SPEAKERS

Artur Cieślik

ACSEC Sp. z o.o., Ekspert wiodący
w ACSEC Sp. z o.o.

[Compliance] Praktyka wdrażania wymagań NIS2/UoKSC w oparciu o wytyczne regulacji europejskich

THE H@CK SUMMIT

13.10 Online

14.10 PGE Narodowy, Warszawa

Wykładowca: Artur Cieślik

MBA, IRCA lead auditor ISO/IEC 27001

IRCA lead auditor ISO/IEC 22301

ISACA Certified Information Systems Auditor (CISA)

redaktor naczelny „IT Professional”

artur.cieslik@politykabezpieczenstwa.com.pl

Artur Cieślik
politykabezpieczenstwa.com.pl

- **Założyciel i główny ekspert ACSEC Sp. z o.o.:**
- Audytor wiodący normy ISO/IEC 27001 IRCA Certified Lead Auditor (nr w rejestrze: 6035034).
- Audytor wiodący normy ISO/IEC 22301 uzyskany zgodnie z IRCA.
- Certified Information Systems Auditor (CISA)
- Członek SABI – Stowarzyszenia Inspektorów Ochrony Danych.
- Członek IIA – Instytutu Audytorów Wewnętrznych IIA Polska
- Redaktor naczelny miesięcznika „IT Professional”.
- Członek rady programowej „ABI Expert”.
- Szkolenia i wykłady: Akademia Leona Koźmińskiego, Politechnika Wrocławska, Uniwersytet Ekonomiczny we Wrocławiu, Uniwersytet im. Kardynała Wyszyńskiego „IT Professional Academy” „Informacja Publiczna”, „Forbes Academy”, „IT w Administracji”.

Ramy wymagania

Dyrektywa na rzecz wysokiego poziomu cyberbezpieczeństwa (NIS2)

Cel:

Zwiększenie ogólnego poziomu cyberbezpieczeństwa w Unii Europejskiej.

Obowiązki:

Nakłada obowiązki na państwa członkowskie i tym samym podmioty działające w sektorach krytycznych.

ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2024/2690

Cel:

Precyzuje wymagania dla środków zarządzania ryzykiem.

Obowiązki:

art. 21 ust. 2 lit. a–j — część wiążąca dla podmiotów w sektorach objętych NIS2.

Ustawa o Krajowym Systemie Cyberbezpieczeństwa

Cel:

Implementacja dyrektywy NIS2 w Polsce i zapewnienie wysokiego poziomu bezpieczeństwa cyberprzestrzeni RP.

Obowiązki:

Podmioty kluczowe i ważne muszą wdrażać zabezpieczenia, szacować ryzyko oraz zgłaszać poważne incydenty do odpowiednich zespołów CSIRT.

IR (UE) 2024/2690 – kogo dotyczy i co dokładnie wymaga

Dyrektywa **NIS2** stawia szereg szczegółowych wymogów, które z założenia mają zbudować zunifikowany system cyberbezpieczeństwa, zapewniający właściwy poziom zabezpieczenia podmiotów, jak również wymiany informacji.

1

Adresaci

— m.in. dostawcy DNS, rejestry TLD, chmura, centra danych, CDN, MSP/MSSP, platformy handlowe, wyszukiwarki, serwisy społecznościowe, dostawcy usług zaufania..

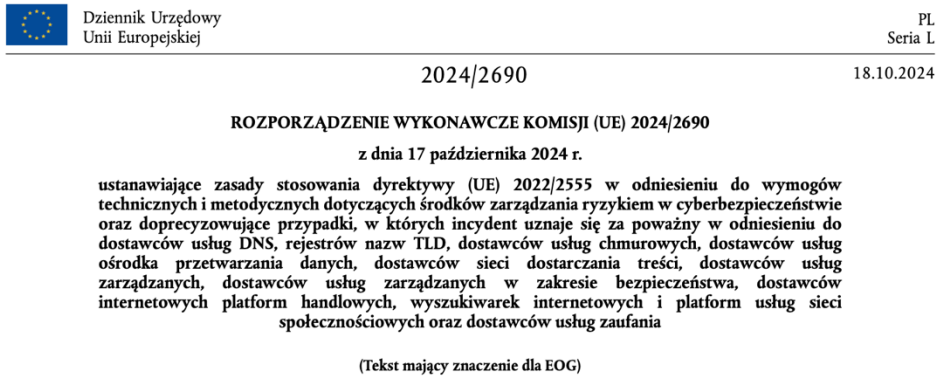
2

Zakres

— uszczegółowienie wymagań z art. 21 NIS2 m.in. zarządzanie ryzykiem, ciągłość i odtwarzanie, bezpieczeństwo łańcucha dostaw, detekcja/reakcja, logging, kryptografia, IAM/MFA, hardening konfiguracji, podatności i łatki, segmentacja, testy.

