



Wymagania NIS2/uKSC: Szkolenie dla kadry zarządzającej

Numer usługi 2026/06/24/17164/3646336

1 217,70 PLN brutto
990,00 PLN netto
202,95 PLN brutto/h
165,00 PLN netto/h
261,33 PLN cena rynkowa ⓘ

Dagma sp. z o.o.

★★★★★ 4,5 / 5

467 ocen

- 📄 Usługa szkoleniowa
- 📺 zdalna w czasie rzeczywistym
- 👥 Zajęcia grupowe
- 🕒 06:00 h
- 📅 16.09.2026 do 16.09.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Wymagania • podstawowe zrozumienie funkcjonowania organizacji oraz odpowiedzialności zarządczej, • brak konieczności wiedzy technicznej – szkolenie kierowane jest przede wszystkim do kierownictwa.
Minimalna liczba uczestników	4
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	07-09-2026
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

Uczestnicy poznają nowe zasady samoidentyfikacji podmiotów, zarządzania ryzykiem, zgłaszania incydentów, bezpieczeństwa łańcucha dostaw oraz wymagania techniczne wynikające z ustawy. Szkolenie dostarcza praktycznej instrukcji wdrożenia UKSC w organizacji, obejmującej analizę ryzyka, dokumentację, nadzór, polityki bezpieczeństwa i przygotowanie do kontroli.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik pozna obowiązki podmiotów kluczowych i ważnych, różnice między nimi oraz zasady samoidentyfikacji	Uczestnik rozróżnia rodzaje podmiotów i potrafi poprawnie je zidentyfikować	Wywiad swobodny
Uczestnik nauczy się, jakie środki bezpieczeństwa techniczne i organizacyjne wdrażać (MFA, SIEM, EDR, monitoring, polityki, backupy, BCP/DRP)	Uczestnik potrafi opisać techniczne i organizacyjne środki bezpieczeństwa	Wywiad swobodny
Uczestnik zrozumie relacje UKSC a NIS2, RODO, DORA, KRI oraz normami ISO (27001, 22301)	Uczestnik potrafi opisać jakie są relacje pomiędzy wytycznymi NIS2, a UKSC, RODO, DORA, KRI oraz ISO (27001, 22301)	Wywiad swobodny

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

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

TAK

Pytanie 2. Czy dokument lub wyrażnie 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 wyrażnie z nim powiązane inne dokumenty związane ze wsparciem potwierdzają zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

1. Wprowadzenie do UKSC i kontekst regulacyjny

- Dlaczego powstała NIS2: rosnące zagrożenia, luki w NIS1
- Cel ustawy: odporność usług kluczowych, ujednolicenie wymogów

2. Kluczowe obowiązki dla zarządu

- Osobista odpowiedzialność członków organu zarządzającego

- Obowiązek szkoleń zarządu
- Zakres nadzoru nad środkami cyberbezpieczeństwa
- Zasada: „Nie można delegować odpowiedzialności na dział IT”

3. Sankcje i odpowiedzialność karna / finansowa

- Podmioty kluczowe: do 10 mln € lub 2% obrotu
- Podmioty ważne: do 7 mln € lub 1,4% obrotu
- Kary osobowe: do 600% wynagrodzenia, zakaz pełnienia funkcji
- Okresowe kary dzienne do 100 000 zł
- Sankcje za brak rejestracji, brak środków, brak zgłoszeń

4. Podmioty kluczowe, ważne i wyłączenia

- Zasady samoidentyfikacji
- Kryteria branżowe i wielkościowe (Załącznik 1 i 2)
- Sektory objęte UKSC (energia, zdrowie, transport, żywność, poczta, chemikalia, centra danych, infrastruktura cyfrowa itd.)
- Wyłączenia: mikro i małe firmy, podmioty poza katalogiem sektorów

5. Podstawowe pojęcia i definicje

- Podmiot kluczowy / ważny
- Incydent, CSIRT, system zarządzania ryzykiem
- Dokumentacja bezpieczeństwa
- NSC – Narodowe Standardy Cyberbezpieczeństwa
- Powiązania z RODO, DORA, KRI, normami ISO

