Możliwość dofinansowania

Szkolenie: Cyberbezpieczeństwo organizacji – zgodność z NIS2 i normą ISO/IEC 27001:2022 (część 1: teoria i fundamenty systemów ochrony).

Numer usługi 2025/08/11/47095/2933443

5 000,00 PLN brutto
5 000,00 PLN netto
250,00 PLN brutto/h
250,00 PLN netto/h

ADN AKADEMIA spółka z ograniczoną odpowiedzialnością spółka komandytowa

4,6 / 5

316 ocen

zdalna w czasie rzeczywistym
Usługa szkoleniowa
20 h
19.01.2026 do 27.01.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Szkolenie skierowane jest do osób odpowiedzialnych za bezpieczeństwo informacji i zgodność prawną w organizacjach, w szczególności do: • pracowników działów IT, compliance, audytu lub zarządzania ryzykiem, • osób pełniących lub przygotowujących się do pełnienia funkcji Inspektora Ochrony Danych, Pełnomocnika ds. Bezpieczeństwa Informacji, Audytora wewnętrznego, • kadry kierowniczej i właścicieli procesów w organizacjach podlegających regulacjom NIS2 (np. sektor energetyczny, zdrowotny, transportowy, wod-kan, administracja, cyfrowy), • osób planujących wdrożenie lub nadzorujących system zarządzania bezpieczeństwem informacji zgodny z ISO/IEC 27001:2022, • pracowników MŚP, instytucji publicznych, NGO i dużych firm, które chcą zwiększyć odporność organizacji na cyberzagrożenia i dostosować się do aktualnych regulacji prawnych i normatywnych.
Minimalna liczba uczestników	5
Maksymalna liczba uczestników	20
Data zakończenia rekrutacji	18-01-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	20
Podstawa uzyskania wpisu do BUR	Certyfikat VCC Akademia Edukacyjna

Cel

Cel edukacyjny

Szkolenie przygotowuje uczestników do uzyskania kwalifikacji w zakresie zarządzania bezpieczeństwem informacji zgodnie z wymaganiami ISO/IEC 27001:2022 oraz zgodności z dyrektywą NIS2, zgodnie z aktualnymi przepisami krajowymi i unijnymi dotyczącymi cyberbezpieczeństwa.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Wyjaśnia podstawowe pojęcia z zakresu cyberbezpieczeństwa (zagrożenie, incydent, podatność, ryzyko)	Rozpoznaje definicje i ich zastosowanie w kontekście ochrony informacji	Test teoretyczny
Wskazuje kluczowe wymagania dyrektywy NIS2 dla organizacji	Rozpoznaje obowiązki podmiotów objętych NIS2 oraz środki organizacyjne	Test teoretyczny
Charakteryzuje strukturę i wymagania normy ISO/IEC 27001:2022	Wskazuje elementy ISMS, cykl PDCA, dokumentację, polityki	Test teoretyczny
Wyjaśnia rolę analizy ryzyka i doboru środków bezpieczeństwa	Wskazuje etapy szacowania ryzyka i przykłady kontroli z Załącznika A	Test teoretyczny
Interpretuje powiązania między wymaganiami NIS2 a systemem ISMS	Wskazuje wspólne elementy i zależności między regulacjami	Test teoretyczny
Dobiera odpowiednie środki kontroli bezpieczeństwa do określonego ryzyka	Rozpoznaje adekwatne środki bezpieczeństwa dla scenariusza	Test teoretyczny
Analizuje wpływ kontekstu organizacji na bezpieczeństwo informacji	Określa przykładowe strony zainteresowane, zagrożenia i ryzyka	Wywiad swobodny
Uzasadnia potrzebę wdrażania systemowego podejścia do bezpieczeństwa informacji	Wskazuje korzyści zgodności z ISO/NIS2 dla organizacji	Wywiad swobodny
Wykazuje gotowość do wspierania zgodności z przepisami prawa i normami	Rozpoznaje konsekwencje braku zgodności, Opisuje etykę cyberbezpieczeństwa	Wywiad swobodny

Kwalifikacje

Inne kwalifikacje

Uