacji w kontekście uproszczonych ram zarządzania ryzykiem związanym z ICT. W ramach tej polityki bezpieczeństwa informacji określa się ogólne zasady i przepisy dotyczące ochrony poufności, integralności, dostępności i autentyczności danych i usług świadczonych przez te podmioty finansowe.

2. W oparciu o ich politykę bezpieczeństwa informacji, o której mowa w ust. 1, podmioty finansowe, o których mowa w ust. 1, ustanawiają i wdrażają środki bezpieczeństwa ICT w celu ograniczenia ich ekspozycji na ryzyko związane z ICT, w tym środki ograniczające ryzyko wdrożone przez zewnętrznych dostawców usług ICT.

   Środki bezpieczeństwa ICT obejmują wszystkie środki, o których mowa w art. 30–38.

Artykuł 30
Klasyfikacja zasobów informacyjnych i zasobów ICT

1. W kontekście uproszczonych ram zarządzania ryzykiem związanym z ICT, o których mowa w art. 16 ust. 1 lit. a) rozporządzenia (UE) 2022/2554, podmioty finansowe, o których mowa w ust. 1 tego artykułu, identyfikują, klasyfikują i dokumentują wszystkie krytyczne lub istotne funkcje, zasoby informacyjne i wspierające je zasoby ICT oraz ich współzależności. W razie potrzeby podmioty finansowe dokonują przeglądu tej identyfikacji i klasyfikacji.

2. Podmioty finansowe, o których mowa w ust. 1, określają wszystkie krytyczne lub istotne funkcje wspierane przez zewnętrznych dostawców usług ICT.

Artykuł 31
Zarządzanie ryzykiem związanym z ICT

1. Podmioty finansowe, o których mowa w art. 16 ust. 1 rozporządzenia (UE) 2022/2554, uwzględniają w swoich uproszczonych ramach zarządzania ryzykiem związanym z ICT wszystkie następujące elementy:

   a) określenie poziomu tolerancji ryzyka w odniesieniu do ryzyka związanego z ICT, zgodnie ze skłonnością podmiotu finansowego do podejmowania ryzyka;

   b) identyfikację i ocenę ryzyka związanego z ICT, na które narażony jest podmiot finansowy;

   c) określenie strategii ograniczania ryzyka przynajmniej w odniesieniu do czynników ryzyka związanego z ICT, które wykraczają poza poziom tolerancji ryzyka podmiotu finansowego;

   d) monitorowanie skuteczności strategii łagodzenia ryzyka, o których mowa w lit. c);

   e) identyfikację i ocenę wszelkich rodzajów ryzyka związanego z ICT i bezpieczeństwem informacji wynikającego z wszelkich poważnych zmian w systemie ICT lub usługach, procesach bądź procedurach ICT oraz z wyników testów bezpieczeństwa ICT i po każdym poważnym incydencie związanym z ICT.

2. Podmioty finansowe, o których mowa w ust. 1, okresowo przeprowadzają i dokumentują ocenę ryzyka ICT współmiernie do profilu ryzyka związanego z ICT podmiotów finansowych.

3. Podmioty finansowe, o których mowa w ust. 1, stale monitorują zagrożenia i podatności, które są istotne dla ich krytycznych lub istotnych funkcji oraz ich zasobów informacyjnych i zasobów ICT, i regularnie dokonują przeglądu scenariuszy ryzyka mających wpływ na te krytyczne lub istotne funkcje.

4. Podmioty finansowe, o których mowa w ust. 1, określają progi alarmowe i kryteria uruchamiania i inicjowania procesów reagowania na incydenty związane z ICT.

Artykuł 32
Bezpieczeństwo fizyczne i środowiskowe

1. Podmioty finansowe, o których mowa w art. 16 ust. 1 rozporządzenia (UE) 2022/2554, określają i wdrażają środki bezpieczeństwa fizycznego opracowane w oparciu o krajobraz zagrożeń i zgodnie z klasyfikacją, o której mowa w art. 30

ust. 1 niniejszego rozporządzenia, ogólny profil ryzyka zasobów ICT oraz dostępnych zasobów informacyjnych.

2. Środki, o których mowa w ust. 1, chronią obiekty podmiotów finansowych oraz, w stosownych przypadkach, ośrodków przetwarzania danych podmiotów finansowych, w których znajdują się zasoby ICT i zasoby informacyjne, przed nieuprawnionym dostępem, atakami i wypadkami, a także przed zagrożeniami środowiskowymi.

