HEALTH-CHECK DOKUMENTACJI SZBI. PRÓBKA RAPORTU

Health-check dokumentacji SZBI

Raport z przeglądu dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji względem ISO/IEC 27001:2022

Próbka produktu. Dokument przedstawia realny układ i poziom szczegółowości raportu, który otrzymuje klient usługi Health-check dokumentacji SZBI. Dane spółki, ustalenia i dowody są fikcyjne i zostały zbudowane na profilu typowego dostawcy B2B SaaS przygotowującego się do certyfikacji. Żadne informacje klientów PushSec nie zostały tu wykorzystane. Próbka zawiera pełną ocenę per obszar oraz 3 z 14 kart ustaleń. Wersja dostarczana klientowi ma klasyfikację Poufne.

Metryka dokumentu

Dokument	Health-check dokumentacji SZBI. Raport z przeglądu
Klient	Demo SaaS Sp. z o.o. (podmiot fikcyjny, dalej: Spółka)
Zakres oceny	ISO/IEC 27001:2022, punkty 4 do 10 oraz kontrole Załącznika A wskazane w Deklaracji Stosowania
Data przeglądu	26.08.2026
Autor	Rafał Dobrosielski, PushSec. Auditor wiodący ISO/IEC 27001 (BSI, IRCA)
Data wydania	31.08.2026
Wersja	1.0. Status: finalny
Klasyfikacja	Materiał demonstracyjny, do publikacji (wersja kliencka: Poufne)
Dystrybucja	Zarząd, Kierownik IT, Pełnomocnik ds. SZBI

Executive Summary

Kontekst i cel. Spółka samodzielnie zbudowała dokumentację SZBI na bazie zakupionego pakietu szablonów i planuje audyt certyfikujący ISO/IEC 27001 w pierwszej połowie 2027 r. Celem przeglądu było ustalenie, czy dokumentacja w stanie na dzień 26.08.2026 jest gotowa do audytu oraz jakie działania są niezbędne przed zgłoszeniem do jednostki certyfikującej.

WNIOSEK GŁÓWNY

Dokumentacja pokrywa strukturę normy, ale system nie jest gotowy do certyfikacji

Źródłem problemu nie jest brak dokumentów, tylko brak powiązania między oceną ryzyka, Deklaracją Stosowania i zapisami z działania systemu. W obecnym stanie audyt certyfikujący zakończyłby się niezgodnościami dużymi. Domknięcie ustaleń wymaga od 18 do 24 dni roboczych po stronie Spółki. Przy starcie we wrześniu realna gotowość audytowa przypada na marzec 2027 r.

Trzy najważniejsze ryzyka

1. Spółka poniesie koszt audytu certyfikującego bez szansy na certyfikat, ponieważ Deklaracja Stosowania nie wynika z oceny ryzyka, a jest sprawdzana już na etapie 1 audytu.

Rekomendowane decyzje Zarządu

1. Zatwierdzić plan domknięcia 14 ustaleń z terminami wskazanymi w sekcji 4. Nakład: od 18 do 24 dni roboczych.

2. Zarząd nie ma udokumentowanej akceptacji ryzyka, więc przy poważnym incydencie Spółka nie wykaże, że decyzje o priorytetach były świadome.
3. Brak zapisów z działania SZBI przesuwa termin certyfikacji niezależnie od jakości polityk, ponieważ jednostka certyfikująca wymaga dowodów z zamkniętego cyklu, a nie samej dokumentacji.

2. Wyznaczyć Pełnomocnika ds. SZBI z gwarantowanym budżetem czasu minimum 4 godzin tygodniowo. Obecnie rola jest przypisana nieformalnie.
3. Zaakceptować formalnie ryzyka rezydualne po uzupełnieniu rejestru. Termin: 30 dni.
4. Zatwierdzić termin audytu wewnętrznego na styczeń 2027 r. oraz zgłoszenie do jednostki certyfikującej nie wcześniej niż na luty 2027 r.

Co działa dobrze. Komplet polityk istnieje, jest zatwierdzony i ma spójną numerację. Procesy techniczne, w szczególności kopie zapasowe, zarządzanie podatnościami i rozdzielenie środowisk, działają w praktyce lepiej, niż opisuje je dokumentacja. Umowy z kluczowymi dostawcami zawierają umowy powierzenia. To realna przewaga: uzupełniamy zapisy do istniejącej praktyki, zamiast budować praktykę od zera.

