UKNF | URZĄD KOMISJI NADZORU FINANSOWEGO

Spojrzenie na wymagania DORA z perspektywy polskiego nadzoru

Departament Cyberbezpieczeństwa UKNF
Warszawa, wrzesień 2023 r.

Zagrożenia rynku finansowego

1. Zwiększający się zakres cyfryzacji i sieci wzajemnych powiązań
2. Brak lub niespójne wymagania prawne
3. Transgraniczność usług
4. Zwiększona aktywność cyberprzestępców
5. Ryzyko dostawców ICT, w tym ryzyko koncentracji

UKNF | URZĄD KOMISJI NADZORU FINANSOWEGO

Główne zagrożenia według ENISA – 2020

- złośliwe oprogramowanie (malware)
- ataki z wykorzystaniem złośliwego kodu na stronach internetowych
- phishing, czyli bezpośrednie wyłudzanie poufnych informacji lub za pomocą złośliwego oprogramowania
- ataki na aplikacje internetowe
- SPAM – niechciana korespondencja
- ataki DDoS – czyli blokowanie dostępu do usług poprzez sztuczne generowanie wzmożonego ruchu
- kradzież tożsamości
- naruszenie poufności, integralności lub dostępności danych
- zagrożenia wewnętrzne powodowane przez pracowników
- Botnet-y – sieci komputerów przejętych przez przestępców
- ingerencja fizyczna, uszkodzenia oraz kradzież
- wyciek danych
- ataki ransomware w celu wyłudzenia okupu za odszyfrowanie lub nieujawnianie wykradzionych danych
- cyberszpiegostwo
- kradzież kryptowalut (cryptojacking)

Główne zagrożenia według ENISA – wyzwania 2030

1. Podatności oprogramowania w łańcuchu dostaw
2. Zaawansowane kampanie dezinformacyjne
3. Wzrost nadzoru nad danymi cyfrowymi przez rządy autorytarne, a w konsekwencji ryzyko utraty prywatności
4. Błędy ludzkie i ataki przeprowadzane na starsze (niewspierane) urządzenia i systemy
5. Ukierunkowane ataki (np. ransomware) z wykorzystaniem IoT
6. Luki w zabezpieczeniach infrastruktury oraz obiektów wykorzystywanych w przestrzeni kosmicznej
7. Wzrost zaawansowanych zagrożeń hybrydowych – zmiana modus operandi – wykorzystywanie AI i uczenia maszynowego do przeprowadzania nowych typów ataków
8. Niedobory specjalistów z obszaru nowych technologii
9. Transgraniczni dostawcy usług ICT jako pojedyncze punkty awarii
10. Nadużywanie sztucznej inteligencji – manipulowanie danymi uczenia się algorytmów, zaawansowana korelacja danych

Pakiet regulacji

UKNF | URZĄD KOMISJI NADZORU FINANSOWEGO

W latach 2019-2022 organy unijne wydały szerszy pakiet regulacji z obszaru cyberbezpieczeństwa i cyberodporności

NIS2

- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii
- Przyjęcie i opublikowanie przepisów implementujących dyrektywę do 17 października 2024 r., stosowanie przepisów od 18 października 2024 r.

DORA

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego
- Stosowane od 17 stycznia 2025 r.

CSA

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych
- Stosowane od 28 czerwca 2021 r.

CER

- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych
- Przyjęcie i opublikowanie przepisów implementujących dyrektywę do 17 października 2024 r., stosowanie przepisów od 18 października 2024 r.

CRA

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi (zmieniające rozporządzenie (UE) 2019/1020)
- W trakcie uzgodnień

1

Powszechność technologii ICT w epoce cyfrowej:

- technologie informacyjno-komunikacyjne (ICT) stanowią wsparcie dla złożonych systemów informacyjnych
- ICT napędzają gospodarkę w najważniejszych sektorach, w tym w sektorach rynku finansowego oraz wzmacniają funkcjonowanie rynku wewnętrznego

2

Powiązania między podmiotami i infrastrukturą rynku finansowego:

- wzajemne powiązania między podmiotami, rynkami finansowymi oraz infrastrukturami rynku finansowego, w tym współzależności między ich systemami, stanowią podatność systemową
- lokalne incydenty szybko się rozprzestrzeniają z podmiotów finansowych na cały system bez przeszkód związanych z granicami geograficznymi

3

Negatywny wpływ na rynki wewnętrzne usług finansowych:

- rozbieżności legislacyjne, w tym w obszarze ryzyka związanego z ICT, mają negatywny wpływ na funkcjonowanie, konkurencyjność rynku wewnętrznego oraz utrudnienia w świadczeniu usług podmiotom prowadzącym działalność transgraniczną
- rozbieżności wynikające ze zmian na poziomie krajowym powodują przeszkody dla funkcjonowania rynku wewnętrznego (np. zakłócenie konkurencyjności przy różnym podejściu do testowania operacyjnej odporności cyfrowej lub monitorowania ryzyka zewnętrznych dostawców usług ICT)

4

Brak lub nakładanie się przepisów w istotnych obszarach:

- częściowe uwzględnienie przepisów dot. ryzyka ICT na szczeblu UE powoduje braki lub nakładanie się przepisów, w szczególności w obszarach: zgłaszanie incydentów związanych z ICT oraz testowanie operacyjnej odporności cyfrowej
- stosowanie nakładających się przepisów wpływa na niespójności, nieefektywność kosztową, wyzwania operacyjne dla podmiotów prowadzących działalność transgraniczną lub posiadających kilka zezwoleń (w szczególności w obszarze zwalczania ryzyka ICT, łagodzenia skutków incydentów ICT)

5

Spójne podejście w oparciu o zasadę proporcjonalności:

- wzmocnienie zaufania do systemu finansowego oraz ochrony jego stabilności, w szczególności w czasach dużej zależności od systemów, platform i infrastruktur ICT, które mają wpływ na zwiększenie ryzyka cyfrowego
- przestrzeganie podstawowych zasad cyberbezpieczeństwa powinno pozwolić na uniknięcie obciążania gospodarki znacznymi kosztami dzięki zminimalizowaniu wpływu i kosztów zakłóceń funkcjonowania ICT

UKNF | URZĄD KOMISJI NADZORU FINANSOWEGO

Stosowanie DORA – jako rozporządzenie unijne stanowi akt prawny bezpośrednio stosowany we wszystkich krajach UE

DORA

Cele wdrożenia rozporządzenia

Rozporządzenie UE 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego (DORA)

1. **Zarządzanie ryzykiem ICT** – zgodnie z zasadą proporcjonalności oraz odpowiedzialności podmiotów nadzorowanych
2. Ujednolicenie, rozbudowanie i scentralizowanie **zgłaszania incydentów poważnych ICT** przez podmioty finansowe na poziomie krajowym i unijnym
3. **Testowanie operacyjnej odporności cyfrowej**, w tym cykliczne testy penetracyjne systemów, protokołów oraz narzędzi ICT, testy TLPT
4. **Zarządzanie ryzykiem dostawców usług ICT**, w tym rozszerzenie obowiązków związanych z analizą ryzyka koncentracji
5. **Stworzenie ram kontroli i nadzoru** krajowych oraz unijnych organów nadzoru, w tym nad kluczowymi dostawcami usług ICT i łańcuchem dostaw

