

[Strona główna](#) / [Audyty NIS2/KSC](#) / [Checklista NIS2/KSC](#)

CHECKLISTA NIS2/KSC

Checklista NIS2/KSC: 40 pytań przed audytem

Checklista NIS2 dla zespołu, który przygotowuje organizację do wymagań ustawy o krajowym systemie cyberbezpieczeństwa: 40 pytań w sześciu obszarach, każde z przepisem. Zaznaczaj odpowiedzi na ekranie, wydrukuj albo pobierz PDF - bez podawania e-maila.

Checklista: innovix.pl/nis2/checklista/ · Innovix sp. z o.o., Aleja Śląska 1, 54-118 Wrocław · audyty@innovix.pl · [+48 575 621 877](tel:+48575621877)

Pytania układają się w kolejności, w jakiej zwykle przygotowuje się organizację: najpierw status i wpis do wykazu, potem odpowiedzialność kierownika podmiotu, system zarządzania bezpieczeństwem informacji, incydenty poważne, dokumentacja i na końcu audyt. Odpowiedź „nie” albo „nie wiem” to punkt do planu wdrożenia - podmioty, które spełniały przesłanki w dniu wejścia nowelizacji w życie, mają na wdrożenie czas do 3 kwietnia 2027 r.

Nie wiesz jeszcze, czy ustawa obejmuje Twoją organizację? Zacznij od kwalityfikatora NIS2/KSC.

Status i wpis do wykazu

Punkt wyjścia: czy i jak ustawa obejmuje organizację.

1. ☐ Czy ustaliliście status organizacji (podmiot kluczowy, ważny albo poza ustawą) i udokumentowaliście uzasadnienie: sektor, rodzaj podmiotu i wielkość razem z przedsiębiorstwami powiązanymi i partnerskimi?
(art. 5)
2. ☐ Czy wiecie, który organ jest właściwy dla Waszego sektora i do którego CSIRT trafiają zgłoszenia incydentów? (art. 41 i 41a; art. 44 ustawy zmieniającej)
3. ☐ Czy złożyliście wniosek o wpis do wykazu w systemie S46 albo uzupełniliście dane po wezwaniu ministra cyfryzacji? (art. 7c ust. 1, art. 7b ust. 2)
4. ☐ Czy dane w wykazie są aktualne, a zmiany zgłaszacie w ciągu 14 dni?
(art. 7c ust. 3)
5. ☐ Czy organizacja korzysta z systemu S46 i ma wyznaczonego administratora konta? (art. 9 ust. 1 pkt 4, art. 7 ust. 2 pkt 11)

Kierownik i organizacja

Za obowiązki odpowiada kierownik podmiotu – także wtedy, gdy powierzył je innym.

6. ☐ Czy kierownik podmiotu podjął decyzje o przygotowaniu, wdrożeniu, przeglądzie i nadzorze systemu zarządzania bezpieczeństwem informacji? (art. 8c, art. 8d pkt 1)
7. ☐ Czy zaplanowano adekwatne środki finansowe na cyberbezpieczeństwo? (art. 8d pkt 2)

8. ☐ Czy kierownik i osoba, której powierzył obowiązki w zakresie cyberbezpieczeństwa, przeszli w tym roku kalendarzowym udokumentowane szkolenie? (art. 8e)
9. ☐ Czy zadania są przydzielone - wewnętrznej strukturze albo dostawcy usług zarządzanych w zakresie cyberbezpieczeństwa na podstawie umowy? (art. 14)
10. ☐ Czy osoby realizujące zadania z art. 8 i 11 przedstawiły przed rozpoczęciem pracy informację z Krajowego Rejestru Karnego? (art. 8f)

System zarządzania bezpieczeństwem informacji

Wymagania art. 8 ust. 1 - dla podmiotów istniejących w dniu wejścia nowelizacji w życie do 3 kwietnia 2027 r.

11. ☐ Czy ryzyko wystąpienia incydentu jest systematycznie szacowane i zarządzane według udokumentowanej metody? (art. 8 ust. 1 pkt 1)
12. ☐ Czy macie polityki bezpieczeństwa systemu informacyjnego i polityki tematyczne, przyjęte decyzją kierownictwa? (art. 8 ust. 1 pkt 2 lit. a)
13. ☐ Czy bezpieczeństwo jest uwzględnione przy nabywaniu, rozwoju, utrzymaniu i eksploatacji systemów, a systemy są testowane - np. testami penetracyjnymi? (art. 8 ust. 1 pkt 2 lit. b)
14. ☐ Czy kontrola dostępu fizycznego i zabezpieczenia środowiskowe obejmują serwerownie i inne miejsca przetwarzania danych? (art. 8 ust. 1 pkt 2 lit. c)
15. ☐ Czy zatrudnianie, zmiana ról i odejścia pracowników obejmują nadawanie i odbieranie uprawnień? (art. 8 ust. 1 pkt 2 lit. d)

16. ☐ Czy oceniacie bezpieczeństwo dostawców produktów, usług i procesów ICT i macie wymagania bezpieczeństwa w umowach? (art. 8 ust. 1 pkt 2 lit. e, ust. 2)
17. ☐ Czy plany ciągłości działania, awaryjne i odtworzenia są wdrożone, udokumentowane i testowane? (art. 8 ust. 1 pkt 2 lit. f)
18. ☐ Czy kopie zapasowe są odseparowane od systemów produkcyjnych, a odtwarzanie z nich jest regularnie testowane? (art. 8 ust. 1 pkt 2 lit. f; załącznik nr 4, cz. I pkt 10-11)
19. ☐ Czy system informacyjny jest monitorowany w trybie ciągłym? (art. 8 ust. 1 pkt 2 lit. g)
20. ☐ Czy macie procedury oceny skuteczności wdrożonych środków technicznych i organizacyjnych? (art. 8 ust. 1 pkt 2 lit. h)
21. ☐ Czy personel przechodzi edukację z cyberbezpieczeństwa, a podstawowe zasady cyberhigieny są znane i stosowane? (art. 8 ust. 1 pkt 2 lit. i-j)
22. ☐ Czy macie zasady stosowania kryptografii, w tym szyfrowania? (art. 8 ust. 1 pkt 2 lit. k)
23. ☐ Czy tam, gdzie to uzasadnione, stosujecie uwierzytelnianie wieloskładnikowe i bezpieczne środki komunikacji? (art. 8 ust. 1 pkt 2 lit. l)
24. ☐ Czy macie aktualną inwentaryzację aktywów i politykę kontroli dostępu opartą na minimalnych uprawnieniach? (art. 8 ust. 1 pkt 2 lit. m-n)
25. ☐ Czy zbieracie informacje o cyberzagrożeniach i podatnościach - np. komunikaty CSIRT i producentów oprogramowania? (art. 8 ust. 1 pkt 3)
26. ☐ Czy oprogramowanie jest regularnie aktualizowane z analizą wpływu, a wykryte podatności usuwane niezwłocznie? (art. 8 ust. 1 pkt 5 lit. b i d)

27. ☐ Czy chronicie poufność, integralność, dostępność i autentyczność danych, także przed nieuprawnioną modyfikacją? (art. 8 ust. 1 pkt 5 lit. a i c)
28. ☐ Jeśli jesteście dostawcą cyfrowym (np. chmura, centrum danych, usługi zarządzane), czy system obejmuje środki z rozporządzenia wykonawczego Komisji (UE) 2024/2690? (art. 8b ust. 1)
29. ☐ Jeśli jesteście podmiotem ważnym publicznym, czy system spełnia wymogi załącznika nr 4 do ustawy i jest przeglądany co najmniej raz w roku? (art. 8 ust. 3; załącznik nr 4, cz. III)

Incydenty

Zgłoszenia przez system S46 w terminach 24 i 72 godzin oraz miesiąca.

30. ☐ Czy macie procedurę zarządzania incydentami: wykrywanie, rejestrowanie, klasyfikację i obsługę? (art. 8 ust. 1 pkt 4, art. 11)
31. ☐ Czy wiecie, kiedy incydent jest poważny - według progów z rozporządzenia, a u dostawców cyfrowych według rozporządzenia 2024/2690? (art. 2 pkt 7, art. 11 ust. 4)
32. ☐ Czy potraficie zgłosić incydent poważny przez S46: wczesne ostrzeżenie w ciągu 24 godzin, zgłoszenie w ciągu 72 godzin, sprawozdanie końcowe w ciągu miesiąca? (art. 11 ust. 1 pkt 4-4c)
33. ☐ Czy użytkownicy Waszych usług mają dostęp do wiedzy o cyberzagrożeniach i kanał zgłaszania incydentów i podatności? (art. 9 ust. 1 pkt 2-3)
34. ☐ Czy procedura przewiduje informowanie użytkowników o poważnych cyberzagrożeniach i incydentach, które wpływają na usługę? (art. 11 ust. 2a-2b)

Dokumentacja i kontakty

Dowody, że system działa - na potrzeby audytu i nadzoru.

- 35. ☐ Czy macie dokumentację normatywną i operacyjną (w tym logi), z nadzorem nad wersjami, przechowywaną co najmniej 2 lata od wycofania? (art. 10)
- 36. ☐ Czy wyznaczyliście osoby do kontaktu z podmiotami krajowego systemu cyberbezpieczeństwa (co najmniej dwie; w mikro- i małej firmie oraz w ważnym podmiocie publicznym - jedną)? (art. 9 ust. 1-3)
- 37. ☐ Czy dokumenty i dowody (zapisy, raporty z testów, rejestr incydentów) można szybko przekazać organowi na żądanie w nadzorze? (art. 53c)

Audyt bezpieczeństwa (podmioty kluczowe)

Podmiot ważny przechodzi audyt tylko na decyzję organu - wtedy te pytania też się przydadzą.

- 38. ☐ Czy zaplanowaliście pierwszy audyt bezpieczeństwa (do 3 kwietnia 2028 r. dla podmiotów kluczowych od dnia wejścia nowelizacji w życie) i kolejne - co najmniej raz na 3 lata? (art. 15 ust. 1, art. 33 ust. 2 nowelizacji)
- 39. ☐ Czy audytor spełnia wymagania ustawy (akredytowana jednostka albo co najmniej dwóch audytorów z certyfikatami lub praktyką) i jest niezależny - nie realizował u Was zadań z art. 8-13 w ciągu roku przed audytem? (art. 15 ust. 2-2a)
- 40. ☐ Czy wiecie, że kopię raportu z audytu przekazuje się organowi właściwemu w ciągu 3 dni roboczych od jego otrzymania? (art. 15 ust. 1a)



CHECKLISTA NIE JEST PORADĄ PRAWNĄ

Pytania streszczają obowiązki z ustawy o krajowym systemie cyberbezpieczeństwa w brzmieniu po nowelizacji. Nie zastępują analizy prawnej ani oceny, czy środki są adekwatne do ryzyka – tę daje audyt zerowy NIS2.

Stan prawny na: 8.10.2026 · Źródło: Ustawa z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (Dz.U. 2026 poz. 252)

Najczęściej zadawane pytania

Czy checklista zastępuje audyt zerowy albo audyt z art. 15?



Czy checklista dotyczy też podmiotów ważnych?



Skąd wiem, czy moja organizacja w ogóle podlega ustawie?



Źródła

Ustawa z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (Dz.U. 2026 poz. 252) (8.10.2026)

Ustawa o krajowym systemie cyberbezpieczeństwa - metryka aktu i akty zmieniające (API ELI Sejmu) (8.10.2026)

Ministerstwo Cyfryzacji - Q&A nowelizacja KSC, aktualizacja październik 2026 (1.10.2026; dokument wyjaśniający, bez mocy prawnej) (8.10.2026)

Rozporządzenie wykonawcze Komisji (UE) 2024/2690 - wymogi techniczne i metodyczne środków zarządzania ryzykiem w cyberbezpieczeństwie (6.10.2026)

Stan prawny na: 8.10.2026 · Aktualizacja: 8.10.2026

