Raport Gap Analysis

NIS2 / ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (UoKSC, t.j. Dz.U. 2026 poz. 20; nowelizacja wdrażająca NIS2: ustawa z 23.01.2026, Dz.U. 2026 poz. 252, w mocy od 3.04.2026) · Analiza luk i ocena dojrzałości

Demo Industrial Sp. z o.o.
Data: 14.09.2026
Nr ref.: GA-2026-09-DI/NIS2___KSC

Klient	Demo Industrial Sp. z o.o.	Branża / sektor	Produkcja (armatura przemysłowa), podmiot ważny KSC
Numer referencyjny	GA-2026-09-DI/NIS2___KSC	Wersja / status dokumentu	1.0 / Finalny
Klasyfikacja	Poufne - Demo Industrial Sp. z o.o. / PushSec	Podstawa stosowania regulacji	Obowiązek ustawowy
Perspektywa oceny	Pełny zakres	Data wizyty	03.09.2026
Data raportu	14.09.2026	Konsultant wiodący	Rafał Dobrosielski
Reprezentant klienta	Anna Kowal	Liczba pracowników	180
Model pracy	Stacjonarny (produkcja), hybrydowy (biuro, sprzedaż)	Lokalizacja	Gliwice (siedziba), Tychy
Zakres oceny	Cała organizacja: zakład w Gliwicach (produkcja, biuro) i zakład w Tychach (magazyn, montaż), systemy ERP, SCADA linii L1 i L2, Microsoft 365, sieć zakładowa, dostawca IT.		

Brief dla zarządu

Niezgodny z wymaganiami regulacji Gotowość: Niegotowy (poniżej 1,5). Średnia dojrzałość 1,2 / 5,0.

44 luki, w tym **4** krytycznych Nakład remediacji: **53,0** dni rob. Quick Wins: **4**

Najważniejsze ryzyka

- Niezłożenie wniosku w terminie to pierwsza i najłatwiejsza do wykrycia niezgodność z ustawą, obarczona karą administracyjną, niezależna od stanu SZBI.
- Bez osób do kontaktu nie da się złożyć kompletnego wniosku o wpis ani odebrać wezwania CSIRT w trakcie incydentu.
- Szacowanie ryzyka jest obowiązkiem ustawowym (art. 8 ust. 1 pkt 1).

Terminy niedyskrecjonalne

- **03.04.2026** Nowelizacja UoKSC wdrażająca NIS2 wchodzi w życie (Dz.U. 2026 poz. 252)
- **03.10.2026** Wniosek o wpis do wykazu podmiotów kluczowych i ważnych: 6 mies. od spełnienia przesłanek (art. 7c ust. 1); dla...
- **03.04.2027** Realizacja obowiązków rozdz. 3: SZBI (art. 8), dokumentacja (art. 10), zgłaszanie incydentów (art. 11-12b), osoby...

Decyzje wymagane od zarządu

- Zatwierdzenie budżetu i zasobów na remediację (szacunek: 53,0 dni roboczych).
- Wyznaczenie właściciela programu remediacji i trybu raportowania postępu do zarządu.
- Formalne wskazanie osoby odpowiedzialnej za obowiązki regulacyjne w organie zarządzającym oraz potwierdzenie klasyfikacji i statusu organizacji.

Szczegóły w dalszej części raportu. Brief nie zastępuje ustaleń z sekcji 1 i tabeli luk.

Spis treści

1. Streszczenie dla zarządu (Executive Summary)
2. Stosowalność regulacji
3. Decyzje wymagane od zarządu
4. Wskaźniki gotowości i werdykt zgodności
5. Ocena dojrzałości według obszarów
6. Zidentyfikowane luki i rekomendacje
7. Obciążenie właścicieli remediacji
8. Efekt cross-framework
9. Karty szczegółowe luk (GA-Z6)
10. Quick Wins
11. Dokumenty wejściowe
12. Wymagania poza przyjętą perspektywą oceny
13. Uczestnicy i ustalenia z wizyty
14. Roadmapa wdrożenia
M. Metodyka i zastrzeżenia
15. Wersja dokumentu i zasady dystrybucji

1 Streszczenie dla zarządu (Executive Summary)

Kontekst. Przeprowadzono analizę luk (gap analysis) dla NIS2 / ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (UoKSC, t.j. Dz.U. 2026 poz. 20; nowelizacja wdrażająca NIS2: ustawa z 23.01.2026, Dz.U. 2026 poz. 252, w mocy od 3.04.2026) w organizacji Demo Industrial Sp. z o.o. Cel oceny: Ocena gotowości do wdrożenia SZBI wg ISO 27001 pod obowiązki podmiotu ważnego (UoKSC) z opcją certyfikacji w 2027 r.. Zakres: Cała organizacja: zakład w Gliwicach (produkcja, biuro) i zakład w Tychach (magazyn, montaż), systemy ERP, SCADA linii L1 i L2, Microsoft 365, sieć zakładowa, dostawca IT. Podstawa stosowania regulacji: obowiązek ustawowy.

PRÓBKA. DANE FIKCYJNE

Werdykt zgodności. **Niezgodny z wymaganiami regulacji** Zidentyfikowano 30 wymagań blokujących (luka o priorytecie krytycznym albo dojrzałość 0-1): N0-3, N0-4, N0-5, N0-9, N0-6, N0-10, N1-1, N1-2 i inne. Do czasu ich usunięcia organizacja nie może wykazać zgodności.

Kluczowe ustalenia. Średnia dojrzałość ocenionego zakresu wynosi **1,2 / 5,0** (Niegotowy (poniżej 1,5) - pełna zgodność wymaga 12+ miesięcy prac od podstaw). Ocenie podlegało **48** wymagań; luki zidentyfikowano w **44** z nich: **4 K** / **11 W** / **29 Ś**. Oznaczono **4** szybkie poprawy (Quick Wins), z których każda wymaga nie więcej niż około 2 tygodni pracy.

Najważniejsze ryzyka biznesowe. Luki krytyczne koncentrują się w obszarach: A. Status podmiotu i obowiązki formalne (2 K), B. Szacowanie ryzyka i podstawa SZBI (1 K), D. Cyberzagrożenia, obsługa i zgłaszanie incydentów, środki ograniczające (1 K). W praktyce oznaczają one m.in.:

- Niezłożenie wniosku w terminie to pierwsza i najłatwiejsza do wykrycia niezgodność z ustawą, obarczona karą administracyjną, niezależna od stanu SZBI. (poz. 1)
- Bez osób do kontaktu nie da się złożyć kompletnego wniosku o wpis ani odebrać wezwania CSIRT w trakcie incydentu. (poz. 2)
- Szacowanie ryzyka jest obowiązkiem ustawowym (art. 8 ust. 1 pkt 1). (poz. 3)
- Niedotrzymanie terminów zgłoszeń jest najczęstszą podstawą działań nadzorczych wobec podmiotów ważnych. (poz. 4)

Nieusunięte, blokują zgodność ustawową i narażają na sankcje. Pełny opis każdego ryzyka w kartach GA-Z6.

Rekomendowane działania.

Natychmiast (0-14 dni) - Quick Wins

- **N0-3** Złożyć wniosek przez system S46 przed 3.10.2026 z danymi podmiotu, sektorem, usługą i osobami do kontaktu. Zachować potwierdzenie złożenia.
- **N0-4** Wyznaczyć zarządzeniem co najmniej dwie osoby (Pełnomocnik ds. SZBI i Kierownik IT), z zastępstwem, telefonem i adresem e-mail dostępnymi całodobowo dla CSIRT. Zgłosić we wniosku o wpis.
- **N0-1** Udokumentować kwalifikację: sektor z załącznika, przesłanka wielkościowa (średnie przedsiębiorstwo, 180 osób), świadczona usługa, data ustalenia, podstawa prawna. Zachować jako dowód dla organu.
- **N4-2** Przeprowadzić udokumentowane szkolenie Zarządu (2 h) do końca 2026 r. i powtarzać corocznie. Zaświadczenie do akt.

Quick Win realizowany jest w oknie 14 dni od daty raportu niezależnie od okna przypisanego priorytetu; tak też prezentowane są terminy tych pozycji w tabelach.

Pilne (do 30 dni) - luki krytyczne

- **N1-1** Patrz c6-1: metodyka i pierwsza ocena ryzyka dla systemu informacyjnego wspierającego usługę, z kryteriami proporcjonalności z ustawy.
- **N3-3** Wdrożyć procedurę incydentów (patrz A.5.24) z klasyfikacją, osobami do kontaktu, szablonami zgłoszeń S46 i ćwiczeniem tabletop przed 3.04.2027.

Krótkoterminowo (30-90 dni) - luki wysokie

- **N0-10** Powołać Pełnomocnika ds. SZBI, przypisać zadania cyberbezpieczeństwa w opisach stanowisk IT, ocenić model: własne struktury z outsourcingiem monitoringu (MSSP) jako opcja realna dla firmy tej wielkości.
- **N1-2** Patrz działanie nadrzędne wskazane w obserwacji.
- **N1-3** Patrz działanie nadrzędne wskazane w obserwacji.
- **N1-4** Patrz działanie nadrzędne wskazane w obserwacji.

  ... oraz 5 pozycji - pełna lista w tabeli luk.

Szacunkowy nakład i horyzont. Łączny szacowany nakład remediacji: **53,0 dni roboczych**. Przewidywany czas dojścia do gotowości: **12+ miesięcy** od rozpoczęcia prac.

Efekt dla pozostałych regulacji. Remediacja zidentyfikowanych luk domyka jednocześnie **103** powiązanych wymagań innych regulacji (ISO/IEC 27001, DORA), szczegóły w sekcji Efekt cross-framework.

Następny krok. PushSec rekomenduje rozpoczęcie od realizacji Quick Wins równolegle z usuwaniem luk krytycznych, według załączonej mapy drogowej (sekcja Roadmapa wdrożenia). Dla nadzoru nad programem remediacji rekomendowany jest komitet sterujący (sponsor z zarządu, Pełnomocnik ds. SZBI, przedstawiciel IT), przegląd postępu co 2 tygodnie w fazie Quick Wins i luk krytycznych, następnie co miesiąc, oraz kwartalne raportowanie statusu do zarządu.

> **Kalendarz ustawowy.** Znowelizowana UoKSC obowiązuje od 3.04.2026. Wniosek o wpis do wykazu podmiotów kluczowych i ważnych składa się w terminie 6 miesięcy od dnia spełnienia przesłanek (art. 7c ust. 1); dla podmiotu spełniającego je w dniu wejścia w życie ustawy termin upływa **3.10.2026**. Obowiązki rozdziału 3 (SZBI, dokumentacja, zgłaszanie incydentów, osoby kontaktowe, szkolenie kierownika) realizuje się w terminie 12 miesięcy, a podmiot kluczowy zapewnia pierwszy audyt bezpieczeństwa w terminie 24 miesięcy od spełnienia przesłanek (art. 16), czyli odpowiednio do **3.04.2027** i **3.04.2028**. Są to terminy niedyskrecjonalne, niezależne od przyjętej w tym raporcie mapy drogowej i nadrzędne wobec okien priorytetów. Ze względów operacyjnych (obciążenie platformy pod koniec terminu) PushSec rekomenduje złożenie wniosku o wpis najpóźniej do końca września 2026.
>
> **Skala sankcji.** UoKSC przewiduje administracyjne kary pieniężne do 10 mln EUR lub 2% przychodu (podmiot kluczowy) i do 7 mln EUR lub 1,4% przychodu (podmiot ważny) oraz odrębną odpowiedzialność finansową kierownika podmiotu. Przepisy o karach są objęte następczą kontrolą Trybunału Konstytucyjnego, co nie zwalnia z obowiązków, ale powinno być monitorowane.
>
> **Założenie klasyfikacji.** Formalna klasyfikacja podmiotu pozostaje luką (poz. 5 w tabeli). Na potrzeby niniejszej oceny przyjęto roboczo status wynikający z sektora i wielkości organizacji; potwierdzenie klasyfikacji warunkuje ostateczny katalog obowiązków i powinno nastąpić w pierwszej kolejności.

PRÓBKA. DANE FIKCYJNE

2 Stosowalność regulacji

Wniosek o objęciu organizacji tą regulacją wraz z rolą i uzasadnieniem. Wniosek wydano na podstawie informacji przekazanych przez organizację; zmiana profilu działalności, wielkości lub portfela usług wymaga jego ponownego przeglądu.

Regulacja lub standard	Wniosek	Rola organizacji	Perspektywa oceny	Kompletność	Uzasadnienie
NIS2 / ustawa o krajowym systemie cyberbezpieczeństwa ustawa z 5.07.2018 o KSC (t.j. Dz.U. 2026 poz. 20) ze zmianą Dz.U. 2026 poz. 252	Do rozstrzygnięcia	-	Pełny zakres	0/11	Brak odpowiedzi rozstrzygających; wymaga uzupełnienia danych o sektorze, wielkości i kategoriach objętych niezależnie od wielkości.

3 Decyzje wymagane od zarządu

Zestawienie rozstrzygnięć, które muszą zapaść na poziomie organu zarządzającego, ponieważ warunkują wykonanie planu remediacji. Pozostałe działania mają charakter operacyjny i są przypisane w tabeli luk.