3. Ochrona przed zagrożeniami środowiskowymi jest współmierna do znaczenia odnośnych obiektów i, w stosownych przypadkach, ośrodków przetwarzania danych oraz do krytyczności prowadzonych w nich operacji lub znajdujących się w nich systemów ICT.

ROZDZIAŁ II
DALSZE ELEMENTY SYSTEMÓW, PROTOKOŁÓW I NARZĘDZI MINIMALIZUJĄCYCH WPŁYW RYZYKA ZWIĄZANEGO Z ICT

Artykuł 33
Kontrola dostępu

1. Podmioty finansowe, o których mowa w art. 16 ust. 1 rozporządzenia (UE) 2022/2554, opracowują, dokumentują i wdrażają procedury kontroli logicznego i fizycznego dostępu oraz egzekwują stosowanie tych procedur, monitorują je i okresowo dokonują ich przeglądu. Procedury te zawierają następujące elementy kontroli logicznego i fizycznego dostępu:

   a) prawa dostępu do zasobów informacyjnych, zasobów ICT i wspieranych przez nie funkcji, a także do miejsc prowadzenia działalności podmiotu finansowego o znaczeniu krytycznym, zgodnie z zasadami wiedzy koniecznej, potrzeby koniecznej i minimalizacji uprawnień, w tym również w kontekście dostępu zdalnego i dostępu awaryjnego;

   b) rozliczalność użytkowników, która zapewnia możliwość identyfikacji użytkowników w odniesieniu do działań prowadzonych w systemach ICT;

   c) procedury zarządzania kontem umożliwiające udzielanie, zmianę lub cofanie praw dostępu do kont użytkownika i kont generycznych, uwzględniając generyczne konta administratora;

   d) metody uwierzytelniania współmierne do klasyfikacji, o której mowa w art. 30 ust. 1, oraz do ogólnego profilu ryzyka zasobów ICT, opartych na wiodących praktykach;

   e) prawa dostępu są okresowo weryfikowane i cofane, gdy nie są już potrzebne.

   Do celów lit. c) podmiot finansowy udziela dostępu uprzywilejowanego, dostępu awaryjnego i dostępu administratora do wszystkich systemów ICT na zasadzie potrzeby koniecznej lub na zasadzie *ad hoc*; dostęp ten rejestruje się zgodnie z art. 34 ust. 1 lit. f).

   Do celów lit. d) podmioty finansowe stosują solidne metody uwierzytelniania oparte na wiodących praktykach w zakresie zdalnego dostępu do sieci podmiotów

finansowych, dostępu uprzywilejowanego, a także dostępu do zasobów ICT wspierających krytyczne lub istotne funkcje, które są publicznie dostępne.

Artykuł 34
Bezpieczeństwo operacji ICT

Podmioty finansowe, o których mowa w art. 16 ust. 1 rozporządzenia (UE) 2022/2554, w ramach swoich systemów, protokołów i narzędzi oraz w odniesieniu do wszystkich zasobów ICT:

a) monitorują cykl życia wszystkich zasobów ICT i zarządzają nimi;

b) w stosownych przypadkach monitorują, czy zasoby ICT są wspierane przez zewnętrznych dostawców usług ICT podmiotów finansowych;

c) określają wymogi w zakresie pojemności ich zasobów ICT oraz środki służące utrzymaniu i poprawie dostępności i efektywności systemów ICT oraz zapobieganiu niedoborom pojemności w zakresie ICT przed ich wystąpieniem;

d) przeprowadzają zautomatyzowane skanowanie pod kątem podatności i oceny zasobów ICT współmierne do ich klasyfikacji, o której mowa w art. 30 ust. 1, oraz do ogólnego profilu ryzyka zasobów ICT, a także wprowadzają poprawki w celu wyeliminowania stwierdzonych podatności;

e) zarządzają ryzykiem związanym z przestarzałymi, niewspieranymi lub dotychczasowymi zasobami ICT;

f) rejestrują zdarzenia związane z kontrolą logicznego i fizycznego dostępu, operacjami ICT, w tym działaniami w zakresie ruchu w systemie i ruchu w sieci, oraz z zarządzaniem zmianą w systemach ICT;

g) określają i wdrażają środki służące do monitorowania i analizowania informacji na temat nietypowych działań i zachowań w odniesieniu do krytycznych lub istotnych operacji ICT;

h) wdrażają środki służące monitorowaniu istotnych i aktualnych informacji na temat cyberzagrożeń;

i) wdrażają środki mające na celu identyfikację ewentualnych wycieków informacji, kodu złośliwego i innych zagrożeń bezpieczeństwa oraz powszechnie znanych podatności obecnych w oprogramowaniu i sprzęcie komputerowym, a także sprawdzanie odpowiednich nowych aktualizacji zabezpieczeń.

