



Kto dużo łąpie, ten mało ściska

Zagrożenia polskiej implementacji DORA i NIS2

Mariusz Busiło
Aether Advisory



Digital Money & Blockchain Forum, 2025.06.11

Agenda



DORA, NIS2 I inne skrótowce



Co jest nie tak z DORA?



Co jest nie tak z NIS2/KSC



Czy jest dla nas jakaś szansa?



DORA a inne regulacje

Główny akt regulacyjny

DORA jest kluczowym aktem w cyberbezpieczeństwie finansowym
ALE POJAWIA SIĘ PROBLEM RELACJI DO INNYCH SEKTORÓW
(np. Włochy vs Polska...)

Istniejące przepisy

Outsourcing regulowany (Prawo bankowe)

Rekomendacje KNF – tutaj bardzo skąpo z odważnymi decyzjami ;)
;)

Komunikat Chmurowy – już został uchylony

Doprecyzowanie

Wymogi DORA są uzupełnione przez RTS i ITS. Najważniejszy dot poddostawców!



Przepisy krajowe dla DORA

Komunikacja

Zgłaszanie poważnych incydentów ICT
ICT

Kontrola

Formy działania KNF w ramach TLPT

Sankcje

Kary za nieprzestrzeganie przepisów
przepisów

Podmioty regulowane DORA

Instytucje kredytowe
Banki i inne podmioty kredytowe



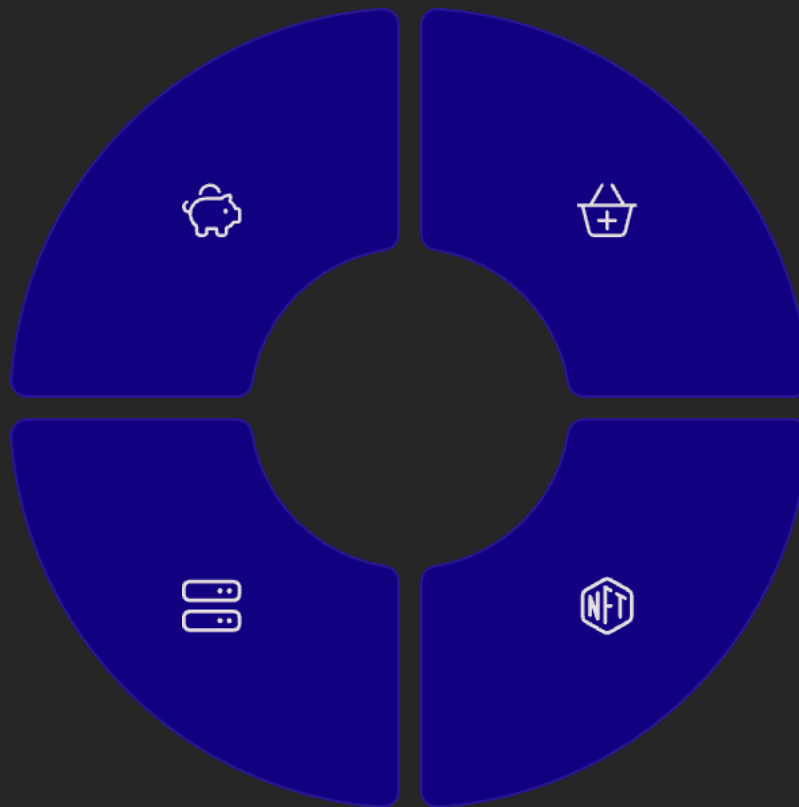
Instytucje płatnicze
Dostawcy usług płatniczych



