Deklaracja Stosowania (SoA) ISO 27001

Szablon Deklaracji Stosowania (Statement of Applicability, pkt 6.1.3 d ISO/IEC 27001:2022) dla 4 grup i 93 zabezpieczeń Załącznika A wraz z uzasadnieniem włączeń, wyłączeń i powiązaniem z analizą ryzyka w DOCX i PDF.

Stan prawny i wymagań: 2026-11-17 | Wersja pliku: 2026-11 | Licencja: CC BY 4.0 · tql.pl/pl/wzory/deklaracja-stosowania-soa-iso-27001

1. Struktura kolumn Deklaracji Stosowania (SoA) wg ISO/IEC 27001:2022

Nr	Element / Pole	Instrukcja wypełnienia	Podstawa
1	Metryka dokumentu SoA, wersja i odniesienie do zakresu SZBI	Numer wydania Deklaracji Stosowania, data zatwierdzenia przez kierownictwo oraz jednoznaczne powiązanie z dokumentem Zakresu SZBI z pkt 4.3.	pkt 4.3, pkt 6.1.3 d oraz pkt 7.5 ISO/IEC 27001:2022
2	Oznaczenie i tytuł zabezpieczenia referencyjnego (Załącznik A lub własne)	Numer i nazwa zabezpieczenia zgodnie z ISO/IEC 27001:2022 (A.5.1 do A.8.34) oraz ewentualne dodatkowe zabezpieczenia spoza Załącznika A.	pkt 6.1.3 c i Załącznik A ISO/IEC 27001:2022
3	Decyzja o stosowaniu (Stosowane: TAK / Wyłączone: NIE)	Jednoznaczne określenie, czy dane zabezpieczenie ma zastosowanie w granicach przyjętego zakresu SZBI organizacji.	pkt 6.1.3 d ISO/IEC 27001:2022
4	Źródło i uzasadnienie włączenia (ryzyko, prawo, umowa, praktyka)	Wskazanie identyfikatorów ryzyk z arkusza szacowania ryzyka, przepisów (RODO, KSC/NIS2) lub klauzul kontraktowych uzasadniających wybór.	pkt 6.1.3 d tiret drugie ISO/IEC 27001:2022
5	Uzasadnienie wyłączenia zabezpieczenia z Załącznika A (gdy NIE)	Konkretny powód architektoniczny lub organizacyjny wyjaśniający, dlaczego wyłączenie nie obniża bezpieczeństwa informacji w badanym zakresie.	pkt 6.1.3 d tiret czwarte ISO/IEC 27001:2022
6	Status wdrożenia operacyjnego (Wdrożone / W trakcie / Planowane)	Rzeczywisty stan realizacji zabezpieczenia w dniu zatwierdzenia SoA; przy statusie W trakcie - odniesienie do Planu postępowania z ryzykiem (RTP).	pkt 6.1.3 d tiret trzecie i pkt 6.1.3 e ISO/IEC 27001:2022
7	Opis sposobu realizacji i referencja do procedury lub konfiguracji	Zwięzły opis, jak organizacja realizuje zabezpieczenie w praktyce, wraz z kodem	wytyczne ISO/IEC 27002:2022 oraz pkt 8.1 ISO/IEC 27001:2022

		procedury, standardu technicznego lub narzędzia IT.	
8	Właściciel zabezpieczenia oraz dowód audytowy (artefakt)	Stanowisko odpowiadające za utrzymanie kontroli oraz weryfikowalny zapis prezentowany audytorowi wewnętrznemu i jednostce certyfikującej.	pkt 5.3 i pkt 9.1 ISO/IEC 27001:2022

2. Przykład wypełnienia wiersza SoA: zabezpieczenie chmurowe A.5.23 w spółce SaaS

Przykład sp. z o.o. utrzymuje aplikację webową w chmurze publicznej na terenie EOG bez własnej serwerowni on-premise i dokumentuje w SoA nadzór nad środowiskiem chmurowym.