Do celów lit. f) podmioty finansowe dostosowują poziom szczegółowości rejestrów do ich celu i wykorzystania zasobów ICT generujących wpisy do tych rejestrów.

Artykuł 35
Bezpieczeństwo danych, systemu i sieci

Podmioty finansowe, o których mowa w art. 16 ust. 1 rozporządzenia (UE) 2022/2554, w ramach swoich systemów, protokołów i narzędzi opracowują i wdrażają zabezpieczenia chroniące sieci przed włamaniami i wykorzystaniem danych niezgodnie z przeznaczeniem i przyczyniające się do zachowania dostępności, autentyczności, integralności i poufności danych. W szczególności podmioty finansowe, uwzględniając klasyfikację, o której mowa w art. 30 ust. 1 niniejszego rozporządzenia, ustanawiają wszystkie następujące elementy:

a) określenie i wdrożenie środków ochrony danych wykorzystywanych, przesyłanych i przechowywanych;

b) określenie i wdrożenie środków bezpieczeństwa dotyczących korzystania z oprogramowania, nośników danych, systemów i urządzeń końcowych wykorzystywanych do przesyłania i przechowywania danych podmiotu finansowego;

c) określenie i wdrożenie środków mających na celu zapobieganie i wykrywanie nieuprawnionych połączeń z siecią podmiotu finansowego oraz zabezpieczenie ruchu między sieciami wewnętrznymi podmiotu finansowego a internetem i innymi połączeniami zewnętrznymi;

d) określenie i wdrożenie środków zapewniających dostępność, autentyczność, integralność i poufność danych podczas transmisji w sieci;

e) proces bezpiecznego usuwania danych znajdujących się w obiektach podmiotu finansowego lub przechowywanych na zewnątrz, których podmiot finansowy nie musi już gromadzić ani przechowywać;

f) proces bezpiecznego pozbywania się lub wycofywania z eksploatacji urządzeń do przechowywania danych w obiektach lub przechowywanych na zewnątrz urządzeń do przechowywania danych, które zawierają informacje poufne;

g) określenie i wdrożenie środków służących zapewnieniu, aby telepraca i korzystanie z prywatnych urządzeń końcowych nie miały negatywnego wpływu na zdolność podmiotu finansowego do prowadzenia działalności krytycznej w odpowiedni, terminowy i bezpieczny sposób.

Artykuł 36
Testy bezpieczeństwa ICT

1. Podmioty finansowe, o których mowa w art. 16 ust. 1 rozporządzenia (UE) 2022/2554, ustanawiają i wdrażają plan testów bezpieczeństwa ICT w celu potwierdzenia skuteczności ich środków bezpieczeństwa ICT opracowanych zgodnie z art. 33, 34 i 35 oraz art. 37 i 38 niniejszego rozporządzenia. Podmioty finansowe zapewniają, aby plan ten uwzględniał zagrożenia i podatności zidentyfikowane w kontekście uproszczonych ram zarządzania ryzykiem związanym z ICT, o których mowa w art. 31 niniejszego rozporządzenia.

2. Podmioty finansowe, o których mowa w ust. 1, dokonują przeglądu, oceny i testów środków bezpieczeństwa ICT, biorąc pod uwagę ogólny profil ryzyka zasobów ICT podmiotu finansowego.

3. Podmioty finansowe, o których mowa w ust. 1, monitorują i oceniają wyniki testów bezpieczeństwa oraz bezzwłocznie odpowiednio aktualizują swoje środki bezpieczeństwa w przypadku systemów ICT wspierających krytyczne lub istotne funkcje.

Artykuł 37
Pozyskiwanie, rozwój i utrzymanie systemów ICT

Podmioty finansowe, o których mowa w art. 16 ust. 1 rozporządzenia (UE) 2022/2554, opracowują i wdrażają, w stosownych przypadkach, procedurę regulującą pozyskiwanie, rozwój i utrzymanie systemów ICT zgodnie z podejściem opartym na analizie ryzyka. Procedura ta:

a) zapewnia, aby przed pozyskaniem lub rozwijaniem systemów ICT wymogi funkcjonalne i niefunkcjonalne, w tym wymogi dotyczące bezpieczeństwa informacji, były jasno określone i zatwierdzone przez daną funkcję biznesową;

b) zapewnia testowanie i zatwierdzanie systemów ICT przed ich pierwszym użyciem i przed wprowadzeniem zmian w środowisku produkcyjnym;

c) obejmuje określenie środków mających na celu ograniczenie ryzyka niezamierzonych zmian lub zamierzonej manipulacji systemami ICT podczas opracowywania i wdrażania w środowisku produkcyjnym.

