Październik 2026

UKSC. OD OBOWIĄZKU DO DZIAŁANIA

Praktyczny toolkit na start

7 obszarów gotowości | 26 pytań kontrolnych | Plan pierwszych 30 dni

Sprawdź, gdzie jest Twoja organizacja, co już masz i od czego warto zacząć wdrożenie nowych wymagań cyberbezpieczeństwa.

LBK &P
LAW FIRM

01 | UKSC W PIGUŁCE. CO TRZEBA WIEDZIEĆ?

Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa (UKSC), wdrażająca unijną dyrektywę NIS2, obowiązuje od 3 kwietnia 2026 r.

Nowe przepisy znacząco rozszerzają krąg organizacji objętych obowiązkami w zakresie cyberbezpieczeństwa. Wprowadzają też bardziej szczegółowe wymagania dotyczące zarządzania ryzykiem, bezpieczeństwa systemów informacyjnych, obsługi incydentów, ciągłości działania i bezpieczeństwa łańcucha dostaw.

CO TO OZNACZA W PRAKTYCE?

Dla organizacji objętych UKSC zgodność z przepisami nie sprowadza się do posiadania odpowiednich polityk i procedur. Wymaga wdrożenia i utrzymywania rzeczywiście funkcjonujących rozwiązań organizacyjnych i technicznych, dostosowanych do działalności oraz występujących ryzyk.

KOGO DOTYCZY UKSC?

Nowe przepisy obejmują określone kategorie podmiotów prowadzących działalność w sektorach istotnych dla gospodarki i bezpieczeństwa państwa, m.in.:

energetyce, transporcie, ochronie zdrowia, bankowości i infrastrukturze rynków finansowych;	**infrastrukturze cyfrowej i zarządzaniu usługami ICT, w tym określonych dostawców usług zarządzanych oraz zarządzanych usług bezpieczeństwa;**	**zaopatrzeniu w wodę i gospodarce ściekowej;**
produkcji przemysłowej w wybranych branżach, przemyśle chemicznym oraz produkcji i dystrybucji żywności;	**gospodarce odpadami, usługach pocztowych, badaniach naukowych i innych sektorach wskazanych w ustawie;**	**określonych kategoriach podmiotów publicznych.**

Ustawa wyróżnia dwie podstawowe kategorie: **podmioty kluczowe** i **podmioty ważne**.

O tym, czy organizacja podlega UKSC i do której kategorii należy, decyduje kombinacja przesłanek ustawowych, w szczególności rodzaju prowadzonej działalności, wielkości przedsiębiorcy oraz szczególnych zasad kwalifikacji.

Uwaga:

Sama nazwa branży albo kod PKD nie przesądza o podleganiu ustawie. Nie zawsze wystarczy też sprawdzić wielkość pojedynczej spółki – znaczenie mają też jej powiązania z innymi przedsiębiorstwami. W niektórych przypadkach obowiązki mają zastosowanie niezależnie od wielkości organizacji.

Najważniejsze terminy

Data	Co oznacza?
3 kwietnia 2026 r.	Wejście w życie nowelizacji UKSC
3 października 2026 r.	Upływ podstawowego terminu na złożenie wniosku o wpis do Wykazu KSC przez podmioty objęte samorejestracją
3 kwietnia 2027 r.	Upływ podstawowego okresu dostosowawczego na wdrożenie obowiązków i rozpoczęcie korzystania z S46
3 kwietnia 2028 r.	Termin pierwszego obowiązkowego audytu dla nowych podmiotów kluczowych objętych tym obowiązkiem
3 kwietnia 2028 r.	Początek stosowania przepisów o administracyjnych karach pieniężnych na zasadach ogólnych, z ustawowymi wyjątkami

Terminy przedstawiają podstawowy harmonogram dla podmiotów spełniających przesłanki ustawowe w dniu wejścia w życie nowelizacji. Szczególne zasady mogą dotyczyć m.in. dotychczasowych operatorów usług kluczowych, podmiotów wpisywanych z urzędu oraz organizacji uzyskujących określony status w późniejszym terminie.

JAKIE SĄ NAJWAŻNIEJSZE OBOWIĄZKI?