3

Zasada proporcjonalności i wymagalność dowodowa



Dziennik Urzędowy
Unii Europejskiej

PL
Seria L

2024/2690

18.10.2024

ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2024/2690

z dnia 17 października 2024 r.

ustanawiające zasady stosowania dyrektywy (UE) 2022/2555 w odniesieniu do wymogów technicznych i metodycznych dotyczących środków zarządzania ryzykiem w cyberbezpieczeństwie oraz doprecyzowujące przypadki, w których incydent uznaje się za poważny w odniesieniu do dostawców usług DNS, rejestrów nazw TLD, dostawców usług chmurowych, dostawców usług ośrodka przetwarzania danych, dostawców sieci dostarczania treści, dostawców usług zarządzanych, dostawców usług zarządzanych w zakresie bezpieczeństwa, dostawców internetowych platform handlowych, wyszukiwarek internetowych i platform usług sieci społecznościowych oraz dostawców usług zaufania

(Tekst mający znaczenie dla EOG)

IR (UE) 2024/2690 — Wymogi techniczne i metodyczne

Punkt i nazwa dokumentu	Skrócony opis zawartości (wg Załącznika)
1.1 Polityka bezpieczeństwa sieci i systemów informatycznych	Najwyższy dokument bezpieczeństwa: podejście i cele, zobowiązanie do doskonalenia i zasobów, zakres dokumentacji i retencji, lista polityk szczegółowych, mierniki wdrożenia/maturity, formalna aprobata zarządu; coroczny przegląd lub po istotnych zmianach/incydentach.
1.2 Matryca ról, odpowiedzialności i uprawnień	Zdefiniowane role i odpowiedzialności, raportowanie do zarządu, separacja obowiązków (tam gdzie możliwe), komunikacja wymagań wobec personelu i stron trzecich; cykliczny przegląd i aktualizacja.
2.1 Ramy zarządzania ryzykiem + Procedury RM	Ustanowienie i utrzymanie ram RM, cykliczna analiza/ocena ryzyka, plan postępowania z ryzykiem, kryteria ryzyka, tolerancja ryzyka, dokumentowanie i akceptacja ryzyk przez kierownictwo; przeglądy co najmniej roczne i po zmianach/incydentach.
2.2 Monitorowanie zgodności (polityka/procedury oraz raportowanie)	Regularne przeglądy zgodności z politykami/standardami, system raportowania do zarządu, monitorowanie w interwałach planowych i po incydentach/zmianach.
2.3 Niezależny przegląd bezpieczeństwa informacji i sieci	Procesy niezależnych przeglądów przez kompetentne osoby, zapewnienie bezstronności, raportowanie wyników do zarządu i działania korygujące; przeglądy w interwałach planowych i po zmianach.
3.1 Polityka obsługi incydentów	Role i odpowiedzialności, detekcja–analiza–containment–odbudowa–dokumentowanie–raportowanie; spójność z BCDR; kategoryzacja, plany komunikacji/eskalacji, przypisanie ról, zestaw dokumentów operacyjnych (runbooki, kontakty, szablony); testy i przeglądy okresowe.
3.2 Procedury monitorowania i logowania	Procedury i narzędzia monitoringu/logowania (ciągłe lub okresowe), lista zasobów objętych logowaniem, zakres logów (ruch, zmiany uprawnień, zdarzenia uwierzytelniania, działania uprzywilejowane, zmiany konfiguracji/backup, logi narzędzi bezpieczeństwa, dostęp fizyczny itd.), progi alarmowe, retencja i ochrona logów, synchronizacja czasu, przeglądy listy logowanych zasobów.
3.3 Mechanizm zgłaszania zdarzeń	Prosty mechanizm zgłaszania przez pracowników, dostawców i klientów; komunikowanie mechanizmu i szkolenia z jego użycia.
3.4 Procedura oceny i klasyfikacji zdarzeń	Kryteria wstępnie zdefiniowane (triage), przegląd zdarzeń powtarzalnych, korelacja logów, ponowna ocena przy nowych informacjach.
3.5 Procedury reagowania na incydenty	Etapy: containment, eradication, recovery; plany komunikacji (z CSIRT/organami, wewnętrzna, z interesariuszami), logowanie działań i gromadzenie dowodów, testy procedur.
3.6 Procedura przeglądów po incydencie (PIR)	Przeglądy po incydentach, identyfikacja przyczyn źródłowych, dokumentacja wniosków, doskonalenie podejścia i procedur; przeglądy cykliczne.
4.1 Plan ciągłości działania i odtwarzania (BC/DR Plan)	Zakres, role, kontakty i kanały komunikacji, warunki aktywacji/dezaktywacji, porządek odtwarzania, plany odtworzeniowe z celami (RTO/RPO), zasoby (backup/redundancje), powrót z trybów tymczasowych; BIA i wymagania ciągłości; testy/przeglądy/aktualizacje z wnioskami z testów.
4.2 Plany tworzenia kopii zapasowych i zarządzania redundancją	Czas odtworzenia, kompletność i poprawność kopii (w tym dane konfiguracyjne i chmura), izolacja i lokalizacja kopii, kontrola dostępu, procedury odtwarzania, retencja; testy integralności i testy odtworzeń; zapewnienie częściowej redundancji zasobów, personelu i łączy.
4.3 Plan/proces zarządzania kryzysowego	Role i odpowiedzialności (w tym dostawcy), łączność z władzami właściwymi/CSIRT, utrzymanie bezpieczeństwa w kryzysie, obsługa informacji od CSIRT/organów; testy/przeglądy/aktualizacje.

