DOKUMENT DEMONSTRACYJNY VCISO, MIESIĄC 1

Diagnoza startowa: ocena dojrzałości programu bezpieczeństwa

Demo Platform Sp. z o.o., ocena z kwietnia 2026 (start usługi vCISO). Sześć domen, skala 0 do 4, ekspozycja regulacyjna, priorytety na 90 dni.

Dokument	Diagnoza startowa: ocena dojrzałości programu bezpieczeństwa
Klient	Demo Platform Sp. z o.o., B2B SaaS, 140 osób, klienci bankowi objęci DORA i klienci w USA (podmiot fikcyjny, dalej: Spółka)
Data oceny	07.04.2026 do 21.04.2026
Zakres	6 domen, 58 kontroli; 9 wywiadów, 71 dokumentów, weryfikacja 12 kontroli bez testów technicznych
Autor	Rafał Dobrosielski, PushSec, vCISO, ISO/IEC 27001 Lead Auditor (BSI, IRCA)
Data wydania	28.04.2026
Wersja / Status	1.0 / Finalny
Klasyfikacja	Materiał demonstracyjny, do publikacji (wersja kliencka: Poufne)

Dokument demonstracyjny. Demo Platform Sp. z o.o. jest organizacją fikcyjną. Diagnoza pokazuje układ i poziom szczegółowości raportu z miesiąca 1 usługi vCISO, na którym opiera się strategia, mapa drogowa 12M i budżet. Uzupełnia health-check dokumentacji SZBI (17 obszarów), który ocenia zgodność dokumentów; tu oceniana jest dojrzałość programu i ekspozycja regulacyjna.

Executive Summary

Kontekst i cel. Spółka jest dostawcą B2B SaaS (140 osób, certyfikat ISO/IEC 27001 od 2024 r.), z dwoma klientami bankowymi objętymi DORA, ofertami z USA warunkowanymi SOC 2 oraz rundą B planowaną na jesień 2026. Od 3.04.2026 obowiązuje nowelizacja UoKSC, a Spółka jako średni przedsiębiorca świadczący usługę chmurową spełnia przesłanki podmiotu ważnego. Zarząd zlecił diagnozę przed startem usługi vCISO.

Wniosek główny. Dojrzałość ogólna 2,1 na 4: kontrole techniczne są na poziomie powtarzalnym lub zdefiniowanym, ale nadzór Zarządu nad ryzykiem i zgodność regulacyjna są na poziomie inicjalnym. Certyfikat ISO 27001 nie pokrywa obowiązków podmiotu ważnego UoKSC (wpis do 3.10.2026, osoby do kontaktów, zgłoszenia przez S46) ani wymagań klientów bankowych z DORA (klauzule art. 30, plan wyjścia, prawo audytu). Przy audycie klienta bankowego lub kontroli organu Spółka wykazałaby dokumenty, ale nie wykazałaby, że Zarząd zarządza ryzykiem.

Trzy najważniejsze ryzyka. [1] Termin wpisu do wykazu podmiotów ważnych upływa 3.10.2026, a Spółka nie ma samoidentyfikacji ani osoby odpowiedzialnej. [2] Dostawca hostingu wspiera usługę dla klientów bankowych bez oceny, klauzul i strategii wyjścia, czego wymagają umowy z tymi klientami. [3] Krytyczne podatności pozostają otwarte średnio 31 dni przy dostępie do produkcji z sieci biurowej.

Rekomendowane decyzje Zarządu. [1] Uchwała o mandacie vCISO: zakres, niezależność od działu inżynierii, linia raportowania do Zarządu. [2] Priorytet Q2 i Q3 2026: obowiązki UoKSC i wymagania klientów objętych DORA (samoidentyfikacja, wpis, klauzule art. 30, procedura zgłaszania). [3] Budżet na 90 dni: 24 tys. zł (MFA dla kont uprzywilejowanych, narzędzie do rejestru ryzyk). [4] Właściciele ryzyk na poziomie członków Zarządu i kierowników.

Co działa dobrze. SZBI jest utrzymywany, audyt nadzoru 2025 bez niezgodności, kopie zapasowe testowane kwartalnie, zespół inżynierii ma proces przeglądu kodu, pipeline z testami i rejestr incydentów od 2023 r. Program budujemy na tej praktyce, nie od zera.