Artykuł 38
Zarządzanie projektami ICT i zmianą w systemach ICT

1. Podmioty finansowe, o których mowa w art. 16 ust. 1 rozporządzenia (UE) 2022/2554, opracowują, dokumentują i wdrażają procedurę zarządzania projektami ICT oraz określają role i obowiązki związane z jej wdrożeniem. Procedura ta obejmuje wszystkie etapy projektów ICT od ich rozpoczęcia do ich zakończenia.

2. Podmioty finansowe, o których mowa w ust. 1, opracowują, dokumentują i wdrażają procedurę zarządzania zmianą w systemach ICT w celu zapewnienia, aby wszystkie zmiany w systemach ICT były rejestrowane, testowane, oceniane, zatwierdzane, wdrażane i weryfikowane w sposób kontrolowany oraz przy zastosowaniu odpowiednich zabezpieczeń w celu zachowania operacyjnej odporności cyfrowej podmiotu finansowego.

Rozdział III
ZARZĄDZANIE CIĄGŁOŚCIĄ DZIAŁANIA W ZAKRESIE ICT

Artykuł 39
Elementy planu ciągłości działania w zakresie ICT

1. Podmioty finansowe, o których mowa w art. 16 ust. 1 rozporządzenia (UE) 2022/2554, opracowują swoje plany ciągłości działania w zakresie ICT, uwzględniając wyniki analizy ich ekspozycji na poważne zakłócenia działalności gospodarczej i scenariusze w tym zakresie oraz wpływ tych zakłóceń i scenariuszy, na które ich zasoby ICT wspierające krytyczne lub istotne funkcje mogą być narażone, w tym scenariusz cyberataku.

2. Plany ciągłości działania w zakresie ICT, o których mowa w ust. 1:

   a) zatwierdza organ zarządzający podmiotu finansowego;

   b) są udokumentowane i łatwo dostępne w przypadku sytuacji awaryjnej lub kryzysowej;

   c) przeznaczają wystarczające zasoby na ich wykonanie;

   d) określają planowane poziomy i ramy czasowe przywrócenia sprawności i wznowienia funkcji oraz kluczowych wewnętrznych i zewnętrznych zależności, w tym zewnętrznych dostawców usług ICT;

   e) określają warunki, które mogą spowodować uruchomienie planów ciągłości działania w zakresie ICT, oraz działania, jakie należy podjąć w celu

zapewnienia dostępności, ciągłości i przywrócenia sprawności zasobów ICT podmiotów finansowych wspierających krytyczne lub istotne funkcje;

f) określają środki przywracania sprawności i odzyskiwania krytycznych lub istotnych funkcji biznesowych, procesów wspierających, zasobów informacyjnych i ich współzależności w celu uniknięcia niekorzystnego wpływu na funkcjonowanie podmiotów finansowych;

g) identyfikują procedury i środki określające zakres danych, które obejmuje kopia zapasowa, oraz minimalną częstotliwość tworzenia kopii zapasowej, w oparciu o krytyczność funkcji wykorzystującej te dane;

h) uwzględniają warianty alternatywne stosowane w sytuacji, gdy przywrócenie sprawności może nie być wykonalne w perspektywie krótkoterminowej ze względu na koszty, ryzyko, logistykę lub nieprzewidziane okoliczności;

i) określają wewnętrzne i zewnętrzne ustalenia dotyczące komunikacji, w tym plany eskalacji;

j) są aktualizowane zgodnie z wnioskami wyciągniętymi z incydentów, testów, stwierdzonych nowych rodzajów ryzyka i zagrożeń, zmienionych celów związanych z przywracaniem sprawności, istotnych zmian w organizacji podmiotu finansowego oraz w zasobach ICT wspierających funkcje krytyczne lub biznesowe.

Do celów lit. f) środki, o których mowa w tej literze, zapewniają łagodzenie skutków awarii kluczowych zewnętrznych dostawców usług.

Artykuł 40
Testowanie planów ciągłości działania

1. Podmioty finansowe, o których mowa w art. 16 ust. 1 rozporządzenia (UE) 2022/2554, co najmniej raz w roku testują swoje plany ciągłości działania, o których mowa w art. 39 niniejszego rozporządzenia, w tym scenariusze, o których mowa w tym artykule, co najmniej raz w roku w odniesieniu do procedur tworzenia kopii zapasowych i przywracania systemów lub przy każdej istotnej zmianie planu ciągłości działania.

