

Dazr Compliance · Karta produktu · SZBI i zabezpieczenia

SZBI oparty na *cyklicznych* zabezpieczeniach.

Każde zabezpieczenie w ISO 27001, RODO, NIS2 i ośmiu kolejnych frameworkach staje się cyklicznym zabezpieczeniem z właścicielem, terminem, dowodem i przypomnieniem.

Zatwierdź deklarację stosowania, powiąż zabezpieczenia z ryzykami, politykami i procesami, które obejmują, i obserwuj pokrycie według frameworku na pulpicie.

ISO 27001 · Zabezpieczenie A.5.18



Access rights

Access rights to information and assets provisioned, reviewed, modified and removed in accordance with the access-control policy.

● **Otwarte** ISO 27001 Ważny do 26 gru 2026

Przypisane do

 mark.jansen@bright ▼

Termin

06.10.2026



Powtarzanie

Bez
powtarzania

Co miesiąc

Co 3 miesiące

Co 6 miesięcy

Co rok

Najważniejsze funkcje

- ✓ **11 frameworków** w jednej przestrzeni roboczej: ISO 27001:2022 (93 zabezpieczenia z załącznika A plus klauzule 4-10), RODO, NIS2, NEN 7510, DORA, EU AI Act, ISO 27701, ISO 22301, SOC 2, BIO i PCI DSS.
- ✓ **Dowody** jako notatki, linki i pliki, z datą ważności i alertami o wygaśnięciu.
- ✓ **Powiązania i procesy**: łącz zabezpieczenia, ryzyka, polityki, procesy, aktywa, dostawców i czynności przetwarzania.
- ✓ **Cykliczne zabezpieczenia** z właścicielem, terminem, opisem, rekomendacją i cyklem przeglądu.
- ✓ **Deklaracja stosowania** z uzasadnieniem dla każdego zabezpieczenia, zatwierdzonymi wersjami, PDF i XLSX.
- ✓ **Pulpit**: pokryte zabezpieczenia według frameworku, pokrycie w czasie i co wymaga Twojej uwagi teraz.

Cykliczne zabezpieczenia z właścicielami

- Przypisz właściciela i termin. Właściciel dostaje e-mail, gdy zabezpieczenie zostanie przypisane, 7 dni przed terminem i co tydzień, gdy jest po terminie.
- Wybierz cykl: jednorazowo, co miesiąc, co 3 miesiące, co 6 miesięcy lub co rok. Plan Enterprise pozwala ustawić własny interwał dla każdego zabezpieczenia.
- Ukończenie zabezpieczenia blokuje jego dowody i planuje następny cykl, więc historia każdego przeglądu pozostaje nienaruszona.
- Komentarze przy każdym zabezpieczeniu trzymają dyskusję obok dowodów; komentować mogą też zewnętrzni audytorzy.
- Dodawaj własne zadania obok zabezpieczeń frameworku od planu Basic, na pracę, której żaden standard nie przewiduje.

Deklaracja stosowania

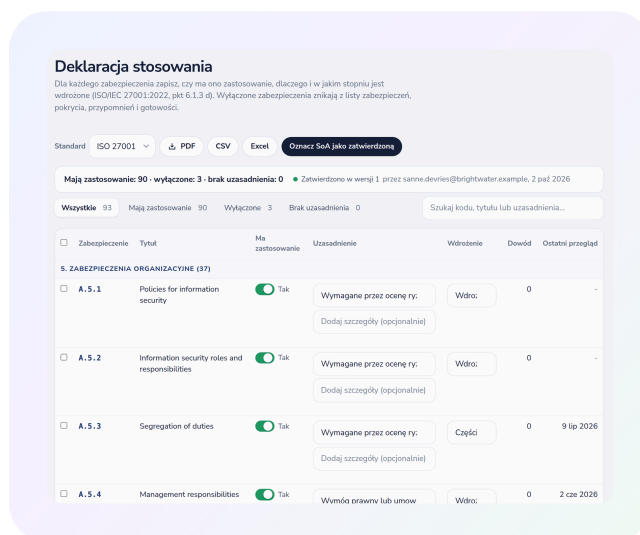
Oznacz każde zabezpieczenie ISO 27001 jako mające zastosowanie lub nie, podaj powód (ocena ryzyka, wymóg prawny lub umowny, wymóg biznesowy lub dobra praktyka) i zapisz status wdrożenia: wdrożone, częściowo, planowane lub niewdrożone. Wyłączenie zabezpieczenia wymaga uzasadnienia, tak jak oczekuje tego klauzula 6.1.3 d. Wyłączone zabezpieczenia znikają z listy zabezpieczeń i z pokrycia.

Zatwierdź wersję, gdy deklaracja stosowania jest gotowa: Dazr zachowuje każdą zatwierdzoną wersję z informacją, kto ją zatwierdził i kiedy, i eksportuje ją jako PDF lub XLSX. W planie Basic i wyższych.

Zabezpieczenia, ryzyka, polityki i procesy, powiązane

Wszystko w przestrzeni roboczej może wskazywać na wszystko inne: zabezpieczenia, ryzyka, polityki, procesy, aktywa, dostawców i czynności przetwarzania. Ryzyko pokazuje zabezpieczenia, które je ograniczają, polityka pokazuje zabezpieczenia, które wspiera, a proces pokazuje zabezpieczenia, ryzyka i aktywa, od których zależy. Powiązania widzą także audytorzy, tylko do odczytu.

Rejestr procesów (Pro i Enterprise) wymienia Twoje procesy biznesowe z opisem, krytycznością i właścicielem, do 500 na przestrzeń roboczą, aby praca nad ciągłością i ryzykiem opierała się na procesach, które się liczą.



Platforma

- ✓ Hosting w UE, tworzone przez Dazr we Włoszech
- ✓ Dane szyfrowane w spoczynku (AES-256-GCM)
- ✓ Logowanie przez Google, Microsoft lub kod e-mail
- ✓ Role: właściciel, administrator, członek, audytor
- ✓ Przeszukiwalny dziennik aktywności z eksportem
- ✓ Angielski, niemiecki, francuski, hiszpański i polski