ZEWNĘTRZNY DZIAŁ BEZPIECZEŃSTWA PUSHSEC. OPIS ROLI, POZIOM 3 Z 3

vCISO. Wirtualny dyrektor ds. bezpieczeństwa informacji

Zarząd ma **jedną osobę odpowiedzialną za bezpieczeństwo na poziomie decyzji**: strategia i budżet powiązane z ryzykiem, zgodność z DORA, UoKSC i KNF pod nadzorem, organizacja obroniona przed regulatorem, klientem enterprise i inwestorem. Raport miesięczny zamiast zaskoczeń.

Poziom 1. Specjalista	Poziom 2. Manager i Pełnomocnik ds. SZBI	**Poziom 3. vCISO**

3 000 zł	**5 / 8 / 10 dni**	**miesięcznie**	**1 klient**
stała dniówka netto	wymiar do wyboru, do 16	raport dla Zarządu	w roli vCISO na raz

1. Co dostajesz

Rola jest rozliczana z produktów, nie z obecności. Każda pozycja ma nazwę, częstotliwość i odbiorcę; w pełnym wymiarze dostajesz wszystkie.

Raport miesięczny dla Zarządu

Stan, ryzyka do decyzji, incydenty, terminy regulacyjne, KRI, wykonanie roadmapy i budżetu, ewidencja dni. Demo publicznie na pushsec.pl/vciso.

Miesięcznie. Zarząd

Strategia i roadmapa 12 do 36 miesięcy

Cele bezpieczeństwa powiązane z celami biznesu, kamienie milowe, właściciele, budżet. Demo mapy 12M na pushsec.pl/vciso.

Raz, przegląd kwartalny. Zarząd, RN

Budżet bezpieczeństwa z uzasadnieniem ryzykowym

Plan roczny, priorytetyzacja inwestycji na bazie ryzyka, business case, kontrola wykonania kwartalnie.

Rocznie, kwartalnie. Zarząd, CFO

Dashboard KRI z apetytem na ryzyko

Kilkanaście wskaźników z progami, trendem i statusem. Każdy wskaźnik poza apetytem ma decyzję Zarządu.

Miesięcznie. Zarząd, RN, regulator

Rejestr informacji i pakiet dla regulatora

Rejestr umów z dostawcami ICT w formacie ITS 2024/2956, odpowiedzi na pisma i ankiety KNF, materiały na kontrolę.

Stale, na żądanie. KNF

Pakiet do data roomu i stanowisko na security review

Dokumentacja przygotowana pod pytania inwestora i klienta enterprise, utrzymywana na bieżąco, żeby przy procesie nie składać jej na kolanie, plus stanowisko negocjacyjne do klauzul.

Zdarzeniowo. Inwestorzy, klienci

Dla kogo ten poziom

- Instytucje płatnicze, pożyczkowe i inne podmioty finansowe objęte DORA i nadzorem KNF.
- Skalujący się SaaS z klientami enterprise, którzy wymagają CISO po drugiej stronie stołu.
- Spółki przed rundą inwestycyjną, przejęciem lub due diligence bezpieczeństwa.
- Organizacje, które urosły z poziomu 2 i potrzebują strategii oraz budżetu, nie tylko zgodności.

Sytuacja wyjściowa, z którą przychodzą klienci

- Wdrożenie DORA zrobione dokumentacyjnie, ale Zarząd nie umie odpowiedzieć na pytania KNF o ryzyko ICT.
- Rejestr informacji o umowach z dostawcami ICT nieprowadzony lub niekompletny.
- Inwestor prosi o pakiet bezpieczeństwa do data roomu, a dokumentacja jest rozproszona.
- Klient enterprise warunkuje umowę spotkaniem z CISO i planem naprawczym.

2. Wymiar współpracy: 10 dni albo mniej

Pełny wymiar to 10 dni roboczych w miesiącu. Mniejszy wymiar nie oznacza gorszej jakości, tylko węższy zakres: część obszarów przechodzi w tryb ograniczony albo poza wymiar. Dniówka jest stała dla poziomu, więc płacisz za dni, a nie za etykietę.

Podstawowy

5 dni

15 000 zł netto / mies.

Skalujący się SaaS z klientami enterprise, spółka po poziomie 2. Strategia, budżet, reprezentacja; praca operacyjna po stronie klienta.

