DOKUMENT DEMONSTRACYJNY VCISO. MAPA DROGOWA BEZPIECZEŃSTWA: 12 MIESIĘCY

Mapa drogowa bezpieczeństwa 12M: Demo Platform Sp. z o.o.

B2B SaaS, 140 osób, klienci bankowi objęci DORA, klienci w USA, runda B (podmiot fikcyjny). Okres: lipiec 2026 do czerwiec 2027. Zatwierdzona przez Zarząd 26.06.2026, stan na 05.10.2026. Wersja robocza mapy jest prowadzona w arkuszu z dashboardem; ten wydruk to widok dla Zarządu.

37	10	8	0	256 000 zł	27%
inicjatyw w 5 filarach	zakończonych po Q3	w toku	opóźnionych	budżet zewnętrzny netto	wykonanie po 3 z 12 miesięcy

Cel programu na 12 miesięcy

Spełnione obowiązki podmiotu ważnego UoKSC (wpis, rozdział 3, osoby do kontaktów, S46) z dowodami na kontrolę; umowy z klientami bankowymi zgodne z art. 30 DORA i plan wyjścia dla hostingu po teście; raport SOC 2 Type I dla klientów w USA; certyfikat ISO/IEC 27001 utrzymany; kwestionariusze klientów w nie więcej niż 5 dni roboczych.

Filar	Inicjatyw	Zakończone	W toku	Budżet (zł)
P1 Governance i rytm zarządczy	8	3	1	3 000
P2 UoKSC i wymagania klientów objętych DORA	10	4	2	28 000
P3 SZBI ISO 27001 i SOC 2	6	0	2	91 000
P4 Bezpieczeństwo technologii	5	1	1	121 000
P5 Ludzie klienci inwestorzy	8	2	2	13 000

KRI na dzień raportu

KRI	Wartość	Apetyt	Trend	Status
Krytyczne podatności otwarte powyżej 14 dni	2	0	spadek z 5	**poza apetytem**
Konta uprzywilejowane bez MFA	0	0	stabilnie	w apetycie
Dostawcy krytyczni bez aktualnej oceny	1 z 6	0	spadek z 3	**poza apetytem**
Czas zamknięcia incydentu wysokiego (h)	4	8	poprawa	w apetycie
Kamienie milowe kwartału w terminie	5 z 6	80%	stabilnie	w apetycie
Czas odpowiedzi na kwestionariusze klientów (dni)	3	5	poprawa	w apetycie

Kamienie milowe

Termin	Kamień milowy	Status
30.09.2026	Priorytet Q3: wniosek o wpis KSC, procedura zgłaszania, klauzule art. 30	Zakończone
15.10.2026	Budżet 2027 i strategia wyjścia dla hostingu zatwierdzone (D-1, D-2)	W toku
08.12.2026	Szkolenie Zarządu; przegląd zarządzania SZBI	Zaplanowane
31.12.2026	Aneksy art. 30 podpisane; audytor SOC 2 wybrany	Zaplanowane
31.03.2027	Test przełączenia; segmentacja wdrożona; SOC 2 Type I	Zaplanowane
03.04.2027	Obowiązki rozdziału 3 UoKSC wdrożone i udokumentowane	Zaplanowane
30.06.2027	Audyt nadzoru ISO zamknięty; strategia na kolejne 12 miesięcy	Zaplanowane