UKNF | URZĄD KOMISJI NADZORU FINANSOWEGO

Terminy

Opublikowanie – **27.12.2022 r.**

Wejście w życie – 20-go dnia po opublikowaniu

Opracowanie 16 aktów wykonawczych – **12-18 m-cy**

Stosowanie – **17.01.2025 r.**

Wymagania

564 szczegółowe wymagania

399 wymagań do zrealizowania przez UKNF

9 rozdziałów, **64** artykuły

106 motywów

Zakres podmiotowy

KNF

Podmioty nadzorowane

Zewnętrzni dostawcy usług ICT

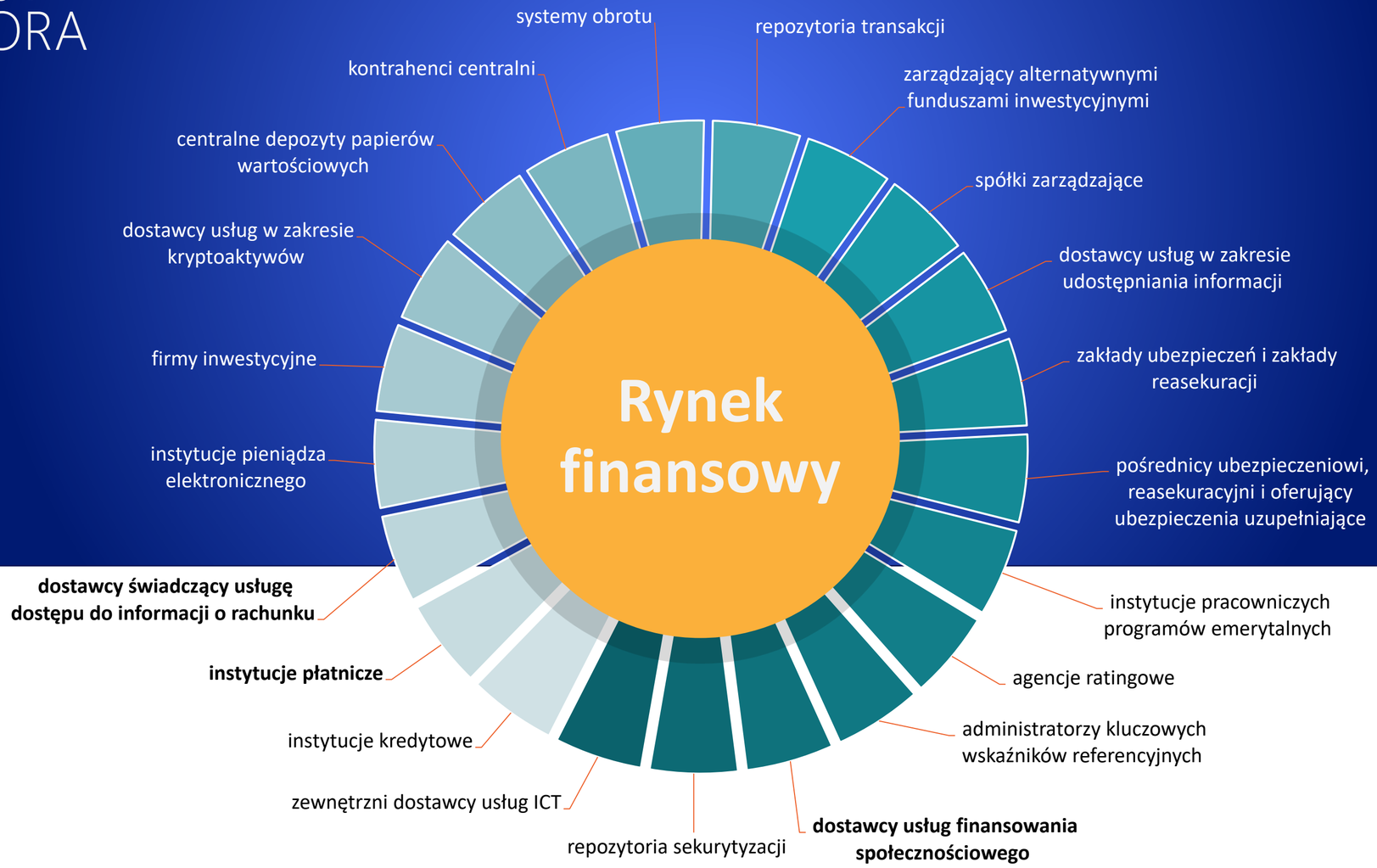
Akty powiązane

Dyrektywa NIS2 – dotyczy cyberbezpieczeństwa

Ustawa o krajowym systemie cyberbezpieczeństwa – dotyczy operatorów usługi kluczowej

Dyrektywa CER – dotyczy ochrony infrastruktury krytycznej

Podmioty objęte DORA



Co przyniesie DORA

Rozporządzenie DORA wprowadza spójny standard zarządzania ryzykiem ICT na całym rynku finansowym UE