- Zatwierdzenie budżetu i zasobów na remediację (szacunek: 53,0 dni roboczych).
- Wyznaczenie właściciela programu remediacji i trybu raportowania postępu do zarządu.
- Formalne wskazanie osoby odpowiedzialnej za obowiązki regulacyjne w organie zarządzającym oraz potwierdzenie klasyfikacji i statusu organizacji.
- Akceptacja ryzyka szczątkowego i planu postępowania z ryzykiem po zakończeniu remediacji.
- Decyzja o programie szkoleń, w tym obowiązkowym szkoleniu kierownictwa, i jego finansowaniu.
- Decyzja o aneksowaniu umów z kluczowymi dostawcami (klauzule bezpieczeństwa, prawo audytu, wyjście).
- Decyzja o terminie i wykonawcy audytu lub oceny zgodności, z uwzględnieniem wymogów niezależności.

4 Wskaźniki gotowości i werdykt zgodności

Niezgodny z wymaganiami regulacji

Zidentyfikowano 30 wymagań blokujących (luka o priorytecie krytycznym albo dojrzałość 0-1): N0-3, N0-4, N0-5, N0-9, N0-6, N0-10, N1-1, N1-2 i inne. Do czasu ich usunięcia organizacja nie może wykazać zgodności.

Werdykt liczony z pokrycia wymagań: każde wymaganie z luką krytyczną albo dojrzałością 0-1 blokuje zgodność, niezależnie od średniej dojrzałości. Wskaźnik gotowości poniżej opisuje dystans do celu, nie status zgodności.

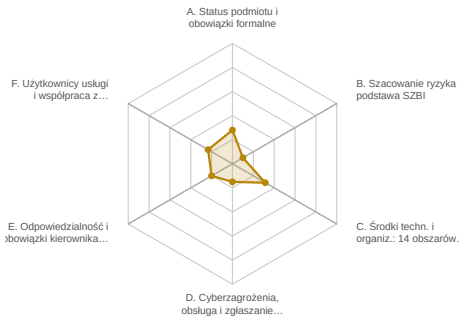
Ocena gotowości: Niegotowy (poniżej 1,5) - pełna zgodność wymaga 12+ miesięcy prac od podstaw

1,2	4	4	100%	100%
Średnia dojrzałość / 5,0	Luki krytyczne	Quick Wins	Postęp oceny	Ocen z dowodem

PRÓBKA, DANE FIKCYJNE

5 Ocena dojrzałości według obszarów

Skala dojrzałości: 0 Nieistniejący (brak działań) · 1 Inicjalny (działania ad-hoc, nieudokumentowane) · 2 Powtarzalny (wdrożenie częściowe lub nieformalne) · 3 Zdefiniowany (wdrożone i udokumentowane, bez regularnej weryfikacji) · 4 Zarządzany (wdrożone, udokumentowane i weryfikowane) · 5 Optymalizujący (pełna zgodność, proces doskonalony)



Obszar	Ocena	Poziom
A. Status podmiotu i obowiązki formalne	1,4	28% skali dojrzałości
B. Szacowanie ryzyka i podstawa SZBI	0,5	10% skali dojrzałości
C. Środki techniczne i organizacyjne: 14 obszarów ustawowych	1,6	31% skali dojrzałości
D. Cyberzagrożenia, obsługa i zgłaszanie incydentów, środki ograniczające	0,8	15% skali dojrzałości
E. Odpowiedzialność i obowiązki kierownika podmiotu	1,0	20% skali dojrzałości
F. Użytkownicy usługi i współpraca z krajowym systemem cyberbezpieczeństwa	1,2	23% skali dojrzałości
G. Perspektywa dostawcy ICT podmiotu kluczowego lub ważnego	-	nie oceniono

6 Zidentyfikowane luki i rekomendacje

Numeracja luk jest ciągła (1-44) i wspólna z kartami szczegółowymi GA-Z6. Tabela obejmuje wyłącznie zidentyfikowane luki; wymagania w pełni spełnione (5/5) oraz wyłączone z zakresu nie są w niej ujmowane i nie wchodzą do sumy nakładu.

PRÓBKA, DANE FIKCYJNE

Nr	Wymaganie	Obszar	Luka	Prior.	Dojrz.	Dowód	Rekomendacja	Właściciel	Dni	Termin
Krytyczne (blokują zgodność ustawową)										
1	**N0-3**	A. Status podmiotu i obowiązki formalne	**Wniosek o wpis do wykazu podmiotów kluczowych i ważnych złożony w S46 w terminie (art....** Wniosek o wpis do wykazu podmiotów kluczowych i ważnych nie został złożony. Termin ustawowy: 3.10.2026.	K QW	0,0	Wywiad	Złożyć wniosek przez system S46 przed 3.10.2026 z danymi podmiotu, sektorem, usługą i osobami do kontaktu. Zachować potwierdzenie złożenia.	Zarząd (A) / Pełnomocnik ds. SZBI (R)	1,0	do 28.09.2026 okno prior.: 30.09.2026
2	**N0-4**	A. Status podmiotu i obowiązki formalne	**Wyznaczenie co najmniej dwóch osób odpowiedzialnych za kontakty z podmiotami KSC (art....** Nie wyznaczono osób odpowiedzialnych za kontakty z podmiotami krajowego systemu cyberbezpieczeństwa.	K QW	0,0	Wywiad	Wyznaczyć zarządzeniem co najmniej dwie osoby (Pełnomocnik ds. SZBI i Kierownik IT), z zastępstwem, telefonem i adresem e-mail dostępnymi całodobowo dla CSIRT. Zgłosić we wniosku o wpis.	Zarząd (A) / Pełnomocnik ds. SZBI (R)	0,5	do 28.09.2026 okno prior.: 30.09.2026
3	**N1-1**	B. Szacowanie ryzyka i podstawa SZBI	**Systematyczne szacowanie ryzyka wystąpienia incydentu w systemie wykorzystywanym do...** Brak systematycznego szacowania ryzyka wystąpienia incydentu.	K	0,0	Wywiad	Patrz c6-1: metodyka i pierwsza ocena ryzyka dla systemu informacyjnego wspierającego usługę, z kryteriami proporcjonalności z ustawy.	Zarząd (A) / Pełnomocnik ds. SZBI (R)	-	30.11.2026
4	**N3-3**	D. Cyberzagrożenia, obsługa i zgłaszanie incydentów, środki ograniczające	**Wczesne ostrzeżenie w 24h i zgłoszenie incydentu poważnego w 72h do CSIRT sektorowego...** Brak zdolności do wczesnego ostrzeżenia w 24 h i zgłoszenia incydentu poważnego w 72 h do CSIRT.	K	0,0	Wywiad	Wdrożyć procedurę incydentów (patrz A.5.24) z klasyfikacją, osobami do kontaktu, szablonami zgłoszeń S46 i ćwiczeniem tabletop przed 3.04.2027.	Kierownik IT (R) / Pełnomocnik ds. SZBI (A)	2,0	31.12.2026
Wysokie (do usunięcia przed oceną zewnętrzną)										
5	**N0-1**	A. Status podmiotu i obowiązki formalne	**Klasyfikacja podmiotu: kluczowy, ważny albo poza zakresem ustawy (art. 5)** Samoidentyfikacja przeprowadzona nieformalnie ("prawnik powiedział, że podlegamy") bez udokumentowanej analizy sektora, progu wielkości i usługi.	W QW	2,0	Wywiad	Udokumentować kwalifikację: sektor z załącznika, przesłanka wielkościowa (średnie przedsiębiorstwo, 180 osób), świadczona usługa, data ustalenia, podstawa prawna. Zachować jako dowód dla organu.	Zarząd (A) / Pełnomocnik ds. SZBI (R)	1,0	do 28.09.2026 okno prior.: 30.09.2026

PRÓBKA, DANE FIKCYJNE

6	**N0-10**	A. Status podmiotu i obowiązki formalne	**Wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo albo umowa z MSSP (art. 14)** Brak wewnętrznej struktury odpowiedzialnej za cyberbezpieczeństwo (2 osoby IT skupione na utrzymaniu) i brak umowy z MSSP.	W	1,0	**Wywiad**	Powołać Pełnomocnika ds. SZBI, przypisać zadania cyberbezpieczeństwa w opisach stanowisk IT, ocenić model: własne struktury z outsourcingiem monitoringu (MSSP) jako opcja realna dla firmy tej wielkości.	Zarząd (A) / Pełnomocnik ds. SZBI (R)	3,0	31.12.2026
7	**N1-2**	B. Szacowanie ryzyka i podstawa SZBI	**Zarządzanie zidentyfikowanym ryzykiem: rejestr, plan postępowania, właściciele,...** Brak: Zarządzanie zidentyfikowanym ryzykiem: rejestr, plan postępowania, właściciele, terminy, przeglądy.	W	0,0	**Wywiad**	Patrz działanie nadrzędne wskazane w obserwacji.	Zarząd (A) / Pełnomocnik ds. SZBI (R)	2,0	28.02.2027
8	**N1-3**	B. Szacowanie ryzyka i podstawa SZBI	**Udokumentowana metodyka szacowania ryzyka z sześcioma kryteriami proporcjonalności z...** Brak: Udokumentowana metodyka szacowania ryzyka z sześcioma kryteriami proporcjonalności z art. 8 ust. 1 pkt 2.	W	0,0	**Wywiad**	Patrz działanie nadrzędne wskazane w obserwacji.	Zarząd (A) / Pełnomocnik ds. SZBI (R)	2,0	28.02.2027
9	**N1-4**	B. Szacowanie ryzyka i podstawa SZBI	**Wyniki szacowania ryzyka udokumentowane i okresowo przeglądane** Brak: Wyniki szacowania ryzyka udokumentowane i okresowo przeglądane.	W	0,0	**Wywiad**	Patrz działanie nadrzędne wskazane w obserwacji.	Zarząd (A) / Pełnomocnik ds. SZBI (R)	2,0	28.02.2027
10	**N1-5**	B. Szacowanie ryzyka i podstawa SZBI	**Kierownik podmiotu zatwierdza wyniki szacowania ryzyka i akceptuje ryzyko szczątkowe** Brak: Kierownik podmiotu zatwierdza wyniki szacowania ryzyka i akceptuje ryzyko szczątkowe.	W	0,0	**Wywiad**	Patrz działanie nadrzędne wskazane w obserwacji.	Zarząd (A) / Pełnomocnik ds. SZBI (R)	2,0	28.02.2027
11	**N2-15**	C. Środki techniczne i organizacyjne: 14 obszarów ustawowych	**Lit. h: polityki i procedury oceny skuteczności środków technicznych i organizacyjnych** Brak: Lit. h: polityki i procedury oceny skuteczności środków technicznych i organizacyjnych.	W	0,0	**Wywiad**	Patrz działanie nadrzędne wskazane w obserwacji.	Zarząd (A) / Pełnomocnik ds. SZBI (R)	2,0	28.02.2027

PRÓBKA, DANE FIKCYJNE

12	**N3-6**	D. Cyberzagrożenia, obsługa i zgłaszanie incydentów, środki ograniczające	**Kryteria uznania incydentu za poważny i udokumentowana decyzja klasyfikacyjna (art. 2...** Brak: Kryteria uznania incydentu za poważny i udokumentowana decyzja klasyfikacyjna (art. 2 pkt 7, art. 11 ust. 4).	W	0,0	**Wywiad**	Patrz działanie nadrzędne wskazane w obserwacji.	Zarząd (A) / Pełnomocnik ds. SZBI (R)	2,0	28.02.2027
13	**N3-5**	D. Cyberzagrożenia, obsługa i zgłaszanie incydentów, środki ograniczające	**Sprawozdanie końcowe w ciągu miesiąca, sprawozdanie okresowe i sprawozdanie z postępu...** Brak: Sprawozdanie końcowe w ciągu miesiąca, sprawozdanie okresowe i sprawozdanie z postępu (art. 11 ust. 1 pkt 4b-4c, art. 12a-12b).	W	0,0	**Wywiad**	Patrz działanie nadrzędne wskazane w obserwacji.	Zarząd (A) / Pełnomocnik ds. SZBI (R)	2,0	28.02.2027
14	**N4-2**	E. Odpowiedzialność i obowiązki kierownika podmiotu	**Coroczne, udokumentowane szkolenie kierownika podmiotu i osoby, której powierzono...** Kierownik podmiotu nie odbył szkolenia z cyberbezpieczeństwa wymaganego corocznie przez ustawę.	W QW	0,0	**Wywiad**	Przeprowadzić udokumentowane szkolenie Zarządu (2 h) do końca 2026 r. i powtarzać corocznie. Zaświadczenie do akt.	Zarząd (A) / Pełnomocnik ds. SZBI (R)	0,5	do 28.09.2026 okno prior.: 31.12.2026
15	**N5-7**	F. Użytkownicy usługi i współpraca z krajowym systemem cyberbezpieczeństwa	**Rozpoczęcie korzystania z systemu S46 po uzyskaniu wpisu do wykazu (art. 9 ust. 1 pkt...** Brak: Rozpoczęcie korzystania z systemu S46 po uzyskaniu wpisu do wykazu (art. 9 ust. 1 pkt 4, art. 46 ust. 1).	W	0,0	**Wywiad**	Patrz działanie nadrzędne wskazane w obserwacji.	Zarząd (A) / Pełnomocnik ds. SZBI (R)	2,0	28.02.2027
Średnie (nieusunięte staną się ustaleniami audytowymi)										
16	**N0-8**	A. Status podmiotu i obowiązki formalne	**Aktualizacja danych w wykazie w terminie 14 dni od zmiany (art. 7c ust. 3, art. 7k)**	Ś	2,0	**Wywiad**	Zakres: aktualizacja danych w wykazie w terminie 14 dni od zmiany (art. 7c ust. 3, art. 7k). Działanie: sformalizować i zatwierdzić istniejącą praktykę, uzupełnić brakujące elementy, zakomunikować w organizacji i przypisać właściciela. Oczekiwany dowód wdrożenia: Procedura aktualizacji danych w wykazie + zapisy wniosków o zmianę wpisu (14 dni). **	Zespół IT / Bezpieczeństwo*	1,0	