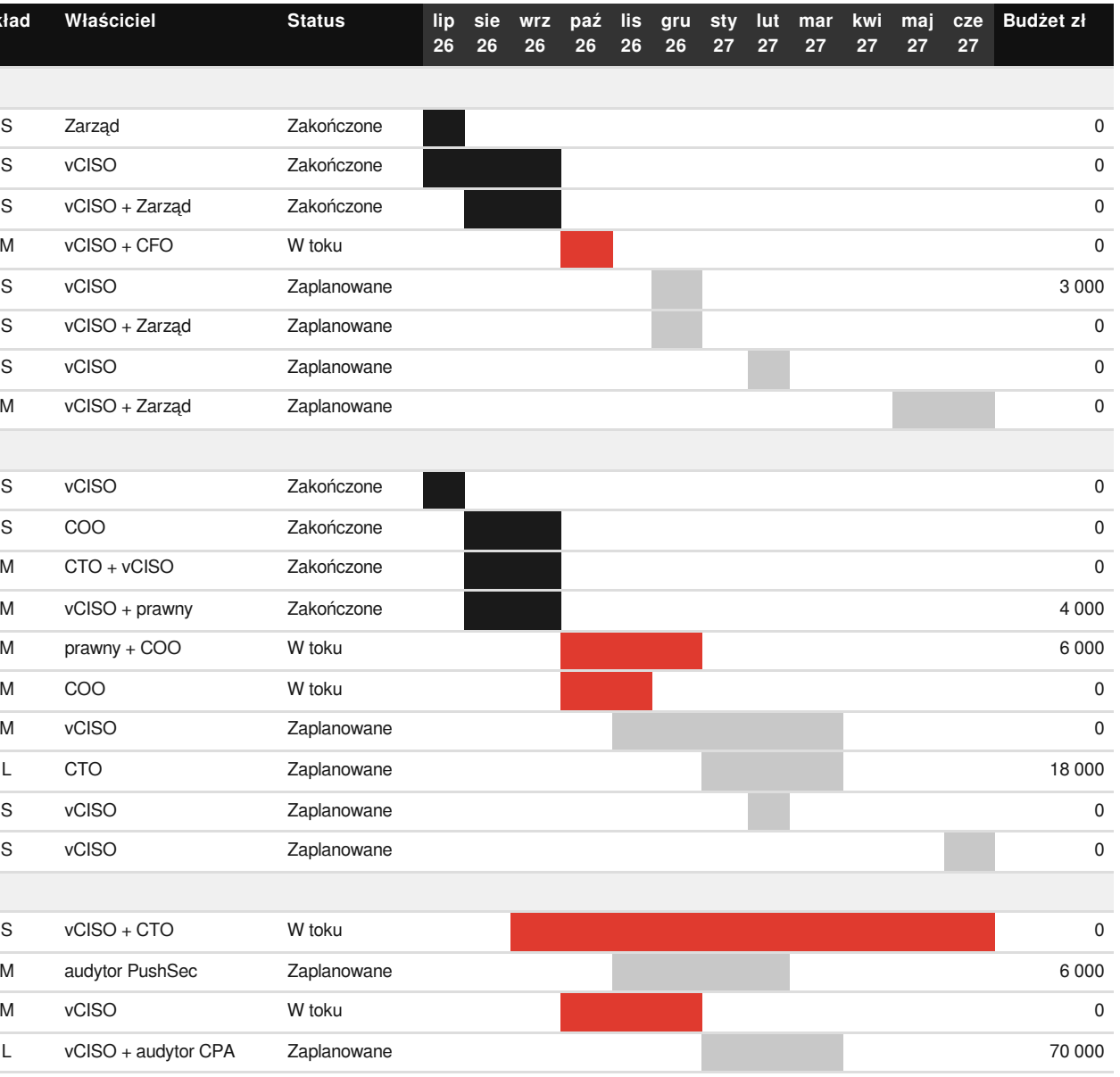
Priorytety kwartałów

Kwartał	Priorytet	Stan
Q3 2026	Obowiązki podmiotu ważnego UoKSC i wymagania klientów objętych DORA	ukończony 30.09
Q4 2026	Przygotowanie do SOC 2 Type I i strategia wyjścia dla dostawców krytycznych	w toku
Q1 2027	Segmentacja dostępu do produkcji i test przełączenia hostingu	zaplanowany
Q2 2027	Audyt nadzoru ISO 27001, zewnętrzny test aplikacji, strategia na kolejny rok	zaplanowany

Gantt: 37 inicjatyw, 12 miesięcy

Legenda: zakończone w toku zaplanowane. Stan na 05.10.2026 (miesiąc 4 programu).