IR (UE) 2024/2690 — Wymogi techniczne i metodyczne

Punkt i nazwa dokumentu	Skrócony opis zawartości (wg Załącznika)
5.1 Polityka bezpieczeństwa łańcucha dostaw	Polityka i klauzule umowne dla dostawców/usługodawców (wymagania bezpieczeństwa, powiadamianie o incydentach, prawo audytu/raportów, obsługa podatności, zasady podwykonawstwa i zakończenia umowy); prowadzenie listy dostawców i usług.
6.1 Proces bezpieczeństwa przy nabyciu usług/produktów ICT	Wymagania bezpieczeństwa dla nabywanych ICT, wsparcie aktualizacji przez cały cykl życia lub wymiana po EoS, informacja o komponentach, kryteria wyboru dostawców wg oceny ryzyka.
6.2 Zasady bezpiecznego rozwoju (SSDLC) i testowania	Reguły bezpiecznego wytwarzania (specyfikacja–projekt–dev–wdrożenie–testy), analiza wymagań bezpieczeństwa, zasady inżynierii bezpiecznych systemów (np. zero trust), wymagania dla środowisk deweloperskich, procesy testów bezpieczeństwa i zarządzanie danymi testowymi (sanityzacja/anonymizacja).
7. Polityka i procedury oceny skuteczności środków	Co, jak i kiedy mierzyć/monitorować, metody analizy i ewaluacji, odpowiedzialności za pomiary, przeglądy i aktualizacje polityki/procedur.
8.1 Program podnoszenia świadomości i cyberhigieny	Harmonogramowane działania uświadamiające dla pracowników/zarządu i – gdzie właściwe – dostawców; spójność z politykami i procedurami, aktualizacja programu względem zagrożeń/technologii.
8.2 Program szkoleń bezpieczeństwa	Szkolenia adekwatne do roli, ocena skuteczności, instrukcje bezpiecznej konfiguracji/obsługi, zagrożenia/cyberhigiena, szkolenia przy zmianie roli; cykliczne i aktualizowane.
9. Polityka i procedury kryptografii	Zasady doboru i stosowania kryptografii dla poufności/integralności/autentyczności w oparciu o klasyfikację aktywów i wyniki oceny ryzyka; przegląd z uwzględnieniem „state of the art”.
10. Polityki bezpieczeństwa zasobów ludzkich	Zrozumienie i zobowiązanie do odpowiedzialności bezpieczeństwa (pracownicy i – gdzie właściwe – dostawcy), m.in. weryfikacje, NDA, onboarding/offboarding, dyscyplina za naruszenia; przeglądy okresowe.
11.1 Polityka kontroli dostępu (fizyczna i logiczna)	Zasady dostępu dla osób i systemów; dostęp tylko dla odpowiednio uwierzytelnionych; przeglądy i aktualizacje po incydentach/zmianach.
11.2 Procedury zarządzania uprawnieniami	Nadawanie/modyfikacja/odbieranie uprawnień wg need-to-know, least privilege, SoD; niezwłoczne zmiany po zakończeniu/zmianie zatrudnienia; okresowe przeglądy.
12.1 Zasady klasyfikacji aktywów	Poziomy klasyfikacji dla wszystkich aktywów (informacja/systems), powiązanie z wymaganiami C/I/A/Au, zgodność z celami BCDR; ewidencja aktywów i właścicieli.
13.1–13.3 Zasady bezpieczeństwa środowiskowego i fizycznego	Zapewnienie ciągłości przez zabezpieczenie mediów pomocniczych; ochrona przed zagrożeniami fizycznymi/środowiskowymi (klimat, pożar, powódź itd.); kontrola dostępu fizycznego (strefy bezpieczeństwa, monitoring, inspekcje).

IR (UE) 2024/2690 — Kryteria istotności incydentu

Rodzaj podmiotu	Definicja kryterium	Wartość/warunek
Wszystkie objęte IR 2024/2690	Znaczny incydent – próg finansowy	Strata bezpośrednia > 500 000 EUR lub > 5% rocznego obrotu (niższa wartość)
Wszystkie objęte IR 2024/2690	Wyciek tajemnicy przedsiębiorstwa	Exfiltracja tajemnicy przedsiębiorstwa (Dyrektywa (UE) 2016/943)
Wszystkie objęte IR 2024/2690	Szkoda na osobie	Śmierć osoby fizycznej lub znaczna szkoda dla zdrowia
Wszystkie objęte IR 2024/2690	Nieautoryzowany dostęp o skutkach operacyjnych	Udany, podejrzanie złośliwy dostęp zdolny spowodować poważne zakłócenia operacyjne
Wszystkie objęte IR 2024/2690	Incydenty powtarzalne (skumulowane)	≥ 2 incydenty w ciągu 6 miesięcy o tej samej przyczynie i łącznie spełniające próg finansowy
Wszystkie objęte IR 2024/2690	Zdarzenia planowe	Planowe przerwy/konserwacje nie stanowią incydentu istotnego
Wszystkie objęte IR 2024/2690	Metodyka liczenia użytkowników	Liczyć klientów oraz powiązane osoby/podmioty korzystające z usług

Sposób implementowania NIS2/IR 2024/2690

W związku z trwającymi pracami nowelizacyjnymi, w implementacji wymagań **NIS2** można uwzględniać **wytyczne ENISA** — Europejskiej Agencji ds. Cyberbezpieczeństwa.

Stosowanie przyjętych praktyk

Wytyczne w dużej części pokrywają się z praktykami przyjętymi w międzynarodowych normach. ENISA wskazuje m.in. na obowiązek określania strategii, ról i odpowiedzialności, przeprowadzania analizy ryzyka i identyfikacji zagrożeń, tworzenia planów zarządzania ryzykiem, czy procedur zarządzania incydentami.

Część z wytycznych wykracza poza zakres norm ISO

Wyróżnić tu należy, m.in.:

- **Bezpieczeństwo łańcucha dostaw** — zarządzanie ryzykiem związanym z dostawcami i partnerami.
- **Bezpieczeństwo w rozwoju i utrzymaniu systemów IT** — wymagania dotyczące bezpiecznego kodowania i testowania.
- **Szczegółowe wymogi testowania** — określające sposoby weryfikacji bezpieczeństwa systemów, przede wszystkim przez testy penetracyjne.
- **Włączanie kadry kierowniczej w procesy bezpieczeństwa** — zarówno w obszarze szkolenia, jak również bezpośredniego ponoszenia odpowiedzialności za spełnienie wymagań NIS2.