Podmioty kluczowe i ważne, z uwzględnieniem właściwych dla nich wymagań, muszą w szczególności:

1. Dokonać wymaganej rejestracji i zapewnić realizację obowiązków związanych z Wykazem KSC oraz S46.
2. Wdrożyć systematyczne zarządzanie ryzykiem cyberbezpieczeństwa i odpowiednie środki bezpieczeństwa.
3. Opracować, wdrożyć i utrzymywać system zarządzania bezpieczeństwem informacji (SZBI).
4. Zapewnić wykrywanie, obsługę, klasyfikowanie i zgłaszanie incydentów.
5. Zarządzać bezpieczeństwem łańcucha dostaw ICT.
6. Zapewnić rozwiązania w zakresie ciągłości działania, odtwarzania i reagowania na sytuacje kryzysowe. Określić odpowiedzialność za cyberbezpieczeństwo, zapewnić właściwy nadzór kierownictwa i wymagane kompetencje.
7. Wykonywać obowiązki dotyczące audytów, kontroli i dokumentowania stosowanych rozwiązań – odpowiednio do swojego statusu.

A CO Z KARAMI?

Nowelizacja przewiduje istotne sankcje administracyjne.



Podmioty kluczowe:
zasadniczo do 10 mln EUR lub 2% rocznych przychodów z działalności gospodarczej – zastosowanie ma wyższa kwota.



Podmioty ważne:
zasadniczo do 7 mln EUR lub 1,4% rocznych przychodów z działalności gospodarczej – zgodnie z ustawowymi zasadami ustalania wysokości kary.

W szczególnych przypadkach naruszeń powodujących określone poważne zagrożenia ustawa przewiduje możliwość nałożenia kary do 100 mln PLN. Przewidziano również odpowiedzialność administracyjną kierowników podmiotów.

Nie każde naruszenie oznacza automatycznie nałożenie kary maksymalnej wysokości. Znaczenie mają przesłanki ustawowe, charakter naruszenia i sposób działania organu nadzorczego.

Warto zapamiętać:

Odroczenie stosowania większości kar nie oznacza odroczenia obowiązku wdrożenia odpowiednich środków bezpieczeństwa.

---

02 | ZANIM ZACZNIESZ – USTAL, GDZIE JESTEŚ

Nie każda organizacja zaczyna w tym samym miejscu.

Niektóre podmioty są już po analizie podlegania UKSC i rejestracji w Wykazie KSC. Inne ustaliły, że przepisy ich nie obejmują. Są też organizacje, które dopiero odkrywają, że nowe obowiązki mogą dotyczyć ich działalności.

Znajdź scenariusz, który najlepiej opisuje sytuację Twojej organizacji.

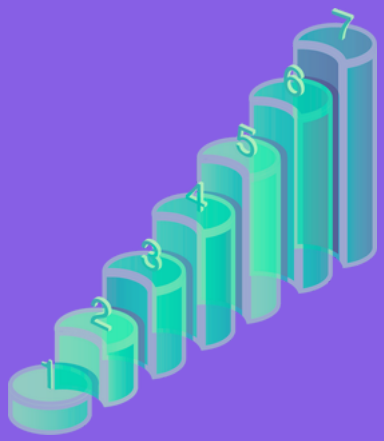
SCENARIUSZ A

„Wiemy, że podlegamy UKSC. Dokonaliśmy wpisu."

Co dalej?

- Zweryfikuj kompletność i aktualność danych ujawnionych w Wykazie.
- Upewnij się, że wyznaczono wymagane osoby kontaktowe i przypisano odpowiedzialność za obowiązki UKSC.
- Sprawdź przygotowanie do korzystania z S46, w szczególności w zakresie obsługi zgłoszeń incydentów.
- Rozpocznij ocenę stanu obecnego i zaplanuj wdrożenie wymagań.

Twój następny krok: Przejdź do 7 obszarów gotowości na kolejnych stronach.



SCENARIUSZ B

„Sprawdziliśmy. UKSC nas nie obejmuje."

Organizacja przeprowadziła ocenę i ustaliła, że nie spełnia ustawowych kryteriów uznania za podmiot kluczowy lub ważny.

Co dalej?

- Udokumentuj przyjęte założenia, ustalenia faktyczne i uzasadnienie oceny.
- Zachowaj materiały, na podstawie których określono status organizacji.
- Przyjmij zasadę okresowej, np. corocznej, weryfikacji oceny oraz ponownego jej przeprowadzania w przypadku istotnych zmian działalności, skali przedsiębiorstwa lub struktury grupy.



BONUS – SPRAWDŹ SWÓJ ŁAŃCUCH DOSTAW

Czy świadczysz usługi na rzecz podmiotów kluczowych lub ważnych?
Jeżeli tak, Twoi klienci mogą oczekiwać określonych zabezpieczeń, informacji o incydentach, dowodów stosowania kontroli bezpieczeństwa lub odpowiednich postanowień umownych. Nawet jeśli UKSC nie obejmuje Cię bezpośrednio, rozważ wdrożenie podstawowych rozwiązań w zakresie cyberbezpieczeństwa, zarządzania incydentami i ciągłości działania.

