

Co przyniesie DORA?



Zwiększający się zakres cyfryzacji i sieci wzajemnych powiązań



Brak lub niespójne wymagania prawne



Transgraniczność usług



Zwiększona aktywność cyberprzestępców



Ryzyko dostawców ICT, w tym ryzyko koncentracji

Główne zagrożenia według ENISA – 2020

- złośliwe oprogramowanie (malware)
- ataki z wykorzystaniem złośliwego kodu na stronach internetowych
- phishing, czyli bezpośrednie wyłudzenie 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

W 2022 roku 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

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



Zapewnienie cyfrowej odporności operacyjnej podmiotów rynku finansowego



Ujednolicenie i harmonizacja obowiązujących przepisów



Ujednolicenie i harmonizacja ram zarządzania ryzykiem ICT, w tym ryzykiem koncentracji dostawców usług ICT



Umożliwienie wymiany informacji między podmiotami nadzorowanymi



Stworzenie ram kontroli krajowych oraz unijnych organów nadzoru, w tym nad kluczowymi dostawcami usług ICT i łańcuchem dostaw



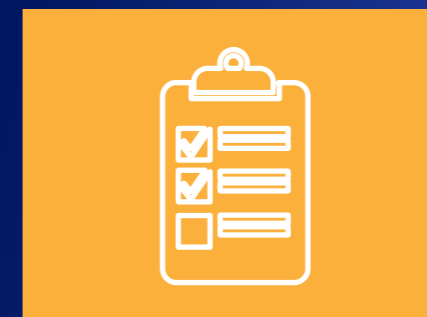
Terminy

Opublikowanie – **27.12.2022 r.**

Wejście w życie – 20-go dnia po opublikowaniu

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

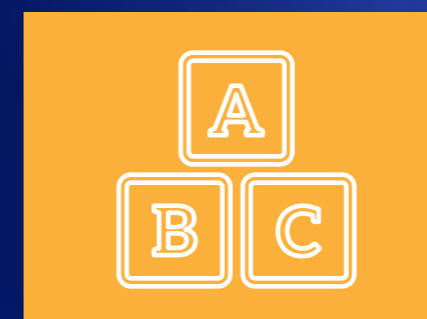
Stosowanie – **17.01.2025 r.**



Wymagania

9 rozdziałów, 64 artykuły

106 motywów



Zakres podmiotowy

Organy nadzoru

Podmioty rynku finansowego

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

Akty wykonawcze RTSy i ITSy

1

Zarządzanie ryzykiem ICT

- RTS w sprawie ram zarządzania ryzykiem ICT
- RTS w sprawie uproszczonych ram zarządzania ryzykiem ICT
- RTS w sprawie TLPT zgodnie z TIBER-EU
- RTS w sprawie polityki korzystania z usług ICT
- RTS w sprawie podwykonawstwa kluczowych lub ważnych funkcji w ramach usług ICT