PRÓBKA, DANE FIKCYJNE

17	**N0-5**	A. Status podmiotu i obowiązki formalne	**Dokumentacja normatywna bezpieczeństwa systemu informacyjnego, w tym dokumentacja...**	Ś	1,0	**Wywiad**	Zakres: dokumentacja normatywna bezpieczeństwa systemu informacyjnego, w tym dokumentacja ochrony infrastruktury (art. 10 ust. 1-3). Działanie: opracować i wdrożyć, udokumentować, zatwierdzić przez kierownictwo i przypisać właściciela. Pierwszy krok: opracowanie dokumentu "Dokumentacja ochrony infrastruktury (art. 10 ust. 3 pkt 2)". Oczekiwany dowód wdrożenia: Wykaz dokumentacji normatywnej wg art. 10 ust. 3, w tym dokumentacja ochrony infrastruktury (7 elementów). **	HR / Pełnomocnik ds. SZBI*	1,0	
18	**N0-9**	A. Status podmiotu i obowiązki formalne	**Dokumentacja operacyjna, nadzór nad dokumentacją, retencja 2 lata i protokoły...**	Ś	1,0	**Wywiad**	Zakres: dokumentacja operacyjna, nadzór nad dokumentacją, retencja 2 lata i protokoły brakowania (art. 10 ust. 4-8). Działanie: opracować i wdrożyć, udokumentować, zatwierdzić przez kierownictwo i przypisać właściciela. Pierwszy krok: opracowanie dokumentu "Instrukcja nadzoru nad dokumentacją: wersjonowanie, retencja 2 lata, protokoły brakowania (art. 10 ust. 6-8)". Oczekiwany dowód wdrożenia: Zasady nadzoru nad dokumentacją (dostęp, ochrona, wersjonowanie), harmonogram retencji 2 lata, protokoły brakowania. **	Zespół IT / Bezpieczeństwo*	1,0	

PRÓBKA, DANE FIKCYJNE

19	**N0-6**	A. Status podmiotu i obowiązki formalne	**Audyt bezpieczeństwa systemu informacyjnego: cykl, pierwszy termin, raport do organu,...**	Ś	1,0	**Wywiad**	Zakres: audyt bezpieczeństwa systemu informacyjnego: cykl, pierwszy termin, raport do organu, karencja audytora (art. 15-16). Działanie: opracować i wdrożyć, udokumentować, zatwierdzić przez kierownictwo i przypisać właściciela. Pierwszy krok: opracowanie dokumentu "Plan audytu bezpieczeństwa systemu informacyjnego (art. 15) z rezerwacją audytorów i procesem przekazania raportu organowi". Oczekiwany dowód wdrożenia: Raport z audytu bezpieczeństwa (podmiot kluczowy: raz na 3 lata, pierwszy do 24 mies.) + dowód przekazania kopii organowi w 3 dni robocze. **	Audyt wewnętrzny / Pełnomocnik ds. SZBI*	1,0	
20	**N2-1**	C. Środki techniczne i organizacyjne: 14 obszarów ustawowych	**Lit. a: polityki szacowania ryzyka oraz bezpieczeństwa systemu informacyjnego, w tym...**	Ś	1,0	**Wywiad**	Zakres: lit. a: polityki szacowania ryzyka oraz bezpieczeństwa systemu informacyjnego, w tym polityki tematyczne. Działanie: opracować i wdrożyć, udokumentować, zatwierdzić przez kierownictwo i przypisać właściciela. Pierwszy krok: opracowanie dokumentu "Polityka Bezpieczeństwa Informacji". Oczekiwany dowód wdrożenia: Polityka bezpieczeństwa i szacowania ryzyka + polityki tematyczne zatwierdzone przez kierownika. **	Zarząd / Pełnomocnik ds. SZBI*	1,0	

PRÓBKA. DANE FIKCYJNE

21	**N2-2**	C. Środki techniczne i organizacyjne: 14 obszarów ustawowych	**Lit. b: bezpieczeństwo w nabywaniu, rozwoju, utrzymaniu i eksploatacji systemu...**	Ś	2,0	**Wywiad**	Zakres: lit. b: bezpieczeństwo w nabywaniu, rozwoju, utrzymaniu i eksploatacji systemu informacyjnego, w tym testowanie. Działanie: sformalizować i zatwierdzić istniejącą praktykę, uzupełnić brakujące elementy, zakomunikować w organizacji i przypisać właściciela. Oczekiwany dowód wdrożenia: Udokumentowany proces bezpiecznego nabywania i rozwoju + wyniki testów bezpieczeństwa systemu. **	Zespół IT / Bezpieczeństwo*	1,0	
22	**N2-11**	C. Środki techniczne i organizacyjne: 14 obszarów ustawowych	**Lit. d: bezpieczeństwo zasobów ludzkich**	Ś	2,0	**Wywiad**	Zakres: lit. d: bezpieczeństwo zasobów ludzkich. Działanie: sformalizować i zatwierdzić istniejącą praktykę, uzupełnić brakujące elementy, zakomunikować w organizacji i przypisać właściciela. Oczekiwany dowód wdrożenia: Zapisy bezpieczeństwa zasobów ludzkich: weryfikacja, umowy, onboarding, offboarding. **	Zespół IT / Bezpieczeństwo*	1,0	
23	**N2-4**	C. Środki techniczne i organizacyjne: 14 obszarów ustawowych	**Lit. e: bezpieczeństwo i ciągłość łańcucha dostaw produktów, usług i procesów ICT, od...**	Ś	1,0	**Wywiad**	Zakres: lit. e: bezpieczeństwo i ciągłość łańcucha dostaw produktów, usług i procesów ICT, od których zależy usługa. Działanie: opracować i wdrożyć, udokumentować, zatwierdzić przez kierownictwo i przypisać właściciela. Pierwszy krok: opracowanie dokumentu "Polityka zarządzania dostawcami + Rejestr dostawców (Register of Information)". Oczekiwany dowód wdrożenia: Polityka łańcucha dostaw ICT + rejestr dostawców z ocenami i klauzulami (art. 8 ust. 2). **	Zakupy / Pełnomocnik ds. SZBI*	1,0	

PRÓBKA, DANE FIKCYJNE

24	**N2-5**	C. Środki techniczne i organizacyjne: 14 obszarów ustawowych	**Lit. f: wdrażanie, dokumentowanie, testowanie i utrzymywanie planów ciągłości...**	Ś	1,0	**Wywiad**	Zakres: lit. f: wdrażanie, dokumentowanie, testowanie i utrzymywanie planów ciągłości działania, planów awaryjnych i planów odtworzenia. Działanie: opracować i wdrożyć, udokumentować, zatwierdzić przez kierownictwo i przypisać właściciela. Pierwszy krok: opracowanie dokumentu "Plan Ciągłości Działania (BCP) + DRP + BIA". Oczekiwany dowód wdrożenia: Plany ciągłości, awaryjne i odtworzenia + zapisy testów i przeglądów. **	Zespół IT / Bezpieczeństwo*	1,0	
25	**N2-6**	C. Środki techniczne i organizacyjne: 14 obszarów ustawowych	**Lit. g: objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi...**	Ś	1,0	**Wywiad**	Zakres: lit. g: objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi monitorowaniem w trybie ciągłym. Działanie: opracować i wdrożyć, udokumentować, zatwierdzić przez kierownictwo i przypisać właściciela. Pierwszy krok: opracowanie dokumentu "Polityka logowania i monitorowania". Oczekiwany dowód wdrożenia: Konfiguracja i zapisy monitorowania w trybie ciągłym (logi, alerty, obsługa). **	Audyt wewnętrzny / Pełnomocnik ds. SZBI*	1,0	

PRÓBKA, DANE FIKCYJNE

26	**N2-8**	C. Środki techniczne i organizacyjne: 14 obszarów ustawowych	**Lit. i: edukacja z zakresu cyberbezpieczeństwa dla personelu podmiotu**	Ś	1,0	**Wywiad**	Zakres: lit. i: edukacja z zakresu cyberbezpieczeństwa dla personelu podmiotu. Działanie: opracować i wdrożyć, udokumentować, zatwierdzić przez kierownictwo i przypisać właściciela. Pierwszy krok: opracowanie dokumentu "Program szkoleń security awareness". Oczekiwany dowód wdrożenia: Program edukacji personelu z zakresu cyberbezpieczeństwa + rejestr uczestnictwa. **	HR / Pełnomocnik ds. SZBI*	1,0	
27	**N2-16**	C. Środki techniczne i organizacyjne: 14 obszarów ustawowych	**Lit. j: podstawowe zasady cyberhigieny**	Ś	2,0	**Wywiad**	Zakres: lit. j: podstawowe zasady cyberhigieny. Działanie: sformalizować i zatwierdzić istniejącą praktykę, uzupełnić brakujące elementy, zakomunikować w organizacji i przypisać właściciela. Oczekiwany dowód wdrożenia: Zasady cyberhigieny (regulamin lub polityka) + dowody wdrożenia (aktualizacje, EDR, MFA, kopie). **	Zespół IT / Bezpieczeństwo*	1,0	
28	**N2-7**	C. Środki techniczne i organizacyjne: 14 obszarów ustawowych	**Lit. k: polityki i procedury stosowania kryptografii, w tym w stosownych przypadkach...**	Ś	2,0	**Wywiad**	Zakres: lit. k: polityki i procedury stosowania kryptografii, w tym w stosownych przypadkach szyfrowania. Działanie: sformalizować i zatwierdzić istniejącą praktykę, uzupełnić brakujące elementy, zakomunikować w organizacji i przypisać właściciela. Oczekiwany dowód wdrożenia: Polityka kryptograficzna + procedura zarządzania kluczami. **	Zarząd / Pełnomocnik ds. SZBI*	1,0	

PRÓBKA, DANE FIKCYJNE

29	**N2-12**	C. Środki techniczne i organizacyjne: 14 obszarów ustawowych	**Lit. l: bezpieczne środki komunikacji elektronicznej w ramach KSC i wewnątrz podmiotu,...**	Ś	2,0	**Wywiad**	Zakres: lit. l: bezpieczne środki komunikacji elektronicznej w ramach KSC i wewnątrz podmiotu, z MFA w stosownych przypadkach. Działanie: sformalizować i zatwierdzić istniejącą praktykę, uzupełnić brakujące elementy, zakomunikować w organizacji i przypisać właściciela. Oczekiwany dowód wdrożenia: Wykaz bezpiecznych kanałów komunikacji (S46, poczta, komunikatory, łączność awaryjna) + raport pokrycia MFA. **	Zespół IT / Bezpieczeństwo*	1,0	
30	**N2-14**	C. Środki techniczne i organizacyjne: 14 obszarów ustawowych	**Lit. m: zarządzanie aktywami**	Ś	2,0	**Wywiad**	Zakres: lit. m: zarządzanie aktywami. Działanie: sformalizować i zatwierdzić istniejącą praktykę, uzupełnić brakujące elementy, zakomunikować w organizacji i przypisać właściciela. Oczekiwany dowód wdrożenia: Rejestr aktywów ICT i informacyjnych z właścicielami i klasyfikacją. **	Zarząd / Pełnomocnik ds. SZBI*	1,0	
31	**N2-9**	C. Środki techniczne i organizacyjne: 14 obszarów ustawowych	**Lit. n: polityki kontroli dostępu**	Ś	2,0	**Wywiad**	Zakres: lit. n: polityki kontroli dostępu. Działanie: sformalizować i zatwierdzić istniejącą praktykę, uzupełnić brakujące elementy, zakomunikować w organizacji i przypisać właściciela. Oczekiwany dowód wdrożenia: Polityka kontroli dostępu + zapisy przeglądów uprawnień. **	Zarząd / Pełnomocnik ds. SZBI*	1,0	

PRÓBKA, DANE FIKCYJNE

32	**N3-1**	D. Cyberzagrożenia, obsługa i zgłaszanie incydentów, środki ograniczające	**Zbieranie informacji o cyberzagrożeniach i podatnościach systemu wykorzystywanego do...**	Ś	1,0	**Wywiad**	Zakres: zbieranie informacji o cyberzagrożeniach i podatnościach systemu wykorzystywanego do świadczenia usługi (art. 8 ust. 1 pkt 3). Działanie: opracować i wdrożyć, udokumentować, zatwierdzić przez kierownictwo i przypisać właściciela. Pierwszy krok: opracowanie dokumentu "Procedura pozyskiwania informacji o cyberzagrożeniach i podatnościach (subskrypcje CSIRT, producenci, CVE)". Oczekiwany dowód wdrożenia: Subskrypcje źródeł o cyberzagrożeniach i podatnościach + zapisy analiz; porozumienia o wymianie informacji (art. 8h), jeśli zawarte. **	Zespół IT / Bezpieczeństwo*	1,0	
33	**N3-2**	D. Cyberzagrożenia, obsługa i zgłaszanie incydentów, środki ograniczające	**Zarządzanie incydentami: wykrywanie, rejestrowanie, obsługa, dostęp CSIRT do rejestru,...**	Ś	1,0	**Wywiad**	Zakres: zarządzanie incydentami: wykrywanie, rejestrowanie, obsługa, dostęp CSIRT do rejestru, wnioski (art. 8 ust. 1 pkt 4, art. 11 ust. 1 pkt 1-3 i 6). Działanie: opracować i wdrożyć, udokumentować, zatwierdzić przez kierownictwo i przypisać właściciela. Pierwszy krok: opracowanie dokumentu "Procedura zarządzania incydentami (z raportowaniem regulacyjnym)". Oczekiwany dowód wdrożenia: Procedura zarządzania incydentami + rejestr incydentów + zasady dostępu CSIRT do rejestru. **	Zarząd / Pełnomocnik ds. SZBI*	1,0	