Twój następny krok: Oceń, jakie wymagania bezpieczeństwa wynikają z Twoich relacji biznesowych i rzeczywistego profilu ryzyka.

SCENARIUSZ C



„Nie jesteśmy pewni, czy UKSC nas dotyczy.”

Organizacja nie przeprowadziła jeszcze samooceny albo nie potrafi jednoznacznie ustalić swojego statusu.

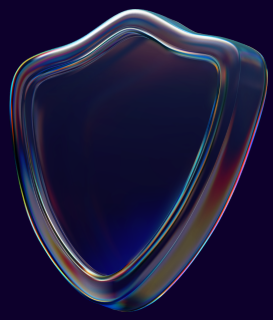
Co dalej?

- Zweryfikuj rodzaj rzeczywiście prowadzonej działalności w odniesieniu do kategorii podmiotów wskazanych w UKSC.
- Ustal wielkość przedsiębiorcy, z uwzględnieniem właściwych zasad dotyczących przedsiębiorstw powiązanych i partnerskich.
- Sprawdź szczególne przepisy, wyjątki i kryteria kwalifikacji, w tym przypadki podlegania niezależnie od wielkości.
- Ustal, czy organizacja ma status podmiotu kluczowego, ważnego, czy pozostaje poza zakresem regulacji.
- Udokumentuj wynik i podejmij wynikające z niego działania.

Jeśli okaże się, że podlegasz UKSC: nie zwlekaj z dopełnieniem obowiązków rejestracyjnych. Podstawowy termin samorejestracji upłynął 3 października 2026 r., dlatego w przypadku opóźnienia należy niezwłocznie ustalić właściwy sposób postępowania i złożyć wymagany wniosek. Sprawdź jednocześnie terminy mające zastosowanie do Twojej organizacji.

Twój następny krok: Przeprowadź i udokumentuj ocenę podlegania. Dopiero potem ustal właściwą ścieżkę dalszych działań.

SCENARIUSZ D



„Podlegamy UKSC, ale nie zakończyliśmy rejestracji.”

Jeżeli obowiązek dokonania wpisu już powstał, nie warto odkładać formalności do czasu zakończenia wdrożenia.

Co dalej?

- Potwierdź status organizacji i podstawę kwalifikacji.
- Sprawdź, czy podmiot nie został już wpisany z urzędu.
- Przygotuj i złóż wymagany wniosek albo uzupełnij dane.
- Równolegle rozpocznij prace wdrożeniowe.

PAMIĘTAJ:
Wpis do Wykazu KSC nie oznacza potwierdzenia zgodności z ustawą. Jest jednym z obowiązków formalnych, a nie końcem procesu wdrożenia.

Twój następny krok:
Uporządkuj sprawy rejestrowe i przejdź do oceny gotowości organizacji.

03 | TWOJA ORGANIZACJA A UKSC: 7 OBSZARÓW GOTOWOŚCI

Masz już potwierdzony status podmiotu kluczowego lub ważnego? Pora sprawdzić, jaki jest rzeczywisty punkt wyjścia do wdrożenia.

Poniższa checklista nie jest audytem zgodności z UKSC. Jej celem jest pomóc w uporządkowaniu informacji, identyfikacji podstawowych luk i ustaleniu pierwszych priorytetów.

JAK KORZYSTAĆ Z CHECKLISTY?

Przy każdym pytaniu zaznacz jedną odpowiedź:

- **TAK** – zagadnienie zostało przeanalizowane, a odpowiednie rozwiązanie istnieje i można je potwierdzić.
- **CZĘŚCIOWO** – pewne elementy funkcjonują, ale wymagają uzupełnienia lub weryfikacji.
- **NIE / NIE WIEMY** – rozwiązanie nie istnieje albo organizacja nie posiada wystarczających informacji.

Odpowiedź „TAK" nie jest równoznaczna z potwierdzeniem zgodności danego obszaru z UKSC.

OBSZAR 1. ZAKRES WDROŻENIA

Czy wiemy, co właściwie ma zostać objęte wdrożeniem?
Zrozumienie zakresu działalności objętej ustawą i jej zależności od systemów informacyjnych jest podstawą prawidłowego planowania dalszych działań.

Pytanie	Tak	Częściowo	Nie / nie wiem
1. Czy zidentyfikowaliśmy usługi i rodzaje działalności, które uzasadniają objęcie organizacji UKSC?	☐	☐	☐
2. Czy zmapowaliśmy kluczowe procesy, systemy i zasoby ICT wykorzystywane przy świadczeniu tych usług?	☐	☐	☐
3. Czy zidentyfikowaliśmy istotne zależności między jednostkami organizacyjnymi, lokalizacjami i podmiotami z grupy?	☐	☐	☐
4. Czy zakres analizy i wdrożenia został udokumentowany oraz uzgodniony z właściwymi osobami?	☐	☐	☐

NA CO ZWRÓCIĆ UWAGĘ?

Zakres podlegania ustawie nie zawsze jest tożsamy z zakresem jednego działu, systemu lub usługi. Zbyt wąskie podejście może prowadzić do pominięcia ważnych zależności i ryzyk. Z kolei brak określenia priorytetów może nadmiernie rozbudować projekt.

CO POWINNO ZOSTAĆ PO TEJ ANALIZIE?

Wstępna mapa działalności, usług, procesów i zasobów ICT oraz opis przyjętego zakresu wdrożenia.

OBSZAR 2. ISTNIEJĄCE ROZWIĄZANIA I DOKUMENTACJA

Czy naprawdę zaczynamy od zera?
Wiele organizacji posiada już procedury, zabezpieczenia i mechanizmy zarządzania bezpieczeństwem. Wyzwaniem jest ustalenie, co można wykorzystać, co wymaga dostosowania, a czego faktycznie brakuje.

Pytanie	Tak	Częściowo	Nie / nie wiem
1. Czy zinwentaryzowaliśmy istniejące polityki, procedury, instrukcje i rejestry związane z cyberbezpieczeństwem?	☐	☐	☐
2. Czy wiemy, które rozwiązania rzeczywiście funkcjonują, a które istnieją głównie w dokumentacji?	☐	☐	☐
3. Czy oceniliśmy, jakie elementy obecnego SZBI lub innych systemów zarządzania można wykorzystać w ramach UKSC?	☐	☐	☐
4. Czy wskazaliśmy dokumenty i procesy wymagające aktualizacji, integracji lub opracowania?	☐	☐	☐

NA CO ZWRÓCIĆ UWAGĘ?

Posiadanie certyfikatu ISO 27001 lub rozbudowanej dokumentacji bezpieczeństwa może stanowić bardzo dobrą podstawę wdrożenia. Nie oznacza jednak automatycznego spełnienia wszystkich wymagań UKSC. Istotne są zakres, aktualność i faktyczne stosowanie przyjętych rozwiązań.

CO POWINNO ZOSTAĆ PO TEJ ANALIZIE?

Wykaz istniejących dokumentów i mechanizmów wraz ze wstępną klasyfikacją: do wykorzystania, do aktualizacji, do opracowania.

OBSZAR 3. ZARZĄDZANIE RYZYKIEM CYBERBEZPIECZEŃSTWA

Czy podejmujemy decyzje o bezpieczeństwie na podstawie ryzyka?
UKSC wymaga podejścia opartego na ryzyku. Samo posiadanie katalogu zabezpieczeń nie wystarcza, jeśli nie wiadomo, przed jakimi zagrożeniami mają chronić i jak odpowiadają na potrzeby organizacji.

Pytanie	Tak	Częściowo	Nie / nie wiem
1. Czy posiadamy udokumentowany proces oceny i zarządzania ryzykiem cyberbezpieczeństwa?	☐	☐	☐
2. Czy zidentyfikowaliśmy istotne zagrożenia, podatności i możliwe skutki incydentów dla naszej działalności?	☐	☐	☐
3. Czy określiliśmy zasady postępowania z ryzykiem, w tym jego ograniczania, monitorowania i akceptowania?	☐	☐	☐
4. Czy wyniki oceny ryzyka wpływają na dobór zabezpieczeń, priorytety oraz decyzje kierownictwa?	☐	☐	☐

NA CO ZWRÓCIĆ UWAGĘ?

Rejestr ryzyka nie powinien być wyłącznie tabelą przygotowywaną na potrzeby audytu. Dobrze zaprojektowany proces pozwala uzasadnić, dlaczego określone zabezpieczenia są potrzebne, a inne mają mniejsze znaczenie.

CO POWINNO ZOSTAĆ PO TEJ ANALIZIE?

Zidentyfikowane wymagania dotyczące metodyki i procesu zarządzania ryzykiem oraz lista obszarów wymagających pogłębionej oceny.

OBSZAR 4. ODPOWIEDZIALNOŚĆ I NADZÓR KIEROWNICTWA

Czy wiadomo, kto za co odpowiada?
Cyberbezpieczeństwo nie jest wyłącznie odpowiedzialnością działu IT. Skuteczne wdrożenie wymaga współpracy funkcji biznesowych, technicznych, bezpieczeństwa, prawnych i kierownictwa.