2

Raportowanie Incydentów

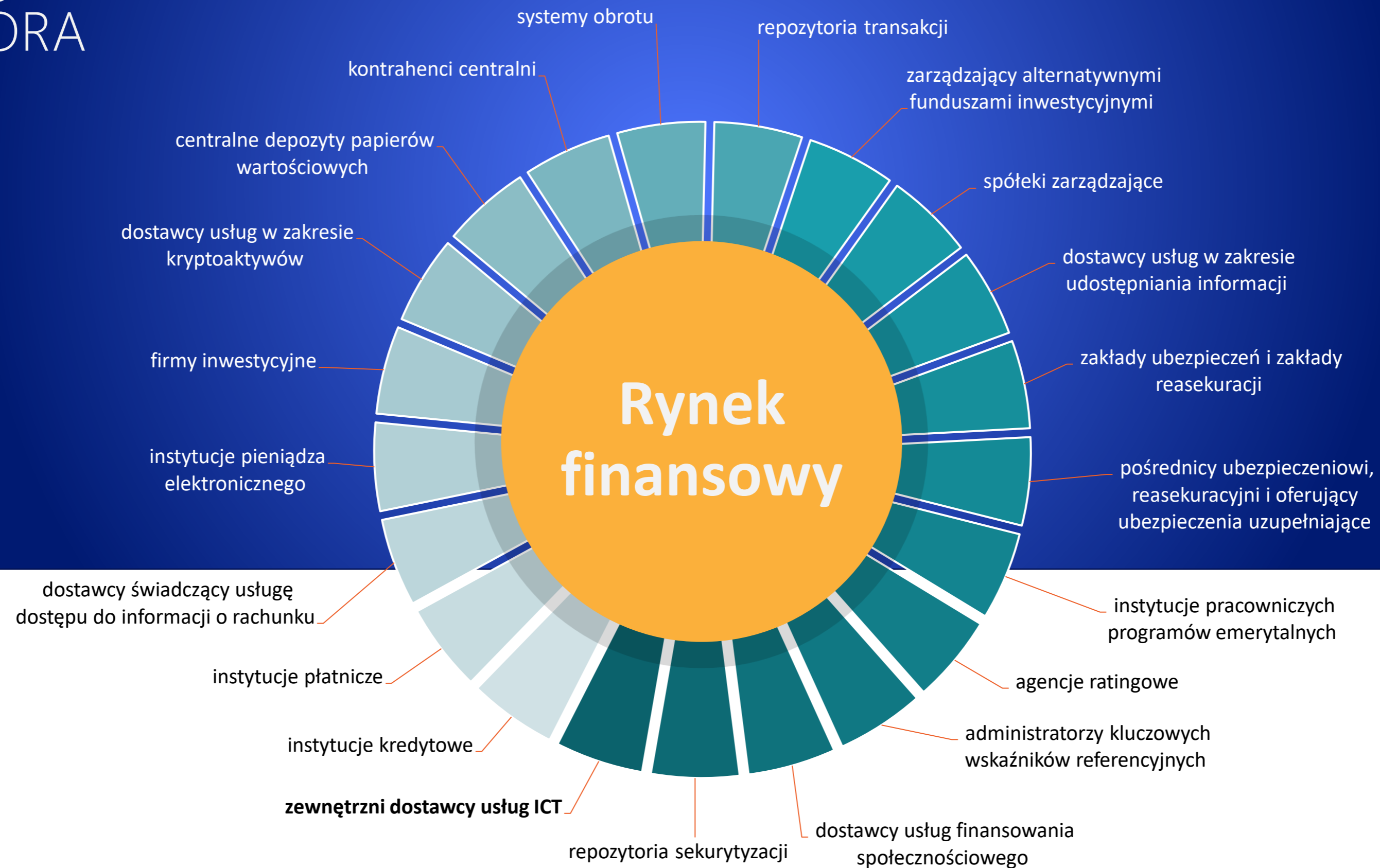
- RTS w sprawie kryteriów klasyfikacji incydentów ICT
- RTS w sprawie zgłaszania poważnych incydentów ICT
- ITS w sprawie standardowych formularzy, wzorów i procedur zgłaszania poważnych incydentów ICT
- Wytyczne w sprawie szacowania kosztów i strat spowodowanych poważnymi incydentami ICT
- RTS w sprawie sprawozdania z wykonalności centralizacji zgłaszania incydentów ICT

3

Ramy nadzoru

- ITS w sprawie standardowych wzorów rejestrów umów dot. korzystania z usług ICT
- Wytyczne w sprawie współpracy między europejskimi i krajowymi organami nadzoru
- RTS w sprawie postępowania w zakresie nadzoru
- Wytyczne w sprawie kryteriów do wyznaczania kluczowych dostawców usług ICT
- Opłaty nadzorcze

Podmioty objęte DORA



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

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

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

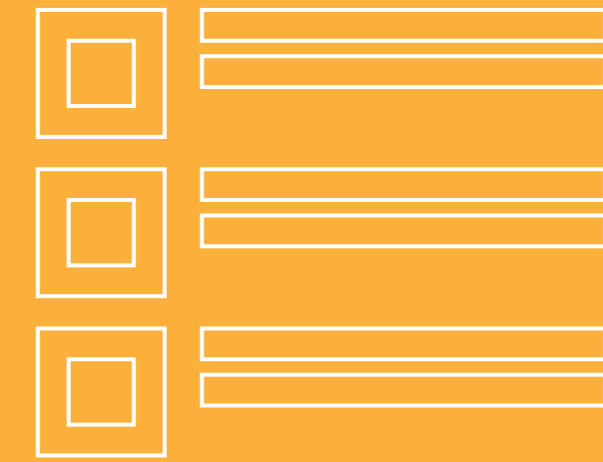
Najważniejsze informacje



- Duża zmiana
- Spójne podejście legislacyjne
- Szerszy pakiet regulacji



- Rosnąca skala zagrożeń
- Zwiększona aktywność przestępców
- Transgraniczność incydentów



- Wspólne standardy
- Obejmuje cały rynek finansowy UE
- Standardy i dobre praktyki dla innych sektorów gospodarki

Dziękujemy za uwagę

Zapraszamy na profile UKNF

