RED INTO GREEN
GRC tool by DAPR

LISTA KONTROLNA · USTAWA O KSC / NIS 2

10 checklist zgodności z ustawą o KSC

Kompletna lista kontrolna drogi do zgodności z NIS 2 w polskim wydaniu - od sprawdzenia statusu po pierwszy audyt.

70 punktów do odhaczenia, podzielonych na dziesięć etapów wdrożenia. Każdy etap ma link do artykułu, który wyjaśnia go krok po kroku.

DLACZEGO CHECKLISTY, A NIE KOLEJNY PORADNIK

Wdrożenie ustawy o krajowym systemie cyberbezpieczeństwa nie jest trudne intelektualnie. Jest trudne organizacyjnie - i to jest zupełnie inny problem.

Obowiązki są rozproszone po kilkudziesięciu przepisach, mają różne terminy i różnych właścicieli. Część leży w IT, część w zarządzie, część w HR, część w zakupach. Dokument, który wszystko opisuje, nie odpowiada na pytanie, które zadaje sobie osoba odpowiedzialna za wdrożenie: co konkretnie mam zrobić w tym tygodniu i po czym poznam, że to zrobiłem.

Checklista odpowiada na oba pytania naraz. Ma jeszcze trzy zalety, które w tym akurat obszarze mają wymierną wartość.

Pokazuje braki, których nie widać w dokumentacji. Zgodność z ustawą powstaje z trzech warstw: przepisu, dokumentu normatywnego, który mówi „jak ma być", i dowodu operacyjnego, który potwierdza, że tak faktycznie jest. Brak którejkolwiek warstwy to luka. Organ nadzoru może wprost żądać dowodów realizacji wymogów z art. 8 ust. 1 (art. 53 ust. 2 pkt 6), a w organizacjach o wysokiej dojrzałości brakuje prawie zawsze tej trzeciej warstwy. Polityki są, dowodów nikt nie zbiera.

Wymusza przypisanie właściciela. Najczęstsza przyczyna niewykonania obowiązku nie jest techniczna. Wszyscy myślą, że robi to ktoś inny.

Chroni przed dowodami, których nie da się odtworzyć. Politykę można napisać z opóźnieniem i nadal będzie ważna. Protokołu z testu planu ciągłości, który się nie odbył, ani listy obecności ze szkolenia, którego nie było, nie napiszesz wstecz.

JAK KORZYSTAĆ Z TEGO MATERIAŁU

Przejdź listy w kolejności - to jednocześnie kolejność wdrożenia. Przy każdym punkcie postaw jedną z trzech ocen:

- **Z** mamy i mamy dowód z ostatnich dwunastu miesięcy
- **C** coś mamy, ale brakuje dokumentu albo dowodu
- **N** nie mamy

Do każdego punktu z oceną C lub N dopisz nazwisko właściciela i miesiąc. Litery C i N to Twoja lista zadań, a nie lista zmartwień.

Stan prawny: lipiec 2026 r. Podstawa: ustawa o krajowym systemie cyberbezpieczeństwa w brzmieniu nadanym ustawą z 23 stycznia 2026 r. wdrażającą dyrektywę NIS 2 (Dz.U. 2026 poz. 252).

01 Status podmiotu - czy i jak podlegasz przepisom

Punkt startowy. Bez tej odpowiedzi każde kolejne działanie jest zgadywaniem.

	WŁAŚCICIEL	TERMIN
☐ Przeprowadź samoidentyfikację statusu podmiotu (kluczowy / ważny / poza zakresem) przy użyciu narzędzia NIS2Tester lub metodyki własnej opartej na załącznikach 1-2 do ustawy.		
☐ Zidentyfikuj, do którego sektora KSC należy Twoja organizacja.		
☐ Sprawdź progi wielkości według definicji z załącznika I do rozporządzenia 651/2014/UE, z uwzględnieniem przedsiębiorstw powiązanych i partnerskich; oceń oba warunki wyłączenia z art. 5 ust. 6-7 - niezależność systemu informacyjnego oraz brak wspólnego świadczenia usług.		
☐ Sporządź arkusz kwalifikacji oraz uchwałę lub notatkę zarządu dokumentującą wynik samoidentyfikacji (art. 5, 5a).		
☐ Zapoznaj się z trzema kluczowymi datami wdrożeniowymi i wpisz je do kalendarza organizacji.		
☐ Sprawdź, czy organy nadzoru już prowadziły lub zapowiedziały kontrole w Twoim sektorze.		

