DOKUMENT DEMONSTRACYJNY VCISO

Raport miesięczny vCISO: wrzesień 2026

Demo Platform Sp. z o.o., usługa vCISO w wymiarze 10 dni miesięcznie. Dla Zarządu: efekty, ryzyka, decyzje, KRI, terminy, dni.

Dokument	Raport miesięczny vCISO nr 2026/09
Klient	Demo Platform Sp. z o.o., B2B SaaS, 140 osób, klienci bankowi objęci DORA i klienci w USA (podmiot fikcyjny, dalej: Spółka)
Autor	Rafał Dobrosielski, PushSec, vCISO
Data	05.10.2026
Wymiar usługi	10 dni
Wersja / Status	1.0 / Finalny
Klasyfikacja	Materiał demonstracyjny, do publikacji (wersja kliencka: Poufne)
Dystrybucja	Zarząd, sponsor usługi, obserwator z ramienia inwestora

Zgodnie z planem	Podwyższone, maleje	0	2 (termin 15.10)	10,0 / 10,0
program	ryzyko łączne	incydenty w miesiącu	decyzje u Zarządu	dni usługi

1. Co zmieniło się dla Spółki w tym miesiącu

Sekcja pisana językiem efektów, nie czynności. Zarząd ma zobaczyć, co organizacja zyskała, co przestało jej grozić i co zostało odblokowane. Czynności są w sekcji 9.

Efekt	Dowód	Znaczenie dla Spółki
Wniosek o wpis do wykazu podmiotów ważnych UoKSC złożony 26.09, przed terminem 3.10	Potwierdzenie złożenia; raport samoidentyfikacji z 06.2026	Obowiązek ustawowy spełniony bez pracy w ostatnim tygodniu; brak podstawy do kary za brak wpisu
Audyt dokumentacyjny klienta bankowego (prawo audytu z umowy DORA) zamknięty bez ustaleń krytycznych	Raport audytora klienta z 22.09, 2 ustalenia niskie	Umowa o wartości 1,4 mln zł rocznie przedłużona bez warunków; materiał do kolejnych audytów
Ryzyko R-12 (narzędzia AI bez zasad) obniżone z wysokiego do średniego	Polityka użycia narzędzi AI v1.0 zatwierdzona 12.09	Zamknięta luka wskazywana w 2 z 3 kwestionariuszy klientów w tym kwartale
Konta uprzywilejowane w 100% z MFA, w tym dostęp do środowiska produkcyjnego	Raport z IdP z 26.09, KRI-2 w apetycie	Najczęstsze pytanie w kwestionariuszach zdjęte z listy ryzyk
Pakiet data room dla funduszu przekazany, 2 pytania otwarte	Pakiet z 18.09, lista pytań	Proces rundy B nie czeka na bezpieczeństwo

2. Podsumowanie dla Zarządu

Szósty miesiąc usługi. Program jest realizowany zgodnie z mapą drogową: priorytet kwartału (dostosowanie do obowiązków podmiotu ważnego UoKSC i wymagań klientów objętych DORA) ukończony, wniosek o wpis złożony, klauzule wg art. 30 DORA w wzorcu umowy zatwierdzone przez Zarząd 30.09. Łączny poziom ryzyka: podwyższony, trend spadkowy; z sześciu ryzyk kluczowych jedno zamknięto, dwa obniżono. Zarząd ma do 15 października dwie decyzje: budżet bezpieczeństwa na 2027 oraz strategię wyjścia dla dostawcy hostingu. Brak decyzji przesunie test przełączenia poza Q1 2027, utrzyma dwa KRI poza apetytem i opóźni odpowiedź na wymaganie klienta bankowego dotyczące planu wyjścia.

3. Ryzyka kluczowe i trend

ID	Ryzyko	Poziom	Trend	Stan działań	Właściciel	Termin
R-07	Krytyczne podatności otwarte powyżej 14 dni w środowisku produkcyjnym	Wysokie	maleje	2 podatności otwarte (z 5). Okno serwisowe 12.10	CTO	12.10.2026
R-19	Dostęp do środowiska produkcyjnego z sieci biurowej bez segmentacji i bez bastionu	Wysokie	stały	Projekt gotowy; czeka na budżet 2027 (D-1)	CTO	31.03.2027
R-23	Koncentracja: jeden dostawca hostingu bez strategii wyjścia; klient bankowy wymaga planu wyjścia (art. 28 ust. 8 DORA)	Wysokie	stały	Plan wyjścia w wersji roboczej; decyzja D-2	COO	15.10.2026
R-12	Użycie narzędzi AI bez zasad; ryzyko wycieku danych klientów	Średnie	maleje	Polityka v1.0 zatwierdzona 12.09; szkolenie 10.2026	COO	31.10.2026
R-31	Dostawcy krytyczni bez aktualnej oceny (hosting)	Średnie	maleje	5 z 6 dostawców krytycznych ocenionych do 30.09; ocena hostingu w toku	vCISO	15.10.2026
R-04	Konta uprzywilejowane bez MFA	Niskie	zamknięte	MFA na 100% kont od 26.09	CTO	zamknięte

Pełny rejestr ryzyk (28 pozycji) prowadzony odrębnie; powyżej wyłącznie ryzyka wymagające uwagi Zarządu.

4. Decyzje wymagane od Zarządu

Nr	Decyzja	Uzasadnienie	Termin
D-1	Zatwierdzić budżet bezpieczeństwa na 2027: 3,1% przychodów, w tym 90 tys. zł na segmentację i bastion (R-19), 70 tys. zł na SOC 2 Type I (audytor CPA) i 25 tys. zł na zewnętrzny test aplikacji	Zamyka R-19, otwiera sprzedaż do klientów w USA (2 oferty warunkowane SOC 2), spełnia wymóg testów z umów DORA. Priorytety wg ryzyka, załącznik B	15.10.2026
D-2	Zatwierdzić strategię wyjścia dla dostawcy hostingu i budżet testu przełączenia w Q1 2027	Zamyka R-23. Wymaganie klienta bankowego z umowy DORA (art. 28 ust. 8) i pytanie w kwestionariuszu drugiego banku	15.10.2026

Decyzje z sierpnia: D-2026-08-1 (polityka użycia narzędzi AI) podjęta 12.09, wdrożona; D-2026-08-2 (właściciele ryzyk) podjęta 18.09, rejestr zaktualizowany.

5. Kluczowe wskaźniki ryzyka (KRI)

KRI	Wartość	Apetyt	Trend	Status i działanie
Krytyczne podatności otwarte powyżej 14 dni	2	0	spadek z 5	Poza apetytem. Okno serwisowe 12.10, właściciel CTO
Konta uprzywilejowane bez MFA	0	0	stabilnie	W apetycie
Dostawcy krytyczni bez aktualnej oceny	1 z 6	0	spadek z 3	Poza apetytem. Ocena hostingu do 15.10
Czas zamknięcia incydentu wysokiego	4 h	do 8 h	poprawa	W apetycie
Kamienie milowe mapy drogowej w terminie (kwartał)	5 z 6	80% i więcej	stabilnie	W apetycie. Opóźniony: test przełączenia, przesunięty na Q1 2027
Czas odpowiedzi na kwestionariusze klientów	3 dni	do 5 dni roboczych	poprawa	W apetycie. 4 kwestionariusze w miesiącu

6. Terminy regulacyjne i kontraktowe

Obowiązek	Podstawa	Termin	Status
Wpis do wykazu podmiotów ważnych	UoKSC art. 7, przepisy przejściowe	03.10.2026	Wniosek złożony 26.09
System zarządzania bezpieczeństwem i środki zarządzania ryzykiem wg rozdziału 3, osoby do kontaktów, gotowość do zgłoszeń przez S46	UoKSC rozdział 3, art. 9, art. 11	03.04.2027	Plan dostosowania w mapie drogowej; SZBI ISO 27001 jako fundament
Plan wyjścia i test przełączenia dla dostawcy hostingu	Umowa z klientem bankowym (DORA art. 28 ust. 8)	Q1 2027	Zależny od D-2
Klauzule wg art. 30 DORA w umowach z 2 klientami bankowymi (aneksy)	DORA art. 30, wymaganie klienta	31.12.2026	Wzorzec zatwierdzony 30.09; aneksy u prawnika
Przegląd zarządzania SZBI	ISO/IEC 27001 pkt 9.3	12.2026	Dane wejściowe w przygotowaniu
Szkolenie AI dla zespołu	AI Act art. 4	31.10.2026	Zaplanowane 21.10

7. Incydenty i zdarzenia bezpieczeństwa

W miesiącu nie wystąpił incydent bezpieczeństwa podlegający zgłoszeniu. Odnotowano 3 zgłoszenia od pracowników (2 podejrzane wiadomości e-mail, 1 zagubiony laptop z pełnym szyfrowaniem dysku); wszystkie zamknięte w dniu zgłoszenia, laptop zdalnie wyczyszczony w 40 minut. Zgłaszalność pracowników rośnie po szkoleniu z sierpnia, co jest pozytywnym sygnałem.

8. Mapa drogowa: status priorytetu kwartału

Priorytet Q3 2026: dostosowanie do obowiązków podmiotu ważnego UoKSC i wymagań klientów objętych DORA. Ukończony: samoidentyfikacja i wniosek o wpis, wyznaczenie osób do kontaktów, wzorzec klauzul art. 30, rejestr dostawców z klasyfikacją, procedura zgłaszania incydentów z kryteriami i szablonem S46. Kolejny priorytet (Q4 2026): przygotowanie do SOC 2 Type I i strategia wyjścia dla dostawców krytycznych. Plan na październik: decyzje D-1 i D-2 (15.10), okno serwisowe podatności (12.10), szkolenie AI (21.10), wybór audytora SOC 2, przygotowanie danych do przeglądu zarządzania.

9. Wykorzystanie dni usługi

Blok	Plan	Wykonanie	Komentarz
Rytm zarządczy i governance	2,0	2,0	Posiedzenie Zarządu 30.09 (klauzule art. 30, wpis KSC); raport; aktualizacja mapy drogowej
Nadzór nad SZBI i ryzykiem	2,0	2,0	Aktualizacja rejestru ryzyk, przegląd KRI, przegląd uprawnień Q3
Blok projektowy: priorytet kwartału	2,0	2,5	Wniosek o wpis KSC, procedura zgłaszania, rejestr dostawców; zasilony 0,5 dnia z bufora
Regulator i zgodność	1,0	1,0	Samoidentyfikacja KSC finalna, osoby do kontaktów, monitoring rozporządzeń wykonawczych
Klienci, inwestorzy i dostawcy	2,0	2,0	Audyt klienta bankowego; pakiet data room; 4 kwestionariusze; ocena 5 dostawców
Konsultacje i bufor	1,0	0,5	Okno konsultacyjne: 3 zgłoszenia; reszta przeniesiona do bloku projektowego
Razem	10,0	10,0	

10. Mierniki usługi

Miernik	Cel	Wrzesień 2026
Raport miesięczny dostarczony w terminie	do 5. dnia roboczego	Tak (05.10)

Miernik	Cel	Wrzesień 2026
Terminy regulacyjne i kontraktowe dotrzymane	100%	100% (2 z 2: wpis KSC, audyt klienta)
Kamienie milowe mapy drogowej w kwartale	80% i więcej	5 z 6 (83%)
Odpowiedź na kwestionariusze i security review klientów	do 5 dni roboczych	średnio 3 dni (4 kwestionariusze)
Nowe umowy objęte przeglądem bezpieczeństwa przed podpisaniem	100%	100% (2 z 2)
KRI poza apetytem bez decyzji Zarządu	0	0 (2 poza apetytem, oba z działaniem)

Załącznik A. Status dokumentacji

Dokument	Wersja	Status	Termin
Raport samoidentyfikacji KSC	1.0	Zatwierdzony 30.06, utrwalony jako zapis	przegląd roczny
Procedura zgłaszania incydentów (CSIRT, UODO, klienci)	2.0	Zatwierdzona 30.09	przegląd 09.2027
Wzorzec klauzul bezpieczeństwa (art. 30 DORA) dla umów z klientami	1.0	Zatwierdzony 30.09	przegląd 09.2027
Rejestr ryzyk	2.1	Zatwierdzony 18.09	cykl kwartalny
Polityka użycia narzędzi AI	1.0	Zatwierdzona 12.09	przegląd 09.2027
Strategia wyjścia: dostawca hostingu	0.9	Szkic, do decyzji D-2	15.10.2026

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.