Raport Gap Analysis

ISO/IEC 27001:2022 z Amd 1:2024 (PN-EN ISO/IEC 27001:2023-08) · Analiza luk i ocena dojrzałości

Demo Industrial Sp. z o.o.
Data: 14.09.2026
Nr ref.: GA-2026-09-DI/ISO_27001

Klient	Demo Industrial Sp. z o.o.	Branża / sektor	Produkcja (armatura przemysłowa), podmiot ważny KSC
Numer referencyjny	GA-2026-09-DI/ISO_27001	Wersja / status dokumentu	1.0 / Finalny
Klasyfikacja	Poufne - Demo Industrial Sp. z o.o. / PushSec	Podstawa stosowania normy	Wdrożenie dobrowolne
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

Wdrożenie niepełne: wymagania blokujące Gotowość: Wymaga intensywnej remediacji (od 1,5 do poniżej 2,5). Średnia dojrzałość 1,7 / 5,0.

110 luk, w tym **12** krytycznych Nakład remediacji: **221,5** dni rob. Quick Wins: **8**

Najważniejsze ryzyka

- Bez właściciela systemu żadne z pozostałych działań remediacyjnych nie ma osoby, która je poprowadzi i rozliczy.
- Bez polityki nie ma podstawy do egzekwowania zasad wobec pracowników i dostawcy IT.
- Nakłady na bezpieczeństwo omijają realne zagrożenia.

Decyzje wymagane od zarządu

- Zatwierdzenie budżetu i zasobów na remediację (szacunek: 221,5 dni roboczych).
- Wyznaczenie właściciela programu remediacji i trybu raportowania postępu do zarządu.
- Akceptacja ryzyka szczątkowego i planu postępowania z ryzykiem po zakończeniu remediacji.

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

PRÓBKA, DANE FIKCYJNE

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. Mocne strony
7. Zidentyfikowane luki i rekomendacje
8. Obciążenie właścicieli remediacji
9. Efekt cross-framework
10. Karty szczegółowe luk (GA-Z6)
11. Quick Wins
12. Dokumenty wejściowe
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 ISO/IEC 27001:2022 z Amd 1:2024 (PN-EN ISO/IEC 27001:2023-08) 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 normy: wdrożenie dobrowolne.

Werdykt zgodności. **Wdrożenie niepełne: wymagania blokujące** Zidentyfikowano 66 wymagań blokujących (luka o priorytecie krytycznym albo dojrzałość 0-1): kl. 4 w.1, kl. 4 w.2, kl. 4 w.3, kl. 4 w.6, kl. 4 w.7, kl. 4 w.8, kl. 4 w.9, kl. 4 w.10 i inne. Do czasu ich usunięcia organizacja nie może wykazać zgodności.

Kluczowe ustalenia. Średnia dojrzałość ocenionego zakresu wynosi **1,7 / 5,0** (Wymaga intensywnej remediacji (od 1,5 do poniżej 2,5) - certyfikacja realna w 9-15 miesięcy przy zaangażowaniu zasobów). Ocenie podlegało **143** wymagania; luki zidentyfikowano w **110** z nich: **12 K** / **32 W** / **66 Ś**. Oznaczono **8** szybkich popraw (Quick Wins), z których każda wymaga nie więcej niż około 2 tygodni pracy.

Najważniejsze ryzyka biznesowe. Luki krytyczne koncentrują się w obszarach: 6. Planowanie (4 K), A.5 Zabezpieczenia organizacyjne (3 K), 5. Przywództwo (2 K) i in.. W praktyce oznaczają one m.in.:

- Bez właściciela systemu żadne z pozostałych działań remediacyjnych nie ma osoby, która je poprowadzi i rozliczy. (poz. 1)
- Bez polityki nie ma podstawy do egzekwowania zasad wobec pracowników i dostawcy IT. (poz. 2)
- Nakłady na bezpieczeństwo omijają realne zagrożenia. (poz. 3)
- Brak rejestru oznacza brak dowodu, że Zarząd wie, jakie ryzyka akceptuje. (poz. 4)
- Bez PPR nie ma mechanizmu, który zamienia ocenę ryzyka w budżet i zadania. (poz. 5)

Nieusunięte, blokują certyfikację i osłabiają pozycję w postępowaniach i relacjach z klientami. Pełny opis każdego ryzyka w kartach GA-Z6.

Rekomendowane działania.

Natychmiast (0-14 dni) - Quick Wins

- **A.8.8** Wdrożyć proces: inwentaryzacja wersji, skan podatności co najmniej kwartalnie, okna serwisowe, priorytety wg CVSS i ekspozycji, osobna ścieżka dla OT uzgodniona z producentem linii. Zacząć od systemów wystawionych do internetu (UTM, VPN, poczta).
- **kl. 9 w.5** Rozszerzyć istniejący roczny przegląd zarządzania ISO 9001 o wejścia z kl. 9.3 ISO 27001: wyniki oceny ryzyka, incydenty, audyty, cele, dostawcy. Protokół z decyzjami Zarządu.
- **A.5.7** Zapisać firmę do komunikatów CSIRT NASK i producentów (UTM, ERP, SCADA), wyznaczyć osobę przeglądającą je co tydzień, powiązać z procesem podatności.
- **A.5.18** Wprowadzić kwartalny przegląd uprawnień w ERP, AD i M365 przez właścicieli systemów, z protokołem i usuwaniem nadmiarowych dostępów. Pierwszy przegląd od razu, jako szybka wygrana.

  ... oraz 4 pozycje - pełna lista w tabeli luk.

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

- **kl. 5 w.2** Powołać Pełnomocnika ds. SZBI zarządzeniem Zarządu z zakresem odpowiedzialności, uprawnieniem do raportowania bezpośrednio do Zarządu i wymiarem czasu (co najmniej 0,25 etatu w fazie wdrożenia). Rozważyć outsourcing roli na okres wdrożenia.
- **kl. 5 w.5** Opracować i zatwierdzić Politykę Bezpieczeństwa Informacji zgodną z kl. 5.2: cele, zakres, zobowiązanie kierownictwa, ramy dla polityk szczegółowych, zasady komunikacji. Zakomunikować wszystkim pracownikom i dostawcy IT.
- **kl. 6 w.1** Przyjąć metodykę szacowania ryzyka zgodną z ISO/IEC 27005 i wymaganiami art. 8 ustawy o KSC (kryteria proporcjonalności), z matrycą prawdopodobieństwo x skutek, kryteriami akceptacji i rolą Zarządu. Przeprowadzić pierwszą ocenę dla systemów wspierających usługę objętą ustawą (ERP, SCADA, poczta, sieć zakładowa).
- **kl. 6 w.3** Utworzyć rejestr ryzyk jako produkt pierwszej oceny: scenariusz, aktywo, właściciel, ocena inherentna i rezydualna, opcja postępowania, termin przeglądu. Zarząd zatwierdza rejestr i akceptuje ryzyka pozostałe.

  ... oraz 7 pozycji - pełna lista w tabeli luk.

Krótkoterminowo (30-90 dni) - luki wysokie

- **kl. 4 w.9** Patrz działanie nadrzędne wskazane w obserwacji.
- **kl. 5 w.8** Patrz działanie nadrzędne wskazane w obserwacji.
- **kl. 6 w.2** Patrz działanie nadrzędne wskazane w obserwacji.
- **kl. 6 w.4** Patrz działanie nadrzędne wskazane w obserwacji.

  ... oraz 23 pozycje - pełna lista w tabeli luk.

Szacunkowy nakład i horyzont. Łączny szacowany nakład remediacji: **221,5 dni roboczych**. Przewidywany czas dojścia do gotowości: **9-15 miesięcy** od rozpoczęcia prac.

Efekt dla pozostałych regulacji. Remediacja zidentyfikowanych luk domyka jednocześnie **35** powiązanych wymagań innych regulacji (DORA, PCI DSS, RODO i in.), 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.

2 Stosowalność regulacji

Wniosek o objęciu organizacji tą normą 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
ISO/IEC 27001 (certyfikacja SZBI) PN-EN ISO/IEC 27001:2023-08 (ISO/IEC 27001:2022 z Amd 1:2024)	Do rozstrzygnięcia	-	Pełny zakres	0/3	Brak rozstrzygającej przesłanki rynkowej lub decyzji zarządu.

PRÓBKA, DANE FIKCYJNE

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: 221,5 dni roboczych).
- Wyznaczenie właściciela programu remediacji i trybu raportowania postępu do zarządu.
- 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

Wdrożenie niepełne: wymagania blokujące

Zidentyfikowano 66 wymagań blokujących (luka o priorytecie krytycznym albo dojrzałość 0-1): kl. 4 w.1, kl. 4 w.2, kl. 4 w.3, kl. 4 w.6, kl. 4 w.7, kl. 4 w.8, kl. 4 w.9, kl. 4 w.10 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.

Podstawa stosowania: Wdrożenie dobrowolne. Norma nie wynika z przepisów prawa. Standard certyfikacyjny lub dobre praktyki wdrażane z inicjatywy organizacji (przewaga rynkowa, wymóg przetargowy, certyfikat). ISO 27001, ISO 22301, SOC 2 i NIST CSF nie są obowiązkiem ustawowym.

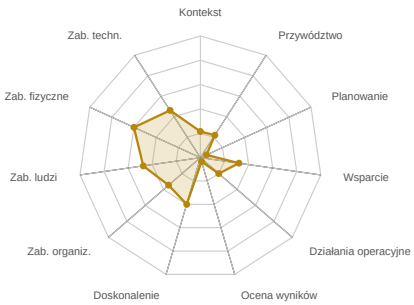
Ocena gotowości: Wymaga intensywnej remediacji (od 1,5 do poniżej 2,5) - certyfikacja realna w 9-15 miesięcy przy zaangażowaniu zasobów

1,7	12	8	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
4. Kontekst organizacji	1,1	22% skali dojrzałości
5. Przywództwo	1,1	22% skali dojrzałości
6. Planowanie	0,3	5% skali dojrzałości
7. Wsparcie	1,6	32% skali dojrzałości
8. Działania operacyjne	1,0	20% skali dojrzałości
9. Ocena wyników	0,2	3% skali dojrzałości
10. Doskonalenie	2,0	40% skali dojrzałości
A.5 Zabezpieczenia organizacyjne	1,7	35% skali dojrzałości
A.6 Zabezpieczenia ludzi	2,4	48% skali dojrzałości
A.7 Zabezpieczenia fizyczne	3,0	60% skali dojrzałości
A.8 Zabezpieczenia techniczne	2,3	46% skali dojrzałości

6 Mocne strony

Żaden obszar nie osiągnął progu mocnej strony (dojrzałość 3,5 bez luk K/W), dlatego wskazano pojedyncze wymagania ocenione na 4-5. Stanowią one fundament, na którym organizacja może oprzeć remediację pozostałych luk.

- **A.5.34** Prywatność i ochrona danych osobowych - A.5 Zabezpieczenia organizacyjne (dojrzałość 4,0)
- **A.6.6** Umowy o zachowaniu poufności (NDA) - A.6 Zabezpieczenia ludzi (dojrzałość 4,0)
- **A.7.1** Granice bezpieczeństwa fizycznego - A.7 Zabezpieczenia fizyczne (dojrzałość 4,0)
- **A.7.2** Fizyczne wejścia - A.7 Zabezpieczenia fizyczne (dojrzałość 4,0)
- **A.7.11** Zasilanie i media pomocnicze - A.7 Zabezpieczenia fizyczne (dojrzałość 4,0)
- **A.8.13** Kopie zapasowe - A.8 Zabezpieczenia techniczne (dojrzałość 4,0)
- **A.8.17** Synchronizacja zegarów - A.8 Zabezpieczenia techniczne (dojrzałość 4,0)

7 Zidentyfikowane luki i rekomendacje

Numeracja luk jest ciągła (1-110) 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 certyfikację)										
1	**kl. 5 w.2**	5. Przywództwo	**Rola CISO** Brak wyznaczonej roli odpowiedzialnej za SZBI. Bezpieczeństwo informacji jest domyślnie "u informatyków", bez umocowania, zakresu i czasu pracy.	K	1,0	**Wywiad**	Powołać Pełnomocnika ds. SZBI zarządzeniem Zarządu z zakresem odpowiedzialności, uprawnieniem do raportowania bezpośrednio do Zarządu i wymiarem czasu (co najmniej 0,25 etatu w fazie wdrożenia). Rozważyć outsourcing roli na okres wdrożenia.	Zarząd (A) / Pełnomocnik ds. SZBI (R)	8,0	15.10.2026
2	**kl. 5 w.5**	5. Przywództwo	**Polityka BI** Nie ma Polityki Bezpieczeństwa Informacji. Istnieje "Regulamin korzystania z komputerów" z 2017 r., 2 strony, bez celów, zakresu i odniesienia do ryzyka.	K	1,0	**Dokument / zapis** Regulamin korzystania z komputerów, wersja 2017	Opracować i zatwierdzić Politykę Bezpieczeństwa Informacji zgodną z kl. 5.2: cele, zakres, zobowiązanie kierownictwa, ramy dla polityk szczegółowych, zasady komunikacji. Zakomunikować wszystkim pracownikom i dostawcy IT.	Zarząd (A) / Pełnomocnik ds. SZBI (R)	6,0	31.10.2026
3	**kl. 6 w.1**	6. Planowanie	**Proces szacowania ryzyka** Brak jakiegokolwiek procesu szacowania ryzyka bezpieczeństwa informacji. Decyzje o zabezpieczeniach zapadają ad hoc, na wniosek IT lub po incydencie.	K	0,0	**Wywiad**	Przyjąć metodykę szacowania ryzyka zgodną z ISO/IEC 27005 i wymaganiami art. 8 ustawy o KSC (kryteria proporcjonalności), z matrycą prawdopodobieństwo x skutek, kryteriami akceptacji i rolą Zarządu. Przeprowadzić pierwszą ocenę dla systemów wspierających usługę objętą ustawą (ERP, SCADA, poczta, sieć zakładowa).	Zarząd (A) / Pełnomocnik ds. SZBI (R)	10,0	30.11.2026
4	**kl. 6 w.3**	6. Planowanie	**Rejestr ryzyk** Brak rejestru ryzyk.	K	0,0	**Wywiad**	Utworzyć rejestr ryzyk jako produkt pierwszej oceny: scenariusz, aktywo, właściciel, ocena inherentna i rezydualna, opcja postępowania, termin przeglądu. Zarząd zatwierdza rejestr i akceptuje ryzyka pozostałe.	Zarząd (A) / Pełnomocnik ds. SZBI (R)	4,0	30.11.2026

PRÓBKA, DANE FIKCYJNE

5	**kl. 6 w.5**	6. Planowanie	**PPR** Brak Planu Postępowania z Ryzykiem.	K	0,0	**Wywiad**	Opracować PPR jako wynik oceny ryzyka: działania, właściciele, terminy, nakłady, kontrole z Aneksu A. PPR zatwierdza Zarząd i przegląda go kwartalnie.	Zarząd (A) / Pełnomocnik ds. SZBI (R)	4,0	15.12.2026
6	**kl. 6 w.6**	6. Planowanie	**SoA** Brak Deklaracji Stosowania.	K	0,0	**Wywiad**	Opracować SoA dla 93 zabezpieczeń Aneksu A z uzasadnieniem stosowania lub wyłączenia każdej kontroli, powiązaną z rejestrem ryzyk i PPR. Utrzymywać w narzędziu, nie w arkuszu bez wersjonowania.	Zarząd (A) / Pełnomocnik ds. SZBI (R)	5,0	31.12.2026
7	**kl. 8 w.2**	8. Działania operacyjne	**Nadzór dostawców** Dostawca IT (umowa serwisowa z 2019 r.) ma pełny dostęp administracyjny do serwerów, ERP i UTM bez klauzul bezpieczeństwa, bez rejestru czynności i bez prawa kontroli.	K	1,0	**Obserwacja** Konfiguracja UTM i AD, sesja zdalna w trakcie wizyty	Aneksować umowę z dostawcą IT: zakres usług, wymagania bezpieczeństwa, obowiązek zgłaszania incydentów w czasie pozwalającym dotrzymać terminów ustawowych, imienne konta, logowanie sesji zdalnych, prawo audytu, zasady podwykonawstwa. Wdrożyć rejestr dostępów zdalnych dostawcy.	Kierownik IT (R) / Pełnomocnik ds. SZBI (A)	6,0	30.11.2026
8	**A.5.19**	A.5 Zabezpieczenia organizacyjne	**Bezpieczeństwo w relacjach z dostawcami** Brak zasad bezpieczeństwa w relacjach z dostawcami: nie ma listy dostawców z dostępem do informacji ani oceny ich ryzyka.	K	1,0	**Obserwacja** Router GSM na linii L2, oględziny hali	Sporządzić rejestr dostawców z dostępem do systemów lub danych (IT, ERP, SCADA, księgowość zewnętrzna, kurier dokumentów), sklasyfikować wg krytyczności i objąć wymaganiami adekwatnymi do klasy.	Kierownik IT (R) / Pełnomocnik ds. SZBI (A)	4,0	30.11.2026
9	**A.5.20**	A.5 Zabezpieczenia organizacyjne	**Bezpieczeństwo w umowach z dostawcami** Umowy z dostawcami IT i OT nie zawierają wymagań bezpieczeństwa.	K	1,0	**Dokument / zapis** Wzór umowy serwisowej 2016	Wprowadzić standardowy załącznik bezpieczeństwa do umów z dostawcami klasy krytycznej i ważnej, w tym zgłaszanie incydentów, dostęp imienny, prawo audytu, poufność, zasady zakończenia współpracy.	Zarząd (A) / Prokurent ds. operacyjnych (R)	3,0	31.12.2026

PRÓBKA, DANE FIKCYJNE

10	**A.5.24**	A.5 Zabezpieczenia organizacyjne	**Planowanie obsługi incydentów** Brak procedury obsługi incydentów. Zdarzenia zgłaszane są telefonicznie do Kierownika IT i nie są rejestrowane.	**K**	1,0	**Wywiad**	Opracować procedurę zarządzania incydentami z klasyfikacją (w tym kryteria incydentu poważnego wg ustawy), rejestrem, rolami, kanałem zgłoszeń dla pracowników, terminami zgłoszeń do CSIRT NASK (24 h, 72 h, miesiąc) i osobami do kontaktu.	Kierownik IT (R) / Pełnomocnik ds. SZBI (A)	5,0	30.11.2026
11	**A.8.8**	A.8 Zabezpieczenia techniczne	**Zarządzanie podatnościami technicznymi** Brak zarządzania podatnościami. Aktualizacje serwerów wykonuje dostawca IT "gdy jest okazja", stacje robocze mają wyłączone aktualizacje automatyczne, SCADA nie był aktualizowany od instalacji.	**K** **QW**	1,0	**Obserwacja** Panel UTM, wersja firmware; Windows Update na ERP-SRV01	Wdrożyć proces: inwentaryzacja wersji, skan podatności co najmniej kwartalnie, okna serwisowe, priorytety wg CVSS i ekspozycji, osobna ścieżka dla OT uzgodniona z producentem linii. Zacząć od systemów wystawionych do internetu (UTM, VPN, poczta).	Kierownik IT (R) / Pełnomocnik ds. SZBI (A)	6,0	do 28.09.2026 okno prior.: 31.10.2026
12	**A.8.22**	A.8 Zabezpieczenia techniczne	**Segregacja sieci** Sieć OT (SCADA, sterowniki linii) jest w jednej sieci z biurem i Wi-Fi gości.	**K**	1,0	**Obserwacja** Skan sieci z Wi-Fi gości w trakcie wizyty	Zaprojektować segmentację: VLAN dla OT z jednokierunkowym dostępem serwisowym przez jump host, osobna sieć gości, sieć biurowa. Dostęp producenta linii przez firmowy VPN z MFA zamiast routera GSM.	Kierownik Utrzymania Ruchu (R) / Kierownik IT (A)	8,0	31.12.2026
Wysokie (do usunięcia przed oceną zewnętrzną)										
13	**kl. 4 w.9**	4. Kontekst organizacji	**Zatwierdzenie zakresu** Nie spełniono: zakres jest udokumentowany i zatwierdzony przez kierownictwo.	**W**	0,0	**Wywiad**	Patrz działanie nadrzędne wskazane w obserwacji.	Zarząd (A) / Pełnomocnik ds. SZBI (R)	2,0	28.02.2027
14	**kl. 5 w.8**	5. Przywództwo	**Treść polityki (5.2)** Nie spełniono: Polityka BI zawiera cele bezpieczeństwa informacji lub ramy ich wyznaczania oraz zobowiązanie do spełnienia mających zastosowanie wymagań (pkt 5.2 lit. b-c).	**W**	0,0	**Wywiad**	Patrz działanie nadrzędne wskazane w obserwacji.	Zarząd (A) / Pełnomocnik ds. SZBI (R)	2,0	28.02.2027
15	**kl. 6 w.2**	6. Planowanie	**Kryteria ryzyka** Nie spełniono: określono kryteria oceny i akceptacji ryzyka.	**W**	0,0	**Wywiad**	Patrz działanie nadrzędne wskazane w obserwacji.	Zarząd (A) / Pełnomocnik ds. SZBI (R)	2,0	28.02.2027