Artykuł: Jak sprawdzić status wobec NIS 2 - przewodnik

02 Rejestracja w Wykazie KSC i pierwsze decyzje zarządu

Formalności, które warunkują resztę. Termin z harmonogramu ministra - dla większości podmiotów 3.10.2026 r.

	WŁAŚCICIEL	TERMIN
☐ Podejmij uchwałę zarządu przypisującą odpowiedzialność za cyberbezpieczeństwo (J2, art. 8c ust. 2) - zrób to przed rejestracją.		
☐ Wyznacz formalnie osobę odpowiedzialną za cyberbezpieczeństwo. Jeśli kierownikiem jest organ wieloosobowy i nie wskażesz nikogo, odpowiedzialność ponoszą wszyscy jego członkowie.		
☐ Ustal, kto podpisze wniosek o wpis i jakim podpisem - kwalifikowanym, zaufanym, osobistym albo kwalifikowaną pieczęcią elektroniczną (art. 7c ust. 6).		
☐ Przygotuj dane z art. 7 ust. 2 pkt 1-18 oraz oświadczenie kierownika o zgodności danych z prawdą (art. 7c ust. 2 i 5), a następnie złóż wniosek w systemie teleinformatycznym z art. 46 ust. 1 (J3).		
☐ Wyznacz i powołaj pisemnie co najmniej dwie osoby kontaktowe (J4, art. 9); podmiot mikro lub mały - jedną.		
☐ Załóż konto w systemie S46, przeszkol osoby kontaktowe i ustaw stały monitoring skrzynki - pismo uznaje się za doręczone po 14 dniach od wysłania, nawet nieotwarte (J10, art. 46, art. 46b ust. 4).		
☐ Przygotuj procedurę aktualizacji danych w wykazie - zmiany adresu, osób, adresów IP, domen i umowy z dostawcą usług bezpieczeństwa zgłaszasz w 14 dni (art. 7c ust. 3).		

Artykuł: Rejestracja w Wykazie KSC i pierwsze decyzje zarządu

03 Audyt luki - pomiar przed wdrożeniem

Mapa terenu. Bez niej łatwo wydać budżet na obszary już pokryte i przeoczyć te, na których organ najłatwiej stwierdzi naruszenie.

	WŁAŚCICIEL	TERMIN
☐ Zaplanuj i przeprowadź audyt luki obejmujący 14 środków bezpieczeństwa i wszystkie obowiązki ustawowe.		
☐ Dla każdego wymagania sprawdź komplet: przepis + dokument normatywny + dowód operacyjny. Brak choćby jednej warstwy = luka.		
☐ Zmapuj wyniki na grupy luk, każdą z przypisaną podstawą prawną - to Twoja lista zadań naprawczych.		
☐ Jeśli posiadasz ISO 27001, zidentyfikuj obszary specyficzne dla KSC, których norma nie pokrywa: raportowanie incydentów, wpis do wykazu, odpowiedzialność i szkolenia kierownika, weryfikacja niekaralności, korzystanie z S46.		
☐ Sporządź raport z audytu luki z priorytetyzacją zadań według ryzyka i terminów ustawowych.		
☐ Przedstaw wyniki zarządowi i uzyskaj formalną akceptację planu naprawczego wraz z budżetem.		

Artykuł: Gap analysis - jak zmierzyć odległość do zgodności

NAJCIĘŻSZA Z DZIESIĘCIU LIST

Z dziesięciu list ta jedna wymaga najwięcej pracy, bo dowody trzeba zebrać z IT, HR, zakupów i od zarządu, a przy każdym braku ocenić, czy chodzi o włączenie rejestru czy o projekt. Da się to przejść samodzielnie. Jeśli wolisz zrobić to z gotową metodyką i podstawą prawną pod każdym punktem - tak wygląda audyt luki u nas.

Zobacz zakres audytu luki KSC

04 Procedura incydentowa - gotowość przed zdarzeniem

Obowiązek działa od objęcia Cię ustawą, nie od zakończenia wdrożenia.

