Możliwość dofinansowania

Jak wdrożyć KSC / NIS2 w praktyce

Numer usługi 2026/08/19/7492/3754690

2 214,00 PLN brutto
1 800,00 PLN netto
276,75 PLN brutto/h
225,00 PLN netto/h
261,33 PLN cena rynkowa

ODO 24 sp. z o.o.

4,6 / 5

4 oceny

Usługa szkoleniowa
zdalna w czasie rzeczywistym
Zajęcia grupowe
08:00 h
07.12.2026 do 07.12.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Usługa jest skierowana przede wszystkim do członków zarządu, kadry kierowniczej, pracowników działów IT, bezpieczeństwa informacji, cyberbezpieczeństwa, compliance oraz osób odpowiedzialnych za wdrożenie i utrzymanie wymagań ustawy o krajowym systemie cyberbezpieczeństwa. Szkolenie jest przeznaczone również dla osób uczestniczących w zarządzaniu ryzykiem, przygotowaniu dokumentacji bezpieczeństwa, obsłudze incydentów oraz współpracy z dostawcami usług i technologii ICT. Udział nie wymaga wcześniejszego ukończenia szkolenia dotyczącego NIS2, jednak wskazana jest podstawowa znajomość funkcjonowania organizacji i wykorzystywanych w niej systemów informatycznych.
Minimalna liczba uczestników	6
Maksymalna liczba uczestników	14
Data zakończenia rekrutacji	04-12-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Podstawa uzyskania wpisu do BUR	Certyfikat systemu zarządzania jakością wg. ISO 9001:2015 (PN-EN ISO 9001:2015) - w zakresie usług szkoleniowych

Cel

Cel edukacyjny

Celem edukacyjnym usługi jest przygotowanie uczestnika do praktycznego stosowania wymagań KSC/NIS2 poprzez identyfikowanie obowiązków organizacji, tworzenie podstawowych polityk i procedur cyberbezpieczeństwa, analizę ryzyka, dobór środków bezpieczeństwa, przygotowanie do obsługi incydentów i audytów oraz organizowanie współpracy z dostawcami, CSIRT i organami nadzorczymi.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik identyfikuje podstawowe obowiązki organizacji wynikające z KSC/NIS2 oraz określa ich znaczenie dla działalności organizacji.	Kryteria weryfikacji: rozpoznaje organizacje objęte wymaganiami KSC/NIS2, wskazuje podstawowe obowiązki organizacji, rozróżnia wymagania organizacyjne i techniczne, wskazuje rolę zarządu w zarządzaniu cyberbezpieczeństwem.	Test teoretyczny
Uczestnik identyfikuje kluczowe aktywa organizacji i ocenia podstawowe ryzyka związane z cyberzagrożeniami.	Kryteria weryfikacji: identyfikuje aktywa wymagające ochrony, rozpoznaje zagrożenia i podatności, określa prawdopodobieństwo i skutki zdarzeń, wskazuje poziom ryzyka, proponuje podstawowe działania ograniczające ryzyko.	Test teoretyczny
Uczestnik rozpoznaje podstawowe elementy analizy ryzyka cyberbezpieczeństwa i określa sposób postępowania z ryzykiem.	Kryteria weryfikacji: identyfikuje aktywa wymagające ochrony, rozpoznaje zagrożenia i podatności, określa czynniki wpływające na poziom ryzyka, wskazuje działania ograniczające zidentyfikowane ryzyko.	Test teoretyczny
Uczestnik rozpoznaje i dobiera podstawowe środki organizacyjne i techniczne służące ograniczaniu ryzyka cyberincydentów.	ryteria weryfikacji: wskazuje środki bezpieczeństwa adekwatne do przedstawionego zagrożenia, rozpoznaje znaczenie kontroli dostępu, wskazuje znaczenie kopii zapasowych i ochrony przed złośliwym oprogramowaniem, rozpoznaje podstawowe zasady zarządzania podatnościami i aktualizacjami.	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik identyfikuje dokumentację niezbędną do wykazania zgodności organizacji z wymaganiami KSC/NIS2 oraz rozpoznaje podstawowe zasady przygotowania organizacji do audytu.	Kryteria weryfikacji: wskazuje rodzaje dokumentacji związanej z zarządzaniem bezpieczeństwem, rozpoznaje dokumentację dotyczącą ryzyka, ciągłości działania i infrastruktury, wskazuje elementy dokumentowania zgodności, rozpoznaje podstawowe działania przygotowujące organizację do audytu lub kontroli.	Test teoretyczny
Uczestnik rozpoznaje zasady zarządzania incydentami cyberbezpieczeństwa oraz określa podstawowe działania związane z ich obsługą i zgłaszaniem.	Kryteria weryfikacji: rozpoznaje zdarzenia wymagające obsługi jako incydent, wskazuje podstawowe etapy obsługi incydentu, określa role i odpowiedzialności w procesie reagowania, wskazuje podstawowe zasady zgłaszania incydentów, rozpoznaje znaczenie planu reagowania na incydenty.	Test teoretyczny
Uczestnik rozpoznaje wymagania dotyczące cyberbezpieczeństwa łańcucha dostaw oraz zasady współpracy z dostawcami, CSIRT i właściwymi organami.	Kryteria weryfikacji: identyfikuje podstawowe ryzyka związane z dostawcami, wskazuje wymagania bezpieczeństwa, które mogą być stosowane wobec dostawców, rozpoznaje znaczenie odpowiednich zapisów umownych, wskazuje podstawowe zasady współpracy z CSIRT i organami właściwymi w zakresie cyberbezpieczeństwa.	Test teoretyczny
Uczestnik określa podstawowe obowiązki zarządu i kadry kierowniczej w zakresie zarządzania cyberbezpieczeństwem wynikające z KSC/NIS2.	Kryteria weryfikacji: wskazuje podstawowe obowiązki zarządu, rozpoznaje decyzje wymagające zaangażowania kadry kierowniczej, określa znaczenie nadzoru zarządu nad cyberbezpieczeństwem, wskazuje zasady współpracy zarządu z działem IT i innymi funkcjami organizacji, rozpoznaje potencjalne konsekwencje niewłaściwego wykonywania obowiązków.	Test teoretyczny