PRÓBKA, DANE FIKCYJNE

34	**N3-4**	D. Cyberzagrożenia, obsługa i zgłaszanie incydentów, środki ograniczające	**Środki ograniczające wpływ incydentów: mechanizmy CIA i autentyczności, aktualizacje z...**	Ś	2,0	**Wywiad**	Zakres: środki ograniczające wpływ incydentów: mechanizmy CIA i autentyczności, aktualizacje z analizą wpływu, ochrona integralności (art. 8 ust. 1 pkt 5 lit. a-c). Działanie: sformalizować i zatwierdzić istniejącą praktykę, uzupełnić brakujące elementy, zakomunikować w organizacji i przypisać właściciela. Oczekiwany dowód wdrożenia: Procedura aktualizacji oprogramowania z analizą wpływu i krytyczności + mechanizmy integralności i CIA. **	HR / Pełnomocnik ds. SZBI*	1,0	
35	**N2-10**	D. Cyberzagrożenia, obsługa i zgłaszanie incydentów, środki ograniczające	**Niezwłoczne działania po dostrzeżeniu podatności lub cyberzagrożeń, w tym czasowe...**	Ś	1,0	**Wywiad**	Zakres: niezwłoczne działania po dostrzeżeniu podatności lub cyberzagrożeń, w tym czasowe ograniczenie ruchu przychodzącego (art. 8 ust. 1 pkt 5 lit. d). Działanie: opracować i wdrożyć, udokumentować, zatwierdzić przez kierownictwo i przypisać właściciela. Pierwszy krok: opracowanie dokumentu "Procedura zarządzania podatnościami i aktualizacjami". Oczekiwany dowód wdrożenia: Procedura zarządzania podatnościami z uprawnieniami do ograniczenia ruchu + raporty skanów i terminów usunięcia. **	Zespół IT / Bezpieczeństwo*	1,0	

PRÓBKA, DANE FIKCYJNE

36	**N5-2**	D. Cyberzagrożenia, obsługa i zgłaszanie incydentów, środki ograniczające	**Współdziałanie z CSIRT podczas obsługi incydentu poważnego i krytycznego, uzupełnianie...**	Ś	1,0	**Wywiad**	Zakres: współdziałanie z CSIRT podczas obsługi incydentu poważnego i krytycznego, uzupełnianie zgłoszeń (art. 11 ust. 1 pkt 5, art. 12 ust. 6-8, art. 32 ust. 3). Działanie: opracować i wdrożyć, udokumentować, zatwierdzić przez kierownictwo i przypisać właściciela. Pierwszy krok: opracowanie dokumentu "Procedura zarządzania incydentami (z raportowaniem regulacyjnym)". Oczekiwany dowód wdrożenia: Zapisy współdziałania z CSIRT: korespondencja, uzupełnienia zgłoszeń, przekazane informacje techniczne. **	Zespół IT / Bezpieczeństwo*	1,0	
37	**N4-1**	E. Odpowiedzialność i obowiązki kierownika podmiotu	**Odpowiedzialność kierownika podmiotu za obowiązki z zakresu cyberbezpieczeństwa i...**	Ś	1,0	**Wywiad**	Zakres: odpowiedzialność kierownika podmiotu za obowiązki z zakresu cyberbezpieczeństwa i wskazanie osoby odpowiedzialnej w organie wieloosobowym (art. 8c). Działanie: opracować i wdrożyć, udokumentować, zatwierdzić przez kierownictwo i przypisać właściciela. Pierwszy krok: opracowanie dokumentu "Uchwała zarządu: osoba odpowiedzialna, odpowiedzialność i zadania kierownika podmiotu (art. 8c-8d)". Oczekiwany dowód wdrożenia: Uchwała lub decyzja wskazująca osobę odpowiedzialną w organie wieloosobowym + zapis odpowiedzialności w regulaminie. **	Zespół IT / Bezpieczeństwo*	1,0	

PRÓBKA. DANE FIKCYJNE

38	**N4-4**	E. Odpowiedzialność i obowiązki kierownika podmiotu	**Realizacja pięciu zadań kierownika: decyzje o SZBI, środki finansowe, przydział zadań...**	Ś	1,0	**Wywiad**	Zakres: realizacja pięciu zadań kierownika: decyzje o SZBI, środki finansowe, przydział zadań i nadzór, świadomość personelu, zgodność (art. 8d). Działanie: opracować i wdrożyć, udokumentować, zatwierdzić przez kierownictwo i przypisać właściciela. Pierwszy krok: opracowanie dokumentu "Uchwała zarządu: osoba odpowiedzialna, odpowiedzialność i zadania kierownika podmiotu (art. 8c-8d)". Oczekiwany dowód wdrożenia: Dowody realizacji zadań kierownika: decyzje o SZBI, budżet cyberbezpieczeństwa, przydział zadań, raporty dla kierownika. **	HR / Pełnomocnik ds. SZBI*	1,0	
39	**N4-3**	E. Odpowiedzialność i obowiązki kierownika podmiotu	**Informacja z KRK o niekaralności za przestępstwa przeciwko ochronie informacji dla...**	Ś	2,0	**Wywiad**	Zakres: informacja z KRK o niekaralności za przestępstwa przeciwko ochronie informacji dla osób realizujących zadania z art. 8 i art. 11 (art. 8f). Działanie: sformalizować i zatwierdzić istniejącą praktykę, uzupełnić brakujące elementy, zakomunikować w organizacji i przypisać właściciela. Oczekiwany dowód wdrożenia: Rejestr informacji z KRK dla osób realizujących zadania z art. 8 i art. 11 (przed dopuszczeniem do zadań). **	HR / Pełnomocnik ds. SZBI*	1,0	

PRÓBKA, DANE FIKCYJNE

40	**N5-5**	F. Użytkownicy usługi i współpraca z krajowym systemem cyberbezpieczeństwa	**Udostępnianie użytkownikom usługi wiedzy o cyberzagrożeniach i skutecznych sposobach...**	Ś	2,0	**Wywiad**	Zakres: udostępnianie użytkownikom usługi wiedzy o cyberzagrożeniach i skutecznych sposobach zabezpieczania się (art. 9 ust. 1 pkt 2, ust. 4). Działanie: sformalizować i zatwierdzić istniejącą praktykę, uzupełnić brakujące elementy, zakomunikować w organizacji i przypisać właściciela. Oczekiwany dowód wdrożenia: Podstrona lub materiały dla użytkowników o cyberzagrożeniach i zabezpieczeniach (lub hiperłącza do CSIRT). **	Zespół IT / Bezpieczeństwo*	1,0	
41	**N5-6**	F. Użytkownicy usługi i współpraca z krajowym systemem cyberbezpieczeństwa	**Kanał umożliwiający użytkownikom zgłoszenie cyberzagrożenia, incydentu lub podatności...**	Ś	1,0	**Wywiad**	Zakres: kanał umożliwiający użytkownikom zgłoszenie cyberzagrożenia, incydentu lub podatności związanych z usługą (art. 9 ust. 1 pkt 3). Działanie: opracować i wdrożyć, udokumentować, zatwierdzić przez kierownictwo i przypisać właściciela. Pierwszy krok: opracowanie dokumentu "Podstrona bezpieczeństwa dla użytkowników, kanał zgłoszeń i szablony komunikatów o incydentach (art. 9, art. 11 ust. 2a-2b)". Oczekiwany dowód wdrożenia: Publicznie opisany kanał zgłaszania cyberzagrożeń, incydentów i podatności przez użytkowników (np. security.txt). **	Zespół IT / Bezpieczeństwo*	1,0	

PRÓBKA, DANE FIKCYJNE

42	**N5-1**	F. Użytkownicy usługi i współpraca z krajowym systemem cyberbezpieczeństwa	**Informowanie użytkowników usług o incydencie poważnym i o poważnym cyberzagrożeniu...**	Ś	1,0	**Wywiad**	Zakres: informowanie użytkowników usług o incydencie poważnym i o poważnym cyberzagrożeniu (art. 11 ust. 2a-2b). Działanie: opracować i wdrożyć, udokumentować, zatwierdzić przez kierownictwo i przypisać właściciela. Pierwszy krok: opracowanie dokumentu "Podstrona bezpieczeństwa dla użytkowników, kanał zgłoszeń i szablony komunikatów o incydentach (art. 9, art. 11 ust. 2a-2b)". Oczekiwany dowód wdrożenia: Wzory i zapisy informowania użytkowników o incydencie poważnym i poważnym cyberzagrożeniu. **	Zespół IT / Bezpieczeństwo*	1,0	
43	**N5-3**	F. Użytkownicy usługi i współpraca z krajowym systemem cyberbezpieczeństwa	**Dobrowolne przekazywanie informacji do CSIRT (art. 13)**	Ś	1,0	**Wywiad**	Zakres: dobrowolne przekazywanie informacji do CSIRT (art. 13). Działanie: opracować i wdrożyć, udokumentować, zatwierdzić przez kierownictwo i przypisać właściciela. Pierwszy krok: opracowanie dokumentu "Procedura zarządzania incydentami (z raportowaniem regulacyjnym)". Oczekiwany dowód wdrożenia: Zapisy dobrowolnych zgłoszeń do CSIRT (art. 13). **	Zespół IT / Bezpieczeństwo*	1,0	

PRÓBKA, DANE FIKCYJNE

44	**N5-4**	F. Użytkownicy usługi i współpraca z krajowym systemem cyberbezpieczeństwa	**Realizacja decyzji, wezwań i środków nadzorczych organu właściwego oraz rekomendacji...**	Ś	2,0	**Wywiad**	Zakres: realizacja decyzji, wezwań i środków nadzorczych organu właściwego oraz rekomendacji Pełnomocnika (art. 15 ust. 1b, art. 32 ust. 2, art. 33, art. 53, art. 67c). Działanie: sformalizować i zatwierdzić istniejącą praktykę, uzupełnić brakujące elementy, zakomunikować w organizacji i przypisać właściciela. Oczekiwany dowód wdrożenia: Rejestr decyzji, wezwań i rekomendacji organu i Pełnomocnika z dowodami realizacji. **	HR / Pełnomocnik ds. SZBI*	1,0	

* Właściciel oznaczony gwiazdką to propozycja przypisania wg wymagania, do potwierdzenia z klientem. ** Rekomendacja wyprowadzona z katalogu wymagań: propozycja konsultanta do walidacji na warsztacie remediacyjnym.

7 Obciążenie właścicieli remediacji

Rozkład zidentyfikowanych luk i szacowanego nakładu na właścicieli remediacji. Właściciele oznaczeni gwiazdką to propozycje przypisania (do potwierdzenia z klientem).

Właściciel remediacji	K	W	Ś	N	Luki razem	Nakład (dni)
Zarząd (A) / Pełnomocnik ds. SZBI (R)	3	11	-	-	**14**	**22,0**
Zespół IT / Bezpieczeństwo*	-	-	15	-	**15**	**15,0**
HR / Pełnomocnik ds. SZBI*	-	-	6	-	**6**	**6,0**
Zarząd / Pełnomocnik ds. SZBI*	-	-	5	-	**5**	**5,0**
Kierownik IT (R) / Pełnomocnik ds. SZBI (A)	1	-	-	-	**1**	**2,0**
Audyt wewnętrzny / Pełnomocnik ds. SZBI*	-	-	2	-	**2**	**2,0**
Zakupy / Pełnomocnik ds. SZBI*	-	-	1	-	**1**	**1,0**
Razem					**44**	**53,0**

Przeliczenie na zasoby. Łączny nakład 53,0 dni roboczych odpowiada około **2,5 osobomiesiąca(-y)** pracy (21 dni roboczych/mies.). Realizacja siłami jednej osoby przy pełnym zaangażowaniu zajmie ok. 3 mies., przy zaangażowaniu połowy etatu ok. 5 mies. - bez uwzględnienia bieżących obowiązków tej osoby.

8 Efekt cross-framework

Wymagania ocenianej normy są zmapowane na wymagania innych regulacji. Remediacja luk z tego raportu domyka jednocześnie **103** powiązanych wymagań poniższych regulacji, co obniża łączny koszt zgodności i pozwala uniknąć dublowania prac.