	WŁAŚCICIEL	TERMIN
☐ Opracuj i wdroż procedurę obsługi incydentów z wyraźnie opisanymi terminami: 24 h na wczesne ostrzeżenie i 72 h na pełne zgłoszenie, oba liczone od wykrycia (J9, art. 11-12b).		
☐ Przygotuj i przetestuj szablony zgłoszeń - wczesne ostrzeżenie, pełne zgłoszenie, sprawozdanie okresowe i końcowe. Test wykonuje osoba dyżurna, nie autor procedury.		
☐ Zdefiniuj kryteria klasyfikacji incydentu jako poważny na podstawie obowiązującego rozporządzenia wydanego na podstawie art. 11 ust. 4; sporządź macierz decyzyjną i rejestr klasyfikacji.		
☐ Wyznacz osoby dyżurne lub model kontaktu w trybie 24/7 - wewnętrzne struktury bezpieczeństwa albo umowa z dostawcą usług zarządzanych (art. 14).		
☐ Przygotuj szablony komunikatów do użytkowników: przy incydencie wpływającym na usługę (art. 11 ust. 2b) i przy poważnym cyberzagrożeniu (art. 11 ust. 2a).		
☐ Przetestuj ścieżkę zgłoszenia w systemie S46 - konto musi być aktywne przed pierwszym incydentem.		
☐ Wprowadź procedurę dobrowolnego zgłaszania incydentów mniejszej wagi, cyberzagrożeń i podatności do CSIRT (art. 13).		

Artykuł: Procedura incydentowa - dlaczego musisz być gotowy wcześniej

05 SZBI - dokumentacja i rdzeń systemu

Termin: 3.04.2027 r. To koniec budowy, nie koniec pracy.

	WŁAŚCICIEL	TERMIN
☐ Opracuj lub zaktualizuj politykę bezpieczeństwa informacji oraz metodykę szacowania ryzyka (środek a, art. 8 ust. 1 pkt 1).		
☐ Stwórz lub zweryfikuj komplet dokumentów tematycznych dla każdego ze środków bezpieczeństwa (lit. a-n).		
☐ Przeprowadź systematyczne szacowanie ryzyka w podejściu all-hazards - sporządź rejestr ryzyk i plan postępowania z ryzykiem.		
☐ Oddziel dokumentację normatywną (polityki, procedury) od operacyjnej (logi, zapisy, protokoły) i zapewnij ich spójność.		
☐ Wdróż nadzór nad dokumentacją: dostęp tylko dla osób upoważnionych, ochrona przed utratą i oznaczanie kolejnych wersji (art. 10 ust. 6).		
☐ Ustal zasady retencji - co najmniej 2 lata od wycofania dokumentu z użytkowania lub zakończenia świadczenia usługi (art. 10 ust. 7), z protokołem brakowania przy niszczeniu (ust. 8).		
☐ Uzyskaj formalną akceptację SZBI przez kierownika podmiotu (art. 8d).		

Artykuł: SZBI - jak zbudować system wymagany przez KSC

06 14 środków bezpieczeństwa

Katalog z art. 8 ust. 1 pkt 2 lit. a-n. Kolejność wdrożenia wyznacza audyt luki.

	WŁAŚCICIEL	TERMIN
☐ Dla każdego z 14 środków sprawdź, czy istnieje dokument normatywny i dowód operacyjny. Brak choćby jednego = luka.		
☐ **Środek e:** stwórz lub zaktualizuj rejestr dostawców ICT z klasyfikacją ryzyka i klauzulami bezpieczeństwa w umowach (art. 8 ust. 2).		
☐ **Środek f:** przetestuj plany ciągłości i odtworzenia - sporządź protokół z testu, zdefiniuj RTO i RPO, wdróż kopie w modelu 3-2-1. Testujesz odtworzenie, nie wykonanie kopii.		
☐ **Środek g:** upewnij się, że monitorowanie systemów działa w trybie ciągłym - własny SOC albo usługa dostawcy, z opisaną ścieżką eskalacji alertów poza godzinami pracy.		
☐ **Środek l:** wdróż uwierzytelnianie wieloskładnikowe w kanałach komunikacji, z priorytetem dla dostępów uprzywilejowanych i zdalnych; prowadź rejestr wyjątków z uzasadnieniem i terminem usunięcia.		
☐ **Środek n:** przeprowadź przegląd uprawnień w zasadzie minimalnych uprawnień i wdróż jego cykl; sprawdź konta techniczne, konta dostawców i konta osób po zmianie stanowiska.		
☐ **Środek k:** zweryfikuj szyfrowanie danych w spoczynku i w transmisji oraz opisz zarządzanie kluczami - kto je generuje, przechowuje, rotuje i odzyskuje.		