Standard

8 dni

24 000 zł netto / mies.

Podmioty finansowe pod DORA i KNF w utrzymaniu, grupa z jedną spółką regulowaną. Pełna funkcja ryzyka ICT.

Pełny Pełny wymiar

10 dni

30 000 zł netto / mies.

Wdrożenie DORA lub przygotowanie do kontroli, due diligence w toku, kilka spółek. Wariant rozszerzony do 16 dni: 48 000.

Obszar	Podstawowy (5 dni)	Standard (8 dni)	Pełny (10 dni)
Strategia, roadmapa, cele i mierniki, przegląd kwartalny z Zarządem	✔	✔	✔
Raport miesięczny dla Zarządu, dashboard KRI, raport kwartalny dla RN	✔	✔	✔
Budżet bezpieczeństwa i priorytetyzacja inwestycji	✔	✔	✔
Reprezentacja przed klientami enterprise i inwestorami, pakiet data room	✔	✔	✔
Funkcja ryzyka ICT wg DORA art. 6 ust. 4, Rejestr informacji, pisma i kontrole KNF	◔	✔	✔
Nadzór nad zgłaszaniem poważnych incydentów, dowodzenie w kryzysie	◔	✔	✔
Dostawcy ICT strategiczni: strategia, klauzule art. 30 DORA, plany wyjścia	◔	✔	✔
Program testów odporności, BIA, ciągłość działania, TLPT	·	◔	✔
Matryca zgodności wieloregulacyjnej i monitoring zmian prawa z oceną wpływu	◔	✔	✔
Pełny zakres poziomów 1 i 2: Pełnomocnik, ryzyko, audytorzy, zapisy, szkolenia	·	◔	✔

✔ w pełnym zakresie ◔ w ograniczonym zakresie (opisany w umowie) · poza wymiarem, dostępne jako projekt w stałej cenie

3. Przykładowy miesiąc w pełnym wymiarze

Tak wygląda typowy miesiąc w utrzymaniu, po pierwszych 90 dniach. Dni są przesuwane między obszarami zależnie od tego, co się dzieje (audyt, incydent, kwestionariusz); ewidencja dni jest w raporcie miesięcznym.

Dzień	Obszar	Co powstaje
1	Zarząd	Spotkanie 60 minut: raport miesięczny, decyzje, priorytety; przygotowanie materiałów
2	Roadmapa i budżet	Status kamieni milowych, korekty, wykonanie budżetu, business case dla jednej inwestycji
3	Ryzyko ICT i KRI	Aktualizacja rejestru ryzyk ICT, przegląd KRI, decyzje dla wskaźników poza apetytem
4	Regulator	Rejestr informacji, korespondencja z KNF, przygotowanie odpowiedzi na ankietę lub pismo, monitoring zmian prawa
5	Dostawcy ICT	Ocena jednego dostawcy krytycznego, przegląd umowy pod art. 30 DORA, plan wyjścia
6	Klienci i inwestorzy	Security review z klientem enterprise, stanowisko do klauzul, aktualizacja pakietu data room
7	Odporność i incydenty	Nadzór nad testami i ćwiczeniami, przegląd incydentów i zgłoszeń, wnioski do roadmapy
8	Nadzór nad SZBI i zespołem	Przegląd pracy poziomów 1 i 2, Deklaracja Stosowania, audyty, niezgodności
9	Governance	Polityki wysokiego poziomu, komitet ryzyka, przygotowanie Zarządu do obowiązków ustawowych, szkolenie Zarządu raz w roku
10	Zamknięcie miesiąca	Raport miesięczny z KRI i ewidencją dni; w miesiącu kończącym kwartał raport dla RN i przegląd strategii

4. Fragment produktu, który dostajesz co miesiąc

Raport miesięczny dla Zarządu. Wrzesień 2026. Fragment: KRI i decyzje

FRAGMENT PRZYKŁADOWY

Demo Platform Sp. z o.o., B2B SaaS, 140 osób, klienci bankowi objęci DORA (podmiot fikcyjny). vCISO, PushSec, wymiar 10 dni. Pełny raport demo na pushsec.pl/vciso