Pytanie	Tak	Częściowo	Nie / nie wiem
1. Czy wyznaczyliśmy koordynatora wdrożenia oraz właścicieli najważniejszych obszarów?	☐	☐	☐
2. Czy określiliśmy role i odpowiedzialności dotyczące zarządzania ryzykiem, incydentami, dostawcami i ciągłością działania?	☐	☐	☐
3. Czy kierownictwo otrzymuje informacje umożliwiające podejmowanie decyzji i nadzorowanie realizacji wymagań?	☐	☐	☐
4. Czy uwzględniliśmy wymagania dotyczące osób kontaktowych, kompetencji, szkoleń i weryfikacji personelu?	☐	☐	☐

NA CO ZWRÓCIĆ UWAGĘ?

Wyznaczenie jednej osoby „od NIS2” nie oznacza przeniesienia na nią całej odpowiedzialności. Wdrożenie powinno obejmować zarówno jasny podział zadań operacyjnych, jak i odpowiednie decyzje, zaangażowanie oraz nadzór kierownictwa.

CO POWINNO ZOSTAĆ PO TEJ ANALIZIE?

Wstępna matryca odpowiedzialności, struktura zarządzania projektem i lista decyzji wymagających udziału kierownictwa.

OBSZAR 5. OBSŁUGA I ZGŁASZANIE INCYDENTÓW

Czy wiemy, co zrobić, kiedy coś pójdzie nie tak?
Incydent cyberbezpieczeństwa może wymagać jednoczesnych działań technicznych, operacyjnych, prawnych i komunikacyjnych. Przy krótkich terminach zgłoszeń kluczowe jest wcześniejsze przygotowanie.

Pytanie	Tak	Częściowo	Nie / nie wiem
1. Czy posiadamy proces wykrywania, rejestrowania, klasyfikowania i obsługi incydentów?	☐	☐	☐
2. Czy określiliśmy kryteria i zasady oceny, które incydenty wymagają zgłoszenia na podstawie UKSC?	☐	☐	☐
3. Czy wskazaliśmy osoby odpowiedzialne za eskalację, podejmowanie decyzji i przekazywanie wymaganych zgłoszeń?	☐	☐	☐
4. Czy uwzględniliśmy incydenty dotyczące dostawców ICT i przygotowanie do komunikacji przez S46?	☐	☐	☐

NA CO ZWRÓCIĆ UWAGĘ?

Procedura obsługi incydentów powinna działać również poza godzinami pracy. Warto sprawdzić, czy organizacja potrafi szybko pozyskać informacje od dostawcy, ustalić skutki zdarzenia i podjąć decyzję o ewentualnym zgłoszeniu.

CO POWINNO ZOSTAĆ PO TEJ ANALIZIE?

Wstępna identyfikacja braków w procesie zarządzania incydentami oraz lista działań niezbędnych do zapewnienia właściwej eskalacji i raportowania.

OBSZAR 6. DOSTAWCY ICT I CIĄGŁOŚĆ DZIAŁANIA

Czy wiemy, od kogo zależy nasza działalność i co stanie się, jeśli coś przestanie działać?
Coraz więcej procesów organizacyjnych zależy od zewnętrznych dostawców, infrastruktury chmurowej, systemów i usług ICT. Dlatego bezpieczeństwo łańcucha dostaw i odporność operacyjna stanowią ważny element UKSC.

Pytanie	Tak	Częściowo	Nie / nie wiem
1. Czy zidentyfikowaliśmy dostawców ICT i usługi zewnętrzne istotne dla działalności objętej UKSC?	□	□	□
2. Czy oceniamy ryzyka związane z dostawcami, w tym ich wpływ na bezpieczeństwo i ciągłość działania?	□	□	□
3. Czy określiliśmy, jakie mogą być skutki niedostępności kluczowych systemów lub usług i jak ograniczyć te skutki?	□	□	□
4. Czy posiadamy odpowiednie plany ciągłości i odtwarzania oraz czy weryfikujemy ich skuteczność?	□	□	□

NA CO ZWRÓCIĆ UWAGĘ?

Sama umowa z dostawcą czy ogólny plan ciągłości działania nie gwarantują możliwości skutecznego odtworzenia usługi. Warto sprawdzić, czy organizacja zna swoje kluczowe zależności, potrafi określić dopuszczalne skutki zakłóceń i wie, jakie działania są możliwe w praktyce.

CO POWINNO ZOSTAĆ PO TEJ ANALIZIE?

Wstępna mapa kluczowych zależności od dostawców i usług ICT oraz lista scenariuszy wymagających analizy i przygotowania działań ciągłościowych.

OBSZAR 7. PLAN WDROŻENIA I MONITOROWANIE POSTĘPÓW

Czy umiemy przełożyć wymagania na konkretne działania?
Nawet dobrze przeprowadzona identyfikacja luk nie prowadzi automatycznie do zgodności. Potrzebny jest plan, który łączy wymagania, odpowiedzialność, zasoby i realne terminy.