Dostawcy ICT
Zewnętrzni dostawcy usług ICT



Dostawcy kryptoaktywów
Platformy kryptowalutowe



Obszary odporności cyfrowej wg DORA

Odporność operacyjna

Plany zarządzania ryzykiem ICT

Identyfikacja i ocena zagrożeń

Zarządzanie incydentami

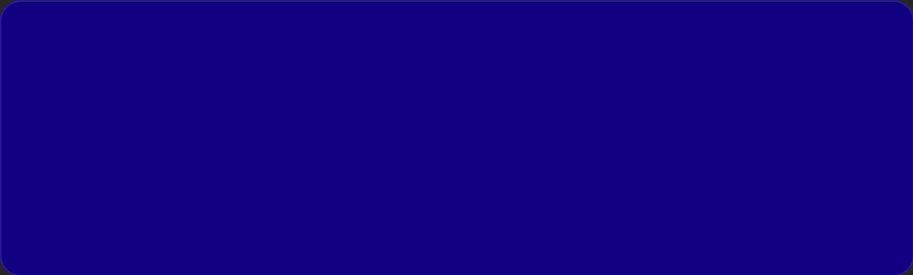
Szybka reakcja na zagrożenia

Monitorowanie i raportowanie

Testowanie i ocena

Regularne testy odpornościowe

Raporty dla firm i nadzoru



Zasoby i działania

Zarządzanie dostawcami ICT



Wymiana informacji

Współpraca w zakresie cyberzagrożeń



Operacyjna odporność cyfrowa



Integralność

Zdolność do zapewnienia operacyjnej integralności