Cel biznesowy

Celem biznesowym usługi jest zwiększenie gotowości organizacji do spełnienia wymagań ustawy o krajowym systemie cyberbezpieczeństwa poprzez uporządkowanie sposobu zarządzania cyberbezpieczeństwem, ryzykiem, dokumentacją i reagowaniem na incydenty. W wyniku usługi uczestnik będzie przygotowany do przełożenia wymagań KSC/NIS2 na konkretne działania organizacyjne, procedury i rozwiązania stosowane w organizacji, w tym do identyfikacji kluczowych aktywów, oceny ryzyka, doboru środków bezpieczeństwa, przygotowania dokumentacji, organizacji procesu obsługi incydentów oraz współpracy z dostawcami i właściwymi podmiotami.

Efekt usługi

Efekt usługi oraz kryteria jego weryfikacji

Efekt 1: Uporządkowanie podstawowego modelu zarządzania cyberbezpieczeństwem w organizacji zgodnie z wymaganiami KSC/NIS2, obejmującego role, odpowiedzialności, polityki i procedury.

Kryteria weryfikacji:

- uczestnik identyfikuje obszary wymagające uregulowania,
- wskazuje podstawowe role i odpowiedzialności,
- rozpoznaje dokumentację i procedury wymagane w organizacji,
- dobiera właściwe rozwiązania do przedstawionych sytuacji.

Efekt 2: Uporządkowanie sposobu identyfikacji i oceny ryzyka cyberbezpieczeństwa oraz doboru środków ograniczających zidentyfikowane ryzyka.

Kryteria weryfikacji:

- uczestnik identyfikuje aktywa, zagrożenia i podatności,
- rozpoznaje czynniki wpływające na poziom ryzyka,
- wskazuje adekwatne środki bezpieczeństwa,
- rozpoznaje działania ograniczające ryzyko.

Efekt 3: Przygotowanie organizacji do uporządkowanego reagowania na incydenty cyberbezpieczeństwa oraz realizacji obowiązków związanych z ich zgłaszaniem.

Kryteria weryfikacji:

- uczestnik rozpoznaje sytuacje wymagające obsługi jako incydent,
- wskazuje podstawowe etapy postępowania,
- określa role i odpowiedzialności,
- wskazuje podstawowe zasady zgłaszania incydentów.

Efekt 4: Uporządkowanie zasad zarządzania bezpieczeństwem łańcucha dostaw i współpracy z dostawcami oraz właściwymi podmiotami w zakresie cyberbezpieczeństwa.

Kryteria weryfikacji:

- uczestnik identyfikuje podstawowe ryzyka związane z dostawcami,
- wskazuje wymagania bezpieczeństwa wobec dostawców,
- rozpoznaje znaczenie odpowiednich zapisów umownych,
- wskazuje zasady współpracy z CSIRT i organami właściwymi.

Metoda potwierdzenia osiągnięcia efektu usługi

Osiągnięcie efektów usługi zostanie potwierdzone na podstawie wyników końcowej walidacji w formie testu teoretycznego. Test obejmie pytania odnoszące się do wymagań KSC/NIS2, zarządzania ryzykiem, dokumentacji cyberbezpieczeństwa, środków bezpieczeństwa, reagowania na incydenty, bezpieczeństwa łańcucha dostaw oraz odpowiedzialności organizacji i zarządu. Wynik testu zostanie udokumentowany.

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem zawierają opis efektów uczenia się?

TAK

Pytanie 2. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji i zgodnie z zaplanowanymi metodami walidacji?

TAK

Pytanie 3. Czy dokument lub wyraźnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Rozpoczęcie szkolenia

- rejestracja uczestników,
- określenie oczekiwań i doświadczeń uczestników,
- test diagnostyczny poziomu wiedzy.

Moduł I. Wprowadzenie do NIS2 i wymagania KSC

- kontekst NIS2,
- najważniejsze zmiany,
- zakres podmiotowy,
- sektory kluczowe i ważne,
- obowiązki organizacji,
- KSC a RODO,
- wymagania organizacyjne,
- wymagania techniczne,
- rola zarządu,
- zarządzanie ryzykiem.

Moduł II. Analiza ryzyka i dokumentacja

- analiza ryzyka w kontekście KSC/NIS2,
- identyfikacja zagrożeń i podatności,
- dobre praktyki i najczęstsze błędy,
- polityki i procedury cyberbezpieczeństwa,
- dokumentacja systemu zarządzania bezpieczeństwem informacji,
- dokumentacja ochrony infrastruktury,
- dokumentacja ciągłości działania,
- dokumentacja techniczna,
- dokumentacja sektorowa,
- dokumentacja operacyjna.

Moduł III. Incydenty i łańcuch dostaw

- zgłaszanie incydentów,
- próg istotności i terminy,
- model obsługi incydentu,
- role i odpowiedzialności,
- plan reagowania,
- współpraca z dostawcami,
- bezpieczeństwo łańcucha dostaw,
- wymagania wobec dostawców,
- klauzule umowne.

Moduł IV. Cyberhigiena i odpowiedzialność zarządu

- cyberhigiena,
- praktyki bezpieczeństwa dla pracowników,
- egzekwowanie zasad cyberhigieny,
- obowiązki zarządu,
- odpowiedzialność osób zarządzających,
- konsekwencje prawne i finansowe,
- decyzje zarządu dotyczące cyberbezpieczeństwa,
- współpraca zarządu z IT i IOD.

Walidacja

- test wiedzy.

Harmonogram

Liczba pozycji harmonogramu: 10

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 10 Rejestracja uczestników i przekazanie informacji organizacyjnych dotyczących przebiegu szkolenia, materiałów oraz zasad udziału	Zajęcia	Tomasz Ochocki	07-12-2026	09:00	09:05	00:05

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
2 z 10 Określenie oczekiwań uczestników, ich doświadczeń oraz obszarów związanych z KSC/NIS2 wymagających szczególnego omówienia	Zajęcia	Tomasz Ochocki	07-12-2026	09:05	09:15	00:10
3 z 10 Moduł I: Wprowadzenie do NIS2 i KSC, zakres obowiązków, sektory kluczowe i ważne, wymagania organizacyjne i techniczne oraz rola zarządu	Zajęcia	Tomasz Ochocki	07-12-2026	09:15	11:00	01:45
4 z 10 -	Przerwa	-	07-12-2026	11:00	11:20	00:20
5 z 10 Moduł II: Analiza ryzyka, polityki i procedury oraz dokumentacja KSC/NIS2: bezpieczeństwo informacji, infrastruktura, ciągłość działania i dokumentacja techniczna	Zajęcia	Tomasz Ochocki	07-12-2026	11:25	13:00	01:35
6 z 10 -	Przerwa	-	07-12-2026	13:00	13:40	00:40

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
7 z 10 Moduł III: Reagowanie na incydenty, zgłaszanie i obsługa incydentów, role i odpowiedzialności, plan reagowania oraz bezpieczeństwo łańcucha dostaw i dostawców	Zajęcia	Tomasz Ochocki	07-12-2026	13:40	15:30	01:50
8 z 10 -	Przerwa	-	07-12-2026	15:30	15:45	00:15
9 z 10 Moduł IV: Cyberhigiena, zasady bezpieczeństwa dla pracowników i IT, odpowiedzialność zarządu oraz współpraca zarządu z IT i IOD	Zajęcia	Tomasz Ochocki	07-12-2026	15:45	17:00	01:15
10 z 10 -	Walidacja	-	07-12-2026	17:00	17:05	00:05

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	08:00
w tym suma godzin zajęć	06:40
w tym suma godzin walidacji	00:05
w tym suma przerw	01:15
Suma godzin dydaktycznych bez przerw	09:00

Cennik

Jeżeli korzystasz z dofinansowania i usługa stanowi usługę kształcenia zawodowego lub przekwalifikowania zawodowego wraz z usługą lub dostawą towarów ściśle związaną z usługami kształcenia zawodowego lub przekwalifikowania zawodowego to możesz mieć możliwość skorzystania za zwolnienia z podatku VAT na podstawie art. 43 ust. 1 pkt 29 lit. c ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług, jeśli usługa w całości jest finansowana ze środków publicznych lub § 3 ust. 1 pkt 14 rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień w przypadku, gdy usługa jest finansowana w co najmniej 70% ze środków publicznych.

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	2 214,00 PLN
Koszt przypadający na 1 uczestnika netto	1 800,00 PLN
Koszt osobogodziny brutto	276,75 PLN
Koszt osobogodziny netto	225,00 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	08:00

Prowadzący

Liczba prowadzących: 1

1 z 1

Tomasz Ochocki

Absolwent Akademii Obrony Narodowej na kierunku „Bezpieczeństwo narodowe” (specjalizacja zarządzanie kryzysowe). Ukończył studia podyplomowe z zakresu analizy bezpieczeństwa i zagrożeń terrorystycznych (Collegium Civitas) oraz ochrony danych osobowych i informacji niejawnych (Uniwersytet Kardynała Stefana Wyszyńskiego). Doktorant Szkoły Głównej Handlowej (Kolegium Ekonomiczno-Społeczne). Audytor wiodący systemu zarządzania bezpieczeństwem informacji (ISO/IEC 27001), systemu zarządzania ciągłością działania (ISO 22301) oraz audytor wewnętrzny systemu zarządzania informacjami o prywatności (ISO/IEC 27701). Współautor komentarza do ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

Odpowiada za pracę i rozwój zespołu merytorycznego. Specjalizuje się w:

- ochronie danych w fazie projektowania (art. 25 RODO),
- analizie ryzyka (art. 32 RODO),
- ocenie skutków dla ochrony danych (art. 35 RODO),
- zarządzaniu naruszeniami (art. 33 i 34 RODO).

Przykłady zrealizowanych projektów:
1.Stworzenie narzędzia do analizy ryzyka i DPIA.
2.Stworzenie narzędzia do ochrony danych osobowych w fazie projektowania.
3.Współtwórca narzędzia do oceny ryzyka związanej z transferem danych do państw trzecich (TIA).
4.Rozwój dokumentacji ochrony danych i bezpieczeństwa informacji.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnik otrzymuje dostęp do zestawu ponad 30 praktycznych wzorów dokumentacji KSC/NIS2, przygotowanych z uwzględnieniem wymagań dyrektywy NIS2, wytycznych ENISA oraz doświadczeń z audytów cyberbezpieczeństwa i wdrożeń w różnych sektorach. Pakiet obejmuje m.in. polityki bezpieczeństwa, procedury zarządzania ryzykiem, procedury audytowe, procedury zarządzania incydentami, dokumentację ciągłości działania, zasady zarządzania dostępem i dostawcami, dokumentację bezpieczeństwa infrastruktury oraz wzory rejestrów i raportowania.

Dodatkowo:

- skrypt prezentacji,
- RODO Nawigator,
- Poradnik RODO,
- poszkoleniowe wsparcie merytoryczne,
- 90-dniowy dostęp do Dr RODO.

Warunki uczestnictwa

Uczestnictwo w szkoleniu nie wymaga wcześniejszego ukończenia szkolenia dotyczącego NIS2 ani formalnych kwalifikacji z zakresu cyberbezpieczeństwa. Ze względu na praktyczny charakter usługi wskazana jest podstawowa znajomość funkcjonowania organizacji, procesów biznesowych oraz wykorzystywanych systemów informatycznych. Szkolenie jest szczególnie przydatne dla osób odpowiedzialnych za zarządzanie organizacją, IT, bezpieczeństwo informacji, cyberbezpieczeństwo i zgodność regulacyjną.

Warunki techniczne

Usługa jest realizowana online w czasie rzeczywistym za pośrednictwem Microsoft Teams. Uczestnik potrzebuje komputera lub laptopa ze stabilnym dostępem do Internetu, aktualnej przeglądarki internetowej lub aplikacji Microsoft Teams oraz sprawnego mikrofonu i głośników lub słuchawek. Uczestnik powinien posiadać adres e-mail umożliwiający otrzymanie linku do szkolenia i materiałów. Materiały szkoleniowe są udostępniane w formie elektronicznej.

Kontakt

Dominik

E-mail d.kantorowicz@odo24.pl
Telefon (+48) 530 950 288