PRÓBKA, DANE FIKCYJNE

16	**kl. 6 w.4**	6. Planowanie	**Ryzyka CIA** Nie spełniono: zidentyfikowano ryzyka dla poufności, integralności i dostępności aktywów informacyjnych.	W	0,0	**Wywiad**	Patrz działanie nadrzędne wskazane w obserwacji.	Zarząd (A) / Pełnomocnik ds. SZBI (R)	2,0	28.02.2027
17	**kl. 6 w.7**	6. Planowanie	**Cele BI** Nie spełniono: organizacja ustanowiła mierzalne cele bezpieczeństwa informacji, udokumentowane, monitorowane, komunikowane i aktualizowane (pkt 6.2).	W	0,0	**Wywiad**	Patrz działanie nadrzędne wskazane w obserwacji.	Zarząd (A) / Pełnomocnik ds. SZBI (R)	2,0	28.02.2027
18	**kl. 6 w.8**	6. Planowanie	**Powiązanie celów** Nie spełniono: cele są powiązane z polityką bezpieczeństwa i wynikami oceny ryzyka.	W	0,0	**Wywiad**	Patrz działanie nadrzędne wskazane w obserwacji.	Zarząd (A) / Pełnomocnik ds. SZBI (R)	2,0	28.02.2027
19	**kl. 6 w.9**	6. Planowanie	**Plan celów** Nie spełniono: istnieje plan osiągania celów z przypisanymi zasobami i terminami.	W	0,0	**Wywiad**	Patrz działanie nadrzędne wskazane w obserwacji.	Zarząd (A) / Pełnomocnik ds. SZBI (R)	2,0	28.02.2027
20	**kl. 7 w.4**	7. Wsparcie	**Szkolenia** Brak szkoleń z bezpieczeństwa informacji. Jedyne szkolenie to instruktaż BHP.	W	1,0	**Wywiad**	Wdrożyć roczny program szkoleń: szkolenie wstępne dla wszystkich (2 h), moduł dla kierownictwa wymagany przez ustawę, moduł dla operatorów OT, symulacja phishingu dwa razy w roku. Rejestrować obecność i wyniki.	Dyrektor HR (R) / Pełnomocnik ds. SZBI (A)	3,0	31.01.2027
21	**kl. 7 w.8**	7. Wsparcie	**Dokumentacja SZBI** Poza regulaminem z 2017 r. i dokumentacją RODO z 2019 r. nie ma dokumentów wymaganych przez normę.	W	1,0	**Dokument / zapis** Dokumentacja RODO 2019, rejestr czynności przetwarzania	Zbudować komplet dokumentacji SZBI w kolejności: polityka, zakres, metodyka ryzyka, rejestr ryzyk, PPR, SoA, procedury operacyjne (incydenty, dostęp, kopie zapasowe, zmiany, dostawcy, ciągłość).	Zarząd (A) / Pełnomocnik ds. SZBI (R)	12,0	28.02.2027
22	**kl. 8 w.4**	8. Działania operacyjne	**Cykliczna ocena ryzyka** Nie spełniono: ocena ryzyka jest przeprowadzana cyklicznie lub przy znaczących zmianach.	W	0,0	**Wywiad**	Patrz działanie nadrzędne wskazane w obserwacji.	Zarząd (A) / Pełnomocnik ds. SZBI (R)	2,0	28.02.2027

PRÓBKA, DANE FIKCYJNE

23	**kl. 8 w.5**	8. Działania operacyjne	**Wdrażanie PPR** Nie spełniono: działania z planu postępowania z ryzykiem są faktycznie wdrażane i śledzone.	W	0,0	**Wywiad**	Patrz działanie nadrzędne wskazane w obserwacji.	Zarząd (A) / Pełnomocnik ds. SZBI (R)	2,0	28.02.2027
24	**kl. 9 w.1**	9. Ocena wyników	**Monitorowanie i pomiary** Nie spełniono: organizacja mierzy skuteczność SZBI - czy istnieją wskaźniki (KPI/KRI) bezpieczeństwa.	W	0,0	**Wywiad**	Patrz działanie nadrzędne wskazane w obserwacji.	Zarząd (A) / Pełnomocnik ds. SZBI (R)	2,0	28.02.2027
25	**kl. 9 w.3**	9. Ocena wyników	**Audyt wewnętrzny** Brak audytu wewnętrznego SZBI. Nigdy nie przeprowadzono.	W	0,0	**Dokument / zapis** Program audytów ISO 9001 2026	Zaplanować pierwszy audyt wewnętrzny po wdrożeniu dokumentacji i minimum 2 miesiącach działania systemu, przez audytora niezależnego od wdrożenia.	Zarząd (A) / Pełnomocnik ds. SZBI (R)	3,0	30.04.2027
26	**kl. 9 w.4**	9. Ocena wyników	**Program audytów** Nie spełniono: istnieje program audytów wewnętrznych z harmonogramem.	W	0,0	**Wywiad**	Patrz działanie nadrzędne wskazane w obserwacji.	Zarząd (A) / Pełnomocnik ds. SZBI (R)	2,0	28.02.2027
27	**kl. 9 w.5**	9. Ocena wyników	**Przegląd zarządzania** Przegląd zarządzania nie obejmuje bezpieczeństwa informacji.	W QW	0,0	**Dokument / zapis** Protokół przeglądu zarządzania ISO 9001, styczeń 2026	Rozszerzyć istniejący roczny przegląd zarządzania ISO 9001 o wejścia z kl. 9.3 ISO 27001: wyniki oceny ryzyka, incydenty, audyty, cele, dostawcy. Protokół z decyzjami Zarządu.	Zarząd (A) / Pełnomocnik ds. SZBI (R)	1,0	do 28.09.2026 okno prior.: 31.01.2027
28	**kl. 9 w.6**	9. Ocena wyników	**Wejścia i wyjścia przeglądu (9.3)** Nie spełniono: przegląd zarządzania obejmuje wymagane wejścia (w tym zmiany potrzeb i oczekiwań stron zainteresowanych, pkt 9.3.2) i udokumentowane wyjścia (pkt 9.3.3).	W	0,0	**Wywiad**	Patrz działanie nadrzędne wskazane w obserwacji.	Zarząd (A) / Pełnomocnik ds. SZBI (R)	2,0	28.02.2027
29	**A.5.1**	A.5 Zabezpieczenia organizacyjne	**Polityki bezpieczeństwa informacji** Brak zestawu polityk szczegółowych.	W	1,0	**Wywiad**	Po zatwierdzeniu polityki nadrzędnej opracować polityki: kontroli dostępu, kopii zapasowych, pracy zdalnej i urządzeń mobilnych, dostawców, klasyfikacji informacji, kryptografii, zarządzania zmianą. Zwięzłe, 2 do 4 stron każda.	Zarząd (A) / Pełnomocnik ds. SZBI (R)	6,0	31.01.2027

PRÓBKA, DANE FIKCYJNE

30	**A.5.7**	A.5 Zabezpieczenia organizacyjne	**Threat intelligence** Brak zorganizowanego pozyskiwania informacji o zagrożeniach i podatnościach.	W QW	1,0	**Wywiad**	Zapisać firmę do komunikatów CSIRT NASK i producentów (UTM, ERP, SCADA), wyznaczyć osobę przeglądającą je co tydzień, powiązać z procesem podatności.	Kierownik IT (R) / Pełnomocnik ds. SZBI (A)	1,0	do 28.09.2026 okno prior.: 31.10.2026
31	**A.5.9**	A.5 Zabezpieczenia organizacyjne	**Inwentaryzacja aktywów** Inwentaryzacja aktywów obejmuje tylko sprzęt biurowy (ewidencja środków trwałych). Brak inwentaryzacji systemów, danych, urządzeń OT i usług chmurowych.	W	2,0	**Dokument / zapis** Ewidencja środków trwałych 2026	Sporządzić rejestr aktywów informacyjnych z właścicielami i klasyfikacją: systemy (ERP, SCADA, M365, CAD), zbiory danych, urządzenia sieciowe i OT, usługi zewnętrzne.	Kierownik IT (R) / Pełnomocnik ds. SZBI (A)	3,0	30.11.2026
32	**A.5.12**	A.5 Zabezpieczenia organizacyjne	**Klasyfikacja informacji** Brak klasyfikacji informacji. Dokumentacja konstrukcyjna (know-how firmy) jest traktowana tak samo jak korespondencja ogólna.	W	1,0	**Wywiad**	Wprowadzić trzy klasy (publiczna, wewnętrzna, poufna) z zasadami przechowywania, przesyłania i udostępniania. Objąć w pierwszej kolejności dokumentację konstrukcyjną i dane klientów.	Zarząd (A) / Pełnomocnik ds. SZBI (R)	3,0	31.12.2026
33	**A.5.15**	A.5 Zabezpieczenia organizacyjne	**Kontrola dostępu** Kontrola dostępu bez zasad: uprawnienia nadawane na prośbę przełożonego mailem, bez przeglądów, bez odbierania przy zmianie stanowiska.	W	2,0	**Obserwacja** Eksport kont z AD i ról z ERP	Wdrożyć politykę kontroli dostępu z zasadą minimalnych uprawnień, macierzą ról dla ERP i udziałów sieciowych, procesem nadawania, zmiany i odbierania dostępu powiązanym z HR.	Kierownik IT (R) / Pełnomocnik ds. SZBI (A)	4,0	31.12.2026
34	**A.5.18**	A.5 Zabezpieczenia organizacyjne	**Prawa dostępu** Brak przeglądów uprawnień.	W QW	2,0	**Wywiad**	Wprowadzić kwartalny przegląd uprawnień w ERP, AD i M365 przez właścicieli systemów, z protokołem i usuwaniem nadmiarowych dostępów. Pierwszy przegląd od razu, jako szybka wygrana.	Kierownik IT (R) / Pełnomocnik ds. SZBI (A)	1,0	do 28.09.2026 okno prior.: 31.10.2026
35	**A.5.30**	A.5 Zabezpieczenia organizacyjne	**Gotowość ICT do ciągłości działania** Brak planu ciągłości ICT. Odtworzenie ERP po awarii w marcu 2026 r. trwało 2 dni i zależało od dostępności jednej osoby u dostawcy.	W	1,0	**Wywiad**	Określić RTO i RPO dla ERP, SCADA, poczty i plików na podstawie BIA, opracować plan odtworzenia, przetestować odtworzenie z kopii co najmniej raz w roku.	Kierownik IT (R) / Pełnomocnik ds. SZBI (A)	4,0	28.02.2027

PRÓBKA, DANE FIKCYJNE

36	**A.5.35**	A.5 Zabezpieczenia organizacyjne	**Niezależny przegląd bezpieczeństwa** Nigdy nie przeprowadzono niezależnego przeglądu bezpieczeństwa.	W	0,0	**Wywiad**	Zaplanować niezależny przegląd (audyt wewnętrzny SZBI plus test penetracyjny brzegu sieci) po wdrożeniu zabezpieczeń priorytetowych.	Zarząd (A) / Pełnomocnik ds. SZBI (R)	2,0	30.04.2027
37	**A.6.3**	A.6 Zabezpieczenia ludzi	**Szkolenia i świadomość** Brak szkoleń i programu świadomości.	W	1,0	**Wywiad**	Jak c7-4: program roczny, moduł dla kierownictwa, moduł OT, symulacje phishingu.	Dyrektor HR (R) / Pełnomocnik ds. SZBI (A)	3,0	31.01.2027
38	**A.6.7**	A.6 Zabezpieczenia ludzi	**Praca zdalna** Praca zdalna bez zasad: prywatne laptopy handlowców z dostępem VPN, brak szyfrowania dysków, brak MFA.	W	2,0	**Wywiad**	Polityka pracy zdalnej i urządzeń: sprzęt firmowy lub minimalne wymagania dla prywatnego, szyfrowanie dysku, MFA na VPN i M365, blokada ekranu.	Kierownik IT (R) / Pełnomocnik ds. SZBI (A)	2,0	31.12.2026
39	**A.6.8**	A.6 Zabezpieczenia ludzi	**Zgłaszanie zdarzeń bezpieczeństwa** Pracownicy nie mają kanału ani obowiązku zgłaszania zdarzeń bezpieczeństwa.	W QW	1,0	**Wywiad**	Ustanowić prosty kanał (adres e-mail i numer wewnętrzny), zasadę "zgłoś, nie oceniaj", potwierdzenie przyjęcia zgłoszenia. Zakomunikować na szkoleniu wstępnym.	Kierownik IT (R) / Pełnomocnik ds. SZBI (A)	1,0	do 28.09.2026 okno prior.: 31.10.2026
40	**A.8.2**	A.8 Zabezpieczenia techniczne	**Uprzywilejowane prawa dostępu** Konta uprzywilejowane współdzielone (konto "serwis" dostawcy, konto "admin" w ERP używane przez 4 osoby).	W	2,0	**Wywiad**	Imienne konta administracyjne, odrębne od kont codziennych, MFA, rejestrowanie sesji uprzywilejowanych, przegląd kwartalny.	Kierownik IT (R) / Pełnomocnik ds. SZBI (A)	3,0	31.12.2026
41	**A.8.5**	A.8 Zabezpieczenia techniczne	**Bezpieczne uwierzytelnianie** MFA tylko dla administratorów domeny. VPN, M365 i ERP z samym hasłem. Polityka haseł: 8 znaków, bez wygasania.	W QW	2,0	**Wywiad**	MFA dla VPN, M365 i dostępu zdalnego dostawców w pierwszej kolejności, potem ERP. Polityka haseł zgodna z aktualnymi wytycznymi (długość, blokada po nieudanych próbach, brak wymuszonej rotacji przy MFA).	Kierownik IT (R) / Pełnomocnik ds. SZBI (A)	2,0	do 28.09.2026 okno prior.: 30.11.2026
42	**A.8.15**	A.8 Zabezpieczenia techniczne	**Logowanie (logging)** Logi zbierane lokalnie na urządzeniach, bez centralizacji i retencji. UTM nadpisuje logi po 7 dniach.	W	2,0	**Wywiad**	Centralne zbieranie logów z UTM, AD, ERP i serwerów z retencją co najmniej 12 miesięcy (ustawa: dokumentacja operacyjna). Alerty dla zdarzeń krytycznych.	Kierownik IT (R) / Pełnomocnik ds. SZBI (A)	4,0	28.02.2027

PRÓBKA, DANE FIKCYJNE

43	**A.8.16**	A.8 Zabezpieczenia techniczne	**Monitorowanie aktywności** Brak monitorowania: nikt nie przegląda logów ani alertów. UTM wysyła powiadomienia na skrzynkę, której nikt nie czyta.	W	1,0	**Wywiad**	Zdefiniować minimalny zestaw monitorowanych zdarzeń, właściciela przeglądu, częstotliwość. Rozważyć usługę zewnętrznego monitoringu (MSSP) jako opcję wymaganą przez ustawę dla struktur odpowiedzialnych za cyberbezpieczeństwo.	Kierownik IT (R) / Pełnomocnik ds. SZBI (A)	3,0	28.02.2027
44	**A.8.32**	A.8 Zabezpieczenia techniczne	**Zarządzanie zmianami** Zmiany w ERP i infrastrukturze bez formalnego procesu. Dostawca wprowadza zmiany po telefonie od Kierownika IT.	W	2,0	**Wywiad**	Prosty proces zmian: wniosek, ocena wpływu, akceptacja, okno, plan wycofania, zapis. Dla OT dodatkowo uzgodnienie z Utrzymaniem Ruchu.	Kierownik IT (R) / Pełnomocnik ds. SZBI (A)	2,0	31.01.2027
Średnie (nieusunięte staną się ustaleniami audytowymi)										
45	**kl. 4 w.1**	4. Kontekst organizacji	**Kontekst wewnętrzny**	Ś	1,0	**Wywiad**	Zapewnić, że organizacja zidentyfikowała kluczowe zagadnienia wewnętrzne (struktura, kultura, zasoby, strategia) wpływające na SZBI. Udokumentować, zatwierdzić przez kierownictwo i przypisać właściciela. Pierwszy krok: opracowanie dokumentu "Polityka Bezpieczeństwa Informacji". Oczekiwany dowód wdrożenia: Analiza kontekstu wewnętrznego (rejestr zagadnień) z datą przeglądu. **	Zarząd / Pełnomocnik ds. SZBI*	1,0	

PRÓBKA, DANE FIKCYJNE

46	**kl. 4 w.2**	4. Kontekst organizacji	**Kontekst zewnętrzny**	Ś	1,0	**Wywiad**	Zapewnić, że organizacja zidentyfikowała kluczowe zagadnienia zewnętrzne (regulacje, rynek, klienci, dostawcy, technologie) wpływające na SZBI. Udokumentować, zatwierdzić przez kierownictwo i przypisać właściciela. Pierwszy krok: opracowanie dokumentu "Polityka Bezpieczeństwa Informacji". Oczekiwany dowód wdrożenia: Analiza kontekstu zewnętrznego: regulacje, rynek, technologia. **	Zarząd / Pełnomocnik ds. SZBI*	1,0	
47	**kl. 4 w.3**	4. Kontekst organizacji	**Przegląd kontekstu**	Ś	1,0	**Wywiad**	Zapewnić, że zagadnienia kontekstu są regularnie przeglądane i aktualizowane. Udokumentować, zatwierdzić przez kierownictwo i przypisać właściciela. Oczekiwany dowód wdrożenia: Zapisy przeglądu kontekstu (protokół przeglądu zarządzania lub rejestr zmian). **	Zarząd / Pełnomocnik ds. SZBI*	1,0	
48	**kl. 4 w.4**	4. Kontekst organizacji	**Strony zainteresowane**	Ś	2,0	**Wywiad**	Zakres: organizacja zidentyfikowała wszystkie relewantne strony zainteresowane (klienci, regulatorzy, dostawcy, pracownicy, akcjonariusze), w tym strony mogące mieć wymagania związane ze zmianami klimatu (Amd 1:2024). Działanie: sformalizować i zatwierdzić istniejącą praktykę, uzupełnić brakujące elementy, zakomunikować w organizacji i przypisać właściciela. Oczekiwany dowód wdrożenia: Rejestr stron zainteresowanych. **	Zarząd / Pełnomocnik ds. SZBI*	1,0	