Pytanie	Tak	Częściowo	Nie / nie wiem
1. Czy zidentyfikowaliśmy najważniejsze luki pomiędzy obecnymi rozwiązaniami a wymaganiami UKSC?	□	□	□
2. Czy potrafimy przełożyć te luki na konkretne działania organizacyjne, techniczne i dokumentacyjne?	□	□	□

3. Czy działania mają określonych właścicieli, priorytety, terminy i niezbędne zasoby?	□	□	□
4. Czy ustaliliśmy sposób monitorowania wdrożenia i weryfikowania skuteczności przyjętych rozwiązań?	□	□	□

NA CO ZWRÓCIĆ UWAGĘ?

Wynikiem gap assessment nie powinna być wyłącznie długa lista niezgodności. Organizacja potrzebuje wiedzieć, co zrobić, w jakiej kolejności, kto odpowiada za realizację oraz jak potwierdzić, że dane wymaganie zostało rzeczywiście wdrożone.

CO POWINNO ZOSTAĆ PO TEJ ANALIZIE?

Plan działań obejmujący zidentyfikowane luki, rekomendowane rozwiązania, właścicieli, priorytety i harmonogram.

---

04 | CO MÓWIĄ TWOJE ODPOWIEDZI?

26 PYTAŃ TO DOPIERO POCZĄTEK.
NAJWAŻNIEJSZE JEST TO, CO ZROBISZ Z ODPOWIEDZIAMI.

Nie traktuj checklisty jako testu, w którym trzeba zdobyć określoną liczbę punktów.
Nie każde pytanie ma takie samo znaczenie, a niektóre wymagają znacznie bardziej szczegółowej oceny. Odpowiedzi mają pomóc ustalić punkt wyjścia, a nie określić procentowy poziom zgodności z UKSC.

JAK INTERPRETOWAĆ WYNIKI?

TAK – mamy podstawy, na których możemy budować
Zweryfikuj aktualność dokumentacji, rzeczywiste funkcjonowanie rozwiązania oraz jego adekwatność do wymagań UKSC.

CZĘŚCIOWO – mamy pewne rozwiązania, ale potrzebujemy je uporządkować
Ustal, co już funkcjonuje, czego brakuje i jakie działania pozwolą wykorzystać istniejące mechanizmy.

NIE / NIE WIEMY – ten obszar wymaga uwagi
Sprawdź, czy problem wynika z braku rozwiązania, niewystarczających informacji, niejasnej odpowiedzialności czy braku właściwej dokumentacji.



TWOJE TRZY PIERWSZE PRIORYTETY

Na podstawie odpowiedzi wskaż trzy obszary wymagające najpilniejszego działania.

PRIORYTET 1	PRIORYTET 3	PRIORYTET 3
Obszar: _____	Obszar: _____	Obszar: _____
Co wymaga wyjaśnienia lub poprawy?	Co wymaga wyjaśnienia lub poprawy?	Co wymaga wyjaśnienia lub poprawy?
Kto powinien zostać zaangażowany?	Kto powinien zostać zaangażowany?	Kto powinien zostać zaangażowany?

TRZY PYTANIA NA KONIEC SAMOOCENY

1. Gdzie brakuje nam rozwiązań, a gdzie tylko wiedzy o tym, co już istnieje?
2. Które zidentyfikowane braki mogą mieć największy wpływ na bezpieczeństwo lub ciągłość działania organizacji?
3. Jakie decyzje i zasoby są potrzebne, aby rozpocząć właściwe wdrożenie?

Warto zapamiętać:

Priorytetów nie należy ustalać wyłącznie na podstawie liczby odpowiedzi „NIE”. Znaczenie mają również obowiązujące terminy, charakter ryzyka, wpływ na działalność oraz zależności między poszczególnymi działaniami.

---

05 | PIERWSZE 30 DNI WDROŻENIA

JAK PRZEJŚĆ OD WSTĘPNEJ SAMOOCENY DO REALNEGO PLANU DZIAŁANIA?

Poniżej przedstawiamy przykładową kolejność prac przygotowawczych, którą można dostosować do wielkości, profilu działalności i aktualnego poziomu dojrzałości organizacji.

TYDZIEŃ 1

Ustal zakres i odpowiedzialność

Co zrobić?

- Potwierdź status organizacji i właściwy zakres wdrożenia.
- Wyznacz koordynatora projektu i zaangażuj właścicieli kluczowych procesów.
- Ustal udział IT, cybersecurity, compliance, działu prawnego i kierownictwa.
- Zidentyfikuj decyzje wymagające podjęcia na poziomie zarządczym.