KRI	Wartość	Apetyt	Trend	Status i działanie
Krytyczne podatności otwarte powyżej 14 dni	2	0	spadek z 5	Poza apetytem. Decyzja: okno serwisowe 12.10, właściciel Kierownik IT
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 30.09
Czas zamknięcia incydentu wysokiego	4 h	do 8 h	poprawa	W apetycie
Kamienie milowe roadmapy 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

Decyzje wymagane od Zarządu

- Budżet 2027: rekomendacja 3,1% przychodów, w tym 90 tys. zł na segmentację i bastion dostępu do produkcji (R-19) oraz 70 tys. zł na SOC 2 Type I dla 2 ofert z USA. Termin: 15.10.
- Strategia wyjścia dla dostawcy hostingu, wymagana umową z klientem bankowym (DORA art. 28 ust. 8): zatwierdzenie planu i budżetu testu przełączenia w Q1 2027. Termin: 15.10.

Co Zarząd powinien wiedzieć

- Wniosek o wpis do wykazu podmiotów ważnych UoKSC złożony 26.09, przed terminem 3.10. Audyt dokumentacyjny klienta bankowego zamknięty 22.09 bez ustaleń krytycznych.
- Due diligence funduszu: pakiet data room przekazany 18.09, 2 pytania otwarte (plan wyjścia hosting, test przełączenia).

Ewidencja dni: rytm zarządczy i governance 2, nadzór nad SZBI i ryzykiem 2, blok projektowy 2, regulator i zgodność 1, klienci i dostawcy 2, konsultacje i bufor 1. Razem 10 z 10.

5. Pierwsze 90 dni

Pierwszy miesiąc zawsze kończy się planem działania, który zostaje u Ciebie, niezależnie od tego, czy kontynuujemy.

Miesiąc 1. Diagnoza i mandat

- Diagnoza stanu: dojrzałość vs DORA, UoKSC, ISO 27001 i oczekiwania KNF; mapa ryzyk i luk z priorytetami.
- Umocowanie roli: zakres uprawnień, niezależność od IT, linia raportowania do Zarządu i RN.
- Plan działania na 12 miesięcy i roadmapa w wersji roboczej, zatwierdzone przez Zarząd.

Miesiąc 2. Strategia i governance

- Strategia bezpieczeństwa i odporności cyfrowej powiązana z celami biznesu.
- Apetyt na ryzyko i pierwszy zestaw KRI. Uruchomienie raportu miesięcznego.
- Przegląd Rejestru informacji i dostawców krytycznych, plan uzupełnień.

Miesiąc 3. Budżet i obrona na zewnątrz

- Budżet bezpieczeństwa z priorytetyzacją inwestycji przedstawiony Zarządowi.
- Pakiet do data roomu lub dla regulatora w wersji bazowej, gotowy do aktualizacji.
- Pierwszy raport kwartalny dla RN i decyzja o zakresie na kolejny kwartał.

6. Rola w skrócie

Poziom w drabince	3 z 3. Zawiera pełny zakres poziomów 1 i 2. Standard dla FinTech i instytucji płatniczych pod nadzorem KNF.
Charakter roli	Strategiczna i zarządcza. Odpowiada za kierunek, priorytety i budżet bezpieczeństwa oraz za to, jak organizacja wygląda w oczach regulatora, klientów i inwestorów.
Komu raportuje	Zarządowi, a w podmiotach nadzorowanych także Radzie Nadzorczej lub komitetowi ryzyka. Udział w posiedzeniach w części dotyczącej ryzyka ICT.
Formalne funkcje	Osoba odpowiedzialna za zarządzanie i nadzór nad ryzykiem ICT w rozumieniu DORA art. 6 ust. 4, z zapewnioną niezależnością od funkcji operacyjnych IT. Osoba kontaktowa dla KNF w sprawach ICT, jeśli Zarząd tak zdecyduje. Pełnomocnik ds. SZBI i osoba kontaktowa dla audytorów (poziom 2).
Wymiar	5, 8 lub 10 dni roboczych miesięcznie, wariant rozszerzony do 16 dni przy wdrożeniu DORA, kontroli lub due diligence.
Cena	Stała dniówka 3 000 zł netto: 15 000, 24 000 lub 30 000 zł miesięcznie; 16 dni to 48 000. CISO na etacie to 36 do 66 tys. zł kosztu pracodawcy.
Kto pełni rolę	Rafał Dobrosielski, ISO/IEC 27001 Lead Auditor (BSI, IRCA), z doświadczeniem wdrożenia DORA w instytucji płatniczej. Zadania operacyjne poziomów 1 i 2 mogą realizować konsultanci PushSec pod jego nadzorem.
Główne ramy odniesienia	DORA z aktami wykonawczymi (CDR 2024/1774, ITS 2024/2956), Uchwała KNF nr 6/2025, UoKSC rozdział 3, ISO/IEC 27001 i 22301, RODO, wymagania klientów enterprise i inwestorów.

7. Zakres odpowiedzialności i co pokrywa

Kolumna Wymaganie pokazuje, które obowiązki z normy lub przepisu dana pozycja pokrywa. Kolumna Dowód pokazuje zapis, którym wykażesz to audytorowi, klientowi albo organowi.

Obszar	Zadania w tej roli	Wymaganie	Dowód
Strategia i roadmapa	Strategia bezpieczeństwa i odporności cyfrowej powiązana z celami biznesu, roadmapa 12 do 36 miesięcy z kamieniami milowymi, cele i mierniki bezpieczeństwa, przegląd roczny.	DORA art. 6 ust. 8; ISO 27001 pkt 5.1, 6.2; UoKSC art. 8 ust. 1	Strategia zatwierdzona przez Zarząd, roadmapa 12M, karta celów i mierników
Governance i odpowiedzialność Zarządu	Struktura ról i komitetów, polityki wysokiego poziomu, przygotowanie Zarządu do obowiązków ustawowych, szkolenia Zarządu z ryzyka ICT, materiały na posiedzenia.	DORA art. 5; UoKSC art. 8 (obowiązki kierownika podmiotu); ISO 27001 pkt 5	Regulamin governance bezpieczeństwa, protokoły Zarządu, zaświadczenia ze szkoleń Zarządu
Budżet i priorytetyzacja inwestycji	Plan budżetu bezpieczeństwa na rok, priorytetyzacja wydatków na podstawie ryzyka, business case dla inwestycji, kontrola realizacji budżetu.	DORA art. 6 ust. 4 (zasoby i budżet funkcji ryzyka ICT); COBIT 2019 EDM02	Budżet roczny z uzasadnieniem ryzykowym, kwartalne wykonanie
Regulator: KNF, organy KSC	Przygotowanie do kontroli i ankiet KNF, odpowiedzi na pisma, nadzór nad zgłaszaniem poważnych incydentów ICT, Rejestr informacji o umowach z dostawcami ICT, plan testów odporności; TLPT wyłącznie po wyznaczeniu przez KNF, z wykonawcą zewnętrznym.	DORA art. 17 do 19, 24 do 27, 28 ust. 3; ITS 2024/2956; Uchwała KNF nr 6/2025; UoKSC art. 11	Pakiet dla regulatora, Rejestr informacji, harmonogram testów, raporty z incydentów
Klienci enterprise i inwestorzy	Reprezentacja w security review i negocjacjach klauzul, odpowiedzi na ankiety strategiczne, pakiet do data roomu, prowadzenie due diligence bezpieczeństwa po stronie spółki.	Wymagania kontraktowe; praktyka due diligence	Pakiet data room, stanowiska negocjacyjne, plan naprawczy dla klienta

Obszar	Zadania w tej roli	Wymaganie	Dowód
Nadzór nad zgodnością wieloregulacyjną	Jedna matryca kontroli dla DORA, UoKSC, ISO 27001, RODO i wymagań KNF, eliminacja duplikacji, monitoring zmian prawa i ich wpływu na roadmapę.	DORA art. 4 i art. 16 (proporcjonalność); UoKSC art. 8i (DORA jako lex specialis)	Matryca zgodności, rejestr zmian regulacyjnych z oceną wpływu
Dostawcy ICT strategiczni	Strategia ryzyka dostawców ICT, ocena dostawców wspierających funkcje krytyczne, klauzule umowne wg art. 30 DORA, strategie wyjścia, koncentracja.	DORA art. 28 do 30; A.5.19 do A.5.23	Strategia ryzyka dostawców, Rejestr informacji, plany wyjścia dla dostawców krytycznych
Odporność, ciągłość, testowanie	Nadzór nad BIA, planami ciągłości i odtwarzania, programem testów odporności, wnioskami z testów i incydentów.	DORA art. 11 do 13, 24 do 25; ISO 22301; A.5.29, A.5.30	Program testów, raporty z ćwiczeń, wnioski wdrożone do roadmapy
Zarządzanie kryzysowe	Dowodzenie w poważnym incydencie: decyzje, komunikacja z Zarządem, klientami, organami i mediami, przegląd po incydencie na poziomie Zarządu.	DORA art. 17 do 19; UoKSC art. 11; RODO art. 33 i 34	Plan zarządzania kryzysowego, raporty z incydentów, decyzje po incydencie
Raportowanie i mierniki	Raport miesięczny dla Zarządu (stan, ryzyka do decyzji, incydenty, terminy, wykorzystanie dni), dashboard KRI z apetytem na ryzyko, raport kwartalny dla Rady Nadzorczej.	ISO 27001 pkt 9.1; COBIT 2019 MEA01; DORA art. 5 ust. 2	Raport miesięczny, dashboard KRI, raport dla RN
Pełny zakres poziomów 1 i 2	Prowadzenie SZBI, ryzyko, dostawcy, audytorzy, przeglądy, szkolenia, zapisy.	Wg opisów poziomów 1 i 2	Wg opisów poziomów 1 i 2

8. Z czego rozliczamy rolę

Miernik	Wartość docelowa	Skąd dane
Terminy regulacyjne dotrzymane (DORA, UoKSC, KNF)	100%	Kalendarz regulacyjny
Poważne incydenty zgłoszone w terminie	100%	Rejestr incydentów, potwierdzenia organów
Kamienie milowe roadmapy zrealizowane w kwartale	80% i więcej	Raport miesięczny
Ustalenia krytyczne z kontroli lub audytu bez planu naprawczego po 30 dniach	0	Rejestr ustaleń
KRI poza apetytem na ryzyko bez decyzji Zarządu	0	Dashboard KRI
Odpowiedź na security review klienta enterprise	do 5 dni roboczych	Ewidencja zapytań
Wykonanie budżetu bezpieczeństwa	w przedziale plus minus 10% planu	Raport kwartalny
Rejestr informacji kompletny i aktualny na dzień przekazania	100% umów ICT	Rejestr informacji

9. Granice roli i sygnały, że potrzebujesz więcej

Poza zakresem tej roli	Gdzie to jest
Odpowiedzialność organu zarządzającego za ryzyko ICT	Zarząd. DORA art. 5 ust. 2 przypisuje ją Zarządowi i nie pozwala jej przenieść; vCISO ją przygotowuje, uzasadnia i wykonuje decyzje
Operacje IT, SOC, administracja systemami, wdrożenia techniczne	Dział IT klienta lub partner techniczny; vCISO wyznacza wymagania i odbiera wyniki
Testy penetracyjne i TLPT	Niezależni testerzy; vCISO planuje program, wybiera wykonawcę i nadzoruje remediację
Audyt wewnętrzny (trzecia linia obrony)	Audyt wewnętrzny klienta lub inny audytor PushSec; vCISO nie audytuje własnej pracy
Funkcja Inspektora Ochrony Danych, obsługa prawna, opinie prawne	Odrębne role; vCISO współpracuje i dostarcza analizę stanu faktycznego
Równoległe pełnienie roli vCISO dla kilku klientów	Nie dotyczy. Rola vCISO jest pełniona dla jednego klienta w danym czasie; to gwarancja koncentracji i dostępności

Sygnały, że zakres wymaga rozszerzenia

- Nakład stale przekracza 16 dni miesięcznie: rozważ etat CISO z PushSec w roli wsparcia i sukcesji, z płatnym przekazaniem.
- Kilka spółek w grupie pod różnymi regulatorami: osobne linie raportowania i dni per spółka.
- Stała obecność na miejscu w wymiarze ponad 2 dni w tygodniu: model hybrydowy z ustaloną obecnością.
- Zakres można też zmniejszyć do poziomu 2, gdy strategia i governance są wdrożone, a organizacja przechodzi w utrzymanie.

Czego potrzebujemy po Twojej stronie

- Mandat od Zarządu: uchwała określająca zakres, niezależność od IT, prawo dostępu do informacji i udziału w posiedzeniach.
- Godzina miesięcznie na spotkanie z Zarządem i 45 minut kwartalnie z Radą Nadzorczą lub komitetem ryzyka; decyzje w sprawach ryzyka w ciągu 14 dni.
- Dostęp do umów, budżetu, rejestrów regulacyjnych, korespondencji z KNF i wyników testów.
- Właściciel budżetu po stronie finansów (CFO) i osoba kontaktowa w IT z decyzyjnością.
- Wszystko, co wymagają poziomy 1 i 2.

10. Koszt tej funkcji na etacie i najczęstsze pytania

36 000 do 66 000 zł/mc

CISO na etacie: 30 do 55 tys. brutto plus ok. 20% kosztów pracodawcy i benefity, rekrutacja 4 do 6 miesięcy, trudna zastępowalność, a na rynku kandydatów z praktyką DORA i KNF jest niewielu.

15 000 do 30 000 zł/mc

Ta rola jako usługa: 5, 8 lub 10 dni; wariant rozszerzony do 16 dni. Poniżej pakietów agencji vCISO (15 do 55 tys. zł/mc), z referencją z instytucji płatniczej.

Od 3 000 zł/dzień

Stała dniówka niezależna od wymiaru. Niżej niż etat przy funkcji, która realnie odpowiada na pytania KNF, inwestora i klienta enterprise, i którą można zmniejszyć, gdy wdrożenie przejdzie w utrzymanie.

Czy zewnętrzny vCISO spełnia wymóg DORA co do funkcji zarządzania ryzykiem ICT?
DORA (art. 6 ust. 4) wymaga przypisania odpowiedzialności za ryzyko ICT funkcji kontrolnej z odpowiednią niezależnością; nie wymaga etatu. Warunkiem jest uchwała Zarządu o zakresie, niezależności od IT i linii raportowania. Projekt dostarczamy w pierwszym miesiącu. Odpowiedzialność Zarządu z art. 5 pozostaje po jego stronie.

Mieliście już taką rolę w podmiocie nadzorowanym?
Tak, w instytucji płatniczej: wdrożenie DORA i model vCISO, z referencją. Znamy praktykę KNF z korespondencji i ankiet, nie tylko z przepisów.

Dlaczego jeden klient na raz?
Bo rola vCISO to dostępność dla Zarządu w dniu, w którym przychodzi pismo z KNF albo pytanie inwestora. Koncentracja na jednym mandacie jest naszym atutem i gwarancją, że nie jesteś w kolejce. Praca operacyjna poziomów 1 i 2 może być delegowana do konsultantów PushSec pod nadzorem vCISO.

5 dni w miesiącu wystarczy?
Dla spółki po poziomie 2, z działającym SZBI i własnym zespołem operacyjnym: tak, to strategia, budżet i reprezentacja. Dla wdrożenia DORA, przygotowania do kontroli lub due diligence: nie, wtedy 10 dni i więcej na 2 do 3 kwartały, potem zejście do utrzymania.

Co z odpowiedzialnością, jeśli KNF stwierdzi nieprawidłowości?
Za decyzje odpowiada Zarząd, tak stanowi DORA i tak zapisujemy w umowie; nie przyjmujemy kar umownych ani gwarancji rezultatu. Po naszej stronie jest jakość rekomendacji, terminowość i dokumentacja decyzji, chroniona OC zawodowym 1,5 mln zł.

11. Warunki współpracy

Dedykacja	Rola vCISO jest pełniona dla jednego klienta w danym czasie. Praca operacyjna niższych poziomów może być delegowana do konsultantów PushSec pod nadzorem vCISO.
Umocowanie	Uchwała Zarządu określająca zakres, niezależność funkcji ryzyka ICT i linię raportowania. Projekt dostarczamy w pierwszym miesiącu.
Odpowiedzialność	W umowach nie przyjmujemy kar umownych ani gwarancji rezultatu. Odpowiedzialność za decyzje regulacyjne pozostaje po stronie Zarządu, zgodnie z DORA art. 5.
Wymiar i cena	Stała dniówka dla poziomu, niezależna od wymiaru. Dni niewykorzystane w miesiącu przechodzą na kolejny miesiąc w ramach kwartału. Ewidencja dni per obszar w raporcie miesięcznym.
Umowa	Minimum 3 miesiące, potem miesięczne wypowiedzenie. Bez zobowiązania rocznego, bez kar umownych.
Zmiana wymiaru lub poziomu	Co kwartał decyzja o wymiarze (w górę lub w dół) i o poziomie drabinki. Bez zmiany dostawcy, z zachowaniem kontekstu.
Czas reakcji	Pierwsza odpowiedź do 2 godzin w dni robocze. Dla incydentów ścieżka uzgodniona na kickoffie.
Nadzór merytoryczny	Każdy poziom działa pod nadzorem certyfikowanego ISO/IEC 27001 Lead Auditora (BSI, IRCA). Standard pracy nie zależy od pojedynczej osoby.
Poufność i dane	NDA przed przekazaniem dokumentacji, umowa powierzenia, gdy zakres tego wymaga.
Własność wyników	Plan działania i cała wytworzona dokumentacja pozostają własnością klienta, także po zakończeniu umowy.
Ubezpieczenie	OC zawodowe konsultanta ds. bezpieczeństwa: 1,5 mln zł, w tym klauzula cyber i RODO 200 tys. zł (Lloyd's).
Forma pracy	Zdalnie lub hybrydowo. Warszawa i okolice: spotkania na miejscu w uzgodnionym rytmie.
Ceny	Netto, doliczamy 23% VAT.

12. Dowody

PushSec łączy podejście praktyczne z uwzględnieniem wymagań regulacyjnych. Dzięki współpracy poprawiliśmy poziom organizacji w obszarze bezpieczeństwa informacji, zgodności oraz odporności operacyjnej.

Fincard, instytucja płatnicza. Wdrożenie DORA, model vCISO

Firma jest rzetelnym partnerem merytorycznym i biznesowym, realizuje usługi z należytą starannością. Powierzone zadania są wykonywane w pełni profesjonalnie i z dbałością o jakość.

DS Stream, firma technologiczna. Audyt i doradztwo ISO 27001

Rafał Dobrosielski wykazał się rzetelnością, kompetencją, dbałością o klienta oraz szeroką znajomością tematyki bezpieczeństwa IT.

NetCredit, firma finansowa. Szkolenia z cyberbezpieczeństwa

Pełne listy referencyjne: pushsec.pl/klienci

Zobacz produkt, zanim zapłacisz

Publiczne próbki dokumentów w tym stylu i na tym poziomie szczegółowości, na dwóch fikcyjnych podmiotach: Demo SaaS Sp. z o.o., 45 osób (startery, poziomy 1 i 2) i Demo Platform Sp. z o.o., B2B SaaS 140 osób z klientami bankowymi (vCISO):

- Raport health-check dokumentacji SZBI (17 obszarów, karty ustaleń)
- Komplet odpowiedzi na kwestionariusz bezpieczeństwa z biblioteką odpowiedzi
- Raport samoidentyfikacji KSC
- Demo diagnozy startowej, raportu miesięcznego dla Zarządu i mapy drogowej 12M vCISO (pushsec.pl/vciso)

pushsec.pl/sklep

Kto za tym stoi

Rafał Dobrosielski, auditor wiodący ISO/IEC 27001 (BSI, IRCA), vCISO. Wdrożenia DORA, ISO 27001 i NIS2/KSC w FinTech, SaaS i kancelariach. Autorska metodyka health-check: 17 obszarów SZBI, 157 punktów kontrolnych. OC zawodowe 1,5 mln zł.

Następny krok: 30 minut, po których dostajesz ofertę w dwóch wariantach

Na bezpłatnej konsultacji ustalamy poziom i wymiar. Po rozmowie otrzymujesz ofertę z wariantem wejściowym i docelowym, z cenami i zakresem per obszar. Małe kupuje się łatwo, dlatego zawsze pokazujemy prostszą ścieżkę.

pushsec.pl/kontakt/?temat=vciso · info@pushsec.pl · (+48) 780 519 553 · Wszystkie poziomy i widełki: pushsec.pl/vciso

Skróty: ISO 27001 oznacza normę ISO/IEC 27001:2022. UoKSC oznacza ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. 2026 poz. 20, ze zm. Dz.U. 2026 poz. 252). DORA oznacza rozporządzenie (UE) 2022/2554. RODO oznacza rozporządzenie (UE) 2016/679. Odwołania do wymagań pokazują, które obowiązki rola pokrywa; nie stanowią opinii prawnej. Fragmenty dokumentów w tym opisie dotyczą fikcyjnych podmiotów Demo SaaS Sp. z o.o. i Demo Platform Sp. z o.o.