Niezawodność

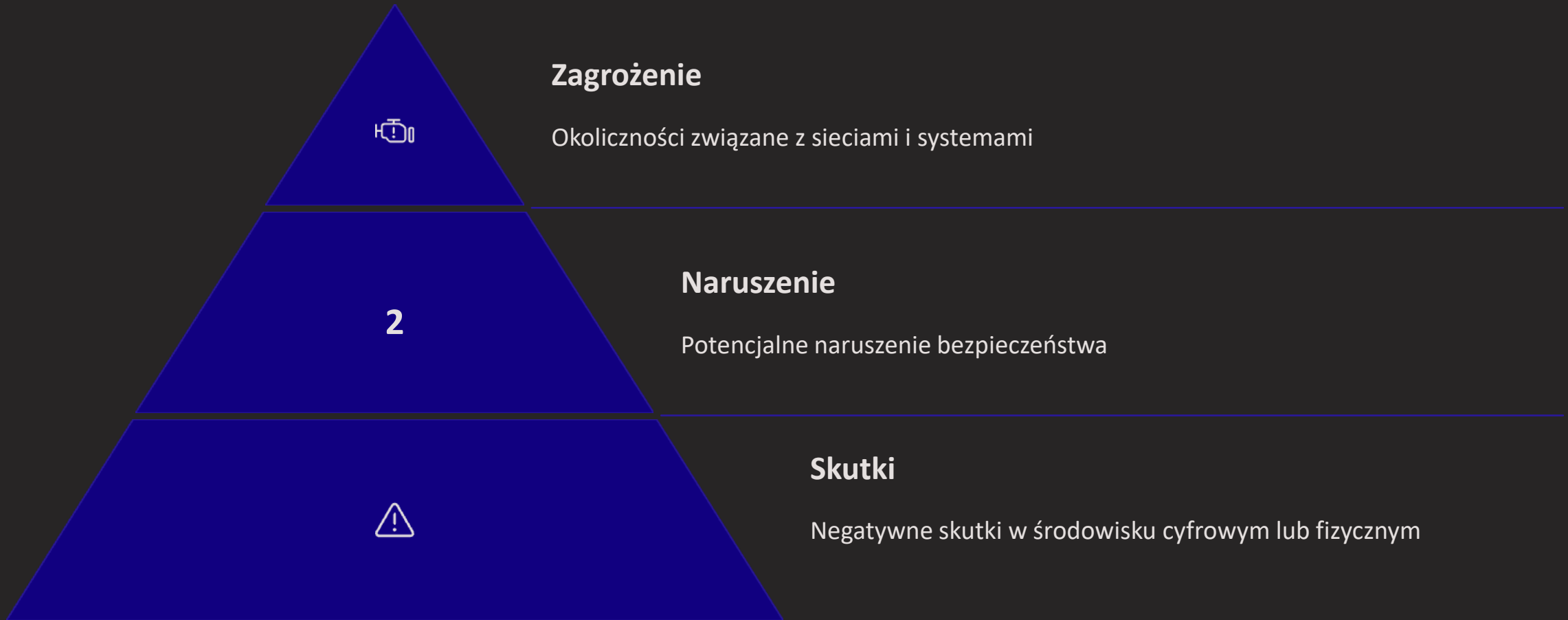
Gwarancja niezawodności systemów



Ciągłość

Wspieranie ciągłości usług finansowych

Ryzyko związane z ICT



Kluczowe definicje DORA

$f(x)$

Krytyczna funkcja

Funkcja, której zakłócenie wpłynęłoby na wyniki finansowe



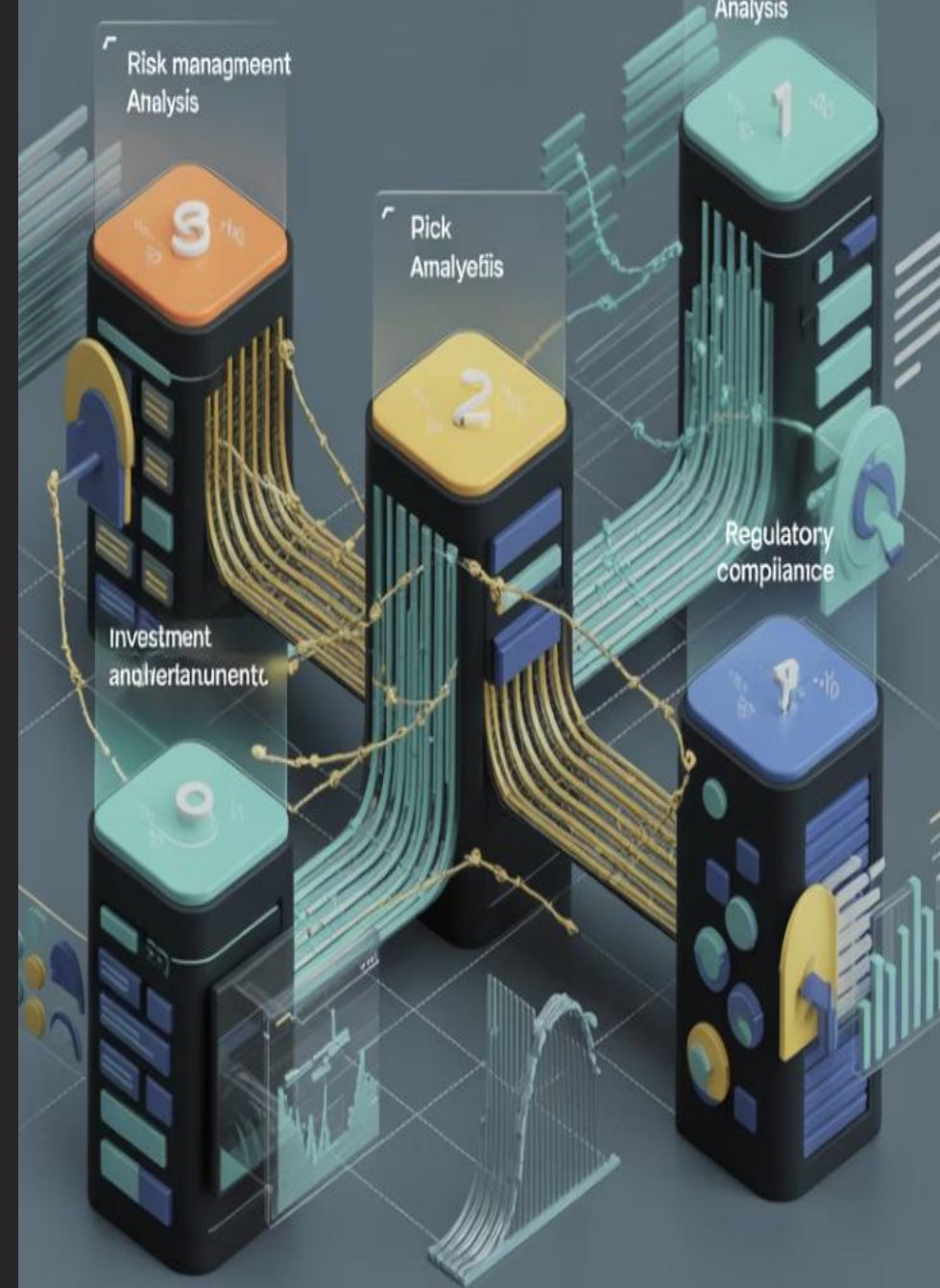
Zewnętrzny dostawca ICT

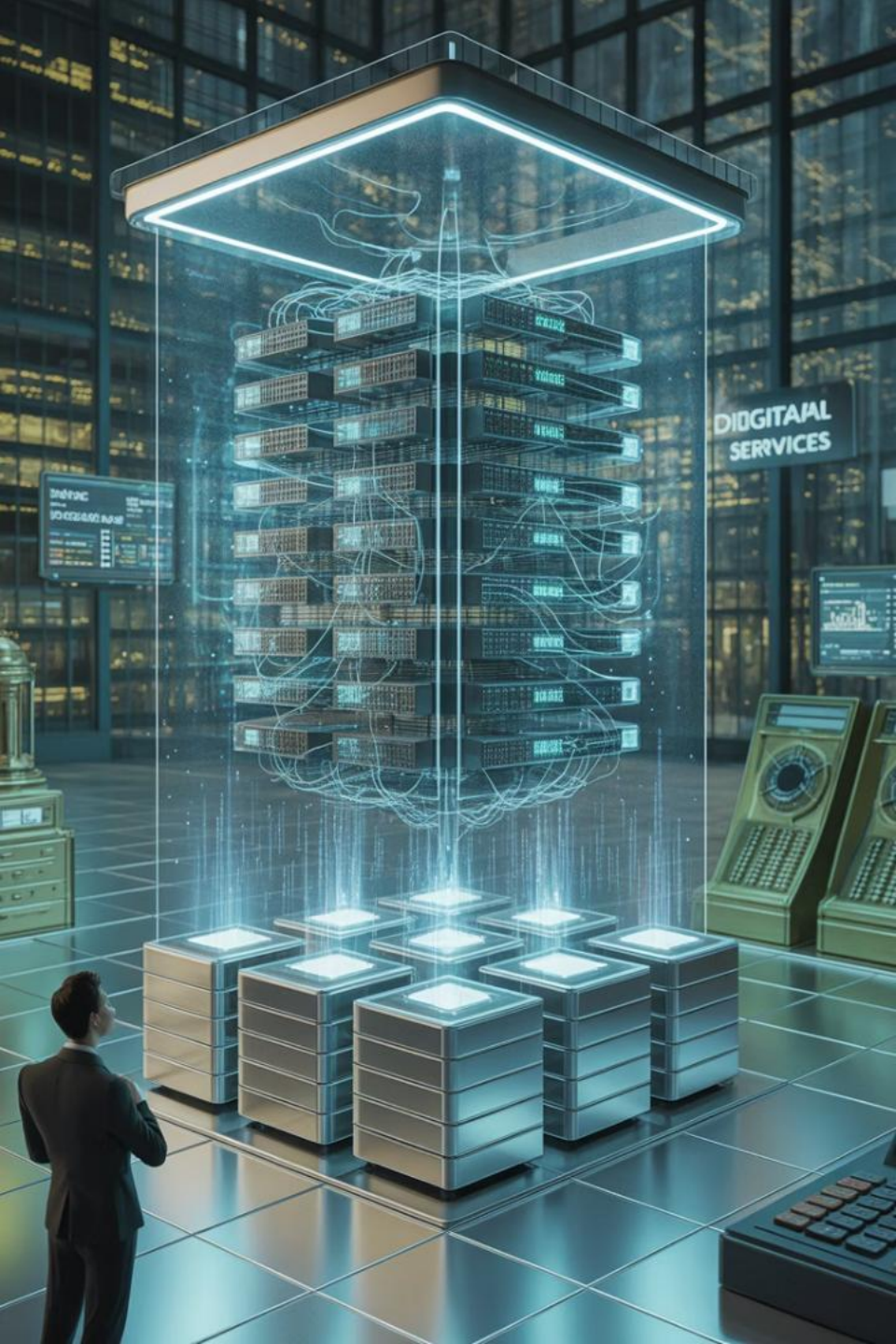
Przedsiębiorstwo świadczące usługi ICT



Ryzyko ICT

Ryzyko związane z korzystaniem z usług ICT





Definicja usługi ICT

Zakres

Usługi cyfrowe i usługi w zakresie zakresie danych

Sposób świadczenia

W sposób ciągły za pośrednictwem pośrednictwem systemów ICT

Wyłączenia

Tradycyjne usługi telefonii analogowej



Główne obowiązki dostawcy ICT dostawcy ICT

1

Umowy

Jasne i kompletne umowy
z podmiotami
finansowymi

2

Bezpieczeństwo

Zapewnienie
odpowiedniego poziomu
poziomu
cyberbezpieczeństwa

3

Współpraca

Pełna współpraca z
organami nadzoru

Świadczenie zwykłych usług ICT (1/2)

Opis funkcji

Jasny i kompletny opis wszystkich funkcji i usług ICT

Lokalizacja

Wskazanie miejsc świadczenia usług i przetwarzania danych

Ochrona danych

Zapewnienie dostępności, autentyczności, integralności i poufności
poufności





Świadczenie zwykłych usług ICT (2/2)

1 Wsparcie

Pomoc przy incydentach związanych z ICT

2 Współpraca

Pełna współpraca z organami nadzoru

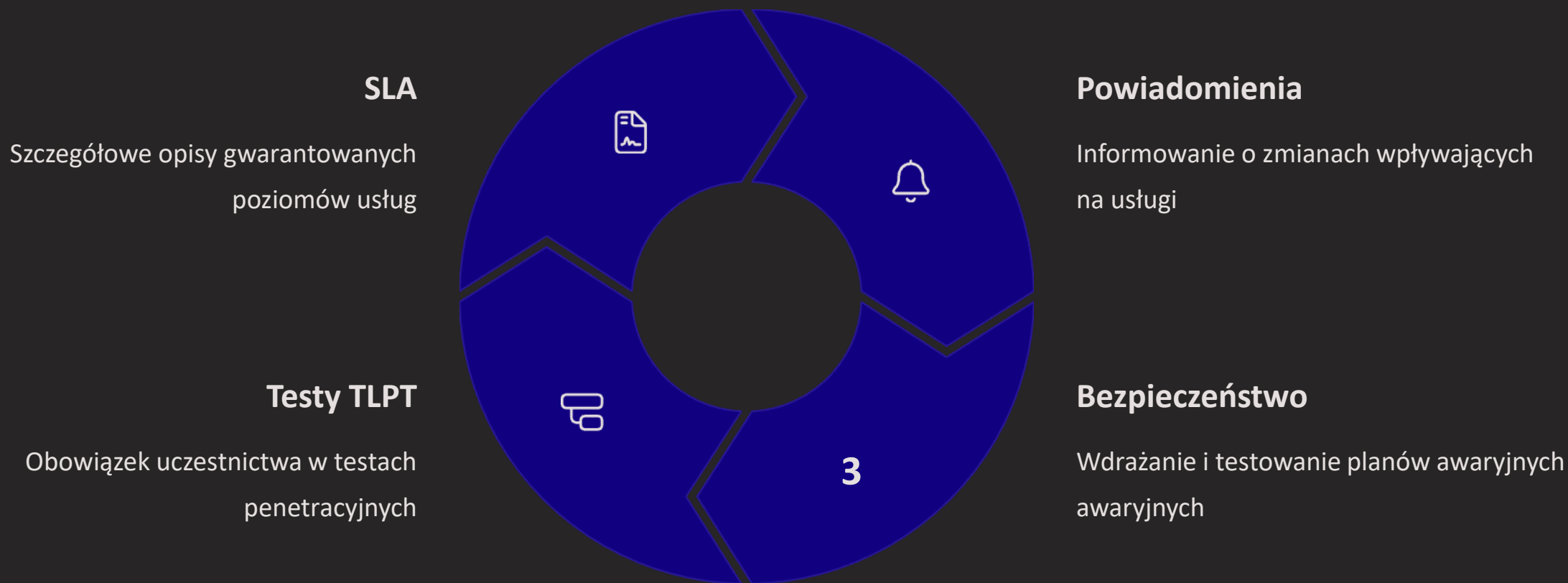
3 Wypowiedzenie

Prawo do wypowiedzenia umowy

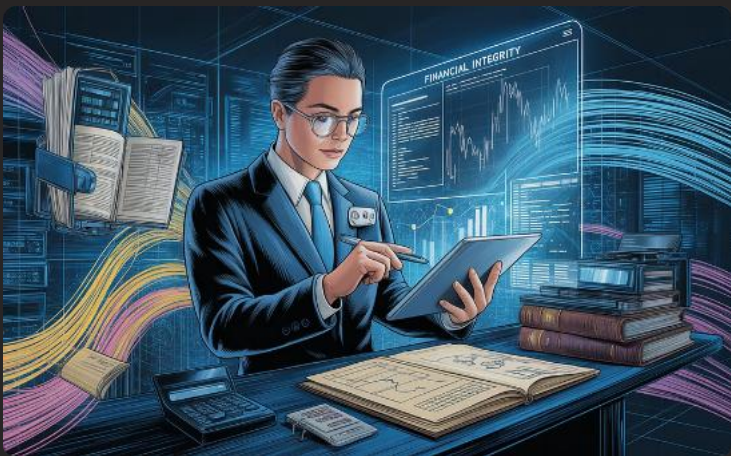
4 Szkolenia

Uczestnictwo w programach zwiększania świadomości bezpieczeństwa

Usługi ICT dla funkcji krytycznych (1/3)



Usługi ICT dla funkcji krytycznych (2/3)



Prawo do audytu

Nieograniczone prawa dostępu i kontroli



Monitorowanie

Bieżące monitorowanie wyników dostawcy



Współpraca

Pełna współpraca podczas kontroli, audytów audytów

Usługi ICT dla funkcji krytycznych (3/3)



Strategie wyjścia z odpowiednim okresem przejściowym

Zapewnienie ciągłości funkcjonowania podmiotu finansowego

Możliwość migracji do innego dostawcy lub rozwiązań wewnętrznych



Testy TLPT

Testy penetracyjne ukierunkowane przez analizę zagrożeń

Kluczowy element weryfikacji odporności cyfrowej

Obowiązkowe dla podmiotów finansowych



Testy TLPT - istota

Definicja

Ramy naśladowujące taktyki agresorów

Kontrolowane testy systemów produkcyjnych

Dostosowane do konkretnych zagrożeń



Obowiązki podmiotów finansowych



Częstotliwość

Nie rzadziej niż co trzy lata



Zakres

Krytyczne funkcje i systemy produkcyjne



Współpraca

Zapewnienie udziału dostawców ICT



Bezpieczeństwo

Środki kontroli ryzyka podczas testów





Zakończenie testów TLPT

1

Sprawozdania

Uzgodnienie sprawozdań
i planów naprawczych

2

Podsumowanie

Przedstawienie ustaleń
ustaleń organowi
wyznaczonemu

3

Poświadczenie

Otrzymanie
poświadczenia zgodności
zgodności z wymogami
wymogami



Testy TLPT - testy zbiorcze



Współpraca

Ustalenia umowne
między podmiotami



Zakres

Odpowiedni zakres usług
ICT



Dostosowanie

Liczba podmiotów
dostosowana do
złożoności



Testerzy TLPT

Kwalifikacje

Najwyższa renoma i odpowiedzialność

Zdolności

Techniczne i organizacyjne

Certyfikacja

Certyfikat lub kodeks postępowania

Niezależność

Niezależne zapewnienie lub audyt

Ubezpieczenie

Odpowiednie ubezpieczenie OC



Obowiązki dostawców ICT

Uczestnictwo

Obowiązek uczestnictwa w TLPT
podmiotu finansowego

Współpraca

Pełna współpraca podczas testów

Umowy

Odpowiednie zapisy w umowach o
świadczenie usług



RTS i ITS

Regulacyjne standardy techniczne (RTS) i wykonawcze standardy techniczne (ITS)

Doprecyzowują wymogi DORA

Opracowywane przez europejskie organy nadzoru

NIS2 / KSC Kogo dotyczy



Podmioty kluczowe

Duże i średnie przedsiębiorstwa w sektorach strategicznych



Podmioty ważne

Mniejsze firmy w sektorach istotnych



Infrastruktura cyfrowa

Telekomunikacja, cloud, centra danych



Podstawowe informacje o NIS2/KSC i DORA

Projekt nowelizacji KSC

Implementacja dyrektywy NIS2
(2022/2555)

Planowane wejście: 18 października
2024

Rozszerzenie na sektor telko,
produkcji, loistyki

Rozporządzenie DORA

Bezpośrednio obowiązujące od
17.01.2025

Dotyczy sektora finansowego i
dostawców ICT

Dyrektywa CER

Odporność podmiotów krytycznych

Wdrażana nowelizacją ustawy o zarządzaniu kryzysowym



KSC: Załącznik nr 1 do KSC

Sektory kluczowe



Energia

Wydobycie, elektryczność, ciepło, paliwa, gaz, wodór



Transport

Lotniczy, kolejowy, wodny, drogowy (ITS)



Bankowość

Instytucje kredytowe, SKOK-i, obrót instrumentami



Infrastruktura cyfrowa

DNS, chmura, centra danych, przedsiębiorcy komunikacji

KSC: Załącznik nr 1 do KSC Sektory kluczowe



Przestrzeń kosmiczna

Operatorzy infrastruktury naziemnej, Polska Polska Agencja Kosmiczna



Podmioty publiczne

NBP, instytuty badawcze, jednostki jednostki finansów finansów publicznych



Produkcja chemikaliów

Przedsiębiorstwa produkcji i dystrybucji substancji



Produkcja

Wyroby medyczne, medyczne, elektronika, urządzenia elektryczne



KSC: Załącznik nr 2 do KSC Sektory ważne



Usługi pocztowe

Operatorzy pocztowi



Gospodarowanie odpadami

Zbieranie, transport, przetwarzanie odpadów



Produkcja żywności

Dystrybucja hurtowa, produkcja przemysłowa



KSC: Podmioty kluczowe i ważne - kogo obejmą przepisy?

Podmioty kluczowe

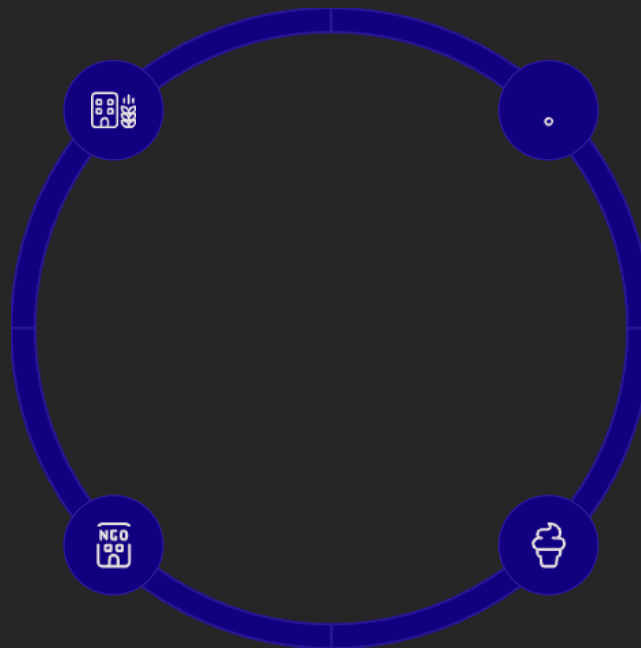
Duże i średnie firmy sektorów kluczowych