REZULTAT:

Uzgodniony zakres projektu, wstępna struktura odpowiedzialności i lista otwartych decyzji.

TYDZIEŃ 2

Ustal, co już masz

Co zrobić?

- Zbierz istniejące polityki, procedury, rejestry i dokumentację cyberbezpieczeństwa.
- Zidentyfikuj stosowane narzędzia i mechanizmy bezpieczeństwa.
- Zgromadź dostępne informacje o zasobach ICT, ryzyku, incydentach i dostawcach.
- Ustal, które rozwiązania można wykorzystać w ramach wdrożenia.

REZULTAT:

Inwentaryzacja stanu obecnego i lista informacji wymagających uzupełnienia.

TYDZIEŃ 3

Zidentyfikuj luki i ryzyka

Co zrobić?

- Porównaj stan obecny z właściwymi wymaganiami UKSC.
- Zidentyfikuj brakujące lub nieadekwatne rozwiązania.
- Ustal, które kwestie wymagają dodatkowych analiz prawnych, organizacyjnych lub technicznych.
- Wstępnie oceń znaczenie zidentyfikowanych luk.

REZULTAT:

Wstępny rejestr luk oraz obszarów wymagających dalszych prac.

TYDZIEŃ 4

Przygotuj plan wdrożenia

Co zrobić?

- Określ działania niezbędne do usunięcia zidentyfikowanych luk.
- Wyznacz właścicieli zadań, priorytety, terminy i zależności.
- Zidentyfikuj potrzeby budżetowe i zasobowe.
- Ustal sposób raportowania postępów i eskalowania problemów.

REZULTAT:

Wstępny plan wdrożenia UKSC, który można przedstawić kierownictwu.

Warto zapamiętać:

Przedstawiony harmonogram nie jest terminem ustawowym ani gwarancją zakończenia gap assessment w ciągu miesiąca. W zależności od organizacji część działań trzeba będzie realizować równolegle, a kwestie pilne – w szczególności istotne ryzyka i zaległe obowiązki – podjąć niezwłocznie.

06 | TRZY PUŁAPKI NA POCZĄTKU WDROŻENIA

PUŁAPKA 1

„Najpierw napiszmy wszystkie polityki”
Dokumentacja jest niezbędna, ale nie powinna powstawać w oderwaniu od rzeczywistych procesów i ryzyk.

Co może pójść nie tak?
Organizacja posiada komplet procedur, które nie odpowiadają jej strukturze, technologii ani sposobowi działania. Formalnie dokumenty istnieją, ale ich stosowanie jest utrudnione albo niemożliwe.

Lepsze podejście: Najpierw ustal stan obecny, ryzyka i wymagania, a następnie opracuj dokumentację odzwierciedlającą rzeczywiste rozwiązania.

PUŁAPKA 2

„Mamy ISO 27001, więc jesteśmy już zgodni z UKSC”
Istniejący system zarządzania bezpieczeństwem informacji może być bardzo dobrą podstawą, ale nie zastępuje oceny podlegania UKSC ani weryfikacji zgodności z konkretnymi wymaganiami ustawy.

Co może pójść nie tak?
Organizacja zakłada, że istniejąca certyfikacja obejmuje wszystkie istotne procesy, systemy i obowiązki, bez sprawdzenia zakresu oraz wymagań krajowych.

Lepsze podejście: Wykorzystaj istniejący SZBI, ale zweryfikuj jego zakres, aktualność i ewentualne luki w odniesieniu do UKSC.

PUŁAPKA 3

„To projekt IT – niech IT się nim zajmie”
Cyberbezpieczeństwo wymaga rozwiązań technicznych, ale również decyzji biznesowych, organizacyjnych i zarządczych.

Co może pójść nie tak?
Dział IT przygotowuje zabezpieczenia i dokumentację, nie mając możliwości samodzielnego ustalenia tolerancji ryzyka, priorytetów biznesowych, odpowiedzialności dostawców czy potrzebnych zasobów.

Lepsze podejście: Zorganizuj wdrożenie jako projekt interdyscyplinarny, z jasno określonym udziałem kierownictwa i właścicieli procesów biznesowych.

NA KONIEC – JEDNA ZASADA

Nie zaczynaj od pytania: „Jakie dokumenty musimy napisać?”.
Zacznij od pytania: **„Jakie ryzyka musimy kontrolować, jakie rozwiązania już mamy i czego rzeczywiście potrzebujemy, żeby spełnić wymagania UKSC?”**

---

07 | I CO DALEJ?

WPIS DO WYKAZU KSC TO POCZĄTEK.
KOLEJNY KROK TO WDROŻENIE, KTÓRE BĘDZIE DZIAŁAŁO W PRAKTYCE.