1. Wynik w liczbach

2,1 / 4	6	D6	7
dojrzałość ogólna	kontroli na poziomie 0	najsłabsza domena (1,5)	ryzyk kluczowych

2. Metoda i skala

Poziom	Nazwa	Opis
0	Brak	Kontrola nie istnieje; brak świadomości lub celowe pominięcie
1	Inicjalny	Ad hoc, nieudokumentowane, zależne od osoby
2	Powtarzalny	Udokumentowane i stosowane, ale niestandaryzowane; wyjątki nierejestrowane
3	Zdefiniowany	Udokumentowane, zatwierdzone, wyjątki rejestrowane, zapisy z działania
4	Zarządzany	Mierzone KPI/KRI, audytowane, doskonalone

Ocena oparta na przeglądzie 71 dokumentów, 9 wywiadach (Zarząd, CTO, inżynieria, operacje, prawny, sprzedaż, HR) oraz weryfikacji 12 kontroli w zakresie dostępnym bez testów penetracyjnych. Wynik odzwierciedla stan na 21.04.2026. Nie jest audytem w rozumieniu pkt 9.2 ISO/IEC 27001.

3. Wynik per domena

Domena	Kontroli	Wynik 0 do 4	Priorytet	Główne odniesienia
D1 Governance, strategia, odpowiedzialność Zarządu	10	1,6	W	ISO 27001 pkt 5, 6, 9; UoKSC art. 8 (kierownik podmiotu)
D2 Zarządzanie aktywami i klasyfikacja informacji	8	2,5	N	A.5.9 do A.5.13; RODO art. 30
D3 Kontrola dostępu i tożsamość	10	2,4	Ś	A.5.15 do A.5.18, A.8.2 do A.8.5
D4 Incydenty, ciągłość i odporność	10	2,2	W	A.5.24 do A.5.30; UoKSC art. 11; umowy z klientami bankowymi (DORA art. 30)
D5 Dostawcy ICT i chmura	8	1,9	W	A.5.19 do A.5.23; DORA art. 28 do 30 przez umowy; ISO 27017
D6 Zgodność regulacyjna i ekspozycja	10	1,5	W	UoKSC po NIS2, DORA przez klientów, RODO, AI Act, SOC 2; A.5.31 do A.5.36
Razem	58	2,1		

4. Ustalenia kluczowe

ID	Ustalenie	Domena	Prio	Właściciel	Termin
DS-01	Brak samoidentyfikacji na gruncie UoKSC i osoby odpowiedzialnej za obowiązki ustawowe; termin wpisu 3.10.2026 nie jest w żadnym kalendarzu	D6	K	Zarząd	30 dni
DS-02	Rejestr ryzyk SZBI nie obejmuje ryzyka dostawców, koncentracji ani wymagań klientów bankowych; 0 z 23 pozycji ma właściciela na poziomie Zarządu	D1	K	COO	60 dni
DS-03	Dostawca hostingu wspierający usługę dla klientów bankowych bez oceny, klauzul i strategii wyjścia; umowy z 2 bankami zawierają zobowiązania (prawo audytu, plan wyjścia), których Spółka nie realizuje	D5	K	COO	90 dni
DS-04	Krytyczne podatności otwarte średnio 31 dni; brak SLA remediacji i raportowania do Zarządu	D3	W	CTO	60 dni
DS-05	MFA nie obejmuje 14 z 22 kont uprzywilejowanych, w tym dostępu do środowiska produkcyjnego z sieci biurowej	D3	K	CTO	30 dni
DS-06	Procedura incydentów bez kryteriów incydentu poważnego z UoKSC i bez ścieżki zgłoszeń do CSIRT, UODO i klientów bankowych w terminach z umów	D4	W	CTO	60 dni
DS-07	Brak testu przełączenia dla usługi produkcyjnej; RTO 8 h deklarowane klientom bez dowodu	D4	W	COO	120 dni

ID	Ustalenie	Domena	Prio	Właściciel	Termin
DS-08	Kwestionariusze klientów wypełniane przez sprzedaż bez biblioteki odpowiedzi; 2 sprzeczne odpowiedzi w 2025 r. wykryte przez klienta bankowego	D6	W	Dyrektor Sprzedaży	60 dni