ID	Inicjatywa	Prio	Nakład	Właściciel	Status	Budżet zł
P1. Governance i rytm zarządczy						
I-01	Mandat vCISO i linia raportowania	Krytyczny	S	Zarząd	Zakończone	0
I-02	Rytm raportowania miesięcznego	Krytyczny	S	vCISO	Zakończone	0
I-03	Apetyt na ryzyko i zestaw KRI	Wysoki	S	vCISO + Zarząd	Zakończone	0
I-04	Budżet bezpieczeństwa 2027	Krytyczny	M	vCISO + CFO	W toku	0
I-05	Szkolenie Zarządu z obowiązków UoKSC	Wysoki	S	vCISO	Zaplanowane	3 000
I-06	Przegląd zarządzania SZBI	Wysoki	S	vCISO + Zarząd	Zaplanowane	0
I-07	Raport roczny dla Zarządu i inwestora	Średni	S	vCISO	Zaplanowane	0
I-08	Strategia i budżet na kolejne 12 miesięcy	Wysoki	M	vCISO + Zarząd	Zaplanowane	0
P2. UoKSC i wymagania klientów objętych DORA						
I-09	Samoidentyfikacja KSC	Krytyczny	S	vCISO	Zakończone	0
I-10	Wniosek o wpis do wykazu podmiotów ważnych	Krytyczny	S	COO	Zakończone	0
I-11	Procedura zgłaszania incydentów (S46 UODO klienci)	Krytyczny	M	CTO + vCISO	Zakończone	0
I-12	Wzorzec klauzul bezpieczeństwa (art. 30 DORA)	Krytyczny	M	vCISO + prawny	Zakończone	4 000
I-13	Aneksy art. 30 z dwoma klientami bankowymi	Wysoki	M	prawny + COO	W toku	6 000
I-14	Strategia wyjścia dla dostawcy hostingu	Krytyczny	M	COO	W toku	0
I-15	Mapa zgodności z rozdziałem 3 UoKSC	Wysoki	M	vCISO	Zaplanowane	0
I-16	Test przełączenia dla usługi produkcyjnej	Wysoki	L	CTO	Zaplanowane	18 000
I-17	Tabletop zgłoszenia przez S46	Średni	S	vCISO	Zaplanowane	0
I-18	Roczny przegląd ekspozycji regulacyjnej	Średni	S	vCISO	Zaplanowane	0
P3. SZBI, ISO 27001 i SOC 2						
I-19	Przegląd uprawnień i aktualizacja SoA	Wysoki	S	vCISO + CTO	W toku	0
I-20	Audyt wewnętrzny SZBI (dwa etapy)	Wysoki	M	audytor PushSec	Zaplanowane	6 000
I-21	SOC 2: wybór audytora i mapowanie kontroli	Krytyczny	M	vCISO	W toku	0
I-22	SOC 2 Type I	Krytyczny	L	vCISO + audytor CPA	Zaplanowane	70 000



ID	Inicjatywa	Prio	Nakład	Właściciel	Status	lip 26	sie 26	wrz 26	paź 26	lis 26	gru 26	sty 27	lut 27	mar 27	kwi 27	maj 27	cze 27	Budżet zł
I-23	Audyt nadzoru ISO/IEC 27001	Wysoki	M	vCISO	Zaplanowane													15 000
I-24	Start okresu obserwacji SOC 2 Type II	Średni	S	vCISO	Zaplanowane													0
P4. Bezpieczeństwo technologii																		
I-25	MFA na 100% kont uprzywilejowanych	Krytyczny	S	CTO	Zakończone													6 000
I-26	SLA remediacji podatności i KRI	Wysoki	M	CTO	W toku													0
I-27	Segmentacja i bastion dostępu do produkcji	Krytyczny	L	CTO	Zaplanowane													90 000
I-28	Standard bezpiecznego wytwarzania v2	Wysoki	M	CTO + vCISO	Zaplanowane													0
I-29	Zewnętrzny test bezpieczeństwa aplikacji	Wysoki	M	CTO	Zaplanowane													25 000
P5. Ludzie, klienci, inwestorzy																		
I-30	Szkolenie awareness całej firmy	Wysoki	S	vCISO + HR	Zakończone													0
I-31	Polityka użycia narzędzi AI	Krytyczny	S	COO	Zakończone													0
I-32	Pakiet data room dla inwestora	Wysoki	M	vCISO	W toku													0
I-33	Szkolenie AI dla zespołu	Wysoki	S	vCISO + HR	W toku													3 000
I-34	Biblioteka odpowiedzi do kwestionariuszy	Wysoki	M	vCISO + sprzedaż	Zaplanowane													0
I-35	Strona bezpieczeństwa (trust page) dla klientów	Średni	M	marketing + vCISO	Zaplanowane													4 000
I-36	Ścieżka bezpieczeństwa w onboardingu	Średni	S	HR	Zaplanowane													0
I-37	Symulacja phishingu i security annex v2	Średni	M	vCISO	Zaplanowane													6 000

Nakład: S do 5 dni, M 5 do 15 dni, L powyżej 15 dni łącznie (PushSec i Spółka). Budżet: koszty zewnętrzne netto (wykonawcy, audytorzy, narzędzia); dni usługi vCISO rozliczane w ryczałcie. Definicja ukończenia: produkt zatwierdzony, zakomunikowany, z właścicielem i terminem przeglądu. Jeden priorytet kwartału prowadzony do ukończenia; zmiany priorytetów uzgadniane jawnie w backlogu miesięcznym i zatwierdzane przez Zarząd.

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; inicjatywy, terminy i kwoty są przykładowe. Wersja kliencka ma klasyfikację Poufne.