Zapewnia wymianę informacji oraz zwraca uwagę na ryzyko związane z łańcuchem dostaw, w tym ryzyko koncentracji

1

Zarządzanie ryzykiem ICT:

- spójna organizacja i ramy zarządzania ryzykiem ICT
- podstawowe zasady i wymagania bezpieczeństwa dla systemów, protokołów i narzędzi ICT
- monitorowanie i kontrola bezpieczeństwa systemów, protokołów i narzędzi ICT
- wykrywanie, reagowanie i przywracanie sprawności, w tym tworzenie kopii zapasowych
- okresowe przeglądy, raportowanie i doskonalenie

2

Zarządzanie incydentami ICT:

- spójne obowiązki zgłaszania incydentów ICT przez wszystkie podmioty rynku finansowego (incydenty poważne związane z ICT, incydenty z PSD2, incydenty związane z fizyczną odpornością, zgłoszenia dotyczące uruchomienia zarządzania kryzysowego)
- centralizacja zbierania zgłoszeń i analizowania incydentów na poziomie krajowym i unijnym

3

Testowanie operacyjnej odporności cyfrowej:

- wymagania dotyczące testowania operacyjnej odporności cyfrowej, w tym ocena podatności i skanowanie, analiza oprogramowania, ocena bezpieczeństwa sieci, przeglądy kodu źródłowego, testy wydajności, testy penetracyjne
- Zaawansowane testy TLPT oparte na analizie zagrożeń (*red team*) - testy działających na bieżąco systemów krytycznych, kompetencje testerów
- certyfikacja podmiotów uprawnionych do przeprowadzania testów TLPT

4

Zarządzanie ryzykiem dostawców usług ICT:

- spójne ramy zarządzania ryzykiem dostawców usług ICT
- identyfikowanie i prowadzenie rejestru umów dostawców usług ICT z uwzględnieniem całego łańcucha dostaw
- standaryzacja postanowień umownych
- ocena ryzyka koncentracji w obszarze ICT

5

Ramy nadzoru i kontroli nad dostawcami usług ICT:

- wyznaczanie kluczowych zewnętrznych dostawców usług ICT
- wnioski o udzielenie informacji, dochodzenia ogólne, kontrole oraz bieżący nadzór wiodącego organu nadzoru (UE)
- wysokie kary pieniężne – maksymalnie 1% średniego dziennego światowego obrotu
- działania następcze od publikacji po zawieszenie

DORA w perspektywie Banków Spółdzielczych

UKNF | URZĄD KOMISJI NADZORU FINANSOWEGO

Główne wyzwania

Rozporządzenie UE 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego (DORA)

1. **Banki Spółdzielcze nie są wyłączone ze stosowania DORA i z perspektywy KNF powinny wypełniać jej wymagania**
2. **Identyfikacja funkcji biznesowych** wpieranych przez ICT, w tym **w szczególności funkcji krytycznych lub istotnych –** punkt startowy do dalszych działań
3. **Zgodność z rekomendacją D ułatwi wdrożenie DORA, ale nie jest wystarczająca.** W ramach kontroli oraz ankiet KRI identyfikujemy nieprawidłowości w stosowaniu rekomendacji D
4. **Testowanie operacyjnej odporności cyfrowej –** zarządzanie podatnościami, testy, w tym: testy penetracyjne, wydajnościowe, skanowanie infrastruktury
5. **Wysoka zależność** w obszarze usług ICT (banki zrzeszające, dostawcy usług ICT, systemy ochrony) powierzanych podmiotom trzecim

DORA

Wybrane wymagania dla Zarządu

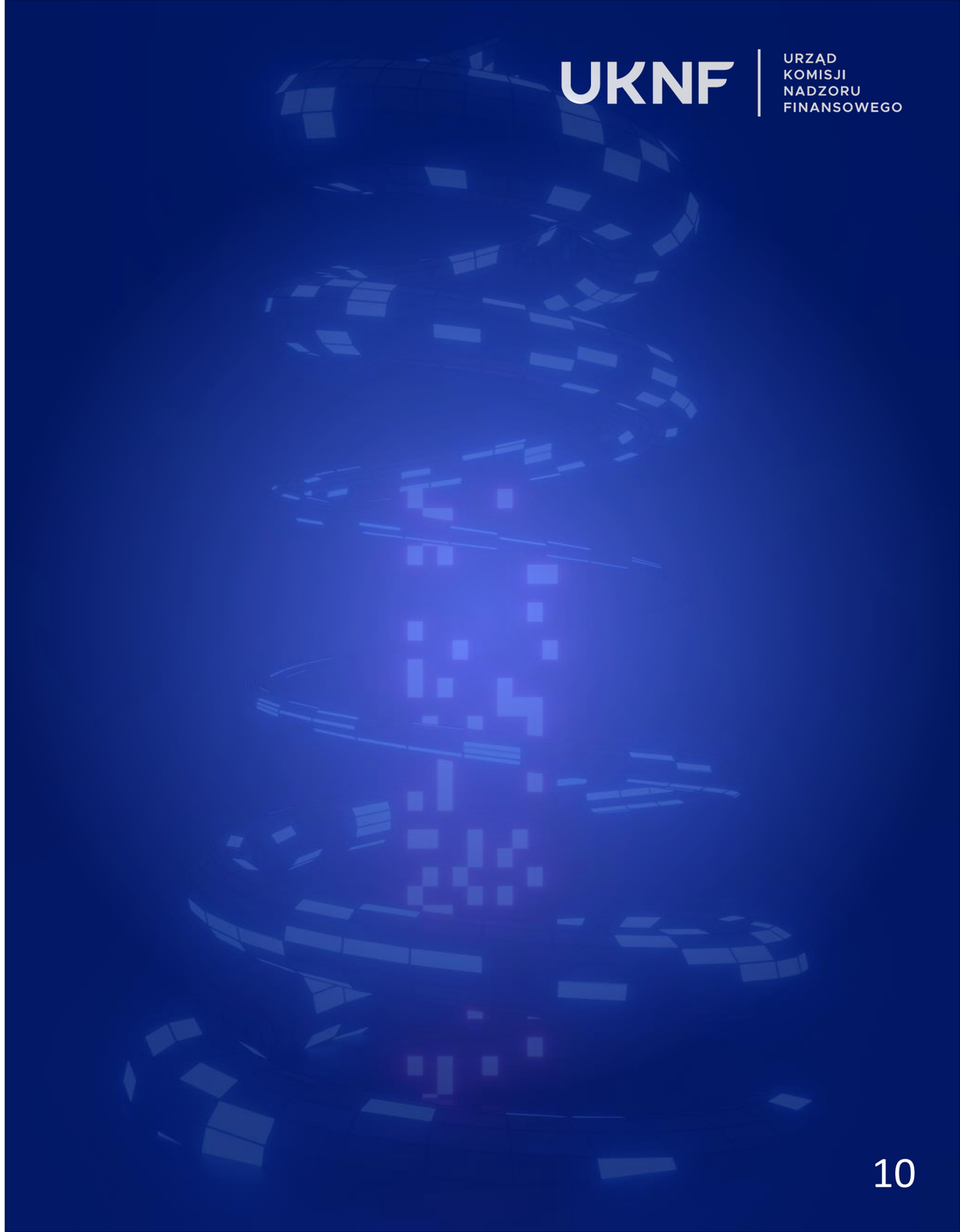
1. **Zarząd określa, zatwierdza i nadzoruje** ramy zarzadzania ryzykiem związanym z ICT **oraz ponosi ostateczną odpowiedzialność za zarządzanie ryzykiem ICT**

2. **Zatwierdza i nadzoruje** wdrażanie strategii na rzecz ciągłości działania. **Wdraża polityki zapewniające** wysokie standardy dostępności, autentyczności, integralności i poufności danych.

3. **Ustala wyraźnie role i obowiązki** w odniesieniu do wszystkich funkcji związanych z ICT. **Zatwierdza politykę** korzystania z dostawców usług ICT

4. **Ponosi pełną odpowiedzialność** za określenie i zatwierdzenie strategii operacyjnej odporności cyfrowej, w tym za określenie poziomu tolerancji ryzyka ICT

5. **Przydziela** odpowiedni budżet w zakresie operacyjnej odporności cyfrowej. **Zatwierdza plan audytów** ICT.