PRÓBKA, DANE FIKCYJNE

Regulacja / norma	Powiązane wymagania	Odwołania
ISO/IEC 27001	**93**	ISO 27001 pkt 10.1, ISO 27001 pkt 10.2, ISO 27001 pkt 4.1, ISO 27001 pkt 4.3, ISO 27001 pkt 5.1, ISO 27001 pkt 5.2, ISO 27001 pkt 5.3, ISO 27001 pkt 6.1, ISO 27001 pkt 7.1, ISO 27001 pkt 7.2, ISO 27001 pkt 7.5, ISO 27001 pkt 8.1, ISO 27001 pkt 8.2, ISO 27001 pkt 8.3, ISO 27001 pkt 9.1, ISO 27001 pkt 9.2, ISO 27001 pkt 9.3, ISO 27001 A.5.1, ISO 27001 A.5.10, ISO 27001 A.5.11, ISO 27001 A.5.12, ISO 27001 A.5.14, ISO 27001 A.5.15, ISO 27001 A.5.16, ISO 27001 A.5.17, ISO 27001 A.5.18, ISO 27001 A.5.19, ISO 27001 A.5.2, ISO 27001 A.5.21, ISO 27001 A.5.22, ISO 27001 A.5.24, ISO 27001 A.5.25, ISO 27001 A.5.26, ISO 27001 A.5.27, ISO 27001 A.5.28, ISO 27001 A.5.29, ISO 27001 A.5.3, ISO 27001 A.5.30, ISO 27001 A.5.31, ISO 27001 A.5.33, ISO 27001 A.5.35, ISO 27001 A.5.36, ISO 27001 A.5.37, ISO 27001 A.5.4, ISO 27001 A.5.5, ISO 27001 A.5.6, ISO 27001 A.5.7, ISO 27001 A.5.8, ISO 27001 A.5.9, ISO 27001 A.6.1, ISO 27001 A.6.2, ISO 27001 A.6.3, ISO 27001 A.6.4, ISO 27001 A.6.5, ISO 27001 A.6.6, ISO 27001 A.6.7, ISO 27001 A.6.8, ISO 27001 A.7.1, ISO 27001 A.7.7, ISO 27001 A.8.1, ISO 27001 A.8.10, ISO 27001 A.8.11, ISO 27001 A.8.12, ISO 27001 A.8.13, ISO 27001 A.8.14, ISO 27001 A.8.15, ISO 27001 A.8.16, ISO 27001 A.8.17, ISO 27001 A.8.18, ISO 27001 A.8.19, ISO 27001 A.8.2, ISO 27001 A.8.20, ISO 27001 A.8.21, ISO 27001 A.8.22, ISO 27001 A.8.23, ISO 27001 A.8.24, ISO 27001 A.8.25, ISO 27001 A.8.26, ISO 27001 A.8.27, ISO 27001 A.8.28, ISO 27001 A.8.29, ISO 27001 A.8.3, ISO 27001 A.8.30, ISO 27001 A.8.31, ISO 27001 A.8.32, ISO 27001 A.8.33, ISO 27001 A.8.34, ISO 27001 A.8.4, ISO 27001 A.8.5, ISO 27001 A.8.6, ISO 27001 A.8.7, ISO 27001 A.8.8, ISO 27001 A.8.9
DORA	**10**	DORA art. 10, DORA art. 11, DORA art. 13, DORA art. 17, DORA art. 18, DORA art. 19, DORA art. 28, DORA art. 45, DORA art. 6, DORA art. 8

Mapowanie ma charakter poglądowy na poziomie wymagań; pełna ocena zgodności z daną regulacją wymaga odrębnej analizy jej zakresu.

9 Karty szczegółowe luk (GA-Z6)

Szczegółowe karty dla luk krytycznych i wysokich, przeznaczone dla zespołu wdrożeniowego. Każda karta zawiera stan obecny, wymaganie normy, ryzyko, rekomendację, właściciela i szacunek nakładu. Numer karty odpowiada numerowi luki w tabeli Zidentyfikowane luki i rekomendacje.

1 N0-3 · A. Status podmiotu i obowiązki formalne

K Krytyczny · Quick Win

Wniosek o wpis do wykazu podmiotów kluczowych i ważnych złożony w S46 w terminie (art. 7c-7d)

Dojrzałość	0,0 / 5 - Nieistniejący
Wymaganie regulacji	Art. 7c ust. 1: wniosek w terminie 6 miesięcy od dnia spełnienia przesłanek uznania za podmiot kluczowy lub ważny; dla podmiotów spełniających je w dniu wejścia w życie nowelizacji (3.04.2026) termin upływa 3.10.2026. Wniosek składa się w systemie teleinformatycznym z art. 46 ust. 1 (S46), z danymi z art. 7 ust. 2 pkt 1-18 (m.in. sektor i rodzaj działalności, zakresy publicznych adresów IP i domeny wykorzystywane w sposób ciągły, osoby do kontaktu, deklaracja wielkości przedsiębiorcy, państwa działalności, główne miejsce prowadzenia działalności, informacja o umowie z MSSP, przedstawiciel), z oświadczeniem kierownika o prawdziwości danych pod rygorem odpowiedzialności karnej (ust. 5), podpisany kwalifikowanym podpisem elektronicznym, podpisem zaufanym, podpisem osobistym albo kwalifikowaną pieczęcią (ust. 6). Wpis następuje z chwilą złożenia wniosku i ma charakter deklaratoryjny (art. 7d ust. 1 i 5). Brak wniosku: wpis z urzędu przez organ z wezwaniem do uzupełnienia danych w 6 miesięcy pod rygorem kary (art. 7j). Zaświadczenie o wpisie na żądanie (art. 7d ust. 6). Podmioty wpisywane z urzędu (przedsiębiorcy telekomunikacyjni, dostawcy usług zaufania, podmioty publiczne, podmioty krytyczne) uzupełniają dane na wezwanie w 6 miesięcy (art. 7a-7b). Powiązania: ISO 27001 A.5.31, ISO 27001 A.5.36
Stan obecny	Wniosek o wpis do wykazu podmiotów kluczowych i ważnych nie został złożony. Termin ustawowy: 3.10.2026.
Obserwacja konsultanta	Zarząd nie wiedział o terminie. Dane do wniosku są dostępne od ręki; blokerem było wyłącznie wyznaczenie osób do kontaktu (patrz n0-4).
Podstawa ustalenia	**Wywiad** Oczekiwany dowód: Potwierdzenie złożenia wniosku o wpis do wykazu w S46 z datą; zaświadczenie o wpisie (art. 7d ust. 6)
Ryzyko	Niezłożenie wniosku w terminie to pierwsza i najłatwiejsza do wykrycia niezgodność z ustawą, obarczona karą administracyjną, niezależna od stanu SZBI.
Rekomendacja	Złożyć wniosek przez system S46 przed 3.10.2026 z danymi podmiotu, sektorem, usługą i osobami do kontaktu. Zachować potwierdzenie złożenia.
Właściciel	Zarząd (A) / Pełnomocnik ds. SZBI (R)
Nakład / termin	1,0 dni rob. · termin: 30.09.2026

PRÓBKA RAPORTU FIKCYJNE

2 N0-4 · A. Status podmiotu i obowiązki formalne

K Krytyczny · Quick Win

Wyznaczenie co najmniej dwóch osób odpowiedzialnych za kontakty z podmiotami KSC (art. 9 ust. 1 pkt 1)

Dojrzałość	0,0 / 5 - Nieistniejący
Wymaganie regulacji	Co najmniej dwie osoby odpowiedzialne za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa (ust. 1 pkt 1); mikro i mały przedsiębiorca oraz podmiot ważny będący podmiotem publicznym co najmniej jedną (ust. 2-3). Dane osób (imię i nazwisko, telefon służbowy, e-mail służbowy; dla administratora konta w S46 dodatkowo PESEL lub identyfikator środka identyfikacji elektronicznej) są elementem wpisu w wykazie (art. 7 ust. 2 pkt 11), więc każda zmiana osoby wymaga wniosku o zmianę wpisu w 14 dni. Zapewnić redundancję (urlopy, nieobecności) i dostępność w oknie 24h na wczesne ostrzeżenie. Przy modelu vCISO jedna osoba może być zewnętrzna, druga wewnętrzna; osoba realizująca zadania z art. 8 lub art. 11 podlega wymogowi KRK z art. 8f. Powiązania: ISO 27001 A.5.2, ISO 27001 A.5.5
Stan obecny	Nie wyznaczono osób odpowiedzialnych za kontakty z podmiotami krajowego systemu cyberbezpieczeństwa.
Obserwacja konsultanta	Rozmówcy zakładali, że kontaktem będzie "informatyk", bez ustaleń na piśmie i bez zastępstwa na urlop.
Podstawa ustalenia	**Wywiad** Oczekiwany dowód: Akt wyznaczenia co najmniej dwóch osób kontaktowych + potwierdzenie ich danych w wykazie
Ryzyko	Bez osób do kontaktu nie da się złożyć kompletnego wniosku o wpis ani odebrać wezwania CSIRT w trakcie incydentu.
Rekomendacja	Wyznaczyć zarządzeniem co najmniej dwie osoby (Pełnomocnik ds. SZBI i Kierownik IT), z zastępstwem, telefonem i adresem e-mail dostępnymi całodobowo dla CSIRT. Zgłosić we wniosku o wpis.
Właściciel	Zarząd (A) / Pełnomocnik ds. SZBI (R)
Nakład / termin	0,5 dni rob. · termin: 30.09.2026

3 N1-1 · B. Szacowanie ryzyka i podstawa SZBI

K Krytyczny

Systematyczne szacowanie ryzyka wystąpienia incydentu w systemie wykorzystywanym do świadczenia usługi (art. 8 ust. 1 pkt 1)

Dojrzałość	0,0 / 5 - Nieistniejący
Wymaganie regulacji	Art. 8 ust. 1: SZBI wdrożony w systemie informacyjnym wykorzystywanym w procesach wpływających na świadczenie usługi przez podmiot. Pkt 1: prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem. Zakres szacowania obejmuje systemy wpływające na usługę objętą ustawą, a nie tylko formalny zakres certyfikatu ISO. Analog klauzul 6.1.2 i 8.2 ISO 27001. Rada Ministrów może określić szczegółowe wymagania SZBI dla rodzaju działalności (art. 8a); oczekiwanie na rozporządzenie nie zawiesza obowiązku. Powiązania: ISO 27001 pkt 6.1, DORA art. 6
Stan obecny	Brak systematycznego szacowania ryzyka wystąpienia incydentu.
Obserwacja konsultanta	Patrz c6-1.
Podstawa ustalenia	**Wywiad** Oczekiwany dowód: Metodyka i zapisy systematycznego szacowania ryzyka dla systemów wpływających na usługę
Ryzyko	Szacowanie ryzyka jest obowiązkiem ustawowym (art. 8 ust. 1 pkt 1). Bez niego pozostałe środki nie mają uzasadnienia proporcjonalności.
Rekomendacja	Patrz c6-1: metodyka i pierwsza ocena ryzyka dla systemu informacyjnego wspierającego usługę, z kryteriami proporcjonalności z ustawy.
Właściciel	Zarząd (A) / Pełnomocnik ds. SZBI (R)
Nakład / termin	do oszacowania · termin: 30.11.2026

PRÓBKA, DANE FIKCYJNE

4 N3-3 · D. Cyberzagrożenia, obsługa i zgłaszanie incydentów, środki ograniczające

K Krytyczny

Wczesne ostrzeżenie w 24h i zgłoszenie incydentu poważnego w 72h do CSIRT sektorowego przez S46 (art. 11 ust. 1 pkt 4-4a, art. 12)

Dojrzałość	0,0 / 5 - Nieistniejący
Wymaganie regulacji	Oba terminy liczone od momentu wykrycia; dostawca usług zaufania zgłasza incydent poważny w 24h (art. 11 ust. 1a). Kanał: system teleinformatyczny z art. 46 ust. 1 (S46, art. 11 ust. 2); przy braku możliwości sposób określony w komunikacie CSIRT publikowanym w BIP (art. 31). Wczesne ostrzeżenie (art. 12 ust. 1): dane podmiotu, osoba zgłaszająca i osoba do wyjaśnień, moment wystąpienia i wykrycia oraz czas trwania, czy działanie bezprawne lub w złej wierze, czy dotyczy innych państw UE; może zawierać wniosek o wytyczne lub wsparcie, CSIRT odpowiada w 24h (ust. 2). Zgłoszenie (ust. 3): wpływ na usługę, liczba użytkowników, zasięg geograficzny, wpływ na inne podmioty, przyczyny i przebieg, działania zapobiegawcze i naprawcze; informacje znane w chwili zgłoszenia, uzupełniane w trakcie (ust. 5); oznaczanie tajemnic prawnie chronionych (ust. 8). Podmiot ważny będący podmiotem publicznym nie przekazuje wczesnego ostrzeżenia ani sprawozdań (art. 12c). Sektor bankowości: DORA art. 19 do KNF (art. 8i). Procedurę przetestować z pomiarem czasu od wykrycia do wysłania. Powiązania: ISO 27001 A.5.24, ISO 27001 A.5.5, DORA art. 19
Stan obecny	Brak zdolności do wczesnego ostrzeżenia w 24 h i zgłoszenia incydentu poważnego w 72 h do CSIRT.
Obserwacja konsultanta	Incydent z lutego 2026 r. zgłoszono wewnętrznie po 2 dniach. Gdyby był poważny, termin 24 h byłby niedotrzymany dwukrotnie.
Podstawa ustalenia	**Wywiad** Oczekiwany dowód: Procedura wczesnego ostrzeżenia (24h) i zgłoszenia (72h) z wzorami treści wg art. 12 + dowód testu czasu reakcji
Ryzyko	Niedotrzymanie terminów zgłoszeń jest najczęstszą podstawą działań nadzorczych wobec podmiotów ważnych. Bez procedury i osób nie da się ich dotrzymać.
Rekomendacja	Wdrożyć procedurę incydentów (patrz A.5.24) z klasyfikacją, osobami do kontaktu, szablonami zgłoszeń S46 i ćwiczeniem tabletop przed 3.04.2027.
Właściciel	Kierownik IT (R) / Pełnomocnik ds. SZBI (A)
Nakład / termin	2,0 dni rob. · termin: 31.12.2026