PRÓBKA, DANE FIKCYJNE

49	**kl. 4 w.5**	4. Kontekst organizacji	**Wymagania stron**	Ś	2,0	**Wywiad**	Zakres: zidentyfikowano wymagania stron zainteresowanych odnoszące się do bezpieczeństwa informacji (wymogi umowne, regulacyjne, RODO). Działanie: sformalizować i zatwierdzić istniejącą praktykę, uzupełnić brakujące elementy, zakomunikować w organizacji i przypisać właściciela. Oczekiwany dowód wdrożenia: Rejestr wymagań stron zainteresowanych (umowy, regulacje, SLA). **	Zarząd / Pełnomocnik ds. SZBI*	1,0	
50	**kl. 4 w.6**	4. Kontekst organizacji	**Dokumentacja wymagań**	Ś	1,0	**Wywiad**	Zapewnić, że wymagania stron zainteresowanych są udokumentowane i regularnie przeglądane. Udokumentować, zatwierdzić przez kierownictwo i przypisać właściciela. Oczekiwany dowód wdrożenia: Rejestr wymagań z datami przeglądów i wersjonowaniem. **	Zarząd / Pełnomocnik ds. SZBI*	1,0	
51	**kl. 4 w.7**	4. Kontekst organizacji	**Zakres SZBI**	Ś	1,0	**Wywiad**	Zapewnić, że istnieje formalnie zdefiniowany zakres SZBI obejmujący lokalizacje, działy, procesy i systemy. Udokumentować, zatwierdzić przez kierownictwo i przypisać właściciela. Pierwszy krok: opracowanie dokumentu "Polityka Bezpieczeństwa Informacji". Oczekiwany dowód wdrożenia: Udokumentowany zakres SZBI (pkt 4.3). **	Zarząd / Pełnomocnik ds. SZBI*	1,0	

PRÓBKA, DANE FIKCYJNE

52	**kl. 4 w.8**	4. Kontekst organizacji	**Interfejsy zewnętrzne**	Ś	1,0	**Wywiad**	Zapewnić, że zakres uwzględnia interfejsy z zewnętrznymi dostawcami i podmiotami przetwarzającymi dane. Udokumentować, zatwierdzić przez kierownictwo i przypisać właściciela. Pierwszy krok: opracowanie dokumentu "Polityka zarządzania dostawcami + Rejestr dostawców (Register of Information)". Oczekiwany dowód wdrożenia: Zakres SZBI z opisem interfejsów i zależności od podmiotów zewnętrznych. **	Zarząd / Pełnomocnik ds. SZBI*	1,0	
53	**kl. 4 w.10**	4. Kontekst organizacji	**Projekt SZBI**	Ś	1,0	**Wywiad**	Zapewnić, że organizacja posiada zaprojektowany SZBI (choćby częściowy) z jasno określonymi procesami. Udokumentować, zatwierdzić przez kierownictwo i przypisać właściciela. Pierwszy krok: opracowanie dokumentu "Polityka Bezpieczeństwa Informacji". Oczekiwany dowód wdrożenia: Mapa procesów SZBI lub księga SZBI. **	Zarząd / Pełnomocnik ds. SZBI*	1,0	
54	**kl. 4 w.11**	4. Kontekst organizacji	**Zakres a kontekst**	Ś	1,0	**Wywiad**	Zapewnić, że przy ustalaniu zakresu SZBI uwzględniono zagadnienia z pkt 4.1 i wymagania stron z pkt 4.2 (pkt 4.3 lit. a-b). Udokumentować, zatwierdzić przez kierownictwo i przypisać właściciela. Pierwszy krok: opracowanie dokumentu "Polityka Bezpieczeństwa Informacji". Oczekiwany dowód wdrożenia: Zapis uwzględnienia kontekstu i wymagań stron przy ustalaniu zakresu SZBI (pkt 4.3 lit. a-b). **	Zarząd / Pełnomocnik ds. SZBI*	1,0	

PRÓBKA, DANE FIKCYJNE

55	**kl. 4 w.12**	4. Kontekst organizacji	**Zmiany klimatu (Amd 1:2024)**	Ś	1,0	**Wywiad**	Zapewnić, że organizacja ustaliła, czy zmiany klimatu są istotnym zagadnieniem dla SZBI (Amd 1:2024, pkt 4.1). Udokumentować, zatwierdzić przez kierownictwo i przypisać właściciela. Pierwszy krok: opracowanie dokumentu "Polityka Bezpieczeństwa Informacji". Oczekiwany dowód wdrożenia: Zapis analizy istotności zmian klimatu dla SZBI (Amd 1:2024) w dokumentacji kontekstu. **	Zarząd / Pełnomocnik ds. SZBI*	1,0	
56	**kl. 4 w.13**	4. Kontekst organizacji	**Wymagania adresowane przez SZBI**	Ś	1,0	**Wywiad**	Zapewnić, że określono, które wymagania stron zainteresowanych będą adresowane przez SZBI (pkt 4.2 lit. c). Udokumentować, zatwierdzić przez kierownictwo i przypisać właściciela. Pierwszy krok: opracowanie dokumentu "Polityka Bezpieczeństwa Informacji". Oczekiwany dowód wdrożenia: Rejestr wymagań stron zainteresowanych z oznaczeniem, które adresuje SZBI (pkt 4.2 lit. c). **	Zarząd / Pełnomocnik ds. SZBI*	1,0	
57	**kl. 5 w.1**	5. Przywództwo	**Zaangażowanie kierownictwa**	Ś	2,0	**Wywiad**	Zakres: najwyższe kierownictwo aktywnie angażuje się w SZBI - czy bezpieczeństwo jest elementem agendy zarządu. Działanie: sformalizować i zatwierdzić istniejącą praktykę, uzupełnić brakujące elementy, zakomunikować w organizacji i przypisać właściciela. Oczekiwany dowód wdrożenia: Protokoły posiedzeń zarządu z punktem dot. bezpieczeństwa. **	Zarząd / Pełnomocnik ds. SZBI*	1,0	

PRÓBKA, DANE FIKCYJNE

58	**kl. 5 w.3**	5. Przywództwo	**Zasoby**	Ś	2,0	**Wywiad**	Zakres: kierownictwo zapewnia wystarczające zasoby (budżet, czas, ludzie) dla bezpieczeństwa informacji. Działanie: sformalizować i zatwierdzić istniejącą praktykę, uzupełnić brakujące elementy, zakomunikować w organizacji i przypisać właściciela. Oczekiwany dowód wdrożenia: Zatwierdzony budżet lub plan zasobów bezpieczeństwa. **	Zarząd / Pełnomocnik ds. SZBI*	1,0	
59	**kl. 5 w.4**	5. Przywództwo	**Integracja strategiczna**	Ś	1,0	**Wywiad**	Zapewnić, że bezpieczeństwo informacji jest zintegrowane z celami strategicznymi organizacji. Udokumentować, zatwierdzić przez kierownictwo i przypisać właściciela. Pierwszy krok: opracowanie dokumentu "Polityka Bezpieczeństwa Informacji". Oczekiwany dowód wdrożenia: Cele strategiczne organizacji z komponentem bezpieczeństwa. **	Zarząd / Pełnomocnik ds. SZBI*	1,0	
60	**kl. 5 w.6**	5. Przywództwo	**Aktualność polityki**	Ś	1,0	**Wywiad**	Zapewnić, że polityka jest aktualna, dostosowana do kontekstu organizacji i zawiera zobowiązanie do doskonalenia. Udokumentować, zatwierdzić przez kierownictwo i przypisać właściciela. Pierwszy krok: opracowanie dokumentu "Polityka Bezpieczeństwa Informacji". Oczekiwany dowód wdrożenia: Polityka BI z datą przeglądu i zobowiązaniem do doskonalenia. **	Zarząd / Pełnomocnik ds. SZBI*	1,0	

PRÓBKA, DANE FIKCYJNE

61	**kl. 5 w.7**	5. Przywództwo	**Komunikacja polityki**	Ś	1,0	**Wywiad**	Zapewnić, że polityka jest zakomunikowana wszystkim pracownikom i dostępna dla zainteresowanych stron. Udokumentować, zatwierdzić przez kierownictwo i przypisać właściciela. Pierwszy krok: opracowanie dokumentu "Polityka Bezpieczeństwa Informacji". Oczekiwany dowód wdrożenia: Dowód komunikacji polityki (intranet, potwierdzenia zapoznania). **	Zarząd / Pełnomocnik ds. SZBI*	1,0	
62	**kl. 5 w.9**	5. Przywództwo	**Role i odpowiedzialności**	Ś	1,0	**Wywiad**	Zapewnić, że role i odpowiedzialności dotyczące bezpieczeństwa informacji są formalnie przypisane i udokumentowane. Udokumentować, zatwierdzić przez kierownictwo i przypisać właściciela. Pierwszy krok: opracowanie dokumentu "Polityka Bezpieczeństwa Informacji". Oczekiwany dowód wdrożenia: Udokumentowane przypisanie ról bezpieczeństwa (pkt 5.3). **	Zarząd / Pełnomocnik ds. SZBI*	1,0	

PRÓBKA, DANE FIKCYJNE

63	**kl. 5 w.10**	5. Przywództwo	**Raportowanie do kierownictwa (5.3)**	Ś	1,0	**Wywiad**	Zapewnić, że przypisano odpowiedzialność za raportowanie najwyższemu kierownictwu o wynikach działania SZBI (pkt 5.3 lit. b). Udokumentować, zatwierdzić przez kierownictwo i przypisać właściciela. Pierwszy krok: opracowanie dokumentu "Polityka Bezpieczeństwa Informacji". Oczekiwany dowód wdrożenia: Zapis przypisania odpowiedzialności za raportowanie wyników SZBI kierownictwu (pkt 5.3 lit. b) + przykładowy raport. **	Zarząd / Pełnomocnik ds. SZBI*	1,0	
64	**kl. 6 w.10**	6. Planowanie	**Zmiany w SZBI są planowane i wprowadzane w sposób kontrolowany (kl. 6.3)**	Ś	2,0	**Wywiad**	Zakres: zmiany w SZBI są planowane i wprowadzane w sposób kontrolowany (kl. 6.3). Działanie: sformalizować i zatwierdzić istniejącą praktykę, uzupełnić brakujące elementy, zakomunikować w organizacji i przypisać właściciela. Oczekiwany dowód wdrożenia: Zapisy planowania zmian SZBI: cel, ocena skutków, zatwierdzenie (kl. 6.3). **	Zespół IT / Bezpieczeństwo*	1,0	
65	**kl. 6 w.11**	6. Planowanie	**Ryzyka i szanse (6.1.1)**	Ś	1,0	**Wywiad**	Zapewnić, że planując SZBI organizacja określiła szanse, a nie tylko ryzyka, które należy uwzględnić (pkt 6.1.1). Udokumentować, zatwierdzić przez kierownictwo i przypisać właściciela. Pierwszy krok: opracowanie dokumentu "Polityka Bezpieczeństwa Informacji". Oczekiwany dowód wdrożenia: Zapis szans zidentyfikowanych przy planowaniu SZBI (pkt 6.1.1) z działaniami. **	Pełnomocnik ds. SZBI / Risk Owner*	1,0	

PRÓBKA, DANE FIKCYJNE

66	**kl. 7 w.1**	7. Wsparcie	**Kompetencje**	Ś	2,0	**Wywiad**	Zakres: organizacja określiła kompetencje niezbędne dla bezpieczeństwa informacji. Działanie: sformalizować i zatwierdzić istniejącą praktykę, uzupełnić brakujące elementy, zakomunikować w organizacji i przypisać właściciela. Oczekiwany dowód wdrożenia: Macierz kompetencji dla ról bezpieczeństwa (pkt 7.2). **	HR / Pełnomocnik ds. SZBI*	1,0	
67	**kl. 7 w.2**	7. Wsparcie	**Kwalifikacje**	Ś	2,0	**Wywiad**	Zakres: pracownicy odpowiedzialni za bezpieczeństwo posiadają odpowiednie kwalifikacje (szkolenia, certyfikaty). Działanie: sformalizować i zatwierdzić istniejącą praktykę, uzupełnić brakujące elementy, zakomunikować w organizacji i przypisać właściciela. Oczekiwany dowód wdrożenia: Certyfikaty, dyplomy i zapisy szkoleń personelu (pkt 7.2). **	HR / Pełnomocnik ds. SZBI*	1,0	
68	**kl. 7 w.3**	7. Wsparcie	**Budżet**	Ś	2,0	**Wywiad**	Zakres: istnieje budżet przeznaczony na bezpieczeństwo informacji. Działanie: sformalizować i zatwierdzić istniejącą praktykę, uzupełnić brakujące elementy, zakomunikować w organizacji i przypisać właściciela. Oczekiwany dowód wdrożenia: Zatwierdzony budżet bezpieczeństwa informacji. **	Zespół IT / Bezpieczeństwo*	1,0	

PRÓBKA, DANE FIKCYJNE

69	**kl. 7 w.5**	7. Wsparcie	**Program awareness**	Ś	1,0	**Wywiad**	Zapewnić, że istnieje program uświadamiania (e-learning, symulacje phishingu, komunikaty). Udokumentować, zatwierdzić przez kierownictwo i przypisać właściciela. Pierwszy krok: opracowanie dokumentu "Program szkoleń security awareness". Oczekiwany dowód wdrożenia: Materiały programu awareness, wyniki symulacji phishingu. **	Zespół IT / Bezpieczeństwo*	1,0	
70	**kl. 7 w.6**	7. Wsparcie	**Świadomość polityk**	Ś	1,0	**Wywiad**	Zapewnić, że pracownicy są świadomi polityk bezpieczeństwa i konsekwencji ich naruszenia. Udokumentować, zatwierdzić przez kierownictwo i przypisać właściciela. Pierwszy krok: opracowanie dokumentu "Polityka Bezpieczeństwa Informacji". Oczekiwany dowód wdrożenia: Potwierdzenia zapoznania z politykami bezpieczeństwa. **	Zarząd / Pełnomocnik ds. SZBI*	1,0	
71	**kl. 7 w.7**	7. Wsparcie	**Plan komunikacji**	Ś	1,0	**Wywiad**	Zapewnić, że istnieje zdefiniowany plan komunikacji w obszarze bezpieczeństwa informacji (co, kiedy, komu, jak). Udokumentować, zatwierdzić przez kierownictwo i przypisać właściciela. Pierwszy krok: opracowanie dokumentu "Polityka Bezpieczeństwa Informacji". Oczekiwany dowód wdrożenia: Plan komunikacji: co, kiedy, komu, jak (pkt 7.4). **	Zespół IT / Bezpieczeństwo*	1,0	

PRÓBKA, DANE FIKCYJNE

72	**kl. 7 w.9**	7. Wsparcie	**Zarządzanie dokumentami**	Ś	2,0	**Wywiad**	Zakres: dokumentacja jest aktualna, wersjonowana i dostępna dla uprawnionych osób. Działanie: sformalizować i zatwierdzić istniejącą praktykę, uzupełnić brakujące elementy, zakomunikować w organizacji i przypisać właściciela. Oczekiwany dowód wdrożenia: Metryki dokumentów: wersja, data, zatwierdzający. **	Zespół IT / Bezpieczeństwo*	1,0	
73	**kl. 8 w.1**	8. Działania operacyjne	**Nadzór operacyjny**	Ś	2,0	**Wywiad**	Zakres: procesy operacyjne związane z bezpieczeństwem są udokumentowane i przestrzegane. Działanie: sformalizować i zatwierdzić istniejącą praktykę, uzupełnić brakujące elementy, zakomunikować w organizacji i przypisać właściciela. Oczekiwany dowód wdrożenia: Udokumentowane procedury operacyjne + zapisy z ich realizacji (pkt 8.1). **	Zespół IT / Bezpieczeństwo*	1,0	
74	**kl. 8 w.3**	8. Działania operacyjne	**Zarządzanie zmianami**	Ś	2,0	**Wywiad**	Zakres: zmiany w systemach i procesach są zarządzane w sposób kontrolowany. Działanie: sformalizować i zatwierdzić istniejącą praktykę, uzupełnić brakujące elementy, zakomunikować w organizacji i przypisać właściciela. Oczekiwany dowód wdrożenia: Zapisy zarządzania zmianą: wnioski, oceny, zatwierdzenia. **	Zarząd / Pełnomocnik ds. SZBI*	1,0	

PRÓBKA, DANE FIKCYJNE

75	**kl. 9 w.2**	9. Ocena wyników	**Raportowanie wyników**	Ś	1,0	**Wywiad**	Zapewnić, że wyniki monitorowania są analizowane i raportowane kierownictwu. Udokumentować, zatwierdzić przez kierownictwo i przypisać właściciela. Pierwszy krok: opracowanie dokumentu "Polityka logowania i monitorowania". Oczekiwany dowód wdrożenia: Raporty dla kierownictwa z analizą wyników monitorowania. **	Audyt wewnętrzny / Pełnomocnik ds. SZBI*	1,0	
76	**kl. 10 w.1**	10. Doskonalenie	**Działania korygujące**	Ś	2,0	**Wywiad**	Zakres: istnieje proces zarządzania niezgodnościami i działaniami korygującymi. Działanie: sformalizować i zatwierdzić istniejącą praktykę, uzupełnić brakujące elementy, zakomunikować w organizacji i przypisać właściciela. Oczekiwany dowód wdrożenia: Procedura zarządzania niezgodnościami i działaniami korygującymi. **	Zarząd / Pełnomocnik ds. SZBI*	1,0	
77	**kl. 10 w.2**	10. Doskonalenie	**Rejestr niezgodności**	Ś	2,0	**Wywiad**	Zakres: organizacja dokumentuje niezgodności, ich przyczyny i podjęte działania. Działanie: sformalizować i zatwierdzić istniejącą praktykę, uzupełnić brakujące elementy, zakomunikować w organizacji i przypisać właściciela. Oczekiwany dowód wdrożenia: Rejestr niezgodności: przyczyny, działania, skuteczność (pkt 10.2). **	Zespół IT / Bezpieczeństwo*	1,0	

PRÓBKA, DANE FIKCYJNE

78	**kl. 10 w.3**	10. Doskonalenie	**Ciągłe doskonalenie**	Ś	2,0	**Wywiad**	Zakres: organizacja wykazuje podejście do ciągłego doskonalenia SZBI. Działanie: sformalizować i zatwierdzić istniejącą praktykę, uzupełnić brakujące elementy, zakomunikować w organizacji i przypisać właściciela. Oczekiwany dowód wdrożenia: Zapisy działań doskonalących (wnioski, inicjatywy, decyzje). **	Zespół IT / Bezpieczeństwo*	1,0	
79	**A.5.2**	A.5 Zabezpieczenia organizacyjne	**Role i odpowiedzialności w bezpieczeństwie**	Ś	1,0	**Wywiad**	Zakres: role i odpowiedzialności w bezpieczeństwie. Działanie: opracować i wdrożyć, udokumentować, zatwierdzić przez kierownictwo i przypisać właściciela. Pierwszy krok: opracowanie dokumentu "Polityka Bezpieczeństwa Informacji". Oczekiwany dowód wdrożenia: Matryca ról i odpowiedzialności bezpieczeństwa. **	Zespół IT / Bezpieczeństwo*	1,0	
80	**A.5.3**	A.5 Zabezpieczenia organizacyjne	**Podział obowiązków (SoD)**	Ś	2,0	**Wywiad**	Zakres: podział obowiązków (SoD). Działanie: sformalizować i zatwierdzić istniejącą praktykę, uzupełnić brakujące elementy, zakomunikować w organizacji i przypisać właściciela. Oczekiwany dowód wdrożenia: Matryca podziału obowiązków / analiza konfliktów uprawnień. **	Zespół IT / Bezpieczeństwo*	1,0	
81	**A.5.4**	A.5 Zabezpieczenia organizacyjne	**Obowiązki kierownictwa**	Ś	2,0	**Wywiad**	Zakres: obowiązki kierownictwa. Działanie: sformalizować i zatwierdzić istniejącą praktykę, uzupełnić brakujące elementy, zakomunikować w organizacji i przypisać właściciela. Oczekiwany dowód wdrożenia: Zapisy egzekwowania polityk przez kierownictwo. **	Zespół IT / Bezpieczeństwo*	1,0	

PRÓBKA, DANE FIKCYJNE

82	**A.5.5**	A.5 Zabezpieczenia organizacyjne	**Kontakt z organami władzy** Brak wyznaczonych osób do kontaktu z CSIRT i organem właściwym.	Ś QW	2,0	**Wywiad**	Wyznaczyć dwie osoby do kontaktów z podmiotami KSC, zgłosić je we wniosku o wpis do wykazu, wpisać do procedury incydentów.	Zarząd (A) / Pełnomocnik ds. SZBI (R)	1,0	do 28.09.2026 okno prior.: 30.09.2026
83	**A.5.6**	A.5 Zabezpieczenia organizacyjne	**Kontakt z grupami specjalistów** Brak kontaktu z grupami branżowymi i CSIRT.	Ś QW	1,0	**Wywiad**	Subskrypcja komunikatów CSIRT NASK, udział w ISAC sektorowym, jeśli dostępny.	Kierownik IT (R) / Pełnomocnik ds. SZBI (A)	0,5	do 28.09.2026 okno prior.: 31.10.2026
84	**A.5.8**	A.5 Zabezpieczenia organizacyjne	**Bezpieczeństwo w zarządzaniu projektami**	Ś	2,0	**Wywiad**	Zakres: bezpieczeństwo w zarządzaniu projektami. Działanie: sformalizować i zatwierdzić istniejącą praktykę, uzupełnić brakujące elementy, zakomunikować w organizacji i przypisać właściciela. Oczekiwany dowód wdrożenia: Wymagania bezpieczeństwa w metodyce zarządzania projektami. **	Zarząd / Pełnomocnik ds. SZBI*	1,0	
85	**A.5.13**	A.5 Zabezpieczenia organizacyjne	**Oznaczanie informacji**	Ś	1,0	**Wywiad**	Zakres: oznaczanie informacji. Działanie: opracować i wdrożyć, udokumentować, zatwierdzić przez kierownictwo i przypisać właściciela. Oczekiwany dowód wdrożenia: Zasady oznaczania + próbka oznaczonych dokumentów. **	Zespół IT / Bezpieczeństwo*	1,0	
86	**A.5.14**	A.5 Zabezpieczenia organizacyjne	**Przekazywanie informacji**	Ś	2,0	**Wywiad**	Zakres: przekazywanie informacji. Działanie: sformalizować i zatwierdzić istniejącą praktykę, uzupełnić brakujące elementy, zakomunikować w organizacji i przypisać właściciela. Oczekiwany dowód wdrożenia: Zasady przekazywania informacji (kanały, umowy). **	Zespół IT / Bezpieczeństwo*	1,0	

PRÓBKA, DANE FIKCYJNE

87	**A.5.17**	A.5 Zabezpieczenia organizacyjne	**Informacje uwierzytelniające**	Ś	2,0	**Wywiad**	Zakres: informacje uwierzytelniające. Działanie: sformalizować i zatwierdzić istniejącą praktykę, uzupełnić brakujące elementy, zakomunikować w organizacji i przypisać właściciela. Oczekiwany dowód wdrożenia: Polityka haseł i sekretów + konfiguracja wymuszenia. **	Zespół IT / Bezpieczeństwo*	1,0	
88	**A.5.21**	A.5 Zabezpieczenia organizacyjne	**Bezpieczeństwo w łańcuchu dostaw ICT**	Ś	1,0	**Wywiad**	Zakres: bezpieczeństwo w łańcuchu dostaw ICT. 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: Wymagania bezpieczeństwa łańcucha dostaw ICT w umowach. **	Zakupy / Pełnomocnik ds. SZBI*	1,0	
89	**A.5.22**	A.5 Zabezpieczenia organizacyjne	**Monitorowanie usług dostawców**	Ś	1,0	**Wywiad**	Zakres: monitorowanie usług dostawców. 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: Zapisy monitorowania i przeglądów usług dostawców. **	Zakupy / Pełnomocnik ds. SZBI*	1,0	

PRÓBKA, DANE FIKCYJNE

90	**A.5.23**	A.5 Zabezpieczenia organizacyjne	**Bezpieczeństwo usług w chmurze**	Ś	2,0	**Wywiad**	Zakres: bezpieczeństwo usług w chmurze. Działanie: sformalizować i zatwierdzić istniejącą praktykę, uzupełnić brakujące elementy, zakomunikować w organizacji i przypisać właściciela. Oczekiwany dowód wdrożenia: Wymagania dla usług chmurowych + umowy z CSP. **	Zespół IT / Bezpieczeństwo*	1,0	
91	**A.5.25**	A.5 Zabezpieczenia organizacyjne	**Klasyfikacja zdarzeń**	Ś	1,0	**Wywiad**	Zakres: klasyfikacja zdarzeń. Działanie: opracować i wdrożyć, udokumentować, zatwierdzić przez kierownictwo i przypisać właściciela. Oczekiwany dowód wdrożenia: Kryteria klasyfikacji zdarzeń bezpieczeństwa. **	Zespół IT / Bezpieczeństwo*	1,0	
92	**A.5.26**	A.5 Zabezpieczenia organizacyjne	**Reagowanie na incydenty**	Ś	2,0	**Wywiad**	Zakres: reagowanie na incydenty. Działanie: sformalizować i zatwierdzić istniejącą praktykę, uzupełnić brakujące elementy, zakomunikować w organizacji i przypisać właściciela. Oczekiwany dowód wdrożenia: Zapisy obsługi incydentów (tickety, raporty). **	Zespół IT / Bezpieczeństwo*	1,0	
93	**A.5.27**	A.5 Zabezpieczenia organizacyjne	**Wnioski z incydentów**	Ś	1,0	**Wywiad**	Zakres: wnioski z incydentów. 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 wniosków po incydentach (lessons learned). **	Zespół IT / Bezpieczeństwo*	1,0	

PRÓBKA, DANE FIKCYJNE

94	**A.5.28**	A.5 Zabezpieczenia organizacyjne	**Zbieranie dowodów**	Ś	1,0	**Wywiad**	Zakres: zbieranie dowodów. Działanie: opracować i wdrożyć, udokumentować, zatwierdzić przez kierownictwo i przypisać właściciela. Oczekiwany dowód wdrożenia: Procedura zabezpieczania dowodów. **	Zespół IT / Bezpieczeństwo*	1,0	
95	**A.5.29**	A.5 Zabezpieczenia organizacyjne	**Bezpieczeństwo podczas zakłóceń**	Ś	2,0	**Wywiad**	Zakres: bezpieczeństwo podczas zakłóceń. Działanie: sformalizować i zatwierdzić istniejącą praktykę, uzupełnić brakujące elementy, zakomunikować w organizacji i przypisać właściciela. Oczekiwany dowód wdrożenia: Plany utrzymania bezpieczeństwa podczas zakłóceń (BCP). **	Zespół IT / Bezpieczeństwo*	1,0	
96	**A.5.36**	A.5 Zabezpieczenia organizacyjne	**Zgodność z politykami i standardami**	Ś	1,0	**Wywiad**	Zakres: zgodność z politykami i standardami. Działanie: opracować i wdrożyć, udokumentować, zatwierdzić przez kierownictwo i przypisać właściciela. Pierwszy krok: opracowanie dokumentu "Polityka Bezpieczeństwa Informacji". Oczekiwany dowód wdrożenia: Zapisy przeglądów zgodności z politykami. **	Zarząd / Pełnomocnik ds. SZBI*	1,0	
97	**A.5.37**	A.5 Zabezpieczenia organizacyjne	**Udokumentowane procedury operacyjne**	Ś	2,0	**Wywiad**	Zakres: udokumentowane procedury operacyjne. Działanie: sformalizować i zatwierdzić istniejącą praktykę, uzupełnić brakujące elementy, zakomunikować w organizacji i przypisać właściciela. Oczekiwany dowód wdrożenia: Udokumentowane procedury operacyjne. **	Zespół IT / Bezpieczeństwo*	1,0	

PRÓBKA, DANE FIKCYJNE

98	**A.6.5**	A.6 Zabezpieczenia ludzi	**Obowiązki po zakończeniu zatrudnienia**	Ś	2,0	**Wywiad**	Zakres: obowiązki po zakończeniu zatrudnienia. Działanie: sformalizować i zatwierdzić istniejącą praktykę, uzupełnić brakujące elementy, zakomunikować w organizacji i przypisać właściciela. Oczekiwany dowód wdrożenia: Zapisy offboardingu z obowiązkami po ustaniu zatrudnienia. **	Zespół IT / Bezpieczeństwo*	1,0	
99	**A.7.7**	A.7 Zabezpieczenia fizyczne	**Czyste biurko i czysty ekran**	Ś	2,0	**Wywiad**	Zakres: czyste biurko i czysty ekran. Działanie: sformalizować i zatwierdzić istniejącą praktykę, uzupełnić brakujące elementy, zakomunikować w organizacji i przypisać właściciela. Oczekiwany dowód wdrożenia: Polityka czystego biurka + wyniki kontroli. **	Administracja / Bezpieczeństwo fizyczne*	1,0	
100	**A.7.10**	A.7 Zabezpieczenia fizyczne	**Nośniki danych**	Ś	2,0	**Wywiad**	Zakres: nośniki danych. Działanie: sformalizować i zatwierdzić istniejącą praktykę, uzupełnić brakujące elementy, zakomunikować w organizacji i przypisać właściciela. Oczekiwany dowód wdrożenia: Ewidencja nośników + procedura obiegu i niszczenia. **	Administracja / Bezpieczeństwo fizyczne*	1,0	
101	**A.7.14**	A.7 Zabezpieczenia fizyczne	**Bezpieczna utylizacja sprzętu**	Ś	2,0	**Wywiad**	Zakres: bezpieczna utylizacja sprzętu. Działanie: sformalizować i zatwierdzić istniejącą praktykę, uzupełnić brakujące elementy, zakomunikować w organizacji i przypisać właściciela. Oczekiwany dowód wdrożenia: Protokoły niszczenia i utylizacji z certyfikatami. **	Administracja / Bezpieczeństwo fizyczne*	1,0	

PRÓBKA, DANE FIKCYJNE

102	**A.8.6**	A.8 Zabezpieczenia techniczne	**Zarządzanie pojemnością**	Ś	2,0	**Wywiad**	Zakres: zarządzanie pojemnością. Działanie: sformalizować i zatwierdzić istniejącą praktykę, uzupełnić brakujące elementy, zakomunikować w organizacji i przypisać właściciela. Oczekiwany dowód wdrożenia: Raporty monitorowania pojemności. **	Zarząd / Pełnomocnik ds. SZBI*	1,0	
103	**A.8.7**	A.8 Zabezpieczenia techniczne	**Ochrona przed złośliwym oprogramowaniem**	Ś	2,0	**Wywiad**	Zakres: ochrona przed złośliwym oprogramowaniem. Działanie: sformalizować i zatwierdzić istniejącą praktykę, uzupełnić brakujące elementy, zakomunikować w organizacji i przypisać właściciela. Oczekiwany dowód wdrożenia: Raport pokrycia ochrony EDR/AV. **	HR / Pełnomocnik ds. SZBI*	1,0	
104	**A.8.9**	A.8 Zabezpieczenia techniczne	**Zarządzanie konfiguracją**	Ś	2,0	**Wywiad**	Zakres: zarządzanie konfiguracją. Działanie: sformalizować i zatwierdzić istniejącą praktykę, uzupełnić brakujące elementy, zakomunikować w organizacji i przypisać właściciela. Oczekiwany dowód wdrożenia: Baseline konfiguracji + rejestr odstępstw. **	Zarząd / Pełnomocnik ds. SZBI*	1,0	
105	**A.8.10**	A.8 Zabezpieczenia techniczne	**Usuwanie informacji**	Ś	2,0	**Wywiad**	Zakres: usuwanie informacji. Działanie: sformalizować i zatwierdzić istniejącą praktykę, uzupełnić brakujące elementy, zakomunikować w organizacji i przypisać właściciela. Oczekiwany dowód wdrożenia: Procedura i zapisy usuwania informacji. **	Zespół IT / Bezpieczeństwo*	1,0	

PRÓBKA, DANE FIKCYJNE

106	**A.8.12**	A.8 Zabezpieczenia techniczne	**Zapobieganie wyciekom danych (DLP)**	Ś	1,0	**Wywiad**	Zakres: zapobieganie wyciekom danych (DLP). Działanie: opracować i wdrożyć, udokumentować, zatwierdzić przez kierownictwo i przypisać właściciela. Oczekiwany dowód wdrożenia: Konfiguracja i raporty DLP. **	Zespół IT / Bezpieczeństwo*	1,0	
107	**A.8.18**	A.8 Zabezpieczenia techniczne	**Użycie uprzywilejowanych narzędzi systemowych**	Ś	2,0	**Wywiad**	Zakres: użycie uprzywilejowanych narzędzi systemowych. Działanie: sformalizować i zatwierdzić istniejącą praktykę, uzupełnić brakujące elementy, zakomunikować w organizacji i przypisać właściciela. Oczekiwany dowód wdrożenia: Ograniczenia narzędzi uprzywilejowanych + logi użycia. **	Zespół IT / Bezpieczeństwo*	1,0	
108	**A.8.24**	A.8 Zabezpieczenia techniczne	**Stosowanie kryptografii**	Ś	2,0	**Wywiad**	Zakres: stosowanie kryptografii. Działanie: sformalizować i zatwierdzić istniejącą praktykę, uzupełnić brakujące elementy, zakomunikować w organizacji i przypisać właściciela. Oczekiwany dowód wdrożenia: Polityka kryptograficzna + zasady zarządzania kluczami. **	Zespół IT / Bezpieczeństwo*	1,0	
109	**A.8.30**	A.8 Zabezpieczenia techniczne	**Zewnętrzny rozwój oprogramowania**	Ś	2,0	**Wywiad**	Zakres: zewnętrzny rozwój oprogramowania. Działanie: sformalizować i zatwierdzić istniejącą praktykę, uzupełnić brakujące elementy, zakomunikować w organizacji i przypisać właściciela. Oczekiwany dowód wdrożenia: Klauzule bezpieczeństwa w umowach z dostawcami dev + zapisy nadzoru. **	Zespół IT / Bezpieczeństwo*	1,0	

PRÓBKA, DANE FIKCYJNE

110	**A.8.31**	A.8 Zabezpieczenia techniczne	**Separacja środowisk**	Ś	2,0	**Wywiad**	Zakres: separacja środowisk. Działanie: sformalizować i zatwierdzić istniejącą praktykę, uzupełnić brakujące elementy, zakomunikować w organizacji i przypisać właściciela. Oczekiwany dowód wdrożenia: Dowód separacji środowisk dev/test/prod. **	IOD / 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.

Oznaczenia wymagań: **A.x.y** to zabezpieczenie z Załącznika A normy, **kl. X w.Y** to kolejne wymaganie klauzuli X (część główna normy, klauzule 4-10).

8 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)	6	18	1	-	**25**	**89,0**
Kierownik IT (R) / Pełnomocnik ds. SZBI (A)	4	12	1	-	**17**	**51,5**
Zespół IT / Bezpieczeństwo*	-	-	27	-	**27**	**27,0**
Zarząd / Pełnomocnik ds. SZBI*	-	-	26	-	**26**	**26,0**
Kierownik Utrzymania Ruchu (R) / Kierownik IT (A)	1	-	-	-	**1**	**8,0**
Dyrektor HR (R) / Pełnomocnik ds. SZBI (A)	-	2	-	-	**2**	**6,0**
Zarząd (A) / Prokurent ds. operacyjnych (R)	1	-	-	-	**1**	**3,0**
HR / Pełnomocnik ds. SZBI*	-	-	3	-	**3**	**3,0**
Administracja / Bezpieczeństwo fizyczne*	-	-	3	-	**3**	**3,0**
Zakupy / Pełnomocnik ds. SZBI*	-	-	2	-	**2**	**2,0**
Pełnomocnik ds. SZBI / Risk Owner*	-	-	1	-	**1**	**1,0**
Audyt wewnętrzny / Pełnomocnik ds. SZBI*	-	-	1	-	**1**	**1,0**
IOD / Pełnomocnik ds. SZBI*	-	-	1	-	**1**	**1,0**
Razem					**110**	**221,5**

PRÓBKA, DANE FIKCYJNE

> **Przeliczenie na zasoby.** Łączny nakład 221,5 dni roboczych odpowiada około **10,5 osobomiesiąca(-y)** pracy (21 dni roboczych/mies.). Realizacja siłami jednej osoby przy pełnym zaangażowaniu zajmie ok. 11 mies., przy zaangażowaniu połowy etatu ok. 21 mies. - bez uwzględnienia bieżących obowiązków tej osoby.

9 Efekt cross-framework

Wymagania ocenianej normy są zmapowane na wymagania innych regulacji. Remediacja luk z tego raportu domyka jednocześnie **35** powiązanych wymagań poniższych regulacji, co obniża łączny koszt zgodności i pozwala uniknąć dublowania prac.

Regulacja / norma	Powiązane wymagania	Odwołania
DORA	**13**	DORA art. 10, DORA art. 11, DORA art. 13, DORA art. 17, DORA art. 18, DORA art. 19, DORA art. 28, DORA art. 30, DORA art. 5, DORA art. 6, DORA art. 7, DORA art. 8, DORA art. 9
PCI DSS	**10**	PCI DSS Req 1, PCI DSS Req 10, PCI DSS Req 2, PCI DSS Req 3, PCI DSS Req 4, PCI DSS Req 5, PCI DSS Req 6, PCI DSS Req 7, PCI DSS Req 8, PCI DSS Req 9
RODO	**8**	RODO art. 17, RODO art. 24, RODO art. 28, RODO art. 30, RODO art. 32, RODO art. 33, RODO art. 39, RODO art. 5
NIS2 / UoKSC	**3**	NIS2 art. 20, NIS2 art. 21, NIS2 art. 23
ISO 22301	**1**	ISO22301 8.4

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

10 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 kl. 5 w.2 · 5. Przywództwo

K Krytyczny

Czy istnieje wyznaczona rola odpowiedzialna za SZBI (CISO / Pełnomocnik ds. bezpieczeństwa)?