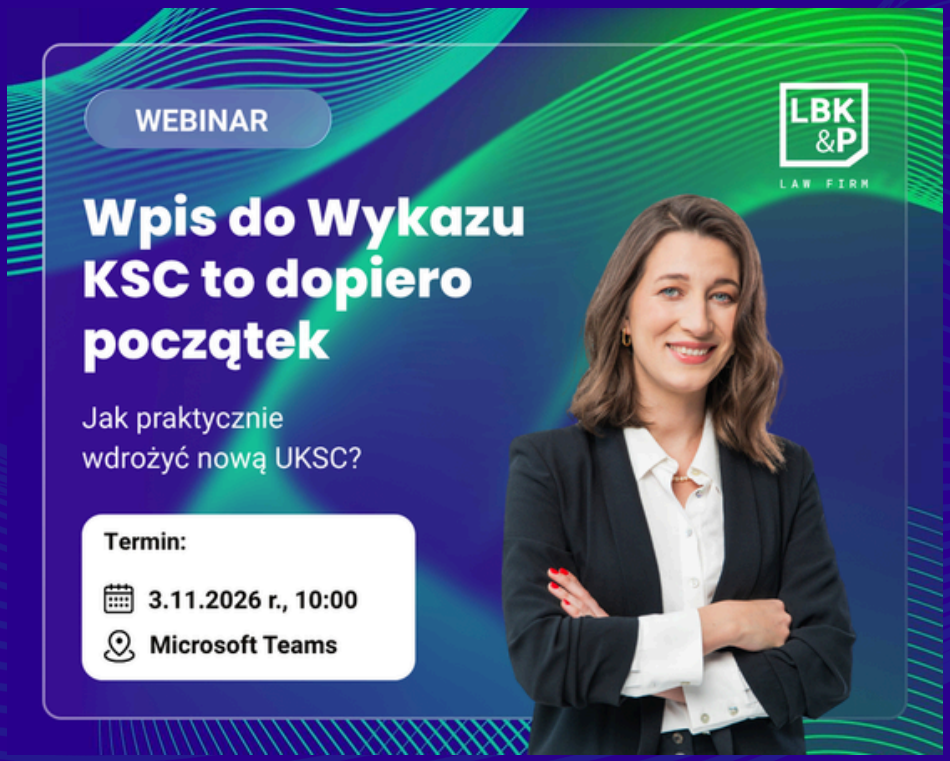
Jeśli przeszedłeś przez checklistę, prawdopodobnie masz już wstępny obraz tego, co w Twojej organizacji zostało uporządkowane, co wymaga weryfikacji i gdzie mogą znajdować się najważniejsze luki.

To dobry punkt wyjścia.

Kolejnym etapem powinno być przeprowadzenie odpowiednio zaplanowanej analizy luk (gap assessment), ustalenie docelowych rozwiązań i przygotowanie realnego planu wdrożenia.

CHCESZ WIEDZIEĆ, JAK ZROBIĆ TO W PRAKTYCE?

ZAREJESTRUJ SIĘ!



Podczas spotkania porozmawiamy m.in. o tym:

- jak dobrze rozpocząć projekt wdrożeniowy;
- jak zaplanować i przeprowadzić gap assessment;
- jak wykorzystać istniejącą dokumentację i procesy;
- jak podejść do wdrożenia SZBI, zarządzania ryzykiem, incydentami i dostawcami;
- gdzie pojawiają się najczęstsze trudności w praktyce.

Podzielimy się także pierwszymi doświadczeniami z realizowanych przez nas projektów wdrożenia nowej UKSC.

O MATERIALE

Niniejszy materiał ma charakter edukacyjny i służy wstępnej samoocenie gotowości organizacyjnej do realizacji obowiązków wynikających z UKSC. Nie stanowi kompletnego zestawienia wymagań prawnych, audytu zgodności ani indywidualnej porady prawnej.

Zakres i sposób realizacji obowiązków wymagają każdorazowo oceny z uwzględnieniem statusu, działalności i uwarunkowań konkretnej organizacji.

Stan prawny: październik 2026 r.
© LBKP 2026.

POZOSTAŃSMY W KONTAKCIE!

LBKP.PL



Paulina Jeziorska

Senior manager, radczyni prawna

Doradza instytucjom finansowym, firmom technologicznym i dostawcom IT w projektach dotyczących DORA, NIS2 i regulacji cyfrowych, łącząc perspektywę prawną z praktycznym rozumieniem technologii.

KONTAKT

+48 570 662 013
pj@lbkp.pl

LBK&P
LAW FIRM

Odwiedź i zaobserwuj nasze social media:

LBPLegal
LBKP
kancelaria_lbkp

Więcej informacji:

Strona internetowa
Kontakt