KONSULTACJA STRATEGICZNA 2H. PRÓBKA NOTATKI PO KONSULTACJI

Konsultacja strategiczna. Notatka po konsultacji

Dwie godziny z auditorem wiodącym, po których zostaje decyzja, plan i kwoty, a nie wrażenie z rozmowy

Próbka produktu. Dokument pokazuje, co klient otrzymuje po konsultacji strategicznej PushSec: pisemną notatkę z rekomendacją, ścieżką, kosztami i następnymi krokami, do wykorzystania na posiedzeniu Zarządu. Spółka i dane są fikcyjne. Podmiot jest ten sam, co w pozostałych próbkach PushSec, ale w momencie sprzed health-checku.

Metryka

Dokument	Notatka po konsultacji strategicznej
Klient	Demo SaaS Sp. z o.o. (podmiot fikcyjny, dalej: Spółka). Uczestnicy: Prezes Zarządu, Dyrektor Operacyjny, Kierownik IT
Termin	10.08.2026, 2 godziny, online
Prowadzący	Rafał Dobrosielski, PushSec. Auditor wiodący ISO/IEC 27001 (BSI, IRCA)
Data wydania	11.08.2026
Klasyfikacja	Materiał demonstracyjny, do publikacji (wersja kliencka: Poufne)

1. Pytanie, z którym przyszła Spółka

Klient enterprise z sektora finansowego uzależnia podpisanie umowy od certyfikatu ISO 27001 albo raportu SOC 2 w ciągu 12 miesięcy. Druga oferta, od klienta z USA, wymienia SOC 2. Spółka ma 45 osób, dokumentację z zakupionych szablonów, brak etatu bezpieczeństwa i budżet do 60 tys. zł na rok. Pytanie: **ISO 27001 czy SOC 2, w jakiej kolejności, za ile i kiedy realnie**.

2. Co ustaliliśmy w trakcie rozmowy

- Portfel klientów: 80% przychodu z UE, w tym trzech klientów objętych DORA; klient z USA to na dziś jedna oferta, bez podpisanej umowy.
- Dokumentacja istnieje, ale nikt jej nie prowadzi; brak zapisów z przeglądów, brak rejestru ryzyka z właścicielami. Ocena wstępna, do potwierdzenia health-checkiem: dokumentacja pokrywa strukturę normy, system nie działa dowodowo.
- Zespół IT (4 osoby) ma dobre praktyki techniczne: kopie, MFA na produkcji, rozdzielone środowiska, roczny pentest. To skraca wdrożenie, bo budujemy zapisy do istniejącej praktyki.
- Nie ma osoby, która mogłaby pełnić rolę Pełnomocnika ds. SZBI w wymiarze 4 godzin tygodniowo; Kierownik IT jest przeciążony.
- Termin: 12 miesięcy od dziś to sierpień 2027. Klient nie wymaga certyfikatu w dniu podpisania, wymaga wiarygodnego harmonogramu i dowodów postępu.

3. Rekomendacja

DECYZJA REKOMENDOWANA

Najpierw ISO 27001, SOC 2 dopiero po podpisaniu umowy z klientem z USA

ISO 27001 domyka wymaganie klienta z UE i klientów objętych DORA, jest rozpoznawany przez wszystkich kontrahentów Spółki i buduje system, na którym SOC 2 Type II można oprzeć bez dublowania pracy (ok. 70% kontroli wspólnych). SOC 2 dla jednej niepodpisanej oferty to koszt audytu CPA i 6 do 12 miesięcy okresu obserwacji bez pewnego przychodu. Jeśli umowa z USA zostanie podpisana, SOC 2 Type I da się dołożyć na gotowym SZBI w ciągu 3 do 4 miesięcy.

4. Ścieżka i koszty

Etap	Kiedy	Co	Koszt orientacyjny netto
0	wrzesień 2026	Health-check dokumentacji SZBI: obiektywny punkt startu, lista ustaleń z terminami, do pokazania klientowi jako dowód postępu	3 400 zł, stała cena
1	wrzesień 2026 do luty 2027	Domknięcie ustaleń i uruchomienie zapisów: poziom 2 zewnętrznego działu bezpieczeństwa (Manager z rolą Pełnomocnika), wymiar 7 dni	15 400 zł/mies. przez 6 mies.
2	styczeń 2027	Audyt wewnętrzny przez niezależnego audytora PushSec i przegląd zarządzania	w cenie poziomu 2 (audytor inny niż Pełnomocnik)
3	marzec do czerwiec 2027	Audyt certyfikujący, etap 1 i 2, jednostka akredytowana	ok. 15 do 25 tys. zł, koszt jednostki, 3 lata z nadzorami
4	od lipca 2027	Utrzymanie: poziom 1 lub 2 w mniejszym wymiarze	od 4 800 zł/mies.
opcja	po podpisaniu umowy z USA	SOC 2 Type I na gotowym SZBI, potem Type II po 6 do 12 mies. obserwacji	audytor CPA ok. 40 do 80 tys. zł plus wsparcie PushSec

Budżet 60 tys. zł nie wystarczy na ścieżkę z poziomem 2 przez 6 miesięcy (ok. 96 tys. zł plus jednostka). Dwie alternatywy w budżecie: poziom 2 w wymiarze 4 dni (8 800 zł/mies., 53 tys. zł za 6 mies.) z większą pracą własną Kierownika IT, albo poziom 1 w wymiarze 6 dni (9 600 zł/mies.) z Pełnomocnikiem po stronie Spółki. Obie wydłużają gotowość o 2 do 3 miesiące. Decyzja należy do Zarządu; rekomendujemy rozmowę z klientem o harmonogramie z certyfikacją w drugiej połowie 2027 r. zamiast cięcia zakresu.

5. Co powiedzieć klientowi enterprise już teraz

- Spółka ma udokumentowany SZBI zgodny z ISO/IEC 27001:2022 i niezależny przegląd dokumentacji zaplanowany na wrzesień 2026 (raport dostępny pod NDA).
- Harmonogram: audyt certyfikujący w pierwszej połowie 2027 r., certyfikat najpóźniej w drugiej połowie 2027 r.; w umowie zobowiązanie do harmonogramu i dowodów postępu, nie do daty certyfikatu.
- Do czasu certyfikatu: odpowiedzi na kwestionariusz bezpieczeństwa klienta z listą kontroli kompensacyjnych i terminów.

6. Następne kroki

Nr	Krok	Kto	Termin
1	Decyzja Zarządu o ścieżce i wymiarze (poziom 2 x 7 dni, poziom 2 x 4 dni albo poziom 1 x 6 dni)	Zarząd	do 20.08.2026
2	Zamówienie health-checku i przekazanie dokumentacji	Dyrektor Operacyjny	do 25.08.2026
3	Rozmowa z klientem enterprise o harmonogramie z dowodami postępu; PushSec przygotuje jednostronicowy brief	Prezes	do 31.08.2026
4	Wybór jednostki certyfikującej i wstępne zapytanie o terminy na 2027 (PushSec przekazuje listę trzech jednostek i wzór zapytania)	Kierownik IT	do 30.09.2026

7. Zastrzeżenia

- Notatka opiera się na informacjach przekazanych ustnie podczas konsultacji; PushSec nie weryfikował dokumentacji ani systemów.
- Koszty jednostki certyfikującej i audytora CPA są orientacyjne i zależą od oferty konkretnego podmiotu.
- Notatka nie jest ofertą handlową. Oferta z zakresem i ceną per obszar jest przygotowywana po decyzji Zarządu o ścieżce.

Konsultacja strategiczna 2 godziny. 790 zł netto

Dwie godziny z auditorem wiodącym ISO 27001, online, zwykle w ciągu 5 dni roboczych od zamówienia. Po konsultacji notatka w tym układzie, zwykle następnego dnia roboczego. Kwota konsultacji jest odliczana od pierwszej faktury, jeśli w ciągu 30 dni zamówisz health-check, kwestionariusz, samoidentyfikację lub poziom drabinki.

Zamówienie: pushsec.pl/sklep · info@pushsec.pl · (+48) 780 519 553

Dokument demonstracyjny PushSec. Dane spółki, ustalenia i dowody są fikcyjne. Układ, klasyfikacja i poziom szczegółowości odpowiadają dokumentowi dostarczanemu klientom. Wersja dostarczana klientowi ma klasyfikację Poufne.