Dojrzałość	1,0 / 5 - Inicjalny
Wymaganie normy	Rola CISO Powiązania: DORA art. 5, NIS2 art. 20, UoKSC art. 14
Stan obecny	Brak wyznaczonej roli odpowiedzialnej za SZBI. Bezpieczeństwo informacji jest domyślnie "u informatyków", bez umocowania, zakresu i czasu pracy.
Obserwacja konsultanta	Prezes wskazał w wywiadzie, że "bezpieczeństwem zajmuje się Pan Marek z IT". Pan Marek potwierdził, że nikt mu tego nie powierzył na piśmie, a jego priorytetem jest utrzymanie ERP i hali. Brak osoby, która zbierze wymagania ustawy i normy w jeden program.
Podstawa ustalenia	**Wywiad** Oczekiwany dowód: Akt powołania CISO / Pełnomocnika z zakresem obowiązków
Ryzyko	Bez właściciela systemu żadne z pozostałych działań remediacyjnych nie ma osoby, która je poprowadzi i rozliczy. Dla podmiotu ważnego to ryzyko niedotrzymania terminu ustawowego 3.04.2027.
Rekomendacja	Powołać Pełnomocnika ds. SZBI zarządzeniem Zarządu z zakresem odpowiedzialności, uprawnieniem do raportowania bezpośrednio do Zarządu i wymiarem czasu (co najmniej 0,25 etatu w fazie wdrożenia). Rozważyć outsourcing roli na okres wdrożenia.
Właściciel	Zarząd (A) / Pełnomocnik ds. SZBI (R)
Nakład / termin	8,0 dni rob. · termin: 15.10.2026

2 kl. 5 w.5 · 5. Przywództwo

K Krytyczny

Czy istnieje formalna, zatwierdzona Polityka Bezpieczeństwa Informacji?

Dojrzałość	1,0 / 5 - Inicjalny
Wymaganie normy	Polityka BI Powiązania: DORA art. 9, NIS2 art. 21, RODO art. 24, UoKSC art. 8 ust. 1 pkt 2 lit. a
Stan obecny	Nie ma Polityki Bezpieczeństwa Informacji. Istnieje "Regulamin korzystania z komputerów" z 2017 r., 2 strony, bez celów, zakresu i odniesienia do ryzyka.
Obserwacja konsultanta	Regulamin z 2017 r. dotyczy wyłącznie stacji roboczych biurowych i nie obejmuje hali produkcyjnej ani systemów OT. Pracownicy działu jakości nie wiedzieli o jego istnieniu.
Podstawa ustalenia	**Dokument / zapis** Regulamin korzystania z komputerów, wersja 2017 Oczekiwany dowód: Zatwierdzona Polityka Bezpieczeństwa Informacji (pkt 5.2)
Ryzyko	Bez polityki nie ma podstawy do egzekwowania zasad wobec pracowników i dostawcy IT. Ustawa o KSC wymaga udokumentowanej polityki bezpieczeństwa systemu informacyjnego (art. 8 ust. 1 pkt 2 lit. a).
Rekomendacja	Opracować i zatwierdzić Politykę Bezpieczeństwa Informacji zgodną z kl. 5.2: cele, zakres, zobowiązanie kierownictwa, ramy dla polityk szczegółowych, zasady komunikacji. Zakomunikować wszystkim pracownikom i dostawcy IT.
Właściciel	Zarząd (A) / Pełnomocnik ds. SZBI (R)
Nakład / termin	6,0 dni rob. · termin: 31.10.2026

PRÓBKA · DANE FIKCYJNE

3 kl. 6 w.1 · 6. Planowanie

K Krytyczny

Czy organizacja posiada formalny proces szacowania ryzyka bezpieczeństwa informacji?

Dojrzałość	0,0 / 5 - Nieistniejący
Wymaganie normy	Proces szacowania ryzyka Powiązania: DORA art. 6, NIS2 art. 21, RODO art. 32, UoKSC art. 8 ust. 1 pkt 1
Stan obecny	Brak jakiegokolwiek procesu szacowania ryzyka bezpieczeństwa informacji. Decyzje o zabezpieczeniach zapadają ad hoc, na wniosek IT lub po incydencie.
Obserwacja konsultanta	Zakup UTM w 2024 r. wynikał z oferty dostawcy, nie z analizy. Awaria serwera ERP w marcu 2026 r. (2 dni przestoju) nie została poddana analizie przyczyn. Kierownik IT rozpoznaje zagrożenia, ale nie ma narzędzia, żeby przedstawić je Zarządowi.
Podstawa ustalenia	**Wywiad** Oczekiwany dowód: Zatwierdzona metodyka oceny ryzyka (pkt 6.1.2)
Ryzyko	Nakłady na bezpieczeństwo omijają realne zagrożenia. Bez oceny ryzyka nie da się uzasadnić SoA ani wykazać organowi spełnienia obowiązku systematycznego szacowania ryzyka.
Rekomendacja	Przyjąć metodykę szacowania ryzyka zgodną z ISO/IEC 27005 i wymaganiami art. 8 ustawy o KSC (kryteria proporcjonalności), z matrycą prawdopodobieństwo x skutek, kryteriami akceptacji i rolą Zarządu. Przeprowadzić pierwszą ocenę dla systemów wspierających usługę objętą ustawą (ERP, SCADA, poczta, sieć zakładowa).
Właściciel	Zarząd (A) / Pełnomocnik ds. SZBI (R)
Nakład / termin	10,0 dni rob. · termin: 30.11.2026

4 kl. 6 w.3 · 6. Planowanie

K Krytyczny

Czy prowadzony jest rejestr ryzyk zawierający właścicieli ryzyk, poziomy, opcje postępowania?

Dojrzałość	0,0 / 5 - Nieistniejący
Wymaganie normy	Rejestr ryzyk Powiązania: DORA art. 6, UoKSC art. 8 ust. 1 pkt 1
Stan obecny	Brak rejestru ryzyk.
Obserwacja konsultanta	Nie istnieje żaden dokument lub arkusz pełniący tę funkcję. Lista "problemów IT" w notatniku Kierownika IT nie ma ocen ani właścicieli.
Podstawa ustalenia	**Wywiad** Oczekiwany dowód: Rejestr ryzyk z właścicielami i poziomami ryzyka
Ryzyko	Brak rejestru oznacza brak dowodu, że Zarząd wie, jakie ryzyka akceptuje. Przy kontroli organu to pierwsze pytanie.
Rekomendacja	Utworzyć rejestr ryzyk jako produkt pierwszej oceny: scenariusz, aktywo, właściciel, ocena inherentna i rezydualna, opcja postępowania, termin przeglądu. Zarząd zatwierdza rejestr i akceptuje ryzyka pozostałe.
Właściciel	Zarząd (A) / Pełnomocnik ds. SZBI (R)
Nakład / termin	4,0 dni rob. · termin: 30.11.2026

5 kl. 6 w.5 · 6. Planowanie

K Krytyczny

Czy istnieje Plan Postępowania z Ryzykiem (PPR) z przypisanymi terminami i właścicielami?

Dojrzałość	0,0 / 5 - Nieistniejący
Wymaganie normy	PPR Powiązania: DORA art. 6, UoKSC art. 8 ust. 1 pkt 1
Stan obecny	Brak Planu Postępowania z Ryzykiem.
Obserwacja konsultanta	Działania naprawcze po awarii ERP (nowy serwer, drugi UPS) zrealizowano, ale bez powiązania z jakąkolwiek oceną i bez decyzji, co z pozostałymi ryzykami.
Podstawa ustalenia	**Wywiad** Oczekiwany dowód: Plan Postępowania z Ryzykiem z terminami i właścicielami (pkt 6.1.3)
Ryzyko	Bez PPR nie ma mechanizmu, który zamienia ocenę ryzyka w budżet i zadania. Certyfikacja i kontrola sprawdzają właśnie to powiązanie.
Rekomendacja	Opracować PPR jako wynik oceny ryzyka: działania, właściciele, terminy, nakłady, kontrole z Aneksu A. PPR zatwierdza Zarząd i przegląda go kwartalnie.
Właściciel	Zarząd (A) / Pełnomocnik ds. SZBI (R)
Nakład / termin	4,0 dni rob. · termin: 15.12.2026

PRÓBKA. DANE FIKCYJNE

6 kl. 6 w.6 · 6. Planowanie

K Krytyczny

Czy organizacja posiada Deklarację Stosowania (SoA) - nawet nieformalną lub częściową?

Dojrzałość	0,0 / 5 - Nieistniejący
Wymaganie normy	SoA
Stan obecny	Brak Deklaracji Stosowania.
Obserwacja konsultanta	Pojęcie SoA było nieznane rozmówcom. Wyłączenia (własny rozwój oprogramowania, maskowanie danych) da się uzasadnić od razu na podstawie profilu firmy.
Podstawa ustalenia	**Wywiad** Oczekiwany dowód: Deklaracja Stosowania z uzasadnieniami włączeń i wyłączeń (pkt 6.1.3 d)
Ryzyko	SoA jest dokumentem obowiązkowym normy (kl. 6.1.3 d). Bez niego nie ma zakresu zabezpieczeń, wobec którego audytor lub organ może cokolwiek ocenić.
Rekomendacja	Opracować SoA dla 93 zabezpieczeń Aneksu A z uzasadnieniem stosowania lub wyłączenia każdej kontroli, powiązaną z rejestrem ryzyk i PPR. Utrzymywać w narzędziu, nie w arkuszu bez wersjonowania.
Właściciel	Zarząd (A) / Pełnomocnik ds. SZBI (R)
Nakład / termin	5,0 dni rob. · termin: 31.12.2026

7 kl. 8 w.2 · 8. Działania operacyjne

K Krytyczny

Czy organizacja nadzoruje dostawców i usługi zewnętrzne w zakresie bezpieczeństwa?

Dojrzałość	1,0 / 5 - Inicjalny
Wymaganie normy	Nadzór dostawców Powiązania: DORA art. 28, NIS2 art. 21, RODO art. 28
Stan obecny	Dostawca IT (umowa serwisowa z 2019 r.) ma pełny dostęp administracyjny do serwerów, ERP i UTM bez klauzul bezpieczeństwa, bez rejestru czynności i bez prawa kontroli.
Obserwacja konsultanta	Dostawca łączy się przez współdzielone konto "serwis" z hasłem znanym trzem osobom po jego stronie. Firma nie wie, kto i kiedy był na serwerze. Umowa nie zawiera słowa "bezpieczeństwo".
Podstawa ustalenia	**Obserwacja** Konfiguracja UTM i AD, sesja zdalna w trakcie wizyty Oczekiwany dowód: Zapisy nadzoru nad dostawcami: oceny, przeglądy umów
Ryzyko	Nadzór nad dostawcą jest wymagany wprost przez ustawę (łańcuch dostaw, lit. e) i normę (kl. 8.1, A.5.19 do A.5.22). Współdzielone konto administratora zewnętrznego to najkrótsza droga do incydentu, którego nie da się nawet przypisać.
Rekomendacja	Aneksować umowę z dostawcą IT: zakres usług, wymagania bezpieczeństwa, obowiązek zgłaszania incydentów w czasie pozwalającym dotrzymać terminów ustawowych, imienne konta, logowanie sesji zdalnych, prawo audytu, zasady podwykonawstwa. Wdrożyć rejestr dostępów zdalnych dostawcy.
Właściciel	Kierownik IT (R) / Pełnomocnik ds. SZBI (A)
Nakład / termin	6,0 dni rob. · termin: 30.11.2026

8 A.5.19 · A.5 Zabezpieczenia organizacyjne

K Krytyczny

A.5.19 Bezpieczeństwo w relacjach z dostawcami

Dojrzałość	1,0 / 5 - Inicjalny
Wymaganie normy	Zarządzanie ryzykiem związanym z dostawcami. Powiązania: DORA art. 28, NIS2 art. 21, RODO art. 28, UoKSC art. 8 ust. 1 pkt 2 lit. e
Stan obecny	Brak zasad bezpieczeństwa w relacjach z dostawcami: nie ma listy dostawców z dostępem do informacji ani oceny ich ryzyka.
Obserwacja konsultanta	Poza dostawcą IT zdalny dostęp do SCADA ma producent linii pakującej (Włochy) przez router GSM zainstalowany w 2021 r. Nikt w firmie nie wie, czy jest aktywny.
Podstawa ustalenia	**Obserwacja** Router GSM na linii L2, oględziny hali Oczekiwany dowód: Polityka bezpieczeństwa w relacjach z dostawcami
Ryzyko	Nieznane wejścia do sieci OT to bezpośrednie zagrożenie ciągłości produkcji, czyli usługi objętej ustawą.
Rekomendacja	Sporządzić rejestr dostawców z dostępem do systemów lub danych (IT, ERP, SCADA, księgowość zewnętrzna, kurier dokumentów), sklasyfikować wg krytyczności i objąć wymaganiami adekwatnymi do klasy.
Właściciel	Kierownik IT (R) / Pełnomocnik ds. SZBI (A)
Nakład / termin	4,0 dni rob. · termin: 30.11.2026

PRÓBKA. DANE FIKCYJNE

9 A.5.20 · A.5 Zabezpieczenia organizacyjne

K Krytyczny

A.5.20 Bezpieczeństwo w umowach z dostawcami

Dojrzałość	1,0 / 5 - Inicjalny
Wymaganie normy	Klauzule bezpieczeństwa w umowach z dostawcami. Powiązania: DORA art. 30, RODO art. 28, UoKSC art. 8 ust. 1 pkt 2 lit. e
Stan obecny	Umowy z dostawcami IT i OT nie zawierają wymagań bezpieczeństwa.
Obserwacja konsultanta	Dział zakupów używa wzoru umowy z 2016 r. Prawnik obsługujący firmę jest gotów opracować załącznik na podstawie dostarczonego przez nas wzorca.
Podstawa ustalenia	**Dokument / zapis** Wzór umowy serwisowej 2016 Oczekiwany dowód: Umowy z klauzulami bezpieczeństwa (próbka)
Ryzyko	Bez klauzul firma nie ma podstawy, żeby wymagać od dostawcy IT zgłaszania incydentów w 24 h, co uniemożliwia dotrzymanie terminu wczesnego ostrzeżenia z ustawy.
Rekomendacja	Wprowadzić standardowy załącznik bezpieczeństwa do umów z dostawcami klasy krytycznej i ważnej, w tym zgłaszanie incydentów, dostęp imienny, prawo audytu, poufność, zasady zakończenia współpracy.
Właściciel	Zarząd (A) / Prokurent ds. operacyjnych (R)
Nakład / termin	3,0 dni rob. · termin: 31.12.2026

10 A.5.24 · A.5 Zabezpieczenia organizacyjne

K Krytyczny

A.5.24 Planowanie obsługi incydentów

Dojrzałość	1,0 / 5 - Inicjalny
Wymaganie normy	Procedury zarządzania incydentami bezpieczeństwa. Powiązania: DORA art. 17, NIS2 art. 23, RODO art. 33, UoKSC art. 8 ust. 1 pkt 4
Stan obecny	Brak procedury obsługi incydentów. Zdarzenia zgłaszane są telefonicznie do Kierownika IT i nie są rejestrowane.
Obserwacja konsultanta	Incydent z lutego 2026 r. (zaszyfrowany komputer w dziale konstrukcyjnym, prawdopodobnie ransomware zatrzymane przez antywirus) nie został nigdzie odnotowany. Nikt nie rozważał, czy podlega zgłoszeniu.
Podstawa ustalenia	**Wywiad** Oczekiwany dowód: Plan i procedura obsługi incydentów
Ryzyko	Podmiot ważny bez procedury nie jest w stanie dotrzymać 24-godzinnego terminu wczesnego ostrzeżenia. Brak rejestru uniemożliwia też wykazanie organowi, że incydenty są obsługiwane.
Rekomendacja	Opracować procedurę zarządzania incydentami z klasyfikacją (w tym kryteria incydentu poważnego wg ustawy), rejestrem, rolami, kanałem zgłoszeń dla pracowników, terminami zgłoszeń do CSIRT NASK (24 h, 72 h, miesiąc) i osobami do kontaktu.
Właściciel	Kierownik IT (R) / Pełnomocnik ds. SZBI (A)
Nakład / termin	5,0 dni rob. · termin: 30.11.2026

11 A.8.8 · A.8 Zabezpieczenia techniczne

K Krytyczny · Quick Win

A.8.8 Zarządzanie podatnościami technicznymi

Dojrzałość	1,0 / 5 - Inicjalny
Wymaganie normy	Skanowanie podatności, patching, SLA dla krytycznych podatności. Powiązania: DORA art. 9, NIS2 art. 21, PCI DSS Req 6, UoKSC art. 8 ust. 1 pkt 5 lit. d
Stan obecny	Brak zarządzania podatnościami. Aktualizacje serwerów wykonuje dostawca IT "gdy jest okazja", stacje robocze mają wyłączone aktualizacje automatyczne, SCADA nie był aktualizowany od instalacji.
Obserwacja konsultanta	UTM działa na firmware z 2023 r. z dwiema publicznie znanymi podatnościami VPN. Serwer ERP: Windows Server 2016 bez poprawek od 8 miesięcy. Kierownik IT wie o problemie, ale nie ma okna serwisowego na hali.
Podstawa ustalenia	**Obserwacja** Panel UTM, wersja firmware; Windows Update na ERP-SRV01 Oczekiwany dowód: Raporty skanów podatności + SLA łatania
Ryzyko	Niezałatane urządzenie brzegowe z VPN to najczęstsza droga wejścia ransomware do firm produkcyjnych. Skutek: zatrzymanie produkcji i incydent poważny z obowiązkiem zgłoszenia.
Rekomendacja	Wdrożyć proces: inwentaryzacja wersji, skan podatności co najmniej kwartalnie, okna serwisowe, priorytety wg CVSS i ekspozycji, osobna ścieżka dla OT uzgodniona z producentem linii. Zacząć od systemów wystawionych do internetu (UTM, VPN, poczta).
Właściciel	Kierownik IT (R) / Pełnomocnik ds. SZBI (A)
Nakład / termin	6,0 dni rob. · termin: 31.10.2026

PRÓBKA, DANE FIKCYJNE

12 A.8.22 · A.8 Zabezpieczenia techniczne

K Krytyczny

A.8.22 Segregacja sieci

Dojrzałość	1,0 / 5 - Inicjalny
Wymaganie normy	VLAN, DMZ, separacja środowisk (prod/dev/test/guest). Powiązania: PCI DSS Req 1
Stan obecny	Sieć OT (SCADA, sterowniki linii) jest w jednej sieci z biurem i Wi-Fi gości.
Obserwacja konsultanta	Laptop gościa podłączony do Wi-Fi w sali konferencyjnej widział adresy sterowników linii L1 i L2 (test w obecności Kierownika IT). Producent linii ma dostęp przez router GSM poza kontrolą firmy.
Podstawa ustalenia	**Obserwacja** Skan sieci z Wi-Fi gości w trakcie wizyty Oczekiwany dowód: Schemat segmentacji sieci + reguły zapór
Ryzyko	Płaska sieć oznacza, że każdy incydent w biurze może zatrzymać produkcję. To główny scenariusz ryzyka dla usługi objętej ustawą.
Rekomendacja	Zaprojektować segmentację: VLAN dla OT z jednokierunkowym dostępem serwisowym przez jump host, osobna sieć gości, sieć biurowa. Dostęp producenta linii przez firmowy VPN z MFA zamiast routera GSM.
Właściciel	Kierownik Utrzymania Ruchu (R) / Kierownik IT (A)
Nakład / termin	8,0 dni rob. · termin: 31.12.2026

13 kl. 4 w.9 · 4. Kontekst organizacji

W Wysoki

Czy zakres jest udokumentowany i zatwierdzony przez kierownictwo?

Dojrzałość	0,0 / 5 - Nieistniejący
Wymaganie normy	Zatwierdzenie zakresu
Stan obecny	Nie spełniono: zakres jest udokumentowany i zatwierdzony przez kierownictwo.
Obserwacja konsultanta	Wymaganie pochodne wobec zakresu SZBI: zostanie spełnione w ramach dokumentacji zakresu i kontekstu (etap planowania).
Podstawa ustalenia	**Wywiad** Oczekiwany dowód: Zakres SZBI zatwierdzony przez kierownictwo (podpis, data)
Ryzyko	Istotne. Luka "zatwierdzenie zakresu" wymaga usunięcia przed oceną zewnętrzną. W praktyce: brak nadzorowanej dokumentacji uniemożliwia wykazanie zgodności i spójne działanie organizacji.
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 kl. 5 w.8 · 5. Przywództwo

W Wysoki

Czy Polityka BI zawiera cele bezpieczeństwa informacji lub ramy ich wyznaczania oraz zobowiązanie do spełnienia mających zastosowanie wymagań (pkt 5.2 lit. b-c)?