AKTY WYKONAWCZE DO DORA

UKNF | URZĄD KOMISJI NADZORU FINANSOWEGO

1 KONSULTACJE PUBLICZNE - 1 PAKIET AKTÓW WYKONAWCZYCH

16.06.2023 – 11.09.2023

2 KONSULTACJE PUBLICZNE - 2 PAKIET AKTÓW WYKONAWCZYCH

Listopad/Grudzień 2023

3 FINALIZACJA 1 PAKIETU AKTÓW WYKONAWCZYCH

17.01.2024

4 FINALIZACJA 2 PAKIETU AKTÓW WYKONAWCZYCH

17.07.2024

Pierwszy pakiet aktów wykonawczych:

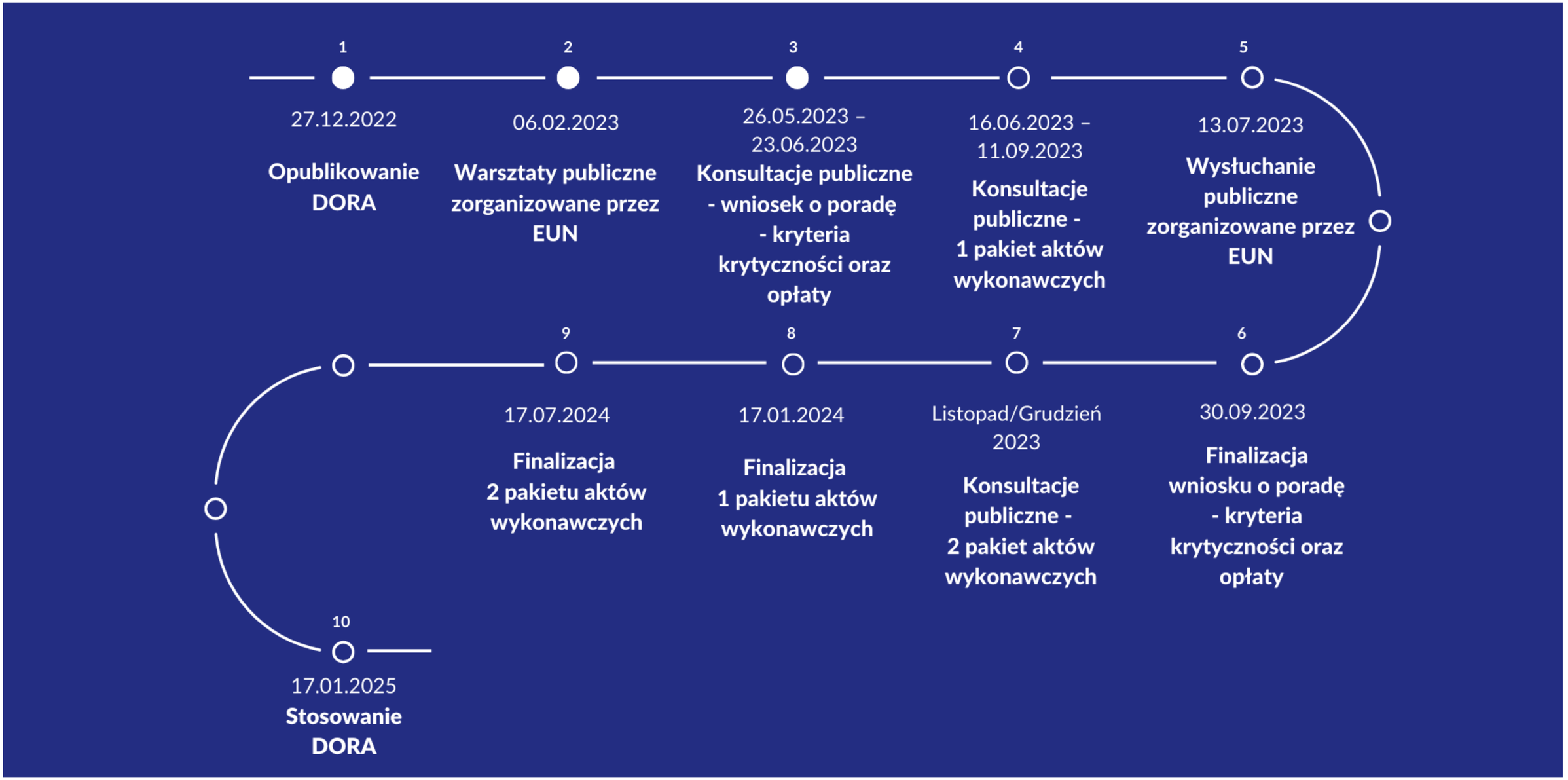
- **RTS** w sprawie ram zarządzania ryzykiem ICT (art. 15)
- **RTS** w sprawie uproszczonych ram zarządzania ryzykiem ICT (art. 16.3)
- **RTS** w sprawie kryteriów klasyfikacji incydentów ICT (art. 18.3)
- **ITS** w sprawie standardowych wzorów rejestru informacji (art. 28.9)
- **RTS** w sprawie polityki dotyczącej korzystania z usług świadczonych przez dostawców ICT (art. 28.10)
- **Porada** w sprawie kryteriów wyznaczania kluczowych dostawców usług ICT (art. 31.8)
- **Porada** w sprawie opłat za nadzór (art. 43.2)