EUROPEAN UNION AGENCY FOR CYBERSECURITY

TECHNICAL IMPLEMENTATION GUIDANCE

TABLE OF CONTENTS

Jeżeli wymagania są jasne, dowody wdrożenia — często już nie

Organizacje potrafią napisać politykę, ale **nie zawsze potrafią udowodnić** jej skuteczność i proporcjonalność

- Wyższe oczekiwania zarządcze
- **IR 2690, TECHNICAL IMPLEMENTATION GUIDANCE** → konkret, nacisk na dowody
- Częsta luka – mapowanie norm ↔ obowiązki
- Łańcuch dostaw i SLA z MSSP
- Ciągłość/odtwarzanie: RTO/RPO, testy w praktyce
- KPI/KRI - co tak naprawdę mierzyć?

Dokumentacja i dowody.

Różnice między dokumentacją papierową a rzeczywistym udowodnieniem zgodności mają kluczowe znaczenie.

Szczególnie istotne dla efektywności audytów i procesów certyfikacyjnych w organizacjach.

DOKUMENTACJA PAPIEROWA

Formalne dokumenty i świadectwa, które są istotne w audytach.

RZECZYWISTE UDOWODNIENIE

Dowody operacyjne oraz testy, które potwierdzają zgodność w praktyce.

WSKAŹNIKI

Istotne jest zdefiniowanie KPI/KRI i posiadanie repozytorium atrefaktów w celu udowodnienia zgodności.

Jedna matryca, by wszystkim rządzić (przykłady).

ENISA → Dowody

- MATRYCA wymóg → kontrola → dowód
- PROPORCJONALNOŚĆ decyzje i uzasadnienie
- Table-top i testy odtworzeniowe

NIST CSF 2.0 → Gov i wskaźniki

- GV–ID–PR–DE–RS–RC jako język zarządu
- KPI/KRI np. MTTD≤15m, MTTP≤7d, MFA≥95%
- Przeglądy kwartalne

ISO/IEC 27001:2022 → Kontrolki

- Zał. A np.: IAM, logi, podatności, BC/DR
- SoA oraz wyjątki z akceptacją ryzyka
- Baselines i audytowalność

Normy ISO dotyczące zarządzania ryzykiem cyberbezpieczeństwa

Norma	Cel
ISO/IEC 27001:2022	Podstawa wdrażania Systemu Zarządzania Bezpieczeństwem Informacji (ISMS)
ISO/IEC 27002:2022	Cele, wytyczne i praktyki kontroli bezpieczeństwa zgodne z normą 27001
ISO/IEC 27005:2022	Strukturalne podejście do oceny ryzyka i jego postępowania
ISO/IEC 27004:2016	Metryki i monitorowanie skuteczności ISMS

Obsługa podatności i incydentów

Norma	Cel
ISO/IEC 29147:2018	Ramy odpowiedzialnego ujawniania podatności
ISO/IEC 30111:2020	Proces analizy, triage’u i łagodzenia podatności
ISO/IEC 27035-1:2023	Zarządzanie cyklem życia incydentów bezpieczeństwa

Łańcuch dostaw i usługi IT

Norma	Cel
ISO/IEC 27036-1:2021	Zasady zabezpieczania interakcji z dostawcami i stronami trzecimi
ISO/IEC 27036-2:2022	Wymagania dotyczące zarządzania ryzykiem cybernetycznym w relacjach z dostawcami
ISO/IEC 20000-1:2018	Najlepsze praktyki zarządzania bezpiecznymi usługami IT zgodnie z normami IS

