KSC Kompas

Checklista wdrożenia NIS2 dla średnich i dużych firm

Wszystkie obowiązki z nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa w jednym dokumencie: od sprawdzenia, czy ustawa Cię dotyczy, przez rejestrację, po działający system zarządzania bezpieczeństwem informacji (SZBI) i gotowość do kontroli.

03.04.2026	Nowelizacja ustawy o KSC wchodzi w życie Od tego dnia liczą się terminy dla podmiotów, które już spełniają kryteria.
03.10.2026	Wniosek o wpis do wykazu podmiotów kluczowych i ważnych Samoidentyfikacja: nikt nie przyśle wezwania, firma zgłasza się sama.
03.04.2027	Wdrożone środki zarządzania ryzykiem (SZBI) Polityki, procedury, środki techniczne, szkolenia i dowody ich działania.
na bieżąco	Zgłaszanie incydentów, przeglądy i doskonalenie Wczesne ostrzeżenie w 24 h, zgłoszenie w 72 h, raport końcowy w ciągu miesiąca.

Jak korzystać z checklisty

Idź sekcjami po kolei. Przy każdym zadaniu wpisz osobę odpowiedzialną i termin, a po wykonaniu odhacz pole.

Kolumna „Dowód do teczki" mówi, jaki dokument lub zapis zachować. Na kontroli liczy się to, co da się pokazać, a nie deklaracje.

Oznaczenia

WSZYSCY KLUCZOWY WAŻNY

Zadania bez oznaczenia dotyczą zarówno podmiotów kluczowych, jak i ważnych. Obowiązki obu grup są niemal takie same, różni je głównie sposób nadzoru i wysokość kar.

Checklista jest materiałem pomocniczym i nie stanowi porady prawnej.

Czy ustawa Cię dotyczy?

od razu

Status zależy od sektora działalności i wielkości firmy. Liczy się faktyczna działalność, a nie sam kod PKD.

	ZADANIE	DOWÓD DO TECZKI	KTO / DO KIEDY
☐	**Przypisz działalność do sektora** z załącznika 1 (sektory kluczowe) lub 2 (inne sektory krytyczne). Sprawdź każdą linię biznesową osobno.	Notatka z analizą sektorów i kodów PKD	
☐	**Ustal wielkość firmy** według zalecenia KE 2003/361: zatrudnienie oraz obrót lub suma bilansowa. Dolicz spółki partnerskie i powiązane (powyżej 25% udziałów).	Wyliczenie z danymi za ostatni zamknięty rok obrotowy	
☐	**Sprawdź wyjątki niezależne od wielkości:** DNS, rejestr TLD, kwalifikowane usługi zaufania, a także telekomunikacja i usługi zaufania u małych firm.	Adnotacja w notatce	
☐	**Określ status:** podmiot kluczowy, ważny albo poza ustawą. Jeśli wychodzi „poza ustawą", sprawdź, czy jesteś dostawcą firm objętych NIS2. Wtedy obowiązki przyjdą przez umowy.	Decyzja zarządu o statusie, podpisana i datowana	

1 Rejestracja w wykazie podmiotów

do 03.10.2026

Wniosek o wpis składa się w systemie teleinformatycznym prowadzonym przez ministra ds. informatyzacji. Przygotuj dane wcześniej, bo system przy końcu terminu bywa przeciążony.

	ZADANIE	DOWÓD DO TECZKI	KTO / DO KIEDY
☐	**Zbierz dane rejestrowe:** nazwa, NIP, REGON, KRS, adres, sektor i podsektor, rodzaj świadczonych usług.	Arkusz danych do wniosku	
☐	**Wypisz państwa UE,** w których świadczysz usługi, oraz zakresy adresów IP i domeny, jeśli wymaga tego formularz dla Twojego sektora.	Lista krajów, IP i domen	
☐	**Wyznacz osoby do kontaktu** w sprawach cyberbezpieczeństwa (np. z CSIRT i organem właściwym), z zastępstwem.	Upoważnienie lub zarządzenie	
☐	**Złóż wniosek o wpis** i zachowaj potwierdzenie.	UPO / potwierdzenie złożenia	
☐	**Ustal procedurę aktualizacji danych** w wykazie (zmiana adresu, usług, osób kontaktowych) i kto za nią odpowiada.	Zapis w procedurze SZBI	

2 Zarząd i organizacja

X–XI 2026

NIS2 (art. 20) przenosi odpowiedzialność na kierownictwo: zarząd zatwierdza środki bezpieczeństwa, nadzoruje ich wdrożenie i osobiście odpowiada za zaniedbania.

	ZADANIE	DOWÓD DO TECZKI	KTO / DO KIEDY
☐	**Uchwała zarządu** o rozpoczęciu wdrożenia, budżecie i przypisaniu odpowiedzialności.	Uchwała / zarządzenie	

	ZADANIE	DOWÓD DO TECZKI	KTO / DO KIEDY
☐	**Wyznacz właściciela SZBI** (osobę odpowiedzialną za koordynację) z realnym czasem na to zadanie.	Zakres obowiązków	....
☐	**Szkolenie członków zarządu** z zarządzania ryzykiem cyberbezpieczeństwa. Obowiązkowe i powtarzane regularnie.	Zaświadczenia imienne z datą	....
☐	**Zdecyduj: zespół własny czy outsourcing** (SOC, MSSP, zewnętrzny inspektor). Wybrany dostawca musi spełniać wymagania ustawy.	Decyzja + umowa z dostawcą	....
☐	**Ustal rytm raportowania do zarządu:** stan ryzyk, incydenty, postęp wdrożenia (np. co kwartał).	Protokoły z przeglądów	....

3 Inwentaryzacja i analiza ryzyka

XI–XII 2026

Fundament SZBI. Środki bezpieczeństwa mają wynikać z ryzyka Twojej firmy, a nie z gotowego szablonu. To pierwsze, o co pyta kontroler.

	ZADANIE	DOWÓD DO TECZKI	KTO / DO KIEDY
☐	**Spis usług i procesów** objętych ustawą oraz systemów, które je obsługują.	Mapa usług i procesów	....
☐	**Rejestr zasobów:** serwery, stacje, urządzenia sieciowe, aplikacje, chmura, dane, z właścicielem każdego zasobu.	Rejestr zasobów (aktualny)	....
☐	**Wybierz metodykę szacowania ryzyka** (np. ISO/IEC 27005) i skalę prawdopodobieństwa oraz skutków.	Opis metodyki	....
☐	**Przeprowadź analizę:** zagrożenia, podatności, skutki dla ciągłości usług.	Rejestr ryzyk z oceną	....
☐	**Plan postępowania z ryzykiem:** dla każdego ryzyka decyzja (ograniczyć, przenieść, zaakceptować), środki i termin.	Plan postępowania zatwierdzony przez zarząd	....
☐	**Akceptacja ryzyka szczątkowego** przez zarząd.	Podpisana akceptacja	....

4 Środki zarządzania ryzykiem

I–III 2027

Dziesięć obszarów z art. 21 ust. 2 NIS2. Każdy musi być pokryty polityką lub procedurą i działającym środkiem technicznym, proporcjonalnie do ryzyka.

a. Polityka analizy ryzyka i bezpieczeństwa systemów `art. 21 ust. 2 lit. a`

☐	**Polityka bezpieczeństwa informacji** zatwierdzona przez zarząd i znana pracownikom.	Polityka + potwierdzenia zapoznania	....

b. Obsługa incydentów `lit. b`

☐	**Procedura obsługi incydentów:** wykrycie, klasyfikacja, reakcja, zgłoszenie, wnioski (szczegóły w sekcji 5).	Procedura + rejestr incydentów	....
☐	**Monitorowanie i logi:** centralne zbieranie zdarzeń (SIEM lub np. Wazuh), określony czas przechowywania.	Konfiguracja, raport z działania	....

c. Ciągłość działania `lit. c`

☐	**Plan ciągłości działania i odtwarzania** po awarii (BCP/DRP) z celami RTO i RPO dla kluczowych usług.	Plan BCP/DRP	....
☐	**Kopie zapasowe 3-2-1**, w tym jedna kopia odizolowana (offline lub niezmienna), zaszyfrowana.	Polityka kopii, harmonogram	....
☐	**Test odtworzenia** z kopii i ćwiczenie planu kryzysowego co najmniej raz w roku.	Protokół testu z wynikiem	....

d. Bezpieczeństwo łańcucha dostaw `lit. d`

☐	**Rejestr dostawców ICT** z oceną krytyczności (szczegóły w sekcji 6).	Rejestr dostawców	....

e. Bezpieczeństwo pozyskiwania, rozwoju i utrzymania systemów `lit. e`

☐	**Zarządzanie podatnościami:** skanowanie, terminy łatania według krytyczności, kanał zgłaszania podatności z zewnątrz.	Procedura, raporty skanów, historia łatek	....
☐	**Wymagania bezpieczeństwa przy zakupie i rozwoju** oprogramowania (testy, przegląd kodu, oddzielne środowiska).	Checklista zakupowa / SDLC	....

f. Ocena skuteczności środków `lit. f`

☐	**Mierniki i przeglądy SZBI:** co mierzysz, jak często, kto ocenia.	Raport z przeglądu	....
☐	KLUCZOWY **Audyt bezpieczeństwa** zgodnie z wymaganiami ustawy, wykonany przez uprawnionego audytora.	Raport z audytu + plan naprawczy	....
☐	**Test penetracyjny** systemów wystawionych do internetu.	Raport z testu	....

g. Cyberhigiena i szkolenia `lit. g`

☐	**Szkolenie wszystkich pracowników** przy zatrudnieniu i cyklicznie (phishing, hasła, zgłaszanie incydentów).	Lista obecności, wyniki testów	.....
☐	**Symulacja phishingu** przynajmniej raz w roku.	Raport z kampanii	.....

h. Kryptografia `lit. h`

☐	**Polityka szyfrowania:** dyski laptopów (np. BitLocker), transmisja (TLS 1.2+), kopie zapasowe, zarządzanie kluczami.	Polityka + raport pokrycia szyfrowaniem	.....

i. Personel, kontrola dostępu, zarządzanie aktywami `lit. i`

☐	**Procedura nadawania i odbierania uprawnień** (przyjęcie, zmiana stanowiska, odejście) z zasadą minimalnych uprawnień.	Procedura + przegląd uprawnień	.....
☐	**Konta uprzywilejowane** (administratorzy) rozdzielone od kont codziennych i monitorowane.	Lista kont admin, logi	.....
☐	**Klauzule poufności i bezpieczeństwa** w umowach z pracownikami i współpracownikami.	Wzór klauzuli	.....

j. Uwierzytelnianie wieloskładnikowe i bezpieczna łączność `lit. j`

☐	**MFA** dla poczty, VPN, dostępu zdalnego, paneli chmurowych i kont administracyjnych.	Raport pokrycia MFA	.....
☐	**Awaryjny kanał łączności** na wypadek utraty poczty i sieci (np. lista telefonów, niezależny komunikator).	Opis kanału w planie kryzysowym	.....

5 Obsługa i zgłaszanie incydentów

gotowe do III 2027

Poważny incydent zgłasza się do właściwego zespołu CSIRT (CSIRT NASK, CSIRT GOV, CSIRT MON lub sektorowego) w ściśle określonych terminach, liczonych od wykrycia (art. 23 NIS2).

0 h	24 h	72 h	1 mies.
Wykrycie incydentu, klasyfikacja: czy jest poważny?	Wczesne ostrzeżenie: czy mógł być wynikiem działań bezprawnych lub mieć skutki transgraniczne	Zgłoszenie incydentu: wstępna ocena, waga, skutki, wskaźniki kompromitacji	Raport końcowy: przyczyna, zastosowane środki, skutki transgraniczne

	ZADANIE	DOWÓD DO TECZKI	KTO / DO KIEDY
☐	**Kryteria „poważnego incydentu”** przełożone na Twoje usługi (czas przestoju, liczba użytkowników, straty).	Tabela klasyfikacji	....
☐	**Ustal, który CSIRT jest właściwy** dla Twojego sektora, i załóż dostęp do systemu zgłoszeń.	Dane kontaktowe, dostęp	....
☐	**Dyżur i ścieżka eskalacji** 24/7 (również w weekendy i święta): kto decyduje o zgłoszeniu.	Grafik dyżurów, macierz eskalacji	....
☐	**Wzory zgłoszeń** na 24 h, 72 h i raport końcowy, wypełnione na przykładowym scenariuszu.	Szablony	....
☐	**Informowanie klientów** o incydencie i możliwych działaniach zaradczych, gdy wymaga tego ustawa lub CSIRT.	Szablon komunikatu	....
☐	**Ćwiczenie incydentu** (np. ransomware) z przejściem całej ścieżki zgłoszenia.	Protokół z ćwiczenia, wnioski	....
☐	**Rejestr incydentów** łącznie z drobnymi zdarzeniami i przyjętymi wnioskami.	Rejestr	....

6 Łańcuch dostaw

I–III 2027

Odpowiadasz za bezpieczeństwo usług, które kupujesz. Dostawca IT z dostępem do Twoich systemów to często najsłabsze ogniwo.

	ZADANIE	DOWÓD DO TECZKI	KTO / DO KIEDY
☐	**Lista dostawców ICT i usług krytycznych** z oceną: dostęp do systemów, dane, wpływ awarii.	Rejestr dostawców	....
☐	**Ankieta bezpieczeństwa** dla dostawców krytycznych (certyfikaty, MFA, kopie, obsługa incydentów).	Wypełnione ankiety	....
☐	**Klauzule w umowach:** obowiązek zgłaszania incydentów, prawo do audytu, poziomy usług, wyjście z umowy.	Aneksy / wzór umowy	....
☐	**Sprawdź dostawców wysokiego ryzyka** w świetle przepisów ustawy o ograniczeniach dla takich dostawców.	Notatka z weryfikacji	....

7 Gotowość do kontroli i utrzymanie

od IV 2027, stale

KLUCZOWY może być skontrolowany w każdej chwili. WAŻNY głównie po incydencie lub sygnale o naruszeniu. Obie grupy muszą umieć wykazać zgodność.

	ZADANIE	DOWÓD DO TECZKI	KTO / DO KIEDY
☐	**Teczka zgodności:** wszystkie dowody z tej checklisty w jednym miejscu, z datami i wersjami.	Repozytorium dokumentów	
☐	**Roczny przegląd zarządczy SZBI:** ryzyka, incydenty, audyty, cele na kolejny rok.	Protokół przeglądu	
☐	**Kalendarz obowiązków cyklicznych:** szkolenia, testy kopii, przeglądy uprawnień, ankiety dostawców, audyty.	Kalendarz / harmonogram	
☐	**Monitoruj zmiany przepisów** i rozporządzeń wykonawczych do ustawy o KSC.	Rejestr zmian prawnych	

Przykładowy harmonogram

IX 2026 – IV 2027

Plan dla firmy, która zaczyna we wrześniu 2026 r. i ma jedną osobę koordynującą oraz wsparcie IT.

OKRES	CO ZROBIĆ	SEKCJA
do 03.10.2026	Samoidentyfikacja, decyzja zarządu o statusie, złożenie wniosku o wpis, osoby do kontaktu	1
X 2026	Uchwała zarządu, właściciel SZBI, budżet, decyzja o outsourcingu, szkolenie zarządu	2
XI 2026	Mapa usług, rejestr zasobów, metodyka i analiza ryzyka	3
XII 2026	Plan postępowania z ryzykiem, akceptacja zarządu, polityka bezpieczeństwa informacji	3, 4a
I 2027	MFA, kopie zapasowe 3-2-1, szyfrowanie, kontrola dostępu, logi i monitoring	4c, h, i, j, b
II 2027	Procedura incydentów i ścieżka zgłoszeń, zarządzanie podatnościami, rejestr i ankiety dostawców	4b, e, 5, 6
III 2027	BCP/DRP i test odtworzenia, szkolenia pracowników, ćwiczenie incydentu, test penetracyjny	4c, f, g, 5
do 03.04.2027	Przegląd kompletności, uzupełnienie teczki zgodności, zatwierdzenie SZBI przez zarząd	7

> **Kary.** Podmiot kluczowy: do 10 mln € lub 2% światowego rocznego obrotu (wyższa z kwot). Podmiot ważny: do 7 mln € lub 1,4% obrotu. Dodatkowo kierownik podmiotu ponosi osobistą odpowiedzialność za niewykonanie obowiązków.

Ważne zastrzeżenie

Checklista opiera się na dyrektywie NIS2 (UE) 2022/2555 i nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa w brzmieniu obowiązującym we wrześniu 2026 r. Nie zastępuje analizy prawnej konkretnej firmy ani rozporządzeń wykonawczych, które mogą doprecyzować wymagania dla Twojego sektora.

KSC Kompas

Aplikacja, która przeprowadzi Cię przez tę checklistę krok po kroku: analiza ryzyka z asystentem AI, gotowe polityki dopasowane do firmy, rejestr incydentów z odliczaniem terminów, ankiety dla dostawców i szkolenia z zaświadczeniami.

Zapisz się na listę oczekujących na stronie testu „Czy NIS2 mnie dotyczy?”