Drugi pakiet aktów wykonawczych:

- **Wytyczne** w sprawie szacowania kosztów i strat spowodowanych poważnymi incydentami ICT (art. 11.11)
- **RTS** w sprawie zasad zgłaszania poważnych incydentów ICT (art. 20.a)
- **ITS** w sprawie standardowych formularzy, wzorów i procedur zgłaszania poważnych incydentów ICT (art. 20.b)
- **Sprawozdanie** z wykonalności dalszej centralizacji zgłaszania poważnych incydentów ICT (EU Hub) (art. 21)
- **RTS** w sprawie określenia testów penetracyjnych (TLPT zgodnie z TIBER-EU) (art. 26.11)
- **RTS** w sprawie obszarów do ustalenia i oceny przy podzlecaniu usług ICT wspierających krytyczne lub istotne funkcje (art. 30.5)
- **Wytyczne** w sprawie współpracy między europejskimi i krajowymi organami w zakresie nadzoru nad DORA (art. 32.7)
- **RTS** w sprawie harmonizacji warunków nadzoru (art. 41)

CO PRZED NAMI?

UKNF | URZĄD KOMISJI NADZORU FINANSOWEGO



UKNF | URZĄD KOMISJI NADZORU FINANSOWEGO

1

Webinarium CEDUR pt. "**Rozporządzenie w sprawie operacyjnej odporności cyfrowej sektora finansowego i inne akty powiązane. Omówienie wybranych wymagań DORA**", 5 edycji 18, 19, 20, 25 i 26 września 2023 roku

Celem webinarium jest przedstawienie podmiotom nadzorowanym wybranych wymagań wynikających z Rozporządzenia w sprawie operacyjnej odporności cyfrowej sektora finansowego.

Webinarium jest skierowane do **przedstawicieli podmiotów rynku finansowego** nadzorowanych przez Komisję Nadzoru Finansowego.

2

Webinarium CEDUR "**Dobre praktyki w zakresie zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach spółdzielczych w oparciu o wymogi wynikające z Rekomendacji D**", 18 października 2023 roku

Celem webinarium jest przedstawienie problematyki zarządzania obszarami technologii informacyjnej i **bezpieczeństwa środowiska teleinformatycznego** dla banków spółdzielczych.

Webinarium jest skierowane do **członków zarządów nadzorujących obszar operacyjny i obszar ryzyka, kierowników działów IT, kierowników działów bezpieczeństwa IT**, zarządzających komórkami ryzyka operacyjnego oraz pracowników innych komórek organizacyjnych zaangażowanych w proces zarządzania obszarami IT i bezpieczeństwa teleinformatycznego w bankach spółdzielczych.

UKNF | URZĄD KOMISJI NADZORU FINANSOWEGO

Dziękuję za uwagę

Zapraszamy na profile UKNF