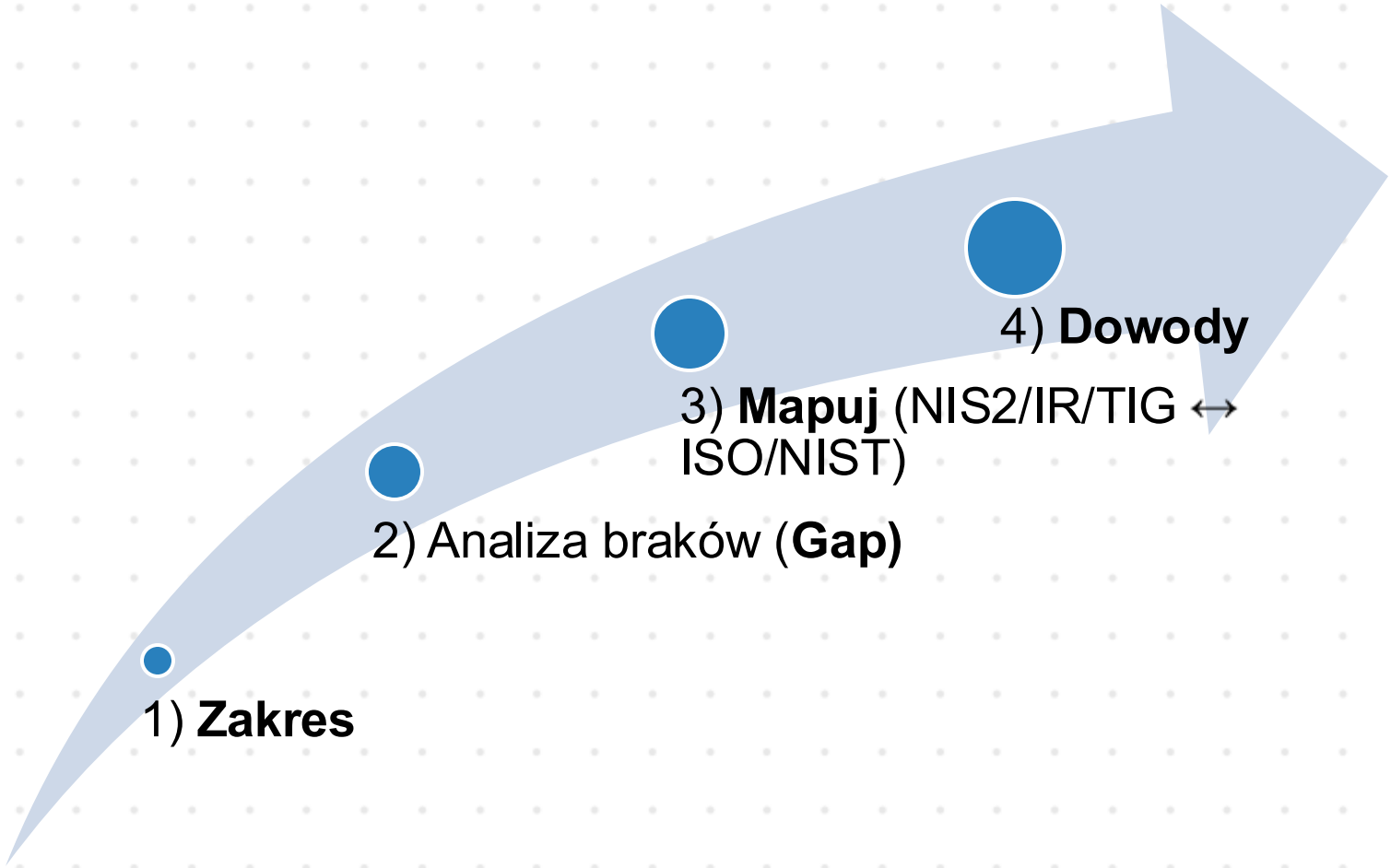
Ciągłość działania

Norma	Cel
ISO 22301:2019	Wymagania dotyczące wdrażania Systemu Zarządzania Ciągłością Działania (BCMS)
ISO 22313:2020	Wytyczne do stosowania kontroli ISO 22301
ISO/TS 22317:2021	Metodyka przeprowadzania Analizy Wpływu na Działalność (BIA)

Rola CISO i nadzoru zarządczego

- **Zatwierdzanie środków bezpieczeństwa** przez kierownictwo, nadzór nad wdrożeniem i rozliczalność (governance).
- **Metryki/KRI dla zarządu**, szczególnie ryzyko resztkowe, pokrycie wymagań, MTTR/MTTD, wskaźniki incydentów istotnych.
- **Integracja z procesami organizacji** – apetyt na ryzyko, SoA, budżet i plan inwestycyjny.

NIS2/IR 2690 – proces wdrożenia.



NIS2/IR 2024/2690 ↔ Warstwa mapowania ↔ ISO/NIST

Od wymogu → przez kontrolę → do dowodu (evidence-first)

01	**Wymóg** Wprowadzenie do NIS2/IR z wytycznymi regulacyjnymi dla bezpieczeństwa.
02	**Kontrola** Implementacja standardów ISO/NIST w celu zapewnienia bezpieczeństwa i zgodności operacyjnej w organizacji.
03	**Dowód** Ustanowienie efektywnych mechanizmów do gromadzenia i analizowania dowodów dla audytów i monitorowania.
04	**Analiza** Regularne przeglądy i analiza wydajności w celu zwiększenia zgodności i bezpieczeństwa.
05	**Zastosowanie strategii** Wdrożenie najlepszych praktyk w celu zapewnienia ciągłego rozwoju i poprawy procesów organizacyjnych.

Jak wpiąć NIS2/IR 2024/2690 w istniejący SZBI (ISO/IEC 27001:2022)

Krok 1: Przegląd SoA i matrycy ryzyk pod kątem wymagalności art. 21 NIS2 i ew. 2024/2690.

Krok 2: Uzupełnienie braków w **Zał. A (93 kontrolki)** – m.in. A.5.7/5.15/5.23 (dostawcy/inne), A.5.30 (ISO 22301), A.8.8 (MFA), A.8.9 (segregacja sieci), A.8.10/8.12 (malware/monitoring), A.8.21 (podatności).

Krok 3: Uporządkowanie dowodów w zakresie polityk, procedur, rejestrów, logów, raportów testów, zapisów ze szkoleń, przeglądów zarządzania.

Jak monitorować wdrożenie/wpięcie NIS2/IR 2024/2690 w istniejący SZBI (ISO/IEC 27001:2022)

Obszar	Status (przykład)	KPI/KRI (przykład docelowych)	Właściciel	Dowód
Governance i przeglądy	Żółty	Przeglądy kwartalne 100%, decyzje ≤ 30 dni	CISO / Zarząd	Protokoły, KRI
Zarządzanie ryzykiem	Żółty	Pokrycie ryzyk ≥ 95%, plany ≥ 90%	CISO / Właściciele	Polityka, rejestr ryzyka
Zgodność (NIS2/IR 2690)	Żółty	Pokrycie dowodami ≥ 95%, raporty w terminach	CISO / Compliance	Matryca, repozytorium dowodów
Gotowość do reagowania na incydenty	Żółty	MTTD ≤ 15 min, MTTR ≤ 4 h, 2 ćwiczenia/rok	CISO / SOC	CIRP, playbooki
MSSP/MSP	Żółty	Przeglądy kwartalne = 100%, niezgodności ≤ 30 dni	CISO / Opiekun dostawcy	Przeglądy kwartalne, zapisy zadań
Metryki i raportowanie	Żółty	Raportowanie w terminie; KPI zgodne z progami	CISO	Wyniki, źródła danych
Szkolenia i świadomość	Zielony	Pokrycie ≥ 98%, CTR ≤ 3%	CISO / HR	Plany szkoleń, wyniki szkoleń i testów
Repozytorium dowodów	Żółty	Aktualność ≤ 90 dni, pokrycie ≥ 95%	CISO / ?	Repozytorium artefaktów

NIS2/IR 2024/2690 → ISO → NIST → CIS

Przykład 1 (Zarządzanie ryzykiem i governance)

NIS2 art. 21 + 2024/2690 → ISO A.5.1, A.5.3, A.5.36 → **ISO/IEC 27005** → NIST CSF 2.0 Govern, Identify (ID.RM) → CIS IG/Control 17 (IR), 4 (Secure Config), 16 (App Security).

Przykład 2 (Łańcuch dostaw/SLA)

2024/2690 supply-chain → ISO A.5.15/A.5.23/A.5.19 → NIST CSF 2.0 GV.SC/ID.SC → CIS 15 (Service Provider Mgmt).

Przykład 3 (BC/DR i odtwarzanie)

2024/2690 continuity/recovery → ISO A.5.29/A.8.13/A.8.14 → **ISO 22301** → NIST CSF 2.0 RC/RS.RP → CIS 11 (Data Recovery).

Przykład 4 (Detekcja/monitoring/logowanie)

2024/2690 detection/logging → ISO A.8.16/A.8.15 → NIST CSF 2.0 DE.MA/DE.AE → CIS 8 (Audit Log Mgmt).

Przykład 5 (IAM/MFA/minimalne uprawnienia)

2024/2690 IAM → ISO A.5.18/A.8.3/A.8.4/A.8.8 → NIST CSF 2.0 PR.AC → CIS 6 (Access Control).

Zalecenia vs. ISO/IEC 27001 (przykłady)

Propozycje uzupełnień w oparciu o wytyczne ENISA (vs. ISO/IEC 27001:2022 Zał. A)	Uzasadnienie
Kryteria incydentu istotnego i regulacyjne terminy raportowania	Zał. A nie definiuje progów prawnych ani terminów raportowania do organów/CSIRT.
Uzasadnienie proporcjonalności zgodnie z IR 2690.	27001 przewiduje podejście oparte na ryzyku, lecz nie wymaga jawnego uzasadnienia odstępstw wobec IR 2690.
Szczegółowe progi i czasy detekcji (np. MTTD krytyczne ≤ 15 min)	Zał. A wymaga monitorowania, ale nie określa progów czasowych.
SBOM dla systemów krytycznych i zarządzanie komponentami	27001 nie wymaga wprost SBOM.
SLA/OLA z MSSP/MSP (24/7, L1/L2/L3) i podział odpowiedzialności	Zał. A adresuje relacje z dostawcami ogólnie, bez precyzyjnych SLA/OLA SOC/EDR/SIEM.
Obowiązkowe testy odtworzeniowe i docelowe RTO/RPO dla usług krytycznych	27001 wymaga mechanizmów BC/ICT readiness, ale nie narzuca częstotliwości i progów.
Specyficzne wymagania dla DNS/TLD/Cloud/CDN/MSSP zgodnie z IR 2690	Zał. A nie pokrywa specyficznych wymogów sektorowych IR (np. DNS resiliency).
Integracja Threat Intelligence z detekcją (czas publikacji i adaptacji)	Zał. A nie określa tempa adaptacji TI do use-case'ów.
Repozytorium dowodów	Zał. A nie narzuca centralnego repozytorium dowodów.
Mierzalne progi patchowania oparte na ryzyku (np. MTTP ≤ 7 dni)	Zał. A nie definiuje progów czasowych dla łatek.
Wymogi komunikacji kryzysowej do regulatorów/klientów	27001 nie narzuca treści i sposoby komunikacji z regulatorem oraz klientem.
IAM/MFA/PAM na systemach krytycznych	Zał. A wskazuje kontrolę dostępu, lecz bez aż tak konkretnych wymagań.
Formalny RACI z CSP/MSSP	Zał. A nie wymaga matrycy RACI dla chmury/MSSP.

Obowiązki podmiotu w PL – UoKSC

Zgłoszenie do wykazu

Podmiot musi dokonać wpisu do rejestru **podmiotów kluczowych**.

Termin: 3 miesiące
(od wejścia ustawy)

Podłączenie do systemu S46-react

Podmiot musi spełnić techniczne wymagania podłączenia do S46, służącego do wymiany informacji.

Termin: 6 miesięcy
(od wejścia ustawy)

Wdrożenie zasad bezpieczeństwa

Podmiot musi wdrożyć wszystkie wymagania, w tym powołać punkt kontaktowy.

Termin: 6 miesięcy
(od wejścia ustawy)

Szkolenie pracowników

Podmiot musi przeszkolić wszystkich pracowników, w tym kierownictwo, celem podniesienia poziomu cyberhigieny.

Termin: 6 miesięcy
(od wejścia ustawy)

Przeprowadzenie audytu

Podmiot musi przeprowadzić niezależny audyt spełnienia wszystkich wymogów NIS2/UoKSC.