Duży i średni przedsiębiorcy komunikacji elektronicznej

Podmioty publiczne

Instytucje państwowe i samorządowe

Spółki użyteczności publicznej



Podmioty ważne

Mikro i mali przedsiębiorcy z sektorów kluczowych

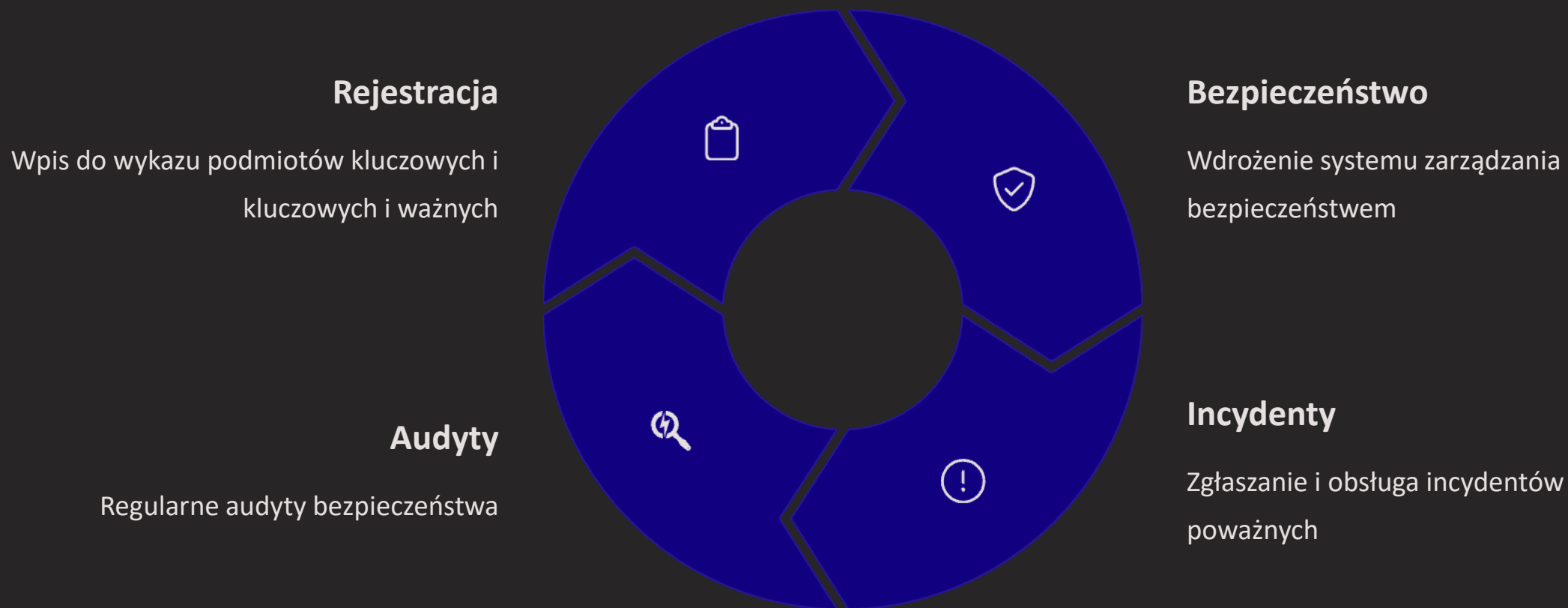
Mikro i mali przedsiębiorcy komunikacji elektronicznej

Infrastruktura cyfrowa

Dostawcy DNS, chmury, centrów danych

Rejestr domen TLD, dostawcy usług zaufania zaufania

NIS2 / KSC Jakie obowiązki



KSC: Kwalifikacja i wyznaczenie podmiotu kluczowego i ważnego

Kwalifikacja własna

Brak decyzji administracyjnej, konieczne zgłoszenie do wykazu

Zgłoszenie do wykazu

Dane identyfikujące, adresy IP, nazwy domen, osoby kontaktowe

Rejestracja w terminie

3 miesiące od spełnienia przesłanek uznania za podmiot

Verification Application Background Check Approval

Company Name ✓

Contact Information ✓

Security Clearance Level ✓

ForceNailing ✓

Deliaju ✓

Submit



KSC: Zarządzanie ryzykiem/Polityki bezpieczeństwa

2+

Osoby kontaktowe

Minimum dwie osoby do kontaktu z podmiotami systemu

24h

Zgłaszanie incydentów

Maksymalny czas na zgłoszenie incydentu poważnego

S46

System teleinformatyczny

Obowiązkowe korzystanie z systemu wymiany informacji

KSC: Zarządzanie incydentami



Wczesne ostrzeżenie

Informacja o potencjalnym zagrożeniu



Zawiadomienie

Zgłoszenie incydentu poważnego w ciągu 24h



Sprawozdanie okresowe

W trakcie obsługi incydentu na wniosek CSIRT



Sprawozdanie końcowe

W ciągu miesiąca od zakończenia obsługi

KSC: S46



System teleinformatyczny

Dedykowany kanał komunikacji
cyberbezpieczeństwa



Rozwiązania chmurowe

Dołączenie bez specjalnych urządzeń



Funkcjonalności

Zgłaszanie incydentów, ocena ryzyka,
wymiana informacji



KSC: Audyty i ocena bezpieczeństwa

Ocena bezpieczeństwa

Testy bezpieczeństwa systemu w celu celu identyfikacji podatności

Przeprowadzający

CSIRT MON, CSIRT NASK, CSIRT GOV GOV lub CSIRT sektorowy

Audyt bezpieczeństwa

Co najmniej raz na 3 lata dla podmiotów kluczowych

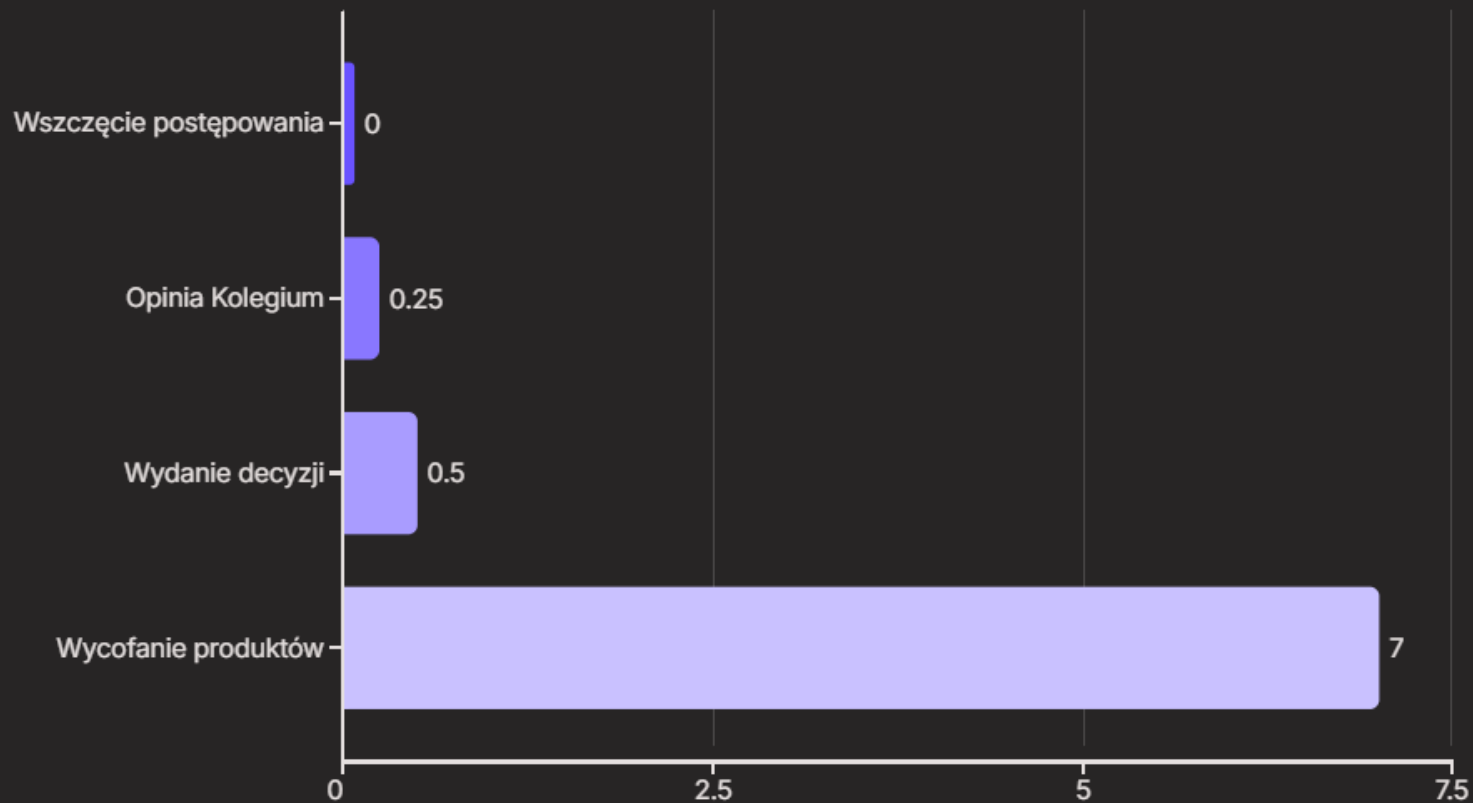
Pierwszy audyt




W terminie 24 miesięcy od uznania za uznania za podmiot kluczowy

Polecenia zabezpieczające

Wydawane przez MC w przypadku incydentu krytycznego

KSC: Dostawca wysokiego ryzyka



-  **Kogo dotyczy**
Podmioty kluczowe i ważne oraz telko z przychodem >10 mln zł
-  **Konsekwencje**
Zakaz wprowadzania i obowiązek wycofania produktów
-  **Termin wycofania**
Do 7 lat od publikacji decyzji

Harmonogram prac nad KSC – wdrożenie DORA i NIS2 w Polsce





Wdrożenie NIS2 do organizacji - etapy



Audyt przedwdrożeniowy

Ocena dojrzałości cyberbezpieczeństwa
cyberbezpieczeństwa

Weryfikacja zgodności z NIS2



Wdrożenie

Wprowadzenie polityk i procedur

Pokrycie wymagań NIS2



Audyt regulacyjny

Wsparcie w przejściu audytu

Potwierdzenie zgodności

Technologia i regulacje? Porządkuję chaos regulacji dla Twojego biznesu.

Ekspert w sektorze publicznym i prywatnym, specjalizacja w telekomunikacji i mediach.

Doświadczenie we wdrażaniu RODO, DORA, AI Act i NIS2.

Członek Komitetu Ochrony Danych w PIIT i Rady KIGEiT.



720AETHER

HQ@AETHERFIELDS.PL