Artykuł: 14 środków bezpieczeństwa krok po kroku

07 Obowiązki cykliczne - życie z KSC po wdrożeniu

Wdrożenie nie ma linii mety. Ma rytm, w którym powstają dowody.

	WŁAŚCICIEL	TERMIN
☐ Stwórz roczny kalendarz obowiązków cyklicznych z imiennymi właścicielami i terminami wskazanymi co do miesiąca.		
☐ Zaplanuj i udokumentuj szkolenie kierownika oraz osoby, której powierzono jego obowiązki - raz w roku kalendarzowym, z zaświadczeniem z udziału (art. 8e).		
☐ Przeprowadź szacowanie ryzyka - sporządź raport i zaktualizowany plan postępowania z ryzykiem (art. 8 ust. 1 pkt 1).		
☐ Zorganizuj przegląd SZBI przez kierownika - sporządź protokół przeglądu zarządzania (art. 8d).		
☐ Przeprowadź ocenę skuteczności środków bezpieczeństwa z raportowaniem mierników (art. 8 ust. 1 pkt 2 lit. h).		
☐ Zaplanuj test planów ciągłości i odtworzenia oraz sporządź protokół z testu (art. 8 ust. 1 pkt 2 lit. f).		
☐ **Podmiot kluczowy:** zaplanuj audyt bezpieczeństwa co najmniej raz na 3 lata, na własny koszt, pierwszy do 3.04.2028 r. Audytorem nie może być osoba realizująca w Twoim podmiocie zadania z art. 8 oraz 9-13 (art. 15 ust. 2a). Kopię raportu przekaż organowi w 3 dni robocze od dnia jego otrzymania (art. 15 ust. 1a).		
☐ Utrzymuj obowiązki ciągłe: monitorowanie systemów, zbieranie informacji o cyberzagrożeniach i podatnościach (art. 8 ust. 1 pkt 3) oraz bieżącą aktualizację dokumentacji.		

Artykuł: Obowiązki cykliczne - jak żyć z KSC po wdrożeniu

08 Obowiązki kadrowe - niekaralność, szkolenia, HR

Obszar, który najczęściej zostaje bez właściciela, bo mieszka poza działem IT.

	WŁAŚCICIEL	TERMIN
☐ Zbierz od osób mających realizować zadania z art. 8 lub 11 informację o osobie z KRK, stwierdzającą niekaralność za przestępstwa przeciwko ochronie informacji - przed rozpoczęciem tych zadań (J5, art. 8f ust. 1). Alternatywa: poświadczenie bezpieczeństwa do klauzuli „poufne" lub wyższej (ust. 3).		
☐ Przeprowadź pierwsze szkolenie kierownika w zakresie wskazanym w art. 8e ust. 2 i zachowaj zaświadczenie uczestnictwa (J11).		
☐ Opracuj procedury onboardingu, offboardingu i zmiany stanowiska w kontekście cyberbezpieczeństwa - klauzule poufności, nadawanie i odbieranie dostępów (środek d).		
☐ Dopisz do checklisty offboardingu pytanie o Wykaz KSC - odejście osoby kontaktowej uruchamia 14 dni na zmianę wpisu (art. 7c ust. 3).		
☐ Stwórz lub zaktualizuj macierz odpowiedzialności RACI dla zadań z zakresu cyberbezpieczeństwa.		
☐ Opracuj program szkoleń dla całego personelu wraz z kampaniami świadomościowymi i testami phishingowymi (środek i).		
☐ Wdróż zasady cyberhigieny w regulaminie i standardach konfiguracji, a następnie sprawdzaj stan techniczny stacji (środek j).		

Artykuł: Niekaralność, szkolenia kierownictwa i bezpieczeństwo HR

09 Łańcuch dostaw ICT

Termin przeglądu: 3.04.2027 r. Mechanizm z art. 67c sięga jednak znacznie dalej.