Termin: do 24 miesięcy
(od wejścia ustawy)

Częste braki (ENISA/IR 2024/2690 vs. ISO/IEC 27001)

Obszar IR 2024/2690	Referencja IR / NIS2	Luka (opis skrócony)	Działania wymagane	Priorytet (Niski/Średni/Wysoki)
Zarządzanie ryzykiem	IR 2024/2690 – risk management; NIS2 art.21(2)(a–j)	Brak formalnego procesu zarządzania ryzykiem BI	Zdefiniować kryteria dla ryzyka, uaktualnić metodykę, powiązać ryzyka z SoA i KPI	Wysoki
Inwentaryzacja i klasyfikacja	IR – zarządzanie aktywami i krytyczność	Niespójna klasyfikacja krytyczności	Ujednolicić klasyfikację i przypisać właścicieli	Średni
Zmiany i konfiguracja	IR – hardening, konfiguracje, change management	Brak baseline dla krytycznych	Zdefiniować baseline, przeprowadzić audyt zgodności	Wysoki
IAM / MFA (uwierzytelnianie wieloskładnikowe) / PAM	IR – IAM i uwierzytelnianie wieloskładnikowe	MFA (uwierzytelnianie wieloskładnikowe) niepełne na kontach uprzywilejowanych	Włączyć MFA (uwierzytelnianie wieloskładnikowe)/PAM; wprowadzić cykl przeglądów/audytów kont	Wysoki
Segmentacja sieci	IR – segmentacja, ograniczenie przepływów	Brak mapy/specyfikacji stref i ACL dla stref	Zdefiniować strefy, wdrożyć ACL/NGFW; testy ruchu	Wysoki
Logowanie i monitorowanie	IR – logowanie, detekcja, retencja	Brak części źródeł w SIEM	Dodać źródła i ustalić retencję	Wysoki
Reagowanie na incydenty	IR – playbooki, komunikacja, zgłoszenia	Brak ćwiczeń, nieaktualna lista kontaktowa	Przeprowadzić ćwiczenia i aktualizować kontakty w zakresie monitorowania 24/7	Średni
Kryteria incydentu istotnego	IR – istotność, zgłaszanie	Brak progów istotności	Przyjąć progi zgodne z IR 2690 i dodać do IRP, przeprowadzić szkolenia	Wysoki
Vulnerability & patching	IR – podatności i łatki	Brak SLA patchy u dostawców	Wdrożyć SLA i automatyzować skany	Wysoki
Anti-malware / EDR	IR –EDR/AV	Brak EDR/AV na VDI	Rozszerzyć EDR/AV na VDI.	Średni
Kryptografia / klucze	IR – crypto, KMS/HSM	Brak centralnego rejestru kluczy krypto.	Utworzyć rejestr i ujednolicić polityki krypto.	Średni
Backup / odtwarzanie	IR – kopia zapasowa/odtwarzanie i testy DR	Testy DR nie są prowadzone dla wszystkich krytycznych systemów	Zaplanować testy DR dla krytycznych systemów i raportować czasy.	Wysoki
ciągłość działania/odtwarzanie / gotowość ICT	IR – ciągłość działania/odtwarzanie	Brakuje BIA dla 2 usług krytycznych.	Wykonać BIA i uaktualnić BCP/DRP, przeprowadzić testy	Wysoki
Supply chain	IR – bezpieczeństwo dostawców	Brak klauzul NIS2 w 36% umów	Zaktualizować wzorce umów o prawa audytu i raportowanie	Wysoki
SBOM / komponenty	IR – oprogramowanie i SBoM	Brak procesu SBoM i SCA	Wdrożyć SCA i gromadzić dane SBOM	Średni
SSDLC	IR – secure SDLC, SAST/DAST	Nie wszystkie produkty objęte SAST/DAST	Rozszerzyć CI o SAST/DAST	Średni
Threat Intel	IR – wykorzystanie TI	Brak playbooka TI→detekcja	Sformalizować proces TI i przetestować sposób postępowania dla detekcji	Średni
Szkolenia	IR – program szkoleń	Brak pomiaru efektywności	Wprowadzić wskaźniki efektywności	Niski
Chmura	IR – podział odpowiedzialności (shared responsibility), logowanie	Niepełny model odpowiedzialności	Zdefiniować RACI, wprowadzić monitorowanie i retencję logów	Wysoki
Komunikacja kryzysowa	IR – komunikacja kryzysowa	Brak szablonów i zapasowych kanałów komunikacji	Przygotować szablony, przeprowadzić test łączności	Średni

Dokumentacja zgodności jako część SZBI

Polityki/procedury

—zarządzanie ryzykiem, incydentami, patchami, backup, logowanie, dostępy, łańcuch dostaw, testy, szkolenia.

Rejestry i artefakty

—rejestr ryzyka, SoA, inwentaryzacja, plan reagowania (IR), BIA/BCP/DRP, DPIA (jeśli RODO), rejestr dostawców/SLA, plan szkoleń, wyniki testów, przeglądy zarządzania.

Ścieżka audytu

—kto zatwierdził, kiedy, jak mierzono skuteczność.