5 N0-1 · A. Status podmiotu i obowiązki formalne

W Wysoki · Quick Win

Klasyfikacja podmiotu: kluczowy, ważny albo poza zakresem ustawy (art. 5)

Dojrzałość	2,0 / 5 - Powtarzalny
Wymaganie regulacji	Art. 5 ust. 1, podmiot kluczowy: m.in. podmiot z załącznika nr 1 przewyższający wymogi średniego przedsiębiorstwa (zał. I rozp. 651/2014), przedsiębiorca komunikacji elektronicznej co najmniej średni, dostawca usług zarządzanych w zakresie cyberbezpieczeństwa (MSSP) co najmniej mały, a niezależnie od wielkości m.in. dostawca usług DNS, kwalifikowany dostawca usług zaufania, podmiot krytyczny, podmiot publiczny z zał. nr 1, rejestr TLD, podmiot świadczący usługi rejestracji nazw domen. Ust. 2, podmiot ważny: m.in. średni przedsiębiorca z zał. nr 1, średni lub większy z zał. nr 2, niekwalifikowany dostawca usług zaufania, mikro lub mały przedsiębiorca komunikacji elektronicznej. Reguły: kluczowy ma pierwszeństwo (ust. 4); wielkość według stanu na dzień sporządzenia sprawozdania finansowego (ust. 5); wyłączenie, gdy system informacyjny jest niezależny od przedsiębiorstw powiązanych lub partnerskich i nie świadczy usług wspólnie z nimi (ust. 6-7); podmiot leczniczy niebędący przedsiębiorcą według zatrudnienia 50/250 (ust. 8). Organ może uznać podmiot za kluczowy lub ważny decyzją (art. 7l). Udokumentować analizę z uzasadnieniem i datą; obowiązki ciążą od dnia spełnienia przesłanek, nie od wpisu do wykazu. Powiązania: ISO 27001 pkt 4.1, ISO 27001 pkt 4.3
Stan obecny	Samoidentyfikacja przeprowadzona nieformalnie ("prawnik powiedział, że podlegamy") bez udokumentowanej analizy sektora, progu wielkości i usługi.
Obserwacja konsultanta	Firma spełnia próg średniego przedsiębiorstwa i działa w sektorze produkcji objętym załącznikiem. Kwalifikacja jako podmiot ważny jest w naszej ocenie prawidłowa, wymaga tylko udokumentowania.
Podstawa ustalenia	**Wywiad** Oczekiwany dowód: Udokumentowana analiza klasyfikacji podmiotu (art. 5) z uzasadnieniem, datą i zatwierdzeniem kierownika
Ryzyko	Istotne. Luka "klasyfikacja podmiotu: kluczowy, ważny albo poza zakresem ustawy (art. 5)" wymaga usunięcia przed oceną zewnętrzną. W praktyce: niedopełnienie obowiązku formalnego jest naruszeniem widocznym dla organu od pierwszego dnia, niezależnie od realnego stanu zabezpieczeń.
Rekomendacja	Udokumentować kwalifikację: sektor z załącznika, przesłanka wielkościowa (średnie przedsiębiorstwo, 180 osób), świadczona usługa, data ustalenia, podstawa prawna. Zachować jako dowód dla organu.
Właściciel	Zarząd (A) / Pełnomocnik ds. SZBI (R)
Nakład / termin	1,0 dni rob. · termin: 30.09.2026

PRÓBKA RAPORTU FIKCYJNE

6 N0-10 · A. Status podmiotu i obowiązki formalne

W Wysoki

Wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo albo umowa z MSSP (art. 14)

Dojrzałość	1,0 / 5 - Inicjalny
Wymaganie regulacji	Do realizacji zadań z art. 8 oraz art. 9-13 podmiot powołuje wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo lub zawiera umowę z dostawcą usług zarządzanych w zakresie cyberbezpieczeństwa (art. 2 pkt 4j: obsługa incydentów, testy, audyty systemów, doradztwo w zarządzaniu ryzykiem). Informacja o umowie z MSSP wraz z danymi dostawcy jest elementem wpisu w wykazie (art. 7 ust. 2 pkt 16). Umowa powinna określać zakres zadań, dostępność w oknach 24h/72h, obowiązek KRK osób dostawcy (art. 8f), współdziałanie z CSIRT i zasady przekazywania danych. Kierownik ponosi odpowiedzialność mimo powierzenia obowiązków (art. 8c ust. 3). Powiązania: ISO 27001 pkt 5.3, ISO 27001 A.5.2, ISO 27001 A.5.19
Stan obecny	Brak wewnętrznej struktury odpowiedzialnej za cyberbezpieczeństwo (2 osoby IT skupione na utrzymaniu) i brak umowy z MSSP.
Obserwacja konsultanta	Patrz c5-2. Dwie osoby IT obsługują 180 stanowisk i halę; bez wsparcia zewnętrznego monitoring 24/7 nie jest realny.
Podstawa ustalenia	**Wywiad** Oczekiwany dowód: Struktura organizacyjna cyberbezpieczeństwa albo umowa z MSSP z zakresem zadań z art. 8 i 9-13
Ryzyko	Istotne. Luka "wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo albo umowa z MSSP (art. 14)" wymaga usunięcia przed oceną zewnętrzną. W praktyce: bez umocowanej struktury lub umowy z MSSP zadania z art. 8 i 9-13 nie mają właściciela, a informacja o dostawcy nie trafi do wykazu.
Rekomendacja	Powołać Pełnomocnika ds. SZBI, przypisać zadania cyberbezpieczeństwa w opisach stanowisk IT, ocenić model: własne struktury z outsourcingiem monitoringu (MSSP) jako opcja realna dla firmy tej wielkości.
Właściciel	Zarząd (A) / Pełnomocnik ds. SZBI (R)
Nakład / termin	3,0 dni rob. · termin: 31.12.2026

7 N1-2 · B. Szacowanie ryzyka i podstawa SZBI

W Wysoki

Zarządzanie zidentyfikowanym ryzykiem: rejestr, plan postępowania, właściciele, terminy, przeglądy

Dojrzałość	0,0 / 5 - Nieistniejący
Wymaganie regulacji	Postępowanie z ryzykiem prowadzące do doboru środków odpowiednich i proporcjonalnych do oszacowanego ryzyka (art. 8 ust. 1 pkt 2). Rejestr ryzyk, plan postępowania z właścicielami i terminami, przegląd po istotnych zmianach, incydentach poważnych i wynikach audytu. Analog klauzul 6.1.3 i 8.3 ISO 27001. Powiązania: ISO 27001 pkt 6.1, ISO 27001 pkt 8.1, ISO 27001 pkt 8.2, ISO 27001 pkt 8.3
Stan obecny	Brak: Zarządzanie zidentyfikowanym ryzykiem: rejestr, plan postępowania, właściciele, terminy, przeglądy.
Obserwacja konsultanta	Wynika z braku procesu szacowania ryzyka (n1-1 / c6-1).
Podstawa ustalenia	**Wywiad** Oczekiwany dowód: Rejestr ryzyk + plan postępowania z ryzykiem z właścicielami i terminami
Ryzyko	Istotne. Luka "zarządzanie zidentyfikowanym ryzykiem: rejestr, plan postępowania, właściciele,..." wymaga usunięcia przed oceną zewnętrzną. W praktyce: decyzje o zabezpieczeniach zapadają bez oceny ryzyka, więc nakłady mogą omijać realne zagrożenia.
Rekomendacja	Patrz działanie nadrzędne wskazane w obserwacji.
Właściciel	Zarząd (A) / Pełnomocnik ds. SZBI (R)
Nakład / termin	2,0 dni rob. · termin: 28.02.2027

PRÓBKA, DANE FIKCYJNE

8 N1-3 · B. Szacowanie ryzyka i podstawa SZBI

W Wysoki

Udokumentowana metodyka szacowania ryzyka z sześcioma kryteriami proporcjonalności z art. 8 ust. 1 pkt 2

Dojrzałość	0,0 / 5 - Nieistniejący
Wymaganie regulacji	Ustawa wymienia kryteria doboru środków technicznych i organizacyjnych: najnowszy stan wiedzy, koszty wdrożenia, wielkość podmiotu, prawdopodobieństwo wystąpienia incydentów, narażenie podmiotu na ryzyka, skutki społeczne i gospodarcze. Metodyka ma pokazywać, jak te kryteria wpływają na ocenę i decyzję o środkach, ponieważ to jest dowód proporcjonalności podczas kontroli organu (art. 53). Skale, kryteria akceptacji, częstotliwość, zakres. Powiązania: ISO 27001 pkt 6.1
Stan obecny	Brak: Udokumentowana metodyka szacowania ryzyka z sześcioma kryteriami proporcjonalności z art. 8 ust. 1 pkt 2.
Obserwacja konsultanta	Wynika z braku procesu szacowania ryzyka (n1-1 / c6-1).
Podstawa ustalenia	**Wywiad** Oczekiwany dowód: Metodyka szacowania ryzyka z sześcioma kryteriami proporcjonalności z art. 8 ust. 1 pkt 2
Ryzyko	Istotne. Luka "udokumentowana metodyka szacowania ryzyka z sześcioma kryteriami proporcjonalności z..." wymaga usunięcia przed oceną zewnętrzną. W praktyce: decyzje o zabezpieczeniach zapadają bez oceny ryzyka, więc nakłady mogą omijać realne zagrożenia, a proporcjonalności nie da się udowodnić.
Rekomendacja	Patrz działanie nadrzędne wskazane w obserwacji.
Właściciel	Zarząd (A) / Pełnomocnik ds. SZBI (R)
Nakład / termin	2,0 dni rob. · termin: 28.02.2027

9 N1-4 · B. Szacowanie ryzyka i podstawa SZBI

W Wysoki

Wyniki szacowania ryzyka udokumentowane i okresowo przeglądane

Dojrzałość	0,0 / 5 - Nieistniejący
Wymaganie regulacji	Zapisy ocen z datami; przegląd cykliczny oraz po incydencie poważnym, istotnej zmianie systemu informacyjnego, zmianie dostawcy, wyniku audytu lub kontroli. Wyniki szacowania ryzyka mogą być dobrowolnie przekazywane do CSIRT (art. 13 ust. 1 pkt 3). Analog klauzuli 8.2 ISO 27001. Powiązania: ISO 27001 pkt 6.1, DORA art. 8
Stan obecny	Brak: Wyniki szacowania ryzyka udokumentowane i okresowo przeglądane.
Obserwacja konsultanta	Wynika z braku procesu szacowania ryzyka (n1-1 / c6-1).
Podstawa ustalenia	**Wywiad** Oczekiwany dowód: Zapisy wyników szacowania ryzyka z datami przeglądów
Ryzyko	Istotne. Luka "wyniki szacowania ryzyka udokumentowane i okresowo przeglądane" wymaga usunięcia przed oceną zewnętrzną. W praktyce: decyzje o zabezpieczeniach zapadają bez oceny ryzyka, więc nakłady mogą omijać realne zagrożenia, a proporcjonalności nie da się udowodnić.
Rekomendacja	Patrz działanie nadrzędne wskazane w obserwacji.
Właściciel	Zarząd (A) / Pełnomocnik ds. SZBI (R)
Nakład / termin	2,0 dni rob. · termin: 28.02.2027

10 N1-5 · B. Szacowanie ryzyka i podstawa SZBI

W Wysoki

Kierownik podmiotu zatwierdza wyniki szacowania ryzyka i akceptuje ryzyko szczątkowe

Dojrzałość	0,0 / 5 - Nieistniejący
Wymaganie regulacji	Art. 8d pkt 1: kierownik podejmuje decyzje w zakresie przygotowania, wdrażania, stosowania, przeglądu i nadzoru SZBI; art. 8c ust. 1: kierownik odpowiada za wykonywanie obowiązków z art. 8. Formalna, udokumentowana akceptacja ryzyka szczątkowego i planu postępowania z ryzykiem, z datą i podpisem. Powiązania: ISO 27001 pkt 6.1, ISO 27001 pkt 9.3
Stan obecny	Brak: Kierownik podmiotu zatwierdza wyniki szacowania ryzyka i akceptuje ryzyko szczątkowe.
Obserwacja konsultanta	Wynika z braku procesu szacowania ryzyka (n1-1 / c6-1).
Podstawa ustalenia	**Wywiad** Oczekiwany dowód: Udokumentowana akceptacja ryzyka szczątkowego przez kierownika podmiotu
Ryzyko	Istotne. Luka "kierownik podmiotu zatwierdza wyniki szacowania ryzyka i akceptuje ryzyko szczątkowe" wymaga usunięcia przed oceną zewnętrzną. W praktyce: odpowiedzialność za obowiązki ustawowe spoczywa osobiście na kierowniku podmiotu, a brak formalnego wskazania osoby i udokumentowanych decyzji przenosi ją na wszystkich członków organu.
Rekomendacja	Patrz działanie nadrzędne wskazane w obserwacji.
Właściciel	Zarząd (A) / Pełnomocnik ds. SZBI (R)
Nakład / termin	2,0 dni rob. · termin: 28.02.2027

PRÓBKA. DANE FIKCYJNE

11 N2-15 · C. Środki techniczne i organizacyjne: 14 obszarów ustawowych

W Wysoki

Lit. h: polityki i procedury oceny skuteczności środków technicznych i organizacyjnych