Dojrzałość	0,0 / 5 - Nieistniejący
Wymaganie normy	Treść polityki (5.2) Powiązania: DORA art. 9, UoKSC art. 8 ust. 1 pkt 2 lit. a
Stan obecny	Nie spełniono: Polityka BI zawiera cele bezpieczeństwa informacji lub ramy ich wyznaczania oraz zobowiązanie do spełnienia mających zastosowanie wymagań (pkt 5.2 lit. b-c).
Obserwacja konsultanta	Wynika z braku Polityki BI (c5-5); zostanie spełnione w ramach jej opracowania.
Podstawa ustalenia	**Wywiad** Oczekiwany dowód: Polityka BI z celami lub ramami ich wyznaczania i zobowiązaniem do spełnienia wymagań (pkt 5.2 lit. b-c)
Ryzyko	Istotne. Luka "treść polityki (5.2)" wymaga usunięcia przed oceną zewnętrzną. W praktyce: bez celów i mierników nie da się ocenić, czy nakłady na bezpieczeństwo przynoszą efekt, ani wykazać tego kierownictwu.
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

15 **kl. 6 w.2 · 6. Planowanie** W Wysoki

Czy określono kryteria oceny i akceptacji ryzyka?

Dojrzałość	0,0 / 5 - Nieistniejący
Wymaganie normy	Kryteria ryzyka Powiązania: DORA art. 6, UoKSC art. 8 ust. 1 pkt 1
Stan obecny	Nie spełniono: określono kryteria oceny i akceptacji ryzyka.
Obserwacja konsultanta	Wynika z braku procesu szacowania ryzyka (c6-1); produkt pierwszej oceny ryzyka i PPR.
Podstawa ustalenia	**Wywiad** Oczekiwany dowód: Kryteria oceny i akceptacji ryzyka w metodyce
Ryzyko	Istotne. Luka "kryteria ryzyka" 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

16 **kl. 6 w.4 · 6. Planowanie** W Wysoki

Czy zidentyfikowano ryzyka dla poufności, integralności i dostępności aktywów informacyjnych?

Dojrzałość	0,0 / 5 - Nieistniejący
Wymaganie normy	Ryzyka CIA Powiązania: DORA art. 8
Stan obecny	Nie spełniono: zidentyfikowano ryzyka dla poufności, integralności i dostępności aktywów informacyjnych.
Obserwacja konsultanta	Wynika z braku procesu szacowania ryzyka (c6-1); produkt pierwszej oceny ryzyka i PPR.
Podstawa ustalenia	**Wywiad** Oczekiwany dowód: Wyniki oceny ryzyka CIA (zapisy, pkt 8.2)
Ryzyko	Istotne. Luka "ryzyka CIA" wymaga usunięcia przed oceną zewnętrzną. W praktyce: nieodbierane lub nadmiarowe uprawnienia (w tym osierocone konta po odejściach) umożliwiają nieautoryzowany dostęp do systemów i danych.
Rekomendacja	Patrz działanie nadrzędne wskazane w obserwacji.
Właściciel	Zarząd (A) / Pełnomocnik ds. SZBI (R)
Nakład / termin	2,0 dni rob. · termin: 28.02.2027

17 **kl. 6 w.7 · 6. Planowanie** W Wysoki

Czy organizacja ustanowiła mierzalne cele bezpieczeństwa informacji, udokumentowane, monitorowane, komunikowane i aktualizowane (pkt 6.2)?

Dojrzałość	0,0 / 5 - Nieistniejący
Wymaganie normy	Cele BI
Stan obecny	Nie spełniono: organizacja ustanowiła mierzalne cele bezpieczeństwa informacji, udokumentowane, monitorowane, komunikowane i aktualizowane (pkt 6.2).
Obserwacja konsultanta	Wynika z braku procesu szacowania ryzyka (c6-1); produkt pierwszej oceny ryzyka i PPR.
Podstawa ustalenia	**Wywiad** Oczekiwany dowód: Udokumentowane cele bezpieczeństwa informacji (pkt 6.2)
Ryzyko	Istotne. Luka "cele BI" wymaga usunięcia przed oceną zewnętrzną. W praktyce: bez logów i monitorowania incydent zostanie wykryty późno lub wcale, a analiza powłamaniowa będzie niemożliwa.
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

18 **kl. 6 w.8 · 6. Planowanie** W Wysoki

Czy cele są powiązane z polityką bezpieczeństwa i wynikami oceny ryzyka?

Dojrzałość	0,0 / 5 - Nieistniejący
Wymaganie normy	Powiązanie celów
Stan obecny	Nie spełniono: cele są powiązane z polityką bezpieczeństwa i wynikami oceny ryzyka.
Obserwacja konsultanta	Wynika z braku procesu szacowania ryzyka (c6-1); produkt pierwszej oceny ryzyka i PPR.
Podstawa ustalenia	**Wywiad** Oczekiwany dowód: Powiązanie celów z polityką i wynikami oceny ryzyka (mapa, tabela)
Ryzyko	Istotne. Luka "powiązanie celów" 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

19 **kl. 6 w.9 · 6. Planowanie** W Wysoki

Czy istnieje plan osiągania celów z przypisanymi zasobami i terminami?

Dojrzałość	0,0 / 5 - Nieistniejący
Wymaganie normy	Plan celów
Stan obecny	Nie spełniono: istnieje plan osiągania celów z przypisanymi zasobami i terminami.
Obserwacja konsultanta	Wynika z braku procesu szacowania ryzyka (c6-1); produkt pierwszej oceny ryzyka i PPR.
Podstawa ustalenia	**Wywiad** Oczekiwany dowód: Plan osiągania celów: zasoby, terminy, odpowiedzialni
Ryzyko	Istotne. Luka "plan celów" wymaga usunięcia przed oceną zewnętrzną.
Rekomendacja	Patrz działanie nadrzędne wskazane w obserwacji.
Właściciel	Zarząd (A) / Pełnomocnik ds. SZBI (R)
Nakład / termin	2,0 dni rob. · termin: 28.02.2027

20 **kl. 7 w.4 · 7. Wsparcie** W Wysoki

Czy pracownicy przechodzą regularne szkolenia z bezpieczeństwa informacji (onboarding + cykliczne)?

Dojrzałość	1,0 / 5 - Inicjalny
Wymaganie normy	Szkolenia Powiązania: DORA art. 13, NIS2 art. 20, RODO art. 39, UoKSC art. 8 ust. 1 pkt 2 lit. i
Stan obecny	Brak szkoleń z bezpieczeństwa informacji. Jedyne szkolenie to instruktaż BHP.
Obserwacja konsultanta	W wywiadach 4 z 6 pracowników biura nie potrafiło wskazać, komu zgłosić podejrzany e-mail. Dział sprzedaży używa prywatnych telefonów do poczty firmowej bez żadnych zasad.
Podstawa ustalenia	**Wywiad** Oczekiwany dowód: Rejestr szkoleń z datami i listami obecności
Ryzyko	Istotne. Luka "szkolenia" wymaga usunięcia przed oceną zewnętrzną. W praktyce: personel nieprzeszkolony jest najtańszym wektorem ataku (phishing, socjotechnika) i źródłem naruszeń nieumyślnych.
Rekomendacja	Wdrożyć roczny program szkoleń: szkolenie wstępne dla wszystkich (2 h), moduł dla kierownictwa wymagany przez ustawę, moduł dla operatorów OT, symulacja phishingu dwa razy w roku. Rejestrować obecność i wyniki.
Właściciel	Dyrektor HR (R) / Pełnomocnik ds. SZBI (A)
Nakład / termin	3,0 dni rob. · termin: 31.01.2027

PRÓBKA, DANE FIKCYJNE

21 kl. 7 w.8 · 7. Wsparcie

W Wysoki

Czy organizacja posiada komplet dokumentów wymaganych przez ISO 27001 (polityki, procedury, rejestry)?

Dojrzałość	1,0 / 5 - Inicjalny
Wymaganie normy	Dokumentacja SZBI Powiązania: UoKSC art. 10
Stan obecny	Poza regulaminem z 2017 r. i dokumentacją RODO z 2019 r. nie ma dokumentów wymaganych przez normę.
Obserwacja konsultanta	Dokumentacja RODO jest dobrej jakości (kancelaria zewnętrzna) i może być fundamentem: rejestr czynności, klauzule, procedura naruszeń. Warto ją włączyć do SZBI zamiast tworzyć równoległy zestaw.
Podstawa ustalenia	**Dokument / zapis** Dokumentacja RODO 2019, rejestr czynności przetwarzania Oczekiwany dowód: Wykaz udokumentowanych informacji SZBI (pkt 7.5)
Ryzyko	Istotne. Luka "dokumentacja SZBI" wymaga usunięcia przed oceną zewnętrzną. W praktyce: brak nadzorowanej dokumentacji uniemożliwia wykazanie zgodności i spójne działanie organizacji.
Rekomendacja	Zbudować komplet dokumentacji SZBI w kolejności: polityka, zakres, metodyka ryzyka, rejestr ryzyk, PPR, SoA, procedury operacyjne (incydenty, dostęp, kopie zapasowe, zmiany, dostawcy, ciągłość).
Właściciel	Zarząd (A) / Pełnomocnik ds. SZBI (R)
Nakład / termin	12,0 dni rob. · termin: 28.02.2027

22 kl. 8 w.4 · 8. Działania operacyjne

W Wysoki

Czy ocena ryzyka jest przeprowadzana cyklicznie lub przy znaczących zmianach?

Dojrzałość	0,0 / 5 - Nieistniejący
Wymaganie normy	Cykliczna ocena ryzyka Powiązania: DORA art. 6, UoKSC art. 8 ust. 1 pkt 1
Stan obecny	Nie spełniono: ocena ryzyka jest przeprowadzana cyklicznie lub przy znaczących zmianach.
Obserwacja konsultanta	Wynika z braku procesu szacowania ryzyka (c6-1); realizowane po pierwszej ocenie.
Podstawa ustalenia	**Wywiad** Oczekiwany dowód: Zapisy cyklicznych ocen ryzyka z datami (pkt 8.2)
Ryzyko	Istotne. Luka "cykliczna ocena ryzyka" 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

23 kl. 8 w.5 · 8. Działania operacyjne

W Wysoki

Czy działania z planu postępowania z ryzykiem są faktycznie wdrażane i śledzone?

Dojrzałość	0,0 / 5 - Nieistniejący
Wymaganie normy	Wdrażanie PPR
Stan obecny	Nie spełniono: działania z planu postępowania z ryzykiem są faktycznie wdrażane i śledzone.
Obserwacja konsultanta	Wynika z braku procesu szacowania ryzyka (c6-1); realizowane po pierwszej ocenie.
Podstawa ustalenia	**Wywiad** Oczekiwany dowód: Zapisy realizacji planu postępowania z ryzykiem (pkt 8.3)
Ryzyko	Istotne. Luka "wdrażanie PPR" 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

24 kl. 9 w.1 · 9. Ocena wyników

W Wysoki

Czy organizacja mierzy skuteczność SZBI - czy istnieją wskaźniki (KPI/KRI) bezpieczeństwa?

Dojrzałość	0,0 / 5 - Nieistniejący
Wymaganie normy	Monitorowanie i pomiary Powiązania: DORA art. 13, UoKSC art. 8 ust. 1 pkt 2 lit. h
Stan obecny	Nie spełniono: organizacja mierzy skuteczność SZBI - czy istnieją wskaźniki (KPI/KRI) bezpieczeństwa.
Obserwacja konsultanta	Brak jakichkolwiek mechanizmów pomiaru i przeglądu SZBI; adresowane po wdrożeniu dokumentacji (audyt wewnętrzny c9-3, przegląd zarządzania c9-5).
Podstawa ustalenia	**Wywiad** Oczekiwany dowód: Zdefiniowane wskaźniki KPI/KRI + wyniki pomiarów (pkt 9.1)
Ryzyko	Istotne. Luka "monitorowanie i pomiary" wymaga usunięcia przed oceną zewnętrzną. W praktyce: bez celów i mierników nie da się ocenić, czy nakłady na bezpieczeństwo przynoszą efekt, ani wykazać tego kierownictwu.
Rekomendacja	Patrz działanie nadrzędne wskazane w obserwacji.
Właściciel	Zarząd (A) / Pełnomocnik ds. SZBI (R)
Nakład / termin	2,0 dni rob. · termin: 28.02.2027

25 kl. 9 w.3 · 9. Ocena wyników

W Wysoki

Czy organizacja przeprowadza lub planuje przeprowadzać audyty wewnętrzne SZBI?

Dojrzałość	0,0 / 5 - Nieistniejący
Wymaganie normy	Audyt wewnętrzny Powiązania: DORA art. 6, NIS2 art. 21, UoKSC art. 8 ust. 1 pkt 2 lit. h
Stan obecny	Brak audytu wewnętrznego SZBI. Nigdy nie przeprowadzono.
Obserwacja konsultanta	Firma ma doświadczenie z audytami jakości (ISO 9001 od 2015 r.) i rozumie mechanizm. Program audytów jakości można rozszerzyć o SZBI.
Podstawa ustalenia	**Dokument / zapis** Program audytów ISO 9001 2026 Oczekiwany dowód: Raporty z przeprowadzonych audytów wewnętrznych (pkt 9.2)
Ryzyko	Istotne. Luka "audyt wewnętrzny" wymaga usunięcia przed oceną zewnętrzną. W praktyce: kierownictwo nie ma zweryfikowanej informacji o skuteczności zabezpieczeń i nie może zarządzać systemem.
Rekomendacja	Zaplanować pierwszy audyt wewnętrzny po wdrożeniu dokumentacji i minimum 2 miesiącach działania systemu, przez audytora niezależnego od wdrożenia.
Właściciel	Zarząd (A) / Pełnomocnik ds. SZBI (R)
Nakład / termin	3,0 dni rob. · termin: 30.04.2027

26 kl. 9 w.4 · 9. Ocena wyników

W Wysoki

Czy istnieje program audytów wewnętrznych z harmonogramem?

Dojrzałość	0,0 / 5 - Nieistniejący
Wymaganie normy	Program audytów
Stan obecny	Nie spełniono: istnieje program audytów wewnętrznych z harmonogramem.
Obserwacja konsultanta	Brak jakichkolwiek mechanizmów pomiaru i przeglądu SZBI; adresowane po wdrożeniu dokumentacji (audyt wewnętrzny c9-3, przegląd zarządzania c9-5).
Podstawa ustalenia	**Wywiad** Oczekiwany dowód: Program audytów wewnętrznych z harmonogramem (pkt 9.2.2)
Ryzyko	Istotne. Luka "program audytów" wymaga usunięcia przed oceną zewnętrzną. W praktyce: kierownictwo nie ma zweryfikowanej informacji o skuteczności zabezpieczeń i nie może zarządzać systemem.
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

27 kl. 9 w.5 · 9. Ocena wyników

W Wysoki · Quick Win

Czy najwyższe kierownictwo przeprowadza przeglądy zarządzania SZBI w zaplanowanych odstępach czasu?

Dojrzałość	0,0 / 5 - Nieistniejący
Wymaganie normy	Przegląd zarządzania Powiązania: NIS2 art. 20, UoKSC art. 8d
Stan obecny	Przegląd zarządzania nie obejmuje bezpieczeństwa informacji.
Obserwacja konsultanta	Przegląd zarządzania jakości odbywa się co roku w styczniu, z protokołem. Dodanie części SZBI to niewielki nakład przy dużym efekcie dowodowym.
Podstawa ustalenia	**Dokument / zapis** Protokół przeglądu zarządzania ISO 9001, styczeń 2026 Oczekiwany dowód: Protokoły przeglądów zarządzania z decyzjami (pkt 9.3)
Ryzyko	Istotne. Luka "przegląd zarządzania" wymaga usunięcia przed oceną zewnętrzną. W praktyce: kierownictwo nie ma zweryfikowanej informacji o skuteczności zabezpieczeń i nie może zarządzać systemem.
Rekomendacja	Rozszerzyć istniejący roczny przegląd zarządzania ISO 9001 o wejścia z kl. 9.3 ISO 27001: wyniki oceny ryzyka, incydenty, audyty, cele, dostawcy. Protokół z decyzjami Zarządu.
Właściciel	Zarząd (A) / Pełnomocnik ds. SZBI (R)
Nakład / termin	1,0 dni rob. · termin: 31.01.2027

28 kl. 9 w.6 · 9. Ocena wyników

W Wysoki

Czy przegląd zarządzania obejmuje wymagane wejścia (w tym zmiany potrzeb i oczekiwań stron zainteresowanych, pkt 9.3.2) i udokumentowane wyjścia (pkt 9.3.3)?