Dobre praktyki wdrożeniowe SZBI w kontekście NIS2

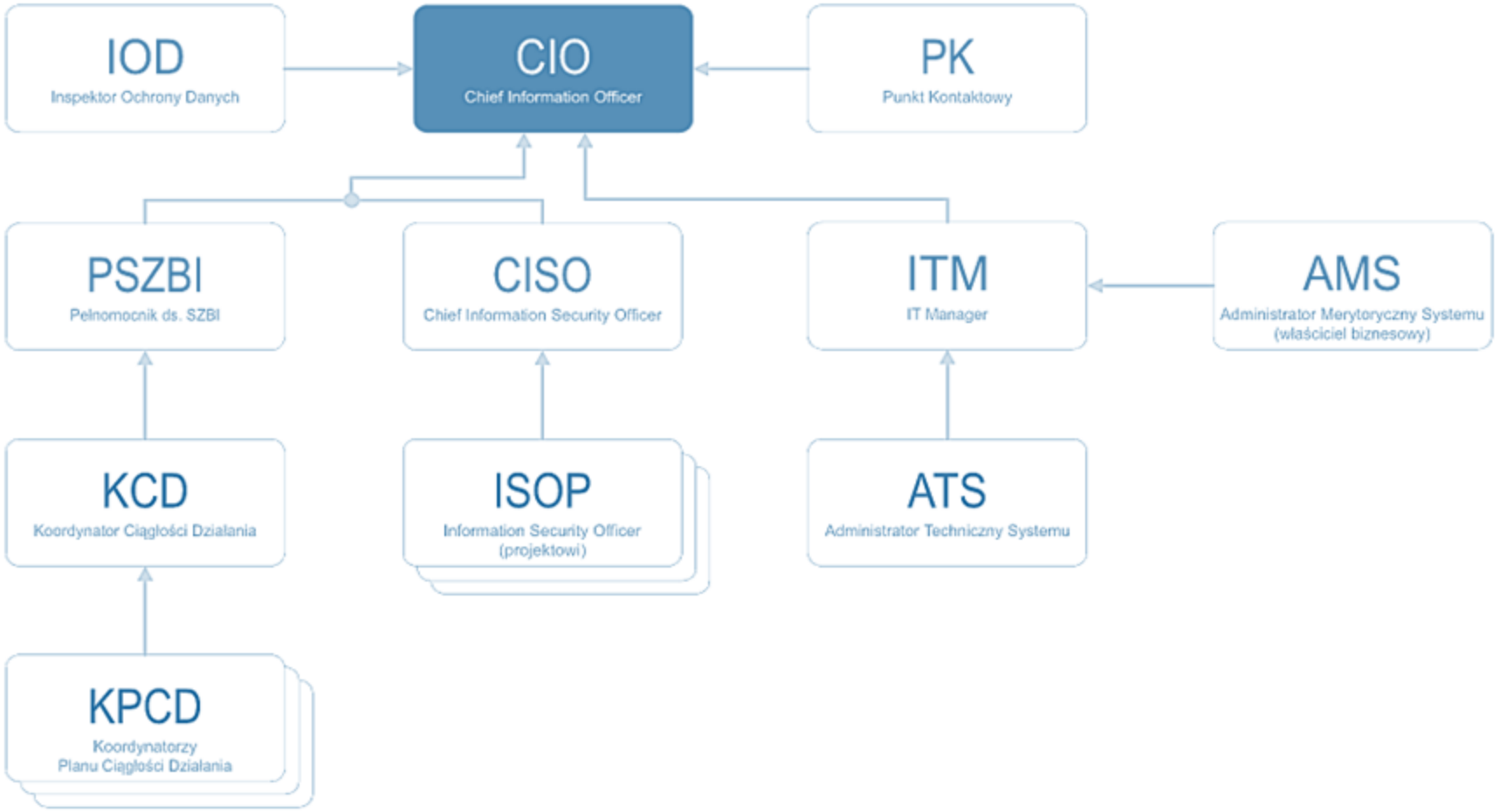
Minimum działające w 90 dni

- inwentaryzacja zasobów wraz z krytycznością, ryzyka, CIRP jako playbook wraz z kanałami raportowania, MFA, segregacja sieci na systemach krytycznych, zarządzanie podatnościami, zasady patchowania.
- wczesne włączenie obszaru zakupów i prawnego do wymagań wobec dostawców, szczególnie w zakresie SLA, prawa audytu, zasad zgłaszania incydentów).
- wdrożenie automatyzacji (SIEM, skanery, skrypty zbierające logi, konfiguracje).
- Regularne table-topy i testy odtworzeniowe.

Przykładowa lista kontrolna CISO

1. Zakres, klasyfikacja informacji, usług i systemów krytycznych (w tym usługi mieszczące się w IR 2024/2690).
2. Ocena Gap – w zakresie NIS2 art. 21 oraz ew. 2024/2690 w stosunku do SoA/Zał A.
3. Plan zgodności z kamieniami milowymi (60/120/180 dni) oraz wskaźnikami KRI.
4. Governance – uchwała zarządu, wskazanie role i odpowiedzialności, ustalenie cyklu przeglądów.
5. Zarządzanie ryzykiem – metodologia, apetyt na ryzyko, rejestr ryzyka, przypisanie właścicieli.
6. IRP/SOC – CIRP, playbooki, kryteria incydentu istotnego, informowanie CSIRT, 24/7.
7. Łańcuch dostaw – audyty, klauzule w umowach, ciągłość usług.
8. BCP/DRP – BIA, strategia, RTO/RPO, testy odtworzeniowe.
9. Narzędzia – MFA, segmentacja, hardening, XDR/AV, logowanie (retencja), kryptografia.
10. Podatności i patchowanie – zasady, SLA, wskaźniki (np. krytyczne/o niskim wpływie), dowody.
11. Szkolenia i świadomość z mierzeniem efektywności.
12. Dowody – mapa wymagań → kontrolka → dowód, repozytorium dowodów.

Przykładowa struktura organizacyjna



Materiały dla uczestników

- Dyrektywa NIS2 (UE) 2022/2555

https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX%3A32022L2555

- IR 2024/2690

https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=OJ:L_202402690

- NIS2 Technical Implementation Guidance (2025)

https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance

- NIST Cybersecurity Framework 2.0 — dokument główny (PDF)

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

- NIST CSF 2.0 — tłumaczenie na język polski (PDF)

https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=959071

- CIS Controls v8.1 — pobierz (oficjalnie)

https://www.cisecurity.org/controls/v8-1

Feedback

Zeskanuj kod i zostaw swoją opinię

THE H@CK SUMMIT

[Compliance] Praktyka wdrażania wymagań NIS2/UoKSC w oparciu o wytyczne regulacji europejskich

Artur Cieślik

https://thehacksummit.com/user.html#!/lecture/THS25-c9c6/rate