Dojrzałość	0,0 / 5 - Nieistniejący
Wymaganie regulacji	Formalny mechanizm weryfikacji, czy zastosowane środki działają: mierniki, testy kontroli, skanowanie i testy penetracyjne, audyty wewnętrzne, przeglądy zarządzania, ćwiczenia planów ciągłości. Wyniki oceny skuteczności są wejściem do kolejnego cyklu szacowania ryzyka (pkt 1) i dowodem dla audytu z art. 15. Analog klauzul 9.1-9.3 oraz A.5.35-A.5.36. Powiązania: ISO 27001 pkt 9.1, ISO 27001 pkt 9.2, ISO 27001 A.5.35, ISO 27001 A.5.36
Stan obecny	Brak: Lit. h: polityki i procedury oceny skuteczności środków technicznych i organizacyjnych.
Obserwacja konsultanta	Wynika z braku SZBI; adresowane w ramach dokumentacji i wdrożenia zabezpieczeń Aneksu A.
Podstawa ustalenia	**Wywiad** Oczekiwany dowód: Polityka i procedura oceny skuteczności środków + wyniki ocen (mierniki, testy, audyty)
Ryzyko	Istotne. Luka "lit. h: polityki i procedury oceny skuteczności środków technicznych i organizacyjnych" wymaga usunięcia przed oceną zewnętrzną. W praktyce: bez oceny skuteczności organizacja nie wie, czy środki działają, a wynik oceny nie zasila kolejnego szacowania ryzyka, co audytor uzna za brak działania systemu.
Rekomendacja	Patrz działanie nadrzędne wskazane w obserwacji.
Właściciel	Zarząd (A) / Pełnomocnik ds. SZBI (R)
Nakład / termin	2,0 dni rob. · termin: 28.02.2027

12 N3-6 · D. Cyberzagrożenia, obsługa i zgłaszanie incydentów, środki ograniczające

W Wysoki

Kryteria uznania incydentu za poważny i udokumentowana decyzja klasyfikacyjna (art. 2 pkt 7, art. 11 ust. 4)

Dojrzałość	0,0 / 5 - Nieistniejący
Wymaganie regulacji	Incydent poważny (art. 2 pkt 7): incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi, straty finansowe dla podmiotu albo wpływa na inne osoby przez wywołanie poważnej szkody materialnej lub niematerialnej. Progi według rodzaju zdarzenia w sektorach określa rozporządzenie Rady Ministrów (liczba użytkowników, czas oddziaływania, zasięg geograficzny, czynniki sektorowe), a dla dostawców usług cyfrowych z art. 8b ust. 1 rozporządzenie wykonawcze (UE) 2024/2690. Procedura ma zawierać matrycę decyzyjną, osobę decydującą, zasadę ostrożności (w razie wątpliwości zgłaszać) oraz odrębną ścieżkę RODO art. 33 do UODO. Sprawdzić, czy rozporządzenie RM dla sektora klienta zostało już wydane. Powiązania: ISO 27001 A.5.25, DORA art. 18
Stan obecny	Brak: Kryteria uznania incydentu za poważny i udokumentowana decyzja klasyfikacyjna (art. 2 pkt 7, art. 11 ust. 4).
Obserwacja konsultanta	Wynika z braku procedury incydentów (A.5.24 / n3-3).
Podstawa ustalenia	**Wywiad** Oczekiwany dowód: Matryca klasyfikacji incydentu poważnego (progi RM lub 2024/2690) + zapisy decyzji klasyfikacyjnych
Ryzyko	Istotne. Luka "kryteria uznania incydentu za poważny i udokumentowana decyzja klasyfikacyjna (art. 2..." wymaga usunięcia przed oceną zewnętrzną. W praktyce: bez progów i matrycy decyzyjnej organizacja nie rozpozna incydentu poważnego na czas, a zegar 24 godzin biegnie od wykrycia, nie od decyzji.
Rekomendacja	Patrz działanie nadrzędne wskazane w obserwacji.
Właściciel	Zarząd (A) / Pełnomocnik ds. SZBI (R)
Nakład / termin	2,0 dni rob. · termin: 28.02.2027

PRÓBKA, DANE FIKCYJNE

13 N3-5 · D. Cyberzagrożenia, obsługa i zgłaszanie incydentów, środki ograniczające

W Wysoki

Sprawozdanie końcowe w ciągu miesiąca, sprawozdanie okresowe i sprawozdanie z postępu (art. 11 ust. 1 pkt 4b-4c, art. 12a-12b)

Dojrzałość	0,0 / 5 - Nieistniejący
Wymaganie regulacji	Sprawozdanie końcowe do właściwego CSIRT sektorowego nie później niż w ciągu miesiąca od dnia zgłoszenia 72h (pkt 4c); treść (art. 12a): szczegółowy opis incydentu z zakłóceniami i szkodami, rodzaj zagrożenia lub przyczyna, zastosowane i wdrażane środki ograniczające ryzyko, skutki transgraniczne. Gdy obsługa nie zakończyła się w tym terminie: sprawozdanie z postępu, a końcowe w ciągu miesiąca od zakończenia obsługi (art. 12b). Sprawozdanie okresowe na wniosek CSIRT (pkt 4b). Wszystkie przez S46 (art. 11 ust. 2). Analog A.5.27. Powiązania: ISO 27001 A.5.27, DORA art. 19
Stan obecny	Brak: Sprawozdanie końcowe w ciągu miesiąca, sprawozdanie okresowe i sprawozdanie z postępu (art. 11 ust. 1 pkt 4b-4c, art. 12a-12b).
Obserwacja konsultanta	Wynika z braku procedury incydentów (A.5.24 / n3-3).
Podstawa ustalenia	**Wywiad** Oczekiwany dowód: Wzór i zapisy sprawozdań końcowych (1 mies.), okresowych i z postępu obsługi
Ryzyko	Istotne. Luka "sprawozdanie końcowe w ciągu miesiąca, sprawozdanie okresowe i sprawozdanie z postępu..." wymaga usunięcia przed oceną zewnętrzną. W praktyce: brak sprawozdania końcowego w terminie miesiąca zamyka incydent formalnie po stronie organizacji, ale nie po stronie CSIRT, i jest odrębnym naruszeniem obowiązku zgłoszeniowego.
Rekomendacja	Patrz działanie nadrzędne wskazane w obserwacji.
Właściciel	Zarząd (A) / Pełnomocnik ds. SZBI (R)
Nakład / termin	2,0 dni rob. · termin: 28.02.2027

14 N4-2 · E. Odpowiedzialność i obowiązki kierownika podmiotu

W Wysoki · Quick Win

Coroczne, udokumentowane szkolenie kierownika podmiotu i osoby, której powierzono obowiązki w zakresie cyberbezpieczeństwa (art. 8e)

Dojrzałość	0,0 / 5 - Nieistniejący
Wymaganie regulacji	Raz w roku kalendarzowym (ust. 1), obejmuje wykonywanie obowiązków z art. 7b ust. 4, art. 7c, art. 7f ust. 3, art. 8, art. 8d, art. 8f ust. 1 i 2, art. 9-12b, art. 14 i art. 15 (ust. 2), udział udokumentowany (ust. 3). Pierwsze szkolenie w terminie realizacji obowiązków rozdz. 3 (dla podmiotów istniejących 3.04.2026 do 3.04.2027), potem w każdym roku kalendarzowym. Dowód: program z zakresem ustawowym, lista obecności lub zaświadczenie z datą. Odrębne od edukacji personelu (lit. i). Powiązania: ISO 27001 A.6.3, ISO 27001 pkt 7.2
Stan obecny	Kierownik podmiotu nie odbył szkolenia z cyberbezpieczeństwa wymaganego corocznie przez ustawę.
Obserwacja konsultanta	Zarząd zadeklarował gotowość; szkolenie można połączyć z przeglądem zarządzania w styczniu 2027 r.
Podstawa ustalenia	**Wywiad** Oczekiwany dowód: Udokumentowany udział kierownika i osoby odpowiedzialnej w corocznym szkoleniu (program, lista, zaświadczenie)
Ryzyko	Istotne. Luka "coroczne, udokumentowane szkolenie kierownika podmiotu i osoby, której powierzono..." wymaga usunięcia przed oceną zewnętrzną. W praktyce: odpowiedzialność za obowiązki ustawowe spoczywa osobiście na kierowniku podmiotu, a brak formalnego wskazania osoby i udokumentowanych decyzji przenosi ją na wszystkich członków organu.
Rekomendacja	Przeprowadzić udokumentowane szkolenie Zarządu (2 h) do końca 2026 r. i powtarzać corocznie. Zaświadczenie do akt.
Właściciel	Zarząd (A) / Pełnomocnik ds. SZBI (R)
Nakład / termin	0,5 dni rob. · termin: 31.12.2026

PRÓBKA, DANE FIKCYJNE

15 N5-7 · F. Użytkownicy usługi i współpraca z krajowym systemem cyberbezpieczeństwa

W Wysoki

Rozpoczęcie korzystania z systemu S46 po uzyskaniu wpisu do wykazu (art. 9 ust. 1 pkt 4, art. 46 ust. 1)

Dojrzałość	0,0 / 5 - Nieistniejący
Wymaganie regulacji	Po wpisie podmiot rozpoczyna korzystanie z systemu teleinformatycznego z art. 46 ust. 1: konto podmiotu, administrator konta (jego dane, w tym PESEL lub identyfikator środka identyfikacji elektronicznej, są w wykazie, art. 7 ust. 2 pkt 11), użytkownicy zapasowi, przetestowany dostęp. S46 jest kanałem wniosków o wpis, wczesnego ostrzeżenia, zgłoszeń, sprawozdań i dobrowolnych informacji (art. 7c ust. 6, art. 11 ust. 2, art. 13 ust. 2). Kanał zapasowy według komunikatu CSIRT w BIP (art. 31 ust. 3). Powiązania: ISO 27001 A.5.5, ISO 27001 A.5.14
Stan obecny	Brak: Rozpoczęcie korzystania z systemu S46 po uzyskaniu wpisu do wykazu (art. 9 ust. 1 pkt 4, art. 46 ust. 1).
Obserwacja konsultanta	Realizowane po uzyskaniu wpisu do wykazu (n0-3).
Podstawa ustalenia	**Wywiad** Oczekiwany dowód: Potwierdzenie aktywnego konta w S46 (administrator, użytkownicy zapasowi) + dowód testu dostępu
Ryzyko	Istotne. Luka "rozpoczęcie korzystania z systemu S46 po uzyskaniu wpisu do wykazu (art. 9 ust. 1 pkt..." wymaga usunięcia przed oceną zewnętrzną. W praktyce: bez działającego i przetestowanego konta w S46 wczesne ostrzeżenie w 24h trzeba wysyłać kanałem zapasowym, co przy pierwszym incydencie kosztuje godziny.
Rekomendacja	Patrz działanie nadrzędne wskazane w obserwacji.
Właściciel	Zarząd (A) / Pełnomocnik ds. SZBI (R)
Nakład / termin	2,0 dni rob. · termin: 28.02.2027

10 Quick Wins

Nr	Wymaganie	Działanie	Termin
1	**N0-3**	**Wniosek o wpis do wykazu podmiotów kluczowych i ważnych złożony w S46 w terminie (art....**: Złożyć wniosek przez system S46 przed 3.10.2026 z danymi podmiotu, sektorem, usługą i osobami do kontaktu. Zachować potwierdzenie złożenia.	do 28.09.2026 okno prior.: 30.09.2026
2	**N0-4**	**Wyznaczenie co najmniej dwóch osób odpowiedzialnych za kontakty z podmiotami KSC (art....**: Wyznaczyć zarządzeniem co najmniej dwie osoby (Pełnomocnik ds. SZBI i Kierownik IT), z zastępstwem, telefonem i adresem e-mail dostępnymi całodobowo dla CSIRT. Zgłosić we wniosku o wpis.	do 28.09.2026 okno prior.: 30.09.2026
5	**N0-1**	**Klasyfikacja podmiotu: kluczowy, ważny albo poza zakresem ustawy (art. 5)**: Udokumentować kwalifikację: sektor z załącznika, przesłanka wielkościowa (średnie przedsiębiorstwo, 180 osób), świadczona usługa, data ustalenia, podstawa prawna. Zachować jako dowód dla organu.	do 28.09.2026 okno prior.: 30.09.2026
14	**N4-2**	**Coroczne, udokumentowane szkolenie kierownika podmiotu i osoby, której powierzono...**: Przeprowadzić udokumentowane szkolenie Zarządu (2 h) do końca 2026 r. i powtarzać corocznie. Zaświadczenie do akt.	do 28.09.2026 okno prior.: 31.12.2026

Termin Quick Win to 14 dni od daty raportu; dla luk z przypisanym priorytetem okno priorytetu podano informacyjnie. Nr odpowiada ciągłej numeracji z tabeli luk.

11 Dokumenty wejściowe

Dostarczono **0 z 31** oczekiwanych dokumentów (0%). Wykaz obejmuje dokumenty wspólne dla projektu oraz dokumenty specyficzne dla NIS2 / KSC; brak dokumentu jest sam w sobie informacją o luce w dokumentacji.