6. Obowiązki zarządu w zakresie zarządzania ryzykiem

- Samoidentyfikacja
- Nadzór nad systemem zarządzania ryzykiem
- Zatwierdzanie planów, ocen dostawców
- Współpraca z CSIRT
- Monitorowanie zgodności

7. Środki bezpieczeństwa – art. 21 NIS2

Organizacyjne:

- polityki bezpieczeństwa, procedury, szkolenia
- procedury reagowania na incydenty
- procedury dostępu, zarządzania zmianą, backupów

Techniczne:

- MFA, zasada najmniejszego uprzywilejowania
- szyfrowanie danych
- SIEM, IDS/IPS, EDR, NDR, SOAR
- segmentacja sieci
- monitoring 24/7
- proces patch management

Operacyjne:

- analiza ryzyka, rejestr ryzyk
- BCP/DRP – RTO / RPO
- bezpieczeństwo łańcucha dostaw

8. Zgłaszanie incydentów

- Wstępne zgłoszenie – 24 h
- Szczegółowe – 72 h
- Raport końcowy – 30 dni
- Współpraca z CSIRT
- Mechanizmy wczesnego ostrzegania
- Powiadamianie użytkowników

9. Instrukcja wdrożenia UKSC – krok po kroku

- 1. Identyfikacja podlegania UKSC
- 2. Powołanie zespołu i struktury odpowiedzialności
- 3. Kompleksowa analiza ryzyka
- 4. Ustanowienie polityk i procedur
- 5. Wdrożenie środków technicznych
- 6. Kontrola dostawców
- 7. Przygotowanie procesu raportowania incydentów
- 8. Budowa systemu szkoleń
- 9. Uporządkowanie ciągłości działania i backupów
- 10. Dowody zgodności i przygotowanie do kontroli
- 11. Raportowanie cykliczne do zarządu
- 12. Ciągłe doskonalenie (PDCA)

Harmonogram

Liczba pozycji harmonogramu: 12

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 12 1. Wprowadzenie do UKSC i kontekst regulacyjny	Zajęcia	Paweł Pudo	16-09-2026	09:00	09:15	00:15
2 z 12 2. Kluczowe obowiązki dla zarządu	Zajęcia	Paweł Pudo	16-09-2026	09:15	09:45	00:30
3 z 12 3. Sankcje i odpowiedzialność karna / finansowa	Zajęcia	Paweł Pudo	16-09-2026	09:45	10:15	00:30
4 z 12 4. Podmioty kluczowe, ważne i wyłączenia	Zajęcia	Paweł Pudo	16-09-2026	10:15	10:45	00:30
5 z 12 -	Przerwa	-	16-09-2026	10:45	11:15	00:30
6 z 12 5. Podstawowe pojęcia i definicje	Zajęcia	Paweł Pudo	16-09-2026	11:15	11:45	00:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
7 z 12 6. Obowiązki zarządu w zakresie zarządzania ryzykiem	Zajęcia	Paweł Pudo	16-09-2026	11:45	12:30	00:45
8 z 12 7. Środki bezpieczeństwa – art. 21 NIS2	Zajęcia	Paweł Pudo	16-09-2026	12:30	13:00	00:30
9 z 12 -	Przerwa	-	16-09-2026	13:00	13:30	00:30
10 z 12 8. Zgłaszanie incydentów	Zajęcia	Paweł Pudo	16-09-2026	13:30	14:00	00:30
11 z 12 9. Instrukcja wdrożenia UKSC – krok po kroku	Zajęcia	Paweł Pudo	16-09-2026	14:00	14:45	00:45
12 z 12 -	Walidacja	-	16-09-2026	14:45	15:00	00:15

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	06:00
w tym suma godzin zajęć	04:45
w tym suma godzin walidacji	00:15
w tym suma przerw	01:00
Suma godzin dydaktycznych bez przerw	06:30

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 2024 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	1 217,70 PLN
Koszt przypadający na 1 uczestnika netto	990,00 PLN
Koszt osobogodziny brutto	202,95 PLN
Koszt osobogodziny netto	165,00 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	06:00

Prowadzący

Liczba prowadzących: 1



1 z 1

Paweł Pudo

doświadczony praktyk IT i cyberbezpieczeństwa, który od ponad 25 lat działa w branży technologicznej, a od kilku lat specjalizuje się w bezpieczeństwie informacji i ochronie przed cyberzagrożeniami.