Dojrzałość	0,0 / 5 - Nieistniejący
Wymaganie normy	Wejścia i wyjścia przeglądu (9.3)
Stan obecny	Nie spełniono: przegląd zarządzania obejmuje wymagane wejścia (w tym zmiany potrzeb i oczekiwań stron zainteresowanych, pkt 9.3.2) i udokumentowane wyjścia (pkt 9.3.3).
Obserwacja konsultanta	Brak jakichkolwiek mechanizmów pomiaru i przeglądu SZBI; adresowane po wdrożeniu dokumentacji (audyt wewnętrzny c9-3, przegląd zarządzania c9-5).
Podstawa ustalenia	**Wywiad** Oczekiwany dowód: Protokół przeglądu zarządzania z kompletem wejść 9.3.2 i udokumentowanymi wyjściami 9.3.3
Ryzyko	Istotne. Luka "wejścia i wyjścia przeglądu (9.3)" wymaga usunięcia przed oceną zewnętrzną. W praktyce: system budowany bez spisanego kontekstu nie pokryje realnych zobowiązań umownych i prawnych organizacji.
Rekomendacja	Patrz działanie nadrzędne wskazane w obserwacji.
Właściciel	Zarząd (A) / Pełnomocnik ds. SZBI (R)
Nakład / termin	2,0 dni rob. · termin: 28.02.2027

29 A.5.1 · A.5 Zabezpieczenia organizacyjne

W Wysoki

A.5.1 Polityki bezpieczeństwa informacji

Dojrzałość	1,0 / 5 - Inicjalny
Wymaganie normy	Zestaw polityk zatwierdzonych przez kierownictwo, opublikowanych i zakomunikowanych. Powiązania: DORA art. 9, NIS2 art. 21, UoKSC art. 8 ust. 1 pkt 2 lit. a
Stan obecny	Brak zestawu polityk szczegółowych.
Obserwacja konsultanta	Zasady istnieją w praktyce (np. backup robiony codziennie), ale nie są spisane, więc zależą od jednej osoby.
Podstawa ustalenia	**Wywiad** Oczekiwany dowód: Zatwierdzone i zakomunikowane polityki tematyczne
Ryzyko	Istotne. Luka "polityki bezpieczeństwa informacji" wymaga usunięcia przed oceną zewnętrzną. W praktyce: brak nadzorowanej dokumentacji uniemożliwia wykazanie zgodności i spójne działanie organizacji.
Rekomendacja	Po zatwierdzeniu polityki nadrzędnej opracować polityki: kontroli dostępu, kopii zapasowych, pracy zdalnej i urządzeń mobilnych, dostawców, klasyfikacji informacji, kryptografii, zarządzania zmianą. Zwięzłe, 2 do 4 stron każda.
Właściciel	Zarząd (A) / Pełnomocnik ds. SZBI (R)
Nakład / termin	6,0 dni rob. · termin: 31.01.2027

PRÓBKA, DANE FIKCYJNE

30 A.5.7 · A.5 Zabezpieczenia organizacyjne

W Wysoki · Quick Win

A.5.7 Threat intelligence

Dojrzałość	1,0 / 5 - Inicjalny
Wymaganie normy	Zbieranie i analiza informacji o zagrożeniach. Powiązania: DORA art. 13, NIS2 art. 21, UoKSC art. 8 ust. 1 pkt 3
Stan obecny	Brak zorganizowanego pozyskiwania informacji o zagrożeniach i podatnościach.
Obserwacja konsultanta	Kierownik IT śledzi kilka portali branżowych prywatnie. Wymaganie ustawy (zbieranie informacji o cyberzagrożeniach) da się spełnić małym nakładem.
Podstawa ustalenia	**Wywiad** Oczekiwany dowód: Źródła threat intelligence + zapisy analiz zagrożeń
Ryzyko	Istotne. Luka "threat intelligence" wymaga usunięcia przed oceną zewnętrzną. W praktyce: znane, niezałatane podatności są wykorzystywane masowo i automatycznie; czas ekspozycji rośnie z każdym tygodniem.
Rekomendacja	Zapisać firmę do komunikatów CSIRT NASK i producentów (UTM, ERP, SCADA), wyznaczyć osobę przeglądającą je co tydzień, powiązać z procesem podatności.
Właściciel	Kierownik IT (R) / Pełnomocnik ds. SZBI (A)
Nakład / termin	1,0 dni rob. · termin: 31.10.2026

31 A.5.9 · A.5 Zabezpieczenia organizacyjne

W Wysoki

A.5.9 Inwentaryzacja aktywów

Dojrzałość	2,0 / 5 - Powtarzalny
Wymaganie normy	Rejestr aktywów informacyjnych z przypisanymi właścicielami. Powiązania: DORA art. 8, RODO art. 30, UoKSC art. 8 ust. 1 pkt 2 lit. m
Stan obecny	Inwentaryzacja aktywów obejmuje tylko sprzęt biurowy (ewidencja środków trwałych). Brak inwentaryzacji systemów, danych, urządzeń OT i usług chmurowych.
Obserwacja konsultanta	Ewidencja księgowa jest kompletna dla sprzętu. Brakuje warstwy informacyjnej. Lista systemów powstała w trakcie wywiadu w 40 minut, co pokazuje, że nakład jest niewielki.
Podstawa ustalenia	**Dokument / zapis** Ewidencja środków trwałych 2026 Oczekiwany dowód: Rejestr aktywów informacyjnych z właścicielami
Ryzyko	Istotne. Luka "inwentaryzacja aktywów" wymaga usunięcia przed oceną zewnętrzną. W praktyce: odpowiedzialność za konfigurację usług chmurowych leży po stronie organizacji; błędna konfiguracja jest dziś częstszą przyczyną wycieków niż włamania.
Rekomendacja	Sporządzić rejestr aktywów informacyjnych z właścicielami i klasyfikacją: systemy (ERP, SCADA, M365, CAD), zbiory danych, urządzenia sieciowe i OT, usługi zewnętrzne.
Właściciel	Kierownik IT (R) / Pełnomocnik ds. SZBI (A)
Nakład / termin	3,0 dni rob. · termin: 30.11.2026

32 A.5.12 · A.5 Zabezpieczenia organizacyjne

W Wysoki

A.5.12 Klasyfikacja informacji

Dojrzałość	1,0 / 5 - Inicjalny
Wymaganie normy	Klasyfikacja informacji wg wartości, wrażliwości i wymagań. Powiązania: RODO art. 32, UoKSC art. 8 ust. 1 pkt 2 lit. m
Stan obecny	Brak klasyfikacji informacji. Dokumentacja konstrukcyjna (know-how firmy) jest traktowana tak samo jak korespondencja ogólna.
Obserwacja konsultanta	Rysunki CAD są na udziale sieciowym dostępnym dla wszystkich pracowników biura, w tym stażystów. Dyrektor techniczny uznał to za istotny problem.
Podstawa ustalenia	**Wywiad** Oczekiwany dowód: Schemat klasyfikacji informacji
Ryzyko	Istotne. Luka "klasyfikacja informacji" wymaga usunięcia przed oceną zewnętrzną. W praktyce: informacje wrażliwe krążą kanałami bez zasad ochrony, co grozi wyciekiem i naruszeniem RODO.
Rekomendacja	Wprowadzić trzy klasy (publiczna, wewnętrzna, poufna) z zasadami przechowywania, przesyłania i udostępniania. Objąć w pierwszej kolejności dokumentację konstrukcyjną i dane klientów.
Właściciel	Zarząd (A) / Pełnomocnik ds. SZBI (R)
Nakład / termin	3,0 dni rob. · termin: 31.12.2026

PRÓBKA, DANE FIKCYJNE

33 A.5.15 · A.5 Zabezpieczenia organizacyjne

W Wysoki

A.5.15 Kontrola dostępu

Dojrzałość	2,0 / 5 - Powtarzalny
Wymaganie normy	Polityka kontroli dostępu oparta na wymaganiach biznesowych i bezpieczeństwa. Powiązania: DORA art. 9, PCI DSS Req 7, UoKSC art. 8 ust. 1 pkt 2 lit. n
Stan obecny	Kontrola dostępu bez zasad: uprawnienia nadawane na prośbę przełożonego mailem, bez przeglądów, bez odbierania przy zmianie stanowiska.
Obserwacja konsultanta	W AD aktywne są 3 konta byłych pracowników (odeszli w 2025 r.). ERP ma 11 kont z rolą administratora, z czego 4 to użytkownicy biznesowi.
Podstawa ustalenia	**Obserwacja** Eksport kont z AD i ról z ERP Oczekiwany dowód: Polityka kontroli dostępu
Ryzyko	Istotne. Luka "kontrola dostępu" wymaga usunięcia przed oceną zewnętrzną. W praktyce: nieodbierane lub nadmiarowe uprawnienia (w tym osierocone konta po odejściach) umożliwiają nieautoryzowany dostęp do systemów i danych.
Rekomendacja	Wdrożyć politykę kontroli dostępu z zasadą minimalnych uprawnień, macierzą ról dla ERP i udziałów sieciowych, procesem nadawania, zmiany i odbierania dostępu powiązanym z HR.
Właściciel	Kierownik IT (R) / Pełnomocnik ds. SZBI (A)
Nakład / termin	4,0 dni rob. · termin: 31.12.2026

34 A.5.18 · A.5 Zabezpieczenia organizacyjne

W Wysoki · Quick Win

A.5.18 Prawa dostępu

Dojrzałość	2,0 / 5 - Powtarzalny
Wymaganie normy	Nadawanie, przegląd i odbieranie praw dostępu. Powiązania: DORA art. 9, PCI DSS Req 7, UoKSC art. 8 ust. 1 pkt 2 lit. n
Stan obecny	Brak przeglądów uprawnień.
Obserwacja konsultanta	Konta byłych pracowników i nadmiarowe role administratora w ERP wynikają wprost z braku przeglądów.
Podstawa ustalenia	**Wywiad** Oczekiwany dowód: Zapisy przeglądów praw dostępu z datami
Ryzyko	Istotne. Luka "prawa dostępu" wymaga usunięcia przed oceną zewnętrzną. W praktyce: nieodbierane lub nadmiarowe uprawnienia (w tym osierocone konta po odejściach) umożliwiają nieautoryzowany dostęp do systemów i danych.
Rekomendacja	Wprowadzić kwartalny przegląd uprawnień w ERP, AD i M365 przez właścicieli systemów, z protokołem i usuwaniem nadmiarowych dostępów. Pierwszy przegląd od razu, jako szybka wygrana.
Właściciel	Kierownik IT (R) / Pełnomocnik ds. SZBI (A)
Nakład / termin	1,0 dni rob. · termin: 31.10.2026

35 A.5.30 · A.5 Zabezpieczenia organizacyjne

W Wysoki

A.5.30 Gotowość ICT do ciągłości działania

Dojrzałość	1,0 / 5 - Inicjalny
Wymaganie normy	ICT jako element planu ciągłości działania. Powiązania: DORA art. 11, ISO22301 8.4, UoKSC art. 8 ust. 1 pkt 2 lit. f
Stan obecny	Brak planu ciągłości ICT. Odtworzenie ERP po awarii w marcu 2026 r. trwało 2 dni i zależało od dostępności jednej osoby u dostawcy.
Obserwacja konsultanta	Kopie zapasowe działają (A.8.13 ocenione wysoko), ale nigdy nie testowano pełnego odtworzenia. Zarząd oszacował koszt dnia przestoju produkcji na poziomie, który uzasadnia inwestycję w plan.
Podstawa ustalenia	**Wywiad** Oczekiwany dowód: Wyniki testów gotowości ICT do ciągłości (DR)
Ryzyko	Istotne. Luka "gotowość ICT do ciągłości działania" wymaga usunięcia przed oceną zewnętrzną. W praktyce: nieodbierane lub nadmiarowe uprawnienia (w tym osierocone konta po odejściach) umożliwiają nieautoryzowany dostęp do systemów i danych.
Rekomendacja	Określić RTO i RPO dla ERP, SCADA, poczty i plików na podstawie BIA, opracować plan odtworzenia, przetestować odtworzenie z kopii co najmniej raz w roku.
Właściciel	Kierownik IT (R) / Pełnomocnik ds. SZBI (A)
Nakład / termin	4,0 dni rob. · termin: 28.02.2027

PRÓBKA, DANE FIKCYJNE

36 A.5.35 · A.5 Zabezpieczenia organizacyjne

W Wysoki

A.5.35 Niezależny przegląd bezpieczeństwa

Dojrzałość	0,0 / 5 - Nieistniejący
Wymaganie normy	Niezależne przeglądy (audyt wewnętrzny, audyt zewnętrzny, testy penetracyjne). Powiązania: DORA art. 6, NIS2 art. 21, UoKSC art. 8 ust. 1 pkt 2 lit. h
Stan obecny	Nigdy nie przeprowadzono niezależnego przeglądu bezpieczeństwa.
Obserwacja konsultanta	Niniejszy audyt zerowy jest pierwszym zewnętrznym spojrzeniem na bezpieczeństwo firmy.
Podstawa ustalenia	**Wywiad** Oczekiwany dowód: Raporty niezależnych przeglądów (audyt, pentest)
Ryzyko	Istotne. Luka "niezależny przegląd bezpieczeństwa" wymaga usunięcia przed oceną zewnętrzną. W praktyce: kierownictwo nie ma zweryfikowanej informacji o skuteczności zabezpieczeń i nie może zarządzać systemem.
Rekomendacja	Zaplanować niezależny przegląd (audyt wewnętrzny SZBI plus test penetracyjny brzegu sieci) po wdrożeniu zabezpieczeń priorytetowych.
Właściciel	Zarząd (A) / Pełnomocnik ds. SZBI (R)
Nakład / termin	2,0 dni rob. · termin: 30.04.2027

37 A.6.3 · A.6 Zabezpieczenia ludzi

W Wysoki

A.6.3 Szkolenia i świadomość

Dojrzałość	1,0 / 5 - Inicjalny
Wymaganie normy	Program szkoleń i uświadamiania z bezpieczeństwa informacji. Powiązania: DORA art. 13, NIS2 art. 20, UoKSC art. 8 ust. 1 pkt 2 lit. i
Stan obecny	Brak szkoleń i programu świadomości.
Obserwacja konsultanta	Patrz c7-4. Operatorzy linii nie wiedzą, że pendrive z domu w panelu HMI to zagrożenie.
Podstawa ustalenia	**Wywiad** Oczekiwany dowód: Rejestr szkoleń + wyniki testów wiedzy
Ryzyko	Istotne. Luka "szkolenia i świadomość" wymaga usunięcia przed oceną zewnętrzną. W praktyce: personel nieprzeszkolony jest najtańszym wektorem ataku (phishing, socjotechnika) i źródłem naruszeń nieumyślnych.
Rekomendacja	Jak c7-4: program roczny, moduł dla kierownictwa, moduł OT, symulacje phishingu.
Właściciel	Dyrektor HR (R) / Pełnomocnik ds. SZBI (A)
Nakład / termin	3,0 dni rob. · termin: 31.01.2027

38 A.6.7 · A.6 Zabezpieczenia ludzi

W Wysoki

A.6.7 Praca zdalna

Dojrzałość	2,0 / 5 - Powtarzalny
Wymaganie normy	Polityka i kontrole bezpieczeństwa dla pracy zdalnej / BYOD. Powiązania: DORA art. 9, UoKSC art. 8 ust. 1 pkt 2 lit. j
Stan obecny	Praca zdalna bez zasad: prywatne laptopy handlowców z dostępem VPN, brak szyfrowania dysków, brak MFA.
Obserwacja konsultanta	Trzech handlowców używa prywatnych laptopów. Jeden z nich potwierdził brak hasła na koncie systemowym.
Podstawa ustalenia	**Wywiad** Oczekiwany dowód: Polityka pracy zdalnej
Ryzyko	Istotne. Luka "praca zdalna" wymaga usunięcia przed oceną zewnętrzną. W praktyce: nieodbierane lub nadmiarowe uprawnienia (w tym osierocone konta po odejściach) umożliwiają nieautoryzowany dostęp do systemów i danych.
Rekomendacja	Polityka pracy zdalnej i urządzeń: sprzęt firmowy lub minimalne wymagania dla prywatnego, szyfrowanie dysku, MFA na VPN i M365, blokada ekranu.
Właściciel	Kierownik IT (R) / Pełnomocnik ds. SZBI (A)
Nakład / termin	2,0 dni rob. · termin: 31.12.2026

PRÓBKA, DANE FIKCYJNE

39 A.6.8 · A.6 Zabezpieczenia ludzi

W Wysoki · Quick Win

A.6.8 Zgłaszanie zdarzeń bezpieczeństwa

Dojrzałość	1,0 / 5 - Inicjalny
Wymaganie normy	Kanał i procedura zgłaszania zdarzeń przez pracowników. Powiązania: DORA art. 17, NIS2 art. 23, UoKSC art. 8 ust. 1 pkt 4
Stan obecny	Pracownicy nie mają kanału ani obowiązku zgłaszania zdarzeń bezpieczeństwa.
Obserwacja konsultanta	Incydent z lutego 2026 r. został zgłoszony po dwóch dniach, bo pracownik "nie chciał robić problemu".
Podstawa ustalenia	**Wywiad** Oczekiwany dowód: Kanał zgłaszania zdarzeń + rejestr zgłoszeń
Ryzyko	Istotne. Luka "zgłaszanie zdarzeń bezpieczeństwa" wymaga usunięcia przed oceną zewnętrzną. W praktyce: bez procedury i progów klasyfikacji organizacja nie dotrzyma ustawowych terminów zgłoszeń, a obsługa incydentu będzie chaotyczna.
Rekomendacja	Ustanowić prosty kanał (adres e-mail i numer wewnętrzny), zasadę "zgłoś, nie oceniaj", potwierdzenie przyjęcia zgłoszenia. Zakomunikować na szkoleniu wstępnym.
Właściciel	Kierownik IT (R) / Pełnomocnik ds. SZBI (A)
Nakład / termin	1,0 dni rob. · termin: 31.10.2026

40 A.8.2 · A.8 Zabezpieczenia techniczne

W Wysoki

A.8.2 Uprzywilejowane prawa dostępu

Dojrzałość	2,0 / 5 - Powtarzalny
Wymaganie normy	Zarządzanie kontami uprzywilejowanymi (PAM), least privilege. Powiązania: DORA art. 9, PCI DSS Req 7, UoKSC art. 8 ust. 1 pkt 2 lit. n
Stan obecny	Konta uprzywilejowane współdzielone (konto "serwis" dostawcy, konto "admin" w ERP używane przez 4 osoby).
Obserwacja konsultanta	Nie da się ustalić, kto wykonał zmianę konfiguracji UTM w czerwcu 2026 r., po której przestał działać VPN.
Podstawa ustalenia	**Wywiad** Oczekiwany dowód: Rejestr kont uprzywilejowanych + zapisy przeglądów
Ryzyko	Istotne. Luka "uprzywilejowane prawa dostępu" wymaga usunięcia przed oceną zewnętrzną. W praktyce: nieodbierane lub nadmiarowe uprawnienia (w tym osierocone konta po odejściach) umożliwiają nieautoryzowany dostęp do systemów i danych.
Rekomendacja	Imienne konta administracyjne, odrębne od kont codziennych, MFA, rejestrowanie sesji uprzywilejowanych, przegląd kwartalny.
Właściciel	Kierownik IT (R) / Pełnomocnik ds. SZBI (A)
Nakład / termin	3,0 dni rob. · termin: 31.12.2026

41 A.8.5 · A.8 Zabezpieczenia techniczne

W Wysoki · Quick Win

A.8.5 Bezpieczne uwierzytelnianie

Dojrzałość	2,0 / 5 - Powtarzalny
Wymaganie normy	MFA, SSO, polityki haseł, zarządzanie sesjami. Powiązania: DORA art. 9, PCI DSS Req 8, UoKSC art. 8 ust. 1 pkt 2 lit. l
Stan obecny	MFA tylko dla administratorów domeny. VPN, M365 i ERP z samym hasłem. Polityka haseł: 8 znaków, bez wygasania.
Obserwacja konsultanta	Licencje M365 obejmują MFA bez dodatkowych kosztów. Wdrożenie to konfiguracja i komunikacja, nie zakup.
Podstawa ustalenia	**Wywiad** Oczekiwany dowód: Raport pokrycia MFA / konfiguracja uwierzytelniania
Ryzyko	Istotne. Luka "bezpieczne uwierzytelnianie" wymaga usunięcia przed oceną zewnętrzną. W praktyce: słabe uwierzytelnianie jest najczęstszym wektorem przejęcia kont; bez MFA pojedynczy phishing daje dostęp do środowiska.
Rekomendacja	MFA dla VPN, M365 i dostępu zdalnego dostawców w pierwszej kolejności, potem ERP. Polityka haseł zgodna z aktualnymi wytycznymi (długość, blokada po nieudanych próbach, brak wymuszonej rotacji przy MFA).
Właściciel	Kierownik IT (R) / Pełnomocnik ds. SZBI (A)
Nakład / termin	2,0 dni rob. · termin: 30.11.2026

PRÓBKA. DANE FIKCYJNE

42 A.8.15 · A.8 Zabezpieczenia techniczne

W Wysoki

A.8.15 Logowanie (logging)

Dojrzałość	2,0 / 5 - Powtarzalny
Wymaganie normy	Centralizacja logów, SIEM, retencja, ochrona logów przed modyfikacją. Powiązania: DORA art. 9, PCI DSS Req 10, UoKSC art. 8 ust. 1 pkt 2 lit. g
Stan obecny	Logi zbierane lokalnie na urządzeniach, bez centralizacji i retencji. UTM nadpisuje logi po 7 dniach.
Obserwacja konsultanta	Po incydencie z lutego 2026 r. nie było już logów pozwalających ustalić źródło. To samo powtórzy się przy incydencie zgłaszanym do CSIRT.
Podstawa ustalenia	**Wywiad** Oczekiwany dowód: Polityka logowania + próbka logów z retencją
Ryzyko	Istotne. Luka "logowanie (logging)" wymaga usunięcia przed oceną zewnętrzną. W praktyce: bez logów i monitorowania incydent zostanie wykryty późno lub wcale, a analiza powłamaniowa będzie niemożliwa.
Rekomendacja	Centralne zbieranie logów z UTM, AD, ERP i serwerów z retencją co najmniej 12 miesięcy (ustawa: dokumentacja operacyjna). Alerty dla zdarzeń krytycznych.
Właściciel	Kierownik IT (R) / Pełnomocnik ds. SZBI (A)
Nakład / termin	4,0 dni rob. · termin: 28.02.2027