PRÓBKA, DANE FIKCYJNE

Dokumenty niedostarczone: specyficzne dla NIS2 / KSC

Kategoria	Brakujące dokumenty
NIS2/KSC - dokumenty specyficzne	Analiza klasyfikacji podmiotu (art. 5) i jurysdykcji (art. 5a) Wniosek o wpis do wykazu podmiotów KSC złożony w S46 (art. 7c) + procedura aktualizacji danych w 14 dni Akt wyznaczenia osób kontaktowych z podmiotami KSC (art. 9 ust. 1 pkt 1) Dokumentacja ochrony infrastruktury wg art. 10 ust. 3 pkt 2 (charakterystyka, ocena stanu ochrony, ryzyko obiektów, zabezpieczenia techniczne, ochrona fizyczna) Procedura zgłaszania incydentów poważnych do CSIRT przez S46 (24h / 72h / 1 mies.) z matrycą klasyfikacji (art. 11-12b) Polityki tematyczne dla 14 obszarów art. 8 ust. 1 pkt 2 lit. a-n, w tym polityka oceny skuteczności środków (lit. h) i zasady cyberhigieny (lit. j) Polityka bezpieczeństwa łańcucha dostaw ICT z kryteriami z art. 8 ust. 2 (lit. e) Uchwała wskazująca osobę odpowiedzialną w zarządzie (art. 8c ust. 2) + dowody realizacji zadań kierownika (art. 8d) Dowody corocznego szkolenia kierownika podmiotu (art. 8e ust. 3) Rejestr informacji z KRK dla osób realizujących zadania z art. 8 i art. 11 (art. 8f) Informacje dla użytkowników o cyberzagrożeniach i kanał zgłoszeń użytkowników (art. 9 ust. 1 pkt 2-3) Raport z audytu bezpieczeństwa systemu informacyjnego (podmiot kluczowy: pierwszy do 24 mies., potem co najmniej raz na 3 lata; kopia do organu w 3 dni robocze, art. 15)

Dokumenty niedostarczone: wspólne dla całego projektu

Kategoria	Brakujące dokumenty
Polityki i procedury	Polityka Bezpieczeństwa Informacji Polityki szczegółowe: dostęp, praca zdalna, hasła, BYOD Regulamin korzystania z systemów IT Instrukcje i procedury operacyjne IT
Zarządzanie ryzykiem	Rejestr ryzyk / Analiza ryzyka Plan Postępowania z Ryzykiem (PPR) Deklaracja Stosowania (SoA)
Aktywa i infrastruktura	Rejestr aktywów informacyjnych Schemat sieci / topologia IT Wykaz dostawców / procesorów danych
Personel i szkolenia	Schemat organizacyjny / role IT i Security Potwierdzenie szkoleń z bezpieczeństwa Wzór umowy o pracę / klauzule NDA
Incydenty i ciągłość	Rejestr incydentów (ostatnie 12 miesięcy) Plan Ciągłości Działania (BCP) / DRP Wyniki testów backupów / DR
Zgodność i audyty	Wyniki audytów / pentestów / assessmentów Certyfikaty i raporty zgodności (ISO, SOC 2, PCI DSS) Rejestr wymagań prawnych (RODO, KNF, NIS2)

PRÓBKA - DANE FIKCYJNE

12 Wymagania poza przyjętą perspektywą oceny

Poniższe wymagania nie były oceniane, ponieważ nie powstają w przyjętej perspektywie (Pełny zakres). Zostały rozważone i świadomie wyłączone; nie wchodzą do średniej dojrzałości, werdyktu ani nakładu remediacji. Zmiana roli organizacji albo zakresu umowy z klientem wymaga ponownego przeglądu tej listy.

ID	Obszar	Wymaganie
N6-1	G. Perspektywa dostawcy ICT podmiotu kluczowego lub ważnego	Weryfikacja, czy organizacja sama nie jest podmiotem kluczowym lub ważnym mimo roli dostawcy
N6-2	G. Perspektywa dostawcy ICT podmiotu kluczowego lub ważnego	Zdolność do wykazania klientowi bezpieczeństwa dostarczanych produktów, usług i procesów ICT (art. 8 ust. 2)
N6-3	G. Perspektywa dostawcy ICT podmiotu kluczowego lub ważnego	Klauzule umowne przenoszące wymagania bezpieczeństwa i prawo weryfikacji
N6-4	G. Perspektywa dostawcy ICT podmiotu kluczowego lub ważnego	Zgłaszanie klientowi incydentów i podatności w oknie pozwalającym mu dotrzymać terminów ustawowych
N6-5	G. Perspektywa dostawcy ICT podmiotu kluczowego lub ważnego	Świadomość ryzyka uznania za dostawcę wysokiego ryzyka i zakazu nabywania (art. 67b-67c)
N6-6	G. Perspektywa dostawcy ICT podmiotu kluczowego lub ważnego	Niekaralność personelu realizującego u klienta zadania z art. 8 lub art. 11 (art. 8f)

13 Uczestnicy i ustalenia z wizyty

Notatki konsultanta:
DANE FIKCYJNE. Projekt demonstracyjny PushSec. Wszystkie nazwy, osoby, zdarzenia i liczby są zmyślone i służą wyłącznie pokazaniu formatu raportu. Wizyta 2 dni (3 do 4.09.2026), praca zdalna 5 dni.

14 Roadmapa wdrożenia

Faza	Zakres
Faza 1 - Quick Wins Dni 1-14	• **N0-3** Złożyć wniosek przez system S46 przed 3.10.2026 z danymi podmiotu, sektorem, usługą i osobami do kontaktu. Zachować potwierdzenie złożenia. (termin QW: do 28.09.2026) • **N0-4** Wyznaczyć zarządzeniem co najmniej dwie osoby (Pełnomocnik ds. SZBI i Kierownik IT), z zastępstwem, telefonem i adresem e-mail dostępnymi całodobowo dla CSIRT. Zgłosić we wniosku o wpis. (termin QW: do 28.09.2026) • **N0-1** Udokumentować kwalifikację: sektor z załącznika, przesłanka wielkościowa (średnie przedsiębiorstwo, 180 osób), świadczona usługa, data ustalenia, podstawa prawna. Zachować jako dowód dla organu. (termin QW: do 28.09.2026) • **N4-2** Przeprowadzić udokumentowane szkolenie Zarządu (2 h) do końca 2026 r. i powtarzać corocznie. Zaświadczenie do akt. (termin QW: do 28.09.2026)
Faza 2 - Fundamenty Dni 1-30	• **N1-1** Patrz c6-1: metodyka i pierwsza ocena ryzyka dla systemu informacyjnego wspierającego usługę, z kryteriami proporcjonalności z ustawy. (termin: 30.11.2026) • **N3-3** Wdrożyć procedurę incydentów (patrz A.5.24) z klasyfikacją, osobami do kontaktu, szablonami zgłoszeń S46 i ćwiczeniem tabletop przed 3.04.2027. (termin: 31.12.2026)
Faza 3 - Wdrożenie Mies. 2-6	• **N0-10** Powołać Pełnomocnika ds. SZBI, przypisać zadania cyberbezpieczeństwa w opisach stanowisk IT, ocenić model: własne struktury z outsourcingiem monitoringu (MSSP) jako opcja realna dla firmy tej wielkości. (termin: 31.12.2026) • **N1-2** Patrz działanie nadrzędne wskazane w obserwacji. (termin: 28.02.2027) • **N1-3** Patrz działanie nadrzędne wskazane w obserwacji. (termin: 28.02.2027) • **N1-4** Patrz działanie nadrzędne wskazane w obserwacji. (termin: 28.02.2027) • **N1-5** Patrz działanie nadrzędne wskazane w obserwacji. (termin: 28.02.2027) • **N2-15** Patrz działanie nadrzędne wskazane w obserwacji. (termin: 28.02.2027) • **N3-6** Patrz działanie nadrzędne wskazane w obserwacji. (termin: 28.02.2027) • **N3-5** Patrz działanie nadrzędne wskazane w obserwacji. (termin: 28.02.2027) • **N5-7** Patrz działanie nadrzędne wskazane w obserwacji. (termin: 28.02.2027)
Faza 4 - Domknięcie i audyt Mies. 6-9	• Audyt wewnętrzny / pre-assessment • Usunięcie niezgodności • Audyt certyfikujący lub potwierdzenie zgodności • Utrzymanie i monitoring

PRÓBKA. DANE FIKCYJNE

M Metodyka i zastrzeżenia

Czym jest metodyka PushSec GA-Z1/Z6. Autorska metodyka gap analizy PushSec, prowadząca ocenę na dwóch komplementarnych poziomach. **GA-Z1** to arkusz zbiorczy: ocena dojrzałości każdego obszaru normy na jednolitej skali 0-5, dająca zarządowi porównywalny obraz całości i podstawę decyzji o kierunku inwestycji. **GA-Z6** to karty szczegółowe luk: dla każdej istotnej luki opisany jest stan obecny, wymaganie normy, ryzyko biznesowe, rekomendacja, właściciel remediacji oraz szacunek nakładu, co stanowi bezpośredni materiał roboczy dla zespołu wdrożeniowego. Niniejszy raport łączy oba poziomy: sekcje zarządcze odpowiadają GA-Z1, karty szczegółowe realizują GA-Z6.

Próba dowodowa. Zakres przeglądu obejmował dokumentację i zapisy udostępnione przez organizację w terminie oceny oraz próbki konfiguracji wskazane przez osoby odpowiedzialne. Szczegółowy wykaz przejrzanych dokumentów zawiera sekcja Dokumenty wejściowe; oceny bez odnotowanego dowodu są w raporcie oznaczone i wymagają potwierdzenia w trakcie remediacji.

Przebieg oceny. Ocena została przeprowadzona w oparciu o trzy źródła dowodowe: wywiady z osobami odpowiedzialnymi za poszczególne obszary, przegląd dostarczonej dokumentacji oraz obserwację faktycznego funkcjonowania zabezpieczeń. Każde wymaganie normy w zakresie oceny otrzymało ocenę dojrzałości 0-5, a zidentyfikowanym lukom przypisano priorytet ryzyka biznesowego (K/W/Ś/N) z wyróżnieniem szybkich poprawek (Quick Wins). Priorytet wyraża ryzyko biznesowe luki w kontekście tej organizacji, nie wagę wymagania w standardzie: to samo wymaganie może mieć różny priorytet u różnych organizacji.

Typologia dowodów (ISO 19011). Każde ustalenie klasyfikowane jest według podstawy: **D** dokument lub zapis, **W** wywiad, **O** obserwacja, **T** test lub próbka techniczna, **B** brak dowodu. Ustalenia bez dowodu dokumentowego wymagają potwierdzenia w trakcie remediacji. Wskaźnik pokrycia dowodowego (odsetek ocenionych wymagań z odnotowanym dowodem) prezentowany jest w sekcji podsumowania.

Skala dojrzałości (0-5): 0 Nieistniejący (brak działań) · 1 Inicjalny (działania ad-hoc, nieudokumentowane) · 2 Powtarzalny (wdrożenie częściowe lub nieformalne) · 3 Zdefiniowany (wdrożone i udokumentowane, bez regularnej weryfikacji) · 4 Zarządzany (wdrożone, udokumentowane i weryfikowane) · 5 Optymalizujący (pełna zgodność, proces doskonalony).

Priorytety luk i okna remediacji. Termin przy priorytecie oznacza **maksymalne zalecane okno domknięcia remediacji, liczone od daty raportu** (nie czas trwania prac): **K** Krytyczny - do 30 dni; luka blokuje zgodność ustawową albo naraża na bezpośrednie ryzyko incydentu lub sankcji · **W** Wysoki - do 90 dni; do usunięcia przed oceną zewnętrzną · **Ś** Średni - do 180 dni; nieusunięta stanie się ustaleniem audytowym · **N** Niski - do 12 miesięcy, w ramach ciągłego doskonalenia. **QW** Quick Win to znacznik nakładu, nie poziom ryzyka ani okno remediacji: remediacja wymaga nie więcej niż ok. 2 tygodni pracy przy wysokim efekcie zgodności, dlatego działania QW realizowane są w pierwszej kolejności, równolegle z lukami krytycznymi. Dla luki z przypisanym priorytetem termin wyznacza okno priorytetu; okno 14 dni dotyczy wyłącznie Quick Winów bez priorytetu.

Skala gotowości: Gotowy (≥ 4,5) · Gotowy z drobnymi lukami (od 3,5 do poniżej 4,5) · Wymaga remediacji celowanej (od 2,5 do poniżej 3,5) · Wymaga intensywnej remediacji (od 1,5 do poniżej 2,5) · Niegotowy (poniżej 1,5). Progi są półotwarte (wartość graniczna należy do wyższego pasma) i odnoszą się do surowej średniej dojrzałości ważonej liczbą ocenionych wymagań; zaokrąglenie stosowane jest wyłącznie w prezentacji. Wymagania N/D i wykluczone z zakresu nie wpływają na średnią.

Ważność i ograniczenia. Analiza jest obrazem stanu na dzień 03.09.2026 i traci aktualność po istotnych zmianach w organizacji, infrastrukturze lub po upływie 12 miesięcy. Ocena oparta jest na informacjach udostępnionych przez organizację; nie stanowi audytu certyfikującego ani porady prawnej.

15 Wersja dokumentu i zasady dystrybucji

Wersja	Data	Autor	Opis
1.0	14.09.2026	Rafał Dobrosielski	Wydanie dokumentu

Dokument jest poufny i przeznaczony dla Demo Industrial Sp. z o.o. oraz osób przez niego wskazanych. Dalsze udostępnianie, w tym przekazanie kontrahentom lub organom, wymaga zgody Klienta. Ustalenia odzwierciedlają stan na dzień 03.09.2026 i zachowują ważność przez 12 miesięcy albo do istotnej zmiany w organizacji, zakresie usług lub stanie prawnym.

Podpis i pieczęć Klienta

Data: _____

Podpis Konsultanta PushSec
Rafał Dobrosielski
Data: _____

PRÓBKA, DANE FIKCYJNE

Próbka raportu PushSec. Demo Industrial Sp. z o.o. jest organizacją fikcyjną; wszystkie ustalenia, osoby i zdarzenia są zmyślone. pushsec.pl