1. Zakres przeglądu

Przegląd objął dokumentację SZBI przekazaną przez Spółkę w repozytorium współdzielonym, w stanie na dzień 26.08.2026. Ocenie podlegało 17 obszarów SZBI, sprawdzanych według listy 157 punktów kontrolnych metodyki PushSec. Kryterium oceny stanowiły wymagania punktów 4 do 10 normy ISO/IEC 27001:2022 oraz kontrole Załącznika A wskazane jako mające zastosowanie w Deklaracji Stosowania Spółki. Normę ISO/IEC 27002:2022 zastosowano wyłącznie jako wskazówkę wdrożeniową.

Profil Spółki: dostawca platformy SaaS do obiegu dokumentów, 45 osób, praca hybrydowa, infrastruktura w chmurze publicznej w regionie eu-central-1, trzech klientów z sektora finansowego, rosnąca liczba kwestionariuszy bezpieczeństwa od klientów korporacyjnych.

Metoda: analiza dokumentów, weryfikacja spójności między dokumentami oraz wywiady zdalne z rolami Kierownik IT i Dyrektor Operacyjny. Przegląd nie obejmował testów technicznych ani weryfikacji konfiguracji systemów. Ustalenia opierają się na dokumentach i zapisach udostępnionych przez Spółkę.

Skala oceny obszaru: Zgodne, Częściowo zgodne, Niezgodne, Nie dotyczy. Priorytet rekomendacji: K krytyczny, W wysoki, Ś średni, N niski.

2. Wynik w liczbach

3	10	4	14
obszary zgodne	częściowo zgodne	niezgodne	ustaleń do domknięcia

Rozkład priorytetów ustaleń: 4 krytyczne, 6 wysokich, 4 średnie. Szacowany łączny nakład domknięcia: od 18 do 24 dni roboczych po stronie Spółki, bez nakładu PushSec.

3. Ocena per obszar

#	Obszar SZBI	Kryterium	Ocena	Ustalenia
1	Kontekst organizacji i zakres SZBI	pkt 4.1 do 4.4	Częściowo zgodne	HC-2026-03
2	Przywództwo i polityka bezpieczeństwa	pkt 5.1, 5.2	**Zgodne**	brak
3	Role, odpowiedzialności i uprawnienia	pkt 5.3, kontrola A.5.2	Częściowo zgodne	HC-2026-04
4	Ocena i postępowanie z ryzykiem	pkt 6.1.1 do 6.1.3, 8.2, 8.3	**Niezgodne**	HC-2026-02

#	Obszar SZBI	Kryterium	Ocena	Ustalenia
5	Deklaracja Stosowania	pkt 6.1.3 lit. d	**Niezgodne**	HC-2026-01
6	Cele bezpieczeństwa i mierniki	pkt 6.2, 9.1	**Niezgodne**	HC-2026-06
7	Zasoby, kompetencje i świadomość	pkt 7.1 do 7.3, kontrola A.6.3	Częściowo zgodne	HC-2026-07
8	Nadzór nad informacją udokumentowaną	pkt 7.5	Częściowo zgodne	HC-2026-08
9	Zarządzanie aktywami i klasyfikacja	kontrole A.5.9 do A.5.13	Częściowo zgodne	HC-2026-09
10	Kontrola dostępu i tożsamość	kontrole A.5.15 do A.5.18, A.8.2 do A.8.5	**Niezgodne**	HC-2026-05
11	Bezpieczeństwo w relacjach z dostawcami	kontrole A.5.19 do A.5.23	Częściowo zgodne	HC-2026-10
12	Zarządzanie incydentami	kontrole A.5.24 do A.5.28	Częściowo zgodne	HC-2026-11
13	Ciągłość działania	kontrole A.5.29, A.5.30, A.8.13, A.8.14	Częściowo zgodne	HC-2026-12
14	Bezpieczeństwo rozwoju oprogramowania	kontrole A.8.25 do A.8.31	**Zgodne**	brak
15	Bezpieczeństwo operacyjne i podatności	kontrole A.8.6 do A.8.12, A.8.15, A.8.16	**Zgodne**	brak
16	Zgodność prawna i ochrona danych osobowych	kontrole A.5.31 do A.5.36	Częściowo zgodne	HC-2026-13
17	Audyt wewnętrzny, przegląd zarządzania, doskonalenie	pkt 9.2, 9.3, 10.1, 10.2	Częściowo zgodne	HC-2026-14