43 A.8.16 · A.8 Zabezpieczenia techniczne

W Wysoki

A.8.16 Monitorowanie aktywności

Dojrzałość	1,0 / 5 - Inicjalny
Wymaganie normy	SOC/SIEM, alerty, monitoring anomalii sieciowych i systemowych. Powiązania: DORA art. 10, NIS2 art. 21, PCI DSS Req 10, UoKSC art. 8 ust. 1 pkt 2 lit. g
Stan obecny	Brak monitorowania: nikt nie przegląda logów ani alertów. UTM wysyła powiadomienia na skrzynkę, której nikt nie czyta.
Obserwacja konsultanta	Skrzynka alertów UTM zawiera 4 200 nieprzeczytanych wiadomości.
Podstawa ustalenia	**Wywiad** Oczekiwany dowód: Reguły monitorowania i alerty (SIEM)
Ryzyko	Istotne. Luka "monitorowanie aktywności" wymaga usunięcia przed oceną zewnętrzną. W praktyce: bez logów i monitorowania incydent zostanie wykryty późno lub wcale, a analiza powłamaniowa będzie niemożliwa.
Rekomendacja	Zdefiniować minimalny zestaw monitorowanych zdarzeń, właściciela przeglądu, częstotliwość. Rozważyć usługę zewnętrznego monitoringu (MSSP) jako opcję wymaganą przez ustawę dla struktur odpowiedzialnych za cyberbezpieczeństwo.
Właściciel	Kierownik IT (R) / Pełnomocnik ds. SZBI (A)
Nakład / termin	3,0 dni rob. · termin: 28.02.2027

44 A.8.32 · A.8 Zabezpieczenia techniczne

W Wysoki

A.8.32 Zarządzanie zmianami

Dojrzałość	2,0 / 5 - Powtarzalny
Wymaganie normy	Change management - CAB, testy przed wdrożeniem, rollback. Powiązania: PCI DSS Req 6, UoKSC art. 8 ust. 1 pkt 5 lit. c
Stan obecny	Zmiany w ERP i infrastrukturze bez formalnego procesu. Dostawca wprowadza zmiany po telefonie od Kierownika IT.
Obserwacja konsultanta	Zmiana konfiguracji UTM w czerwcu 2026 r. (bez zapisu) spowodowała 1 dzień bez VPN dla handlowców.
Podstawa ustalenia	**Wywiad** Oczekiwany dowód: Zapisy zarządzania zmianami: wnioski, zatwierdzenia
Ryzyko	Istotne. Luka "zarządzanie zmianami" wymaga usunięcia przed oceną zewnętrzną. W praktyce: brak nadzoru nad dostawcami przenosi ryzyko ich incydentów na organizację bez umownych podstaw reakcji i wyjścia.
Rekomendacja	Prosty proces zmian: wniosek, ocena wpływu, akceptacja, okno, plan wycofania, zapis. Dla OT dodatkowo uzgodnienie z Utrzymaniem Ruchu.
Właściciel	Kierownik IT (R) / Pełnomocnik ds. SZBI (A)
Nakład / termin	2,0 dni rob. · termin: 31.01.2027

PRÓBKA. DANE FIKCYJNE

11 Quick Wins

Nr	Wymaganie	Działanie	Termin
11	**A.8.8**	**Zarządzanie podatnościami technicznymi**: Wdrożyć proces: inwentaryzacja wersji, skan podatności co najmniej kwartalnie, okna serwisowe, priorytety wg CVSS i ekspozycji, osobna ścieżka dla OT uzgodniona z producentem linii. Zacząć od systemów wystawionych do internetu (UTM, VPN, poczta).	do 28.09.2026 okno prior.: 31.10.2026
27	**kl. 9 w.5**	**Przegląd zarządzania**: Rozszerzyć istniejący roczny przegląd zarządzania ISO 9001 o wejścia z kl. 9.3 ISO 27001: wyniki oceny ryzyka, incydenty, audyty, cele, dostawcy. Protokół z decyzjami Zarządu.	do 28.09.2026 okno prior.: 31.01.2027
30	**A.5.7**	**Threat intelligence**: Zapisać firmę do komunikatów CSIRT NASK i producentów (UTM, ERP, SCADA), wyznaczyć osobę przeglądającą je co tydzień, powiązać z procesem podatności.	do 28.09.2026 okno prior.: 31.10.2026
34	**A.5.18**	**Prawa dostępu**: Wprowadzić kwartalny przegląd uprawnień w ERP, AD i M365 przez właścicieli systemów, z protokołem i usuwaniem nadmiarowych dostępów. Pierwszy przegląd od razu, jako szybka wygrana.	do 28.09.2026 okno prior.: 31.10.2026
39	**A.6.8**	**Zgłaszanie zdarzeń bezpieczeństwa**: Ustanowić prosty kanał (adres e-mail i numer wewnętrzny), zasadę "zgłoś, nie oceniaj", potwierdzenie przyjęcia zgłoszenia. Zakomunikować na szkoleniu wstępnym.	do 28.09.2026 okno prior.: 31.10.2026
41	**A.8.5**	**Bezpieczne uwierzytelnianie**: MFA dla VPN, M365 i dostępu zdalnego dostawców w pierwszej kolejności, potem ERP. Polityka haseł zgodna z aktualnymi wytycznymi (długość, blokada po nieudanych próbach, brak wymuszonej rotacji przy MFA).	do 28.09.2026 okno prior.: 30.11.2026
82	**A.5.5**	**Kontakt z organami władzy**: Wyznaczyć dwie osoby do kontaktów z podmiotami KSC, zgłosić je we wniosku o wpis do wykazu, wpisać do procedury incydentów.	do 28.09.2026 okno prior.: 30.09.2026
83	**A.5.6**	**Kontakt z grupami specjalistów**: Subskrypcja komunikatów CSIRT NASK, udział w ISAC sektorowym, jeśli dostępny.	do 28.09.2026 okno prior.: 31.10.2026

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.

PRÓBKA, DANE FIKCYJNE

12 Dokumenty wejściowe

Dostarczono **0 z 40** oczekiwanych dokumentów (0%). Wykaz obejmuje dokumenty wspólne dla projektu oraz dokumenty specyficzne dla ISO 27001; brak dokumentu jest sam w sobie informacją o luce w dokumentacji.

Dokumenty niedostarczone: specyficzne dla ISO 27001

Kategoria	Brakujące dokumenty
ISO 27001 - dokumenty systemowe SZBI	Zakres SZBI (granice i obszar stosowania, pkt 4.3) Cele bezpieczeństwa informacji i plan ich osiągnięcia (pkt 6.2) Protokoły przeglądów zarządzania (pkt 9.3) Rejestr niezgodności i działań korygujących (pkt 10.2) Wyniki monitorowania i pomiarów skuteczności SZBI (pkt 9.1) Program audytów wewnętrznych z harmonogramem (pkt 9.2) Zapisy z realizacji procesów operacyjnych SZBI (pkt 8.1) Wyniki oceny ryzyka i realizacji planu postępowania z ryzykiem (pkt 8.2-8.3) Procedura zarządzania incydentami bezpieczeństwa (A.5.24-A.5.26)
ISO 27001 - polityki tematyczne (A.5.1)	Polityka kryptograficzna i zarządzania kluczami (A.8.24) Polityka klasyfikacji i oznaczania informacji (A.5.12-A.5.13) Polityka kopii zapasowych (A.8.13) Polityka logowania zdarzeń i monitorowania (A.8.15-A.8.16) Procedura zarządzania podatnościami technicznymi (A.8.8) Procedura zarządzania zmianą (A.8.32) Zasady bezpiecznego rozwoju oprogramowania (A.8.25-A.8.28) Polityka retencji, usuwania danych i niszczenia nośników (A.5.33, A.7.10, A.7.14) Polityka bezpieczeństwa w relacjach z dostawcami (A.5.19-A.5.22) Polityka bezpieczeństwa sieci (A.8.20-A.8.22) Polityka urządzeń końcowych i nośników wymiennych (A.8.1, A.7.9-A.7.10) Procedura nadzoru nad udokumentowanymi informacjami (pkt 7.5)

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)

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.

PRÓBKA, DANE FIKCYJNE

14 Roadmapa wdrożenia

Faza	Zakres
Faza 1 - Quick Wins Dni 1-14	• **A.8.8** Wdrożyć proces: inwentaryzacja wersji, skan podatności co najmniej kwartalnie, okna serwisowe, priorytety wg CVSS i ekspozycji, osobna ścieżka dla OT uzgodniona z producentem linii. Zacząć od systemów wystawionych do internetu (UTM, VPN, poczta). (termin QW: do 28.09.2026) • **kl. 9 w.5** Rozszerzyć istniejący roczny przegląd zarządzania ISO 9001 o wejścia z kl. 9.3 ISO 27001: wyniki oceny ryzyka, incydenty, audyty, cele, dostawcy. Protokół z decyzjami Zarządu. (termin QW: do 28.09.2026) • **A.5.7** Zapisać firmę do komunikatów CSIRT NASK i producentów (UTM, ERP, SCADA), wyznaczyć osobę przeglądającą je co tydzień, powiązać z procesem podatności. (termin QW: do 28.09.2026) • **A.5.18** Wprowadzić kwartalny przegląd uprawnień w ERP, AD i M365 przez właścicieli systemów, z protokołem i usuwaniem nadmiarowych dostępów. Pierwszy przegląd od razu, jako szybka wygrana. (termin QW: do 28.09.2026) • **A.6.8** Ustanowić prosty kanał (adres e-mail i numer wewnętrzny), zasadę "zgłoś, nie oceniaj", potwierdzenie przyjęcia zgłoszenia. Zakomunikować na szkoleniu wstępnym. (termin QW: do 28.09.2026) • **A.8.5** MFA dla VPN, M365 i dostępu zdalnego dostawców w pierwszej kolejności, potem ERP. Polityka haseł zgodna z aktualnymi wytycznymi (długość, blokada po nieudanych próbach, brak wymuszonej rotacji przy MFA). (termin QW: do 28.09.2026) • **A.5.5** Wyznaczyć dwie osoby do kontaktów z podmiotami KSC, zgłosić je we wniosku o wpis do wykazu, wpisać do procedury incydentów. (termin QW: do 28.09.2026) • **A.5.6** Subskrypcja komunikatów CSIRT NASK, udział w ISAC sektorowym, jeśli dostępny. (termin QW: do 28.09.2026)
Faza 2 - Fundamenty Dni 1-30	• **kl. 5 w.2** Powołać Pełnomocnika ds. SZBI zarządzeniem Zarządu z zakresem odpowiedzialności, uprawnieniem do raportowania bezpośrednio do Zarządu i wymiarem czasu (co najmniej 0,25 etatu w fazie wdrożenia). Rozważyć outsourcing roli na okres wdrożenia. (termin: 15.10.2026) • **kl. 5 w.5** Opracować i zatwierdzić Politykę Bezpieczeństwa Informacji zgodną z kl. 5.2: cele, zakres, zobowiązanie kierownictwa, ramy dla polityk szczegółowych, zasady komunikacji. Zakomunikować wszystkim pracownikom i dostawcy IT. (termin: 31.10.2026) • **kl. 6 w.1** Przyjąć metodykę szacowania ryzyka zgodną z ISO/IEC 27005 i wymaganiami art. 8 ustawy o KSC (kryteria proporcjonalności), z matrycą prawdopodobieństwo x skutek, kryteriami akceptacji i rolą Zarządu. Przeprowadzić pierwszą ocenę dla systemów wspierających usługę objętą ustawą (ERP, SCADA, poczta, sieć zakładowa). (termin: 30.11.2026) • **kl. 6 w.3** Utworzyć rejestr ryzyk jako produkt pierwszej oceny: scenariusz, aktywo, właściciel, ocena inherentna i rezydualna, opcja postępowania, termin przeglądu. Zarząd zatwierdza rejestr i akceptuje ryzyka pozostałe. (termin: 30.11.2026) • **kl. 6 w.5** Opracować PPR jako wynik oceny ryzyka: działania, właściciele, terminy, nakłady, kontrole z Aneksu A. PPR zatwierdza Zarząd i przegląda go kwartalnie. (termin: 15.12.2026) • **kl. 6 w.6** Opracować SoA dla 93 zabezpieczeń Aneksu A z uzasadnieniem stosowania lub wyłączenia każdej kontroli, powiązaną z rejestrem ryzyk i PPR. Utrzymywać w narzędziu, nie w arkuszu bez wersjonowania. (termin: 31.12.2026) • **kl. 8 w.2** Aneksować umowę z dostawcą IT: zakres usług, wymagania bezpieczeństwa, obowiązek zgłaszania incydentów w czasie pozwalającym dotrzymać terminów ustawowych, imienne konta, logowanie sesji zdalnych, prawo audytu, zasady podwykonawstwa. Wdrożyć rejestr dostępów zdalnych dostawcy. (termin: 30.11.2026) • **A.5.19** Sporządzić rejestr dostawców z dostępem do systemów lub danych (IT, ERP, SCADA, księgowość zewnętrzna, kurier dokumentów), sklasyfikować wg krytyczności i objąć wymaganiami adekwatnymi do klasy. (termin: 30.11.2026) • **A.5.20** Wprowadzić standardowy załącznik bezpieczeństwa do umów z dostawcami klasy krytycznej i ważnej, w tym zgłaszanie incydentów, dostęp imienny, prawo audytu, poufność, zasady zakończenia współpracy. (termin: 31.12.2026) • **A.5.24** Opracować procedurę zarządzania incydentami z klasyfikacją (w tym kryteria incydentu poważnego wg ustawy), rejestrem, rolami, kanałem zgłoszeń dla pracowników, terminami zgłoszeń do CSIRT NASK (24 h, 72 h, miesiąc) i osobami do kontaktu. (termin: 30.11.2026) • **A.8.22** Zaprojektować segmentację: VLAN dla OT z jednokierunkowym dostępem serwisowym przez jump host, osobna sieć gości, sieć biurowa. Dostęp producenta linii przez firmowy VPN z MFA zamiast routera GSM. (termin: 31.12.2026)

PRÓBKA. DANE FIKCYJNE

Faza 3 - Wdrożenie Mies. 2-6	• **kl. 4 w.9** Patrz działanie nadrzędne wskazane w obserwacji. (termin: 28.02.2027) • **kl. 5 w.8** Patrz działanie nadrzędne wskazane w obserwacji. (termin: 28.02.2027) • **kl. 6 w.2** Patrz działanie nadrzędne wskazane w obserwacji. (termin: 28.02.2027) • **kl. 6 w.4** Patrz działanie nadrzędne wskazane w obserwacji. (termin: 28.02.2027) • **kl. 6 w.7** Patrz działanie nadrzędne wskazane w obserwacji. (termin: 28.02.2027) • **kl. 6 w.8** Patrz działanie nadrzędne wskazane w obserwacji. (termin: 28.02.2027) • **kl. 6 w.9** Patrz działanie nadrzędne wskazane w obserwacji. (termin: 28.02.2027) • **kl. 7 w.4** Wdrożyć roczny program szkoleń: szkolenie wstępne dla wszystkich (2 h), moduł dla kierownictwa wymagany przez ustawę, moduł dla operatorów OT, symulacja phishingu dwa razy w roku. Rejestrować obecność i wyniki. (termin: 31.01.2027) • **kl. 7 w.8** Zbudować komplet dokumentacji SZBI w kolejności: polityka, zakres, metodyka ryzyka, rejestr ryzyk, PPR, SoA, procedury operacyjne (incydenty, dostęp, kopie zapasowe, zmiany, dostawcy, ciągłość). (termin: 28.02.2027) • **kl. 8 w.4** Patrz działanie nadrzędne wskazane w obserwacji. (termin: 28.02.2027) • **kl. 8 w.5** Patrz działanie nadrzędne wskazane w obserwacji. (termin: 28.02.2027) • **kl. 9 w.1** Patrz działanie nadrzędne wskazane w obserwacji. (termin: 28.02.2027) • **kl. 9 w.3** Zaplanować pierwszy audyt wewnętrzny po wdrożeniu dokumentacji i minimum 2 miesiącach działania systemu, przez audytora niezależnego od wdrożenia. (termin: 30.04.2027) • **kl. 9 w.4** Patrz działanie nadrzędne wskazane w obserwacji. (termin: 28.02.2027) • **kl. 9 w.6** Patrz działanie nadrzędne wskazane w obserwacji. (termin: 28.02.2027) • **A.5.1** Po zatwierdzeniu polityki nadrzędnej opracować polityki: kontroli dostępu, kopii zapasowych, pracy zdalnej i urządzeń mobilnych, dostawców, klasyfikacji informacji, kryptografii, zarządzania zmianą. Zwięzłe, 2 do 4 stron każda. (termin: 31.01.2027) • **A.5.9** Sporządzić rejestr aktywów informacyjnych z właścicielami i klasyfikacją: systemy (ERP, SCADA, M365, CAD), zbiory danych, urządzenia sieciowe i OT, usługi zewnętrzne. (termin: 30.11.2026) • **A.5.12** Wprowadzić trzy klasy (publiczna, wewnętrzna, poufna) z zasadami przechowywania, przesyłania i udostępniania. Objąć w pierwszej kolejności dokumentację konstrukcyjną i dane klientów. (termin: 31.12.2026) • **A.5.15** Wdrożyć politykę kontroli dostępu z zasadą minimalnych uprawnień, macierzą ról dla ERP i udziałów sieciowych, procesem nadawania, zmiany i odbierania dostępu powiązanym z HR. (termin: 31.12.2026) • **A.5.30** Określić RTO i RPO dla ERP, SCADA, poczty i plików na podstawie BIA, opracować plan odtworzenia, przetestować odtworzenie z kopii co najmniej raz w roku. (termin: 28.02.2027) • **A.5.35** Zaplanować niezależny przegląd (audyt wewnętrzny SZBI plus test penetracyjny brzegu sieci) po wdrożeniu zabezpieczeń priorytetowych. (termin: 30.04.2027) • **A.6.3** Jak c7-4: program roczny, moduł dla kierownictwa, moduł OT, symulacje phishingu. (termin: 31.01.2027) • **A.6.7** Polityka pracy zdalnej i urządzeń: sprzęt firmowy lub minimalne wymagania dla prywatnego, szyfrowanie dysku, MFA na VPN i M365, blokada ekranu. (termin: 31.12.2026) • **A.8.2** Imienne konta administracyjne, odrębne od kont codziennych, MFA, rejestrowanie sesji uprzywilejowanych, przegląd kwartalny. (termin: 31.12.2026) • **A.8.15** Centralne zbieranie logów z UTM, AD, ERP i serwerów z retencją co najmniej 12 miesięcy (ustawa: dokumentacja operacyjna). Alerty dla zdarzeń krytycznych. (termin: 28.02.2027) • **A.8.16** Zdefiniować minimalny zestaw monitorowanych zdarzeń, właściciela przeglądu, częstotliwość. Rozważyć usługę zewnętrznego monitoringu (MSSP) jako opcję wymaganą przez ustawę dla struktur odpowiedzialnych za cyberbezpieczeństwo. (termin: 28.02.2027) • **A.8.32** Prosty proces zmian: wniosek, ocena wpływu, akceptacja, okno, plan wycofania, zapis. Dla OT dodatkowo uzgodnienie z Utrzymaniem Ruchu. (termin: 31.01.2027)
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 popraw (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 certyfikację 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