5. Mapa ekspozycji regulacyjnej

Reżim	Czy dotyczy	Podstawa ustalenia	Najbliższy termin	Luka
UoKSC po NIS2	Tak: podmiot ważny (średni przedsiębiorca, usługa chmurowa, zał. 1)	kryteria wielkości; motyw 33 NIS2	Wpis do wykazu: 3.10.2026; rozdział 3: 3.04.2027	Samoidentyfikacja, wpis, osoby do kontaktów, procedura S46
DORA	Nie wprost; pośrednio przez umowy z 2 klientami bankowymi	art. 28 do 30 przeniesione umownie	Aneksy: wg umów	Klauzule art. 30, plan wyjścia, prawo audytu
RODO	Tak, jako procesor	art. 28, 30, 32, 33	przegląd RCP 06.2026	RCP aktualny; lista podprocesorów do publikacji
AI Act	Tak, art. 4 (AI literacy); funkcje AI w produkcie do klasyfikacji	inwentarz systemów AI	obowiązuje	Szkolenie; klasyfikacja funkcji AI w produkcie
CRA	Do weryfikacji: SaaS bez komponentu instalowanego u klienta poza zakresem; SDK dla klientów wymaga analizy	model produktu	analiza do 06.2026	Klasyfikacja SDK
SOC 2	Wymóg kontraktowy 2 klientów z USA	oferty z 03.2026	Type I: Q1 2027	Mapowanie kontroli, audytor CPA

6. Ryzyka kluczowe

ID	Ryzyko	Poziom	Właściciel	Pierwsze działanie
R-01	Brak wpisu do wykazu w terminie i brak osób do kontaktów; kontrola organu stwierdza brak nadzoru Zarządu	Wysokie	Zarząd	Samoidentyfikacja, wniosek o wpis, uchwała o mandacie vCISO
R-04	Przejęcie konta uprzywilejowanego bez MFA z dostępem do produkcji	Wysokie	CTO	MFA na 100% kont w 30 dni
R-07	Wykorzystanie krytycznej podatności otwartej ponad 14 dni	Wysokie	CTO	SLA remediacji i KRI
R-19	Ruch boczny z sieci biurowej do środowiska produkcyjnego (brak segmentacji i bastionu)	Wysokie	CTO	Projekt segmentacji do budżetu 2027
R-23	Niedostępność usługi dla klientów bankowych przy awarii hostingu bez strategii wyjścia; naruszenie umowy	Wysokie	COO	Ocena dostawcy, klauzule, plan wyjścia
R-12	Wyciek danych klientów przez narzędzia AI bez zasad	Wysokie	COO	Polityka użycia AI
R-31	Dostawcy krytyczni bez aktualnej oceny (4 z 6)	Średnie	vCISO	Cykl ocen do 30.09

7. Priorytety na 90 dni i propozycja mapy drogowej

Okres	Priorytet	Efekt	Nakład i budżet
Dni 1 do 30	Mandat vCISO, MFA na kontach uprzywilejowanych, właściciele ryzyk, samoidentyfikacja KSC	R-04 zamknięte; status ustawowy Spółki ustalony z dowodem	4 dni PushSec; 6 tys. zł (MFA)
Dni 31 do 60	Rejestr ryzyk z właścicielami, apetyt na ryzyko, KRI, mapa drogowa 12M do zatwierdzenia, biblioteka odpowiedzi do kwestionariuszy	Zarząd widzi ryzyka w jednym rejestrze; kwestionariusze przestają się różnić	6 dni PushSec; 18 tys. zł (narzędzie do rejestru)
Dni 61 do 90	Wniosek o wpis do wykazu, osoby do kontaktów, procedura zgłaszania (S46, UODO, klienci), wzorzec klauzul art. 30, SLA remediacji, ocena dostawców (start), pierwszy raport miesięczny	Obowiązki UoKSC z terminem 3.10 spełnione z zapasem; wymagania klientów bankowych z właścicielem	6 dni PushSec; 0 zł
Po dniu 90	Q3: aneksy art. 30, rejestr dostawców. Q4: SOC 2 (audytor), strategia wyjścia hosting, budżet 2027. Q1 2027: segmentacja, test przełączenia, SOC 2 Type I. Q2 2027: rozdział 3 UoKSC, audyt nadzoru ISO	Obowiązki ustawowe i kontraktowe w cyklu rocznym z dowodami	Mapa drogowa 12M, budżet 2027 ok. 215 tys. zł

8. Zastrzeżenia

- Ocena opiera się na informacjach przekazanych przez Spółkę i obserwacjach w czasie 10 dni roboczych; nie stanowi audytu bezpieczeństwa ani testów penetracyjnych.
- Wynik odzwierciedla stan na 21.04.2026; zmiany po tej dacie nie są uwzględnione.
- Ustalenia dotyczące ekspozycji regulacyjnej nie są opinią prawną.

Rafał Dobrosielski, vCISO, ISO/IEC 27001 Lead Auditor (BSI, IRCA), PushSec. info@pushsec.pl, (+48) 780 519 553

Dokument demonstracyjny PushSec. Demo Platform Sp. z o.o. jest podmiotem fikcyjnym; dane, ryzyka i kwoty są przykładowe. Wersja kliencka ma klasyfikację Poufne.