Prowadzi szkolenia i projekty edukacyjne z zakresu cyberbezpieczeństwa oraz zastosowania nowych technologii (w tym AI) w biznesie. Skupia się przede wszystkim na praktycznym podejściu i realnych zagrożeniach, z jakimi mierzą się organizacje i użytkownicy.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały dydaktyczne w formie elektronicznej.

Warunki uczestnictwa

Prosimy o zapisanie się na szkolenie przez naszą stronę internetową <https://szkolenia.dagma.eu/pl> w celu rezerwacji miejsca.

Informacje dodatkowe

- W cenę szkolenia nie wchodzi koszty związane z dojazdem, wyżywieniem oraz noclegiem
- Harmonogram ma charakter ramowy i trener może na potrzeby grupy szkoleniowej zmienić długość poszczególnych modułów, przy zachowaniu niezmienną łącznej liczby godzin usługi szkoleniowej.
- Uczestnik otrzyma zaświadczenie DAGMA Szkolenia IT o ukończeniu szkolenia
- Uczestnik ma możliwość złożenia reklamacji po zrealizowanej usłudze, sporządzając ją w formie pisemnej (na wniosku reklamacyjnym) i odsyłając na adres szkolenia@dagma.pl. Reklamacja zostaje rozpatrzona do 30 dni od dnia otrzymania dokumentu przez DAGMA SZKOLENIA IT.
- Organizator szkolenia zastrzega sobie prawo do zmiany trenera prowadzącego/walidującego jeśli z przyczyn niezależnych od Organizatora (np. zdarzenie losowe) wyznaczony trener nie będzie mógł przeprowadzić szkolenia. Przy czym Organizator zobowiązuje się do zapewnienia w zastępstwie trenera o takich samych/zbliżonych kompetencjach.

Warunki techniczne

WARUNKI TECHNICZNE:

a) platforma/rodzaj komunikatora, za pośrednictwem którego prowadzona będzie usługa:

- **ZOOM**
- w przypadku kilku uczestników przebywających w jednym pomieszczeniu, istnieją dwie możliwości udziału w szkoleniu:

1) każda osoba bierze udział w szkoleniu osobno (korzystając z oddzielnych komputerów), wówczas należy wyciszyć dźwięki z otoczenia by uniknąć sprzężeń;

2) otrzymujecie jedno zaproszenie, wówczas kilka osób uczestniczy w szkoleniu za pośrednictwem jednego komputera

- Można łatwo udostępniać sobie ekran, oglądać pliki, bazę handlową, XLS itd.

b) minimalne wymagania sprzętowe, jakie musi spełniać komputer Uczestnika lub inne urządzenie do zdalnej komunikacji:

- Uczestnik potrzebuje komputer z przeglądarką Chrome lub Edge (NIE firefox), mikrofon, głośniki.

c) minimalne wymagania dotyczące parametrów łącza sieciowego, jakim musi dysponować Uczestnik:

- łącze internetowe o przepustowości minimum 10Mbit,

d) niezbędne oprogramowanie umożliwiające Uczestnikom dostęp do prezentowanych treści i materiałów:

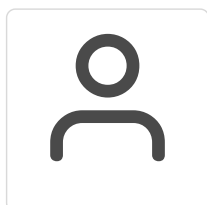
- uczestnik na tydzień przed szkoleniem otrzyma maila organizacyjnego, ze szczegółową instrukcją pobrania darmowej platformy ZOOM.
- Z platformy MS Teams można korzystać za pośrednictwem przeglądarki, nie trzeba nic instalować.

e) okres ważności linku:

- link będzie aktywny od pierwszego dnia rozpoczęcia się szkolenia do ostatniego dnia trwania usługi

Szczegóły, związane z prowadzonymi przez nas szkoleniami online, znajdziesz na naszej stronie: <https://szkolenia.dagma.eu/pl/training-list>

Kontakt



Anna Koruba

E-mail koruba.a@dagma.pl

Telefon (+48) 32 7931 180