	WŁAŚCICIEL	TERMIN
☐ Stwórz lub zaktualizuj rejestr dostawców ICT z klasyfikacją krytyczności, rodzajem dostępu i imiennym właścicielem relacji (J12, art. 8 ust. 1 pkt 2 lit. e).		
☐ Opracuj kartę oceny dostawcy uwzględniającą cztery kryteria z art. 8 ust. 2: podatności dostawcy, ogólną jakość jego produktów, usług i procesów ICT, wyniki skoordynowanej oceny bezpieczeństwa Grupy Współpracy oraz wyniki postępowania z art. 67b.		
☐ Przejrzyj umowy z kluczowymi dostawcami pod kątem klauzul bezpieczeństwa - poziomy usług, obowiązek informowania o incydentach i podatnościach, prawo do dowodów, zasady dostępu zdalnego, podwykonawcy, zwrot i usunięcie danych.		
☐ Sprawdź, czy wobec któregokolwiek z Twoich dostawców nie wydano decyzji na podstawie art. 67b lub 67c.		
☐ Wdróż cykliczny, co najmniej roczny przegląd i ponowną ocenę dostawców krytycznych.		
☐ Sprawdź, czy Twoja organizacja podlega rozporządzeniu CIR 2024/2690 (dostawcy infrastruktury cyfrowej i usług zaufania).		
☐ Opracuj procedurę reagowania na decyzję o dostawcy wysokiego ryzyka - zakaz wprowadzania do użytkowania oraz plan wycofania w terminie liczonym od ogłoszenia decyzji w Monitorze Polskim (art. 67c).		

Artykuł: Łańcuch dostaw ICT i dostawcy wysokiego ryzyka

10 Harmonogram i test obronności wdrożenia

Domknięcie. Trzy daty, jedna lista zadań i jeden test, który zrobisz sam.

	WŁAŚCICIEL	TERMIN
☐ Stwórz harmonogram wdrożenia z terminami dla obowiązków jednorazowych J1-J13 oraz dla obowiązków cyklicznych.		
☐ Zweryfikuj, czy dla każdego obowiązku istnieje komplet: przepis + dokument normatywny + dowód operacyjny. Dokumentacja bez dowodów to wdrożenie papierowe.		
☐ Upewnij się, że procedura incydentowa i konto S46 działają, zanim wejdziesz do Wykazu KSC.		
☐ Sprawdź, czy kierownik podmiotu przeszedł szkolenie i czy ma udokumentowane uczestnictwo (art. 8e).		
☐ **Podmiot kluczowy:** zaplanuj umowę z audytorem i audyt bezpieczeństwa do 3.04.2028 r. (art. 15 ust. 1, art. 33 ust. 2 ustawy zmieniającej).		
☐ Rozważ przystąpienie do wymiany informacji o cyberzagrożeniach (art. 8h) - porozumienia branżowe i zasady oznaczania odbiorców. Przystąpienie do porozumienia jest daną rejestrową w wykazie.		
☐ **Grupa spółek:** wdróż model piasty i szprych - centralizuj wzorce, dokumentację, umowę z dostawcą usług bezpieczeństwa i szkolenia; każdej spółce zapewnij minimum lokalne (uchwała, rejestracja, konto S46, udział kierownika w szkoleniu).		
☐ Przeprowadź test obronności: wybierz losowe wymaganie i poproś o dowód z ostatnich dwunastu miesięcy. Czas, w jakim go dostaniesz, jest najuczciwszą oceną wdrożenia.		

Artykuł: Konsekwencje i oś czasu - co się stanie, jeśli nie wdrożysz na czas

MASZ JUŻ LISTĘ

Potrzebujesz jeszcze kolejności

Jeśli po przejściu tych dziesięciu list masz więcej liter C i N niż Z, to normalny wynik pierwszego podejścia - i dokładnie ten moment, w którym warto zamienić listę na plan.

Checklista pokazuje, czego brakuje. Audyt luki odpowiada na trzy pytania, na które sama lista nie odpowie: które braki są najpilniejsze, ile pracy naprawdę wymaga każdy z nich i jaka podstawa prawna stoi za każdym zadaniem.

AUDYT LUKI KSC

Sprawdź, jak wygląda audyt luki KSC

135 granularnych wymagań w 27 grupach luk, każda przypięta do konkretnego przepisu. Efektem jest raport, który zarząd może przyjąć jako plan naprawczy z budżetem i właścicielami - a nie prezentacja o zgodności.

Zobacz zakres audytu luki KSC

KONTAKT

kontakt@redintogreen.pl
redintogreen.pl