Uwaga metodyczna. Ocena Niezgodne oznacza, że wymaganie normy nie jest spełnione w dokumentacji i przy audycie certyfikującym stanowiłoby podstawę niezgodności. Ocena Częściowo zgodne oznacza, że dokument istnieje, ale nie zawiera wszystkich elementów wymaganych przez normę lub nie jest spójny z pozostałą dokumentacją. Health-check ocenia dokumentację i zapisy, nie zastępuje audytu wewnętrznego wymaganego punktem 9.2 normy.

4. Zestawienie ustaleń

ID	Ustalenie	Prio	Właściciel	Termin
HC-2026-01	Deklaracja Stosowania niepowiązana z oceną ryzyka, brak uzasadnień wyłączeń	K	Pełnomocnik SZBI	14 dni
HC-2026-02	Rejestr ryzyka bez właścicieli ryzyka i bez akceptacji ryzyka rezydualnego	K	Zarząd	30 dni
HC-2026-03	Zakres SZBI nie rozstrzyga granicy odpowiedzialności w chmurze publicznej	W	Kierownik IT	30 dni
HC-2026-04	Rola Pełnomocnika ds. SZBI przypisana nieformalnie, bez zakresu i budżetu czasu	W	Zarząd	30 dni
HC-2026-05	Brak zapisów potwierdzających wykonanie cyklicznych działań SZBI	K	Pełnomocnik SZBI	60 dni

ID	Ustalenie	Prio	Właściciel	Termin
HC-2026-06	Cele bezpieczeństwa bez mierników i bez powiązania z monitorowaniem	W	Pełnomocnik SZBI	45 dni
HC-2026-07	Program szkoleń świadomościowych bez planu rocznego i weryfikacji efektu	Ś	Dział HR	90 dni
HC-2026-08	Polityki odwołują się do ISO/IEC 27001:2013 i nieaktualnej numeracji kontroli	Ś	Pełnomocnik SZBI	45 dni
HC-2026-09	Inwentarz aktywów nie obejmuje usług SaaS używanych przez działy biznesowe	W	Kierownik IT	60 dni
HC-2026-10	Brak kryteriów oceny i cyklicznego przeglądu dostawców krytycznych	W	Dyrektor Operacyjny	60 dni
HC-2026-11	Procedura incydentów bez kryteriów klasyfikacji i ścieżki zgłoszeń zewnętrznych	K	Kierownik IT	30 dni
HC-2026-12	Plan ciągłości działania bez analizy wpływu na biznes i bez zapisu z testu	Ś	Dyrektor Operacyjny	90 dni
HC-2026-13	Rejestr czynności przetwarzania nieaktualizowany od 2024 r.	Ś	Dyrektor Operacyjny	60 dni
HC-2026-14	Brak programu i harmonogramu audytów wewnętrznych	W	Pełnomocnik SZBI	45 dni

5. Karty ustaleń

Poniżej trzy karty w układzie stosowanym w pełnym raporcie. Pełny raport zawiera kartę dla każdego z 14 ustaleń.

HC-2026-01. Deklaracja Stosowania niepowiązana z oceną ryzyka, brak uzasadnień wyłączeń	
Klasyfikacja	Niezgodne. Priorytet K, krytyczny
Kryterium	pkt 6.1.3 lit. d ISO/IEC 27001:2022
Stan stwierdzony	Deklaracja Stosowania zawiera wszystkie 93 kontrole Załącznika A wraz ze statusem stosowania. Kolumna uzasadnienia pozostaje pusta dla 11 kontroli oznaczonych jako niemające zastosowania. Dokument nie zawiera odniesienia do identyfikatorów ryzyk z rejestru ryzyka ani informacji o stanie wdrożenia poszczególnych kontroli.
Dowód	Plik SoA_v1.0.xlsx z dnia 12.03.2026, arkusz Kontrole. Wywiad z rolą Kierownik IT z dnia 26.08.2026.
Skutek i ryzyko	Deklaracja Stosowania jest jednym z pierwszych dokumentów sprawdzanych na etapie 1 audytu certyfikującego. W obecnej postaci nie wykazuje, że dobór kontroli wynika z oceny ryzyka, co norma wymaga wprost. Skutkiem będzie niezgodność duża, wstrzymanie przejścia do etapu 2 i przesunięcie certyfikacji o jeden cykl audytowy, typowo od 6 do 10 tygodni, przy zachowanym koszcie jednostki certyfikującej.
Rekomendacja	Uzupełnić uzasadnienia wyłączenia dla 11 kontroli, wskazując przyczynę biznesową lub techniczną. Dodać do Deklaracji Stosowania kolumnę z identyfikatorem ryzyka uzasadniającego zastosowanie kontroli oraz kolumnę stanu wdrożenia. Zatwierdzić dokument jako wersję 2.0.
Właściciel	Pełnomocnik ds. SZBI
Termin	14 dni. Ustalenie kwalifikuje się jako quick win, nakład około 1,5 dnia roboczego.

HC-2026-02. Rejestr ryzyka bez właścicieli ryzyka i bez akceptacji ryzyka rezydualnego	
Klasyfikacja	Niezgodne. Priorytet K, krytyczny
Kryterium	pkt 6.1.2 lit. c ppkt 2 (właściciele ryzyka), pkt 6.1.3 lit. f (akceptacja ryzyk rezydualnych), pkt 8.2 i 8.3 ISO/IEC 27001:2022
Stan stwierdzony	Rejestr ryzyka zawiera 34 pozycje z oceną prawdopodobieństwa i skutku. Kolumna właściciela ryzyka jest wypełniona w 6 pozycjach. Rejestr nie zawiera oceny ryzyka rezydualnego po zastosowaniu kontroli. Brak zapisu potwierdzającego akceptację ryzyk przez kierownictwo. Ostatnia aktualizacja rejestru nastąpiła 12.03.2026, mimo uruchomienia nowego środowiska produkcyjnego w czerwcu 2026 r.
Dowód	Plik Rejestr_ryzyka_2026.xlsx, data modyfikacji 12.03.2026. Wywiad z rolą Dyrektor Operacyjny z dnia 26.08.2026.
Skutek i ryzyko	Bez właścicieli ryzyka działania zaradcze nie mają adresata i w praktyce nie są realizowane. Bez zapisu akceptacji Spółka nie wykaże, że Zarząd świadomie przyjął ryzyka rezydualne. Przy poważnym incydencie lub przy audycie kontrahenta z sektora finansowego brak tego zapisu utrudnia wykazanie należytej staranności i osłabia pozycję negocjacyjną w rozmowie o odpowiedzialności kontraktowej.
Rekomendacja	Przypisać właściciela ryzyka na poziomie roli do każdej z 34 pozycji. Uzupełnić ocenę ryzyka rezydualnego. Zaktualizować rejestr o zmiany środowiskowe z czerwca 2026 r. Zatwierdzić ryzyka rezydualne protokołem z posiedzenia Zarządu i przechowywać protokół jako zapis SZBI.
Właściciel	Zarząd, przy wsparciu Pełnomocnika ds. SZBI
Termin	30 dni. Nakład około 3 dni roboczych.

HC-2026-05. Brak zapisów potwierdzających wykonanie cyklicznych działań SZBI	
Klasyfikacja	Niezgodne. Priorytet K, krytyczny
Kryterium	pkt 7.5.3, 9.1 i 9.3 ISO/IEC 27001:2022, kontrole A.5.18 i A.6.3
Stan stwierdzony	Polityka kontroli dostępu przewiduje przegląd uprawnień co 6 miesięcy. W repozytorium dokumentacji nie odnaleziono zapisu z żadnego przeglądu. Nie odnaleziono również listy uczestników szkolenia świadomościowego za rok 2026 ani protokołu z przeglądu zarządzania. Wywiad potwierdził, że przegląd uprawnień był wykonywany doraźnie przy odejściach pracowników, bez utrwalenia wyniku.
Dowód	Przegląd struktury repozytorium dokumentacji SZBI na dzień 26.08.2026, katalogi Zapisy i Szkolenia puste. Wywiad z rolą Kierownik IT.
Skutek i ryzyko	Dokumentacja opisuje system, który nie ma dowodu działania. Jednostka certyfikująca ocenia funkcjonowanie SZBI na podstawie zapisów z zamkniętego cyklu, nie na podstawie samych procedur. Brak zapisów oznacza, że termin audytu certyfikującego wyznacza kalendarz zbierania dowodów, a nie gotowość dokumentacji. To najsilniejszy czynnik przesuwający termin certyfikacji w tym przeglądzie.
Rekomendacja	Uruchomić rejestr zapisów SZBI wskazujący dla każdego działania cyklicznego częstotliwość, właściciela i miejsce przechowywania dowodu. Wykonać zaległy przegląd uprawnień i utrwalić jego wynik. Przeprowadzić szkolenie świadomościowe z listą uczestników i testem sprawdzającym. Zaplanować pierwszy przegląd zarządzania na grudzień 2026 r.
Właściciel	Pełnomocnik ds. SZBI
Termin	60 dni na uruchomienie rejestru i wykonanie zaległych działań. Nakład około 4 dni roboczych.

Karty ustaleń HC-2026-03, HC-2026-04 oraz HC-2026-06 do HC-2026-14 znajdują się w pełnej wersji raportu.

6. Proponowane następne kroki

Etap	Horyzont	Zakres	Efekt
Etap 1	do 14 dni	Domknięcie ustaleń typu quick win: HC-2026-01 oraz aktualizacja odwołań normatywnych w politykach	Deklaracja Stosowania i polityki gotowe do przedstawienia audytorowi
Etap 2	do 60 dni	Domknięcie ustaleń krytycznych i wysokich: ryzyko, zakres SZBI, role, incydenty, dostawcy, program audytów	System spójny wewnętrznie, dokumentacja gotowa do audytu wewnętrznego
Etap 3	od 60 do 120 dni	Zbieranie zapisów z pełnego cyklu, szkolenia, przegląd uprawnień, test planu ciągłości działania	Dowody działania SZBI za zamknięty okres
Etap 4	styczeń 2027	Audyt wewnętrzny SZBI zgodnie z pkt 9.2 oraz przegląd zarządzania zgodnie z pkt 9.3	Warunek formalny zgłoszenia do jednostki certyfikującej spełniony
Etap 5	marzec do czerwca 2027	Audyt certyfikujący, etap 1 i etap 2	Certyfikat ISO/IEC 27001:2022

Wsparcie PushSec, opcjonalne. Spółka może zrealizować etapy 1 do 3 samodzielnie na podstawie tego raportu. Każde ustalenie zawiera rekomendację na poziomie wykonawczym. Jeśli Spółka zdecyduje o wsparciu zewnętrznym, naturalnym zakresem jest audyt wewnętrzny w etapie 4, ponieważ Pełnomocnik ds. SZBI nie może audytować własnej pracy, co wynika z wymogu bezstronności audytu w pkt 9.2 normy. Domykanie ustaleń etapów 1 do 3 jest objęte zakresem poziomu 2 i 3 zewnętrznego działu bezpieczeństwa PushSec.

7. Zastrzeżenia

- Przegląd objął dokumentację i zapisy udostępnione przez Spółkę w okresie od 20.08.2026 do 26.08.2026. Dokumenty nieprzekazane nie były przedmiotem oceny.
- Health-check nie jest audytem wewnętrznym w rozumieniu pkt 9.2 ISO/IEC 27001:2022 i nie zastępuje audytu certyfikującego.
- Przegląd nie obejmował weryfikacji technicznej konfiguracji systemów ani testów bezpieczeństwa.
- Ocena odzwierciedla stan na dzień 26.08.2026. Zmiany wprowadzone po tej dacie nie są uwzględnione.
- Raport zawiera osąd ekspercki auditora wiodącego. Ostateczna ocena zgodności należy do jednostki certyfikującej.

Health-check dokumentacji SZBI. 3 400 zł netto, stała cena

Realizacja od przekazania dokumentacji do wydania raportu: 10 dni roboczych. Raport obejmuje 17 obszarów SZBI, kartę dla każdego ustalenia, priorytety, właścicieli, terminy i szacunek nakładu. Bez wyceny indywidualnej.

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.