2. Testowanie planów ciągłości działania, o którym mowa w ust. 1, wykazuje, że podmioty finansowe, o których mowa w tym ustępie, są w stanie utrzymać rentowność swojej działalności do czasu przywrócenia operacji krytycznych i zidentyfikować wszelkie niedoskonałości w tych planach.

3. Podmioty finansowe, o których mowa w ust. 1, dokumentują wyniki testowania planów ciągłości działania, a wszelkie niedoskonałości stwierdzone w ramach tych testów są analizowane, eliminowane i zgłaszane organowi zarządzającemu.

ROZDZIAŁ IV
SPRAWOZDANIE Z PRZEGLĄDU UPROSZCZONYCH RAM ZARZĄDZANIA RYZYKIEM ZWIĄZANYM Z ICT

Artykuł 41
Format i treść sprawozdania z przeglądu uproszczonych ram zarządzania ryzykiem związanym z ICT

1. Podmioty finansowe, o których mowa w art. 16 ust. 1 rozporządzenia (UE) 2022/2554, przedkładają sprawozdanie z przeglądu ram zarządzania ryzykiem związanym z ICT, o którym mowa w ust. 2 tego artykułu, w formacie elektronicznym umożliwiającym wyszukiwanie.

2. Sprawozdanie, o którym mowa w ust. 1, zawiera wszystkie następujące informacje:

   a) część wprowadzającą, która zawiera:

      (i) opis kontekstu sprawozdania pod względem charakteru, skali i stopnia złożoności usług, działań i operacji podmiotu finansowego, jego organizacji, zidentyfikowanych funkcji krytycznych, strategii, dużych bieżących projektów lub działań oraz relacji i zależności podmiotu finansowego od wewnętrznych i zleconych na zasadzie outsourcingu usług i systemów ICT lub skutków, jakie całkowita utrata lub poważna degradacja takich systemów miałaby dla krytycznych lub istotnych funkcji oraz efektywności rynku;

      (ii) podsumowanie na poziomie wykonawczym stwierdzonego obecnego i krótkoterminowego ryzyka związanego z ICT, krajobrazu zagrożeń, ocenionej skuteczności kontroli oraz poziomu cyberbezpieczeństwa podmiotu finansowego;

      (iii) informacje na temat obszaru będącego przedmiotem sprawozdania;

      (iv) podsumowanie istotnych zmian w ramach zarządzania ryzykiem związanym z ICT od czasu poprzedniego sprawozdania;

      (v) podsumowanie i opis wpływu istotnych zmian w uproszczonych ramach zarządzania ryzykiem związanym z ICT od czasu poprzedniego sprawozdania;

   b) w stosownych przypadkach data zatwierdzenia sprawozdania przez organ zarządzający podmiotu finansowego;

   c) opis przyczyn wszczęcia przeglądu, w tym:

      (i) w przypadku wszczęcia przeglądu zgodnie z instrukcjami nadzorczymi – dowody potwierdzające takie instrukcje;

      (ii) w przypadku wszczęcia przeglądu w następstwie wystąpienia incydentów związanych z ICT – wykaz wszystkich incydentów związanych z ICT wraz z analizą przyczyn incydentów;

   d) daty rozpoczęcia i zakończenia okresu objętego przeglądem;

   e) informacje na temat osoby odpowiedzialnej za przegląd;

f) podsumowanie ustaleń oraz samoocenę wagi słabości, niedoskonałości i luk stwierdzonych w ramach zarządzania ryzykiem związanym z ICT w okresie objętym przeglądem, w tym ich szczegółową analizę;

g) środki naprawcze określone na potrzeby wyeliminowania słabości, niedoskonałości i luk w uproszczonych ramach zarządzania ryzykiem związanym z ICT oraz przewidywany termin wdrożenia tych środków, w tym działania następcze w związku ze słabościami, niedociągnięciami i lukami wskazanymi w poprzednich sprawozdaniach, w przypadku gdy te słabości, niedociągnięcia i luki nie zostały jeszcze usunięte;

h) ogólne wnioski dotyczące przeglądu uproszczonych ram zarządzania ryzykiem związanym z ICT, w tym wszelkie dalsze planowane zmiany.

TYTUŁ IV PRZEPISY KOŃCOWE

Artykuł 42
Wejście w życie

Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po jego opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich.

Sporządzono w Brukseli dnia 13.3.2024 r.

W imieniu Komisji
Przewodnicząca
Ursula VON DER LEYEN