Nr	Pole	Przykładowy zapis w dokumentacji
1	Metryka dokumentu SoA, wersja i odniesienie do zakresu SZBI	Deklaracja Stosowania SZBI wyd. 3.0 z 17.11.2026 r., zatwierdzona przez Zarząd Przykład sp. z o.o.; obejmuje wytwarzanie i utrzymanie aplikacji SaaS w Warszawie
2	Oznaczenie i tytuł zabezpieczenia referencyjnego (Załącznik A lub własne)	A.5.23 Bezpieczeństwo informacji przy korzystaniu z usług w chmurze
3	Decyzja o stosowaniu (Stosowane: TAK / Wyłączone: NIE)	TAK - zabezpieczenie stosowane w całym zakresie produkcyjnym i deweloperskim SZBI
4	Źródło i uzasadnienie włączenia (ryzyko, prawo, umowa, praktyka)	Ryzyka R-07 (błędna konfiguracja zasobów IaaS) i R-14 (utrata dostępności chmury); wymóg art. 28 i 32 RODO oraz umów SLA z klientami enterprise
5	Uzasadnienie wyłączenia zabezpieczenia z Załącznika A (gdy NIE)	Dotyczy np. A.7.14 lub A.8.25 wyłącznie przy pełnym uzasadnieniu; np. dla A.5.14: brak fizycznego transportu nośników wymiennych, całkowity zakaz w polityce
6	Status wdrożenia operacyjnego (Wdrożone / W trakcie / Planowane)	Wdrożone operacyjnie (przegląd konfiguracji CSPM oraz matryca współodpowiedzialności AWS/Azure zweryfikowane 10.10.2026 r.)
7	Opis sposobu realizacji i referencja do procedury lub konfiguracji	Procedura PBI-06 Korzystanie z chmury obliczeniowej: wymuszone SSO + MFA, szyfrowanie KMS, IaC w Terraform z przeglądem bezpieczeństwa przed wdrożeniem
8	Właściciel zabezpieczenia oraz dowód audytowy (artefakt)	Właściciel: Architekt Chmury / Lider DevOps; dowód: kwartalny raport zgodności kont chmurowych, rejestr dostawców chmury i logi IAM

3. Najczęstsze błędy i sposób ich uniknięcia

Błąd	Skutek	Jak uniknąć	Podstawa
Korzystanie na audycie ze starej struktury 114 zabezpieczeń w 14 działach z wycofanego wydania ISO/IEC 27001:2013	Niezgodność duża już podczas przeglądu dokumentacji Etapu 1 - okres przejściowy zakończył się, a certyfikacja wymaga układu 93 zabezpieczeń z wydania 2022.	Przebuduj arkusz SoA na 4 sekcje (A.5, A.6, A.7, A.8) i uwzględnij 11 nowych zabezpieczeń (m.in. Threat Intelligence A.5.7, chmura A.5.23, ICT dla ciągłości A.5.30, maskowanie danych A.8.11, bezpieczne kodowanie A.8.28).	Załącznik A normy ISO/IEC 27001:2022
Kopiowanie identycznego zdania „Wymaganie normy / Dobra praktyka" jako uzasadnienia dla wszystkich 93 wierszy	Audytor wykazuje brak powiązania między szacowaniem ryzyka (pkt 6.1.2) a doborem zabezpieczeń w SoA (pkt 6.1.3).	Przypisz do włączonych zabezpieczeń konkretne identyfikatory ryzyk z rejestru analizy ryzyka albo konkretne obowiązki prawne i kontraktowe.	pkt 6.1.3 b i d ISO/IEC 27001:2022
Całkowite wyłączenie grupy A.7 (Zabezpieczenia fizyczne) pod pretekstem pracy zdalnej lub chmury publicznej	Zakwestionowanie wyłączenia - nawet w modelu remote-first firma posiada laptopy służbowe, dokumenty rejestrowe, siedzibę lub sprzęt sieciowy wymagający ochrony.	Zamiast wyłączać całe A.7, opisz proporcjonalny sposób realizacji: szyfrowanie i ochronę fizyczną sprzętu poza biurem (A.7.9), utylizację dysków (A.7.14) oraz powołanie się na raporty SOC 2 / ISO 27001 dostawcy data center dla serwerów.	pkt 6.1.3 d i sekcja A.7 ISO/IEC 27001:2022
Deklarowanie statusu „Wdrożone" dla zabezpieczeń, które dopiero widnieją w planie zakupowym lub nie mają ani jednego zapisu	Podczas próby losowej na Etapie 2 brak dowodów działania (np. brak raportu z testu ciągłości ICT A.5.30 lub przeglądu kodów A.8.28) skutkuje niezgodnością.	Przed audytem certyfikującym zamknij wdrożenie kluczowych kontroli i zbierz realne dowody operacyjne, a działania długofalowe ujmij rzetelnie w Planie postępowania z ryzykiem.	pkt 6.1.3 d tiret trzecie oraz pkt 6.1.3 e ISO/IEC 27001:2022
Brak aktualizacji Deklaracji Stosowania po wdrożeniu nowych systemów AI, zmianie chmury lub przeglądzie ryzyka	Rozjazd między żywą architekturą IT organizacji a zatwierdzonym dokumentem SoA ujawniany na corocznym audycie nadzoru.	Powiąż obowiązkowy przegląd aktualności SoA z każdą zmianą istotną w architekturze, poważnym incydentem oraz corocznym przeglądem zarządzania (pkt 9.3).	pkt 6.3, pkt 8.3 i pkt 9.3 ISO/IEC 27001:2022

Opracował: Ireneusz Kozera, audytor wiodący ISO (TQL, www.tql.pl). Licencja CC BY 4.0: wzór ma charakter pomocniczo-informacyjny i przed wdrożeniem wymaga dopasowania do procesów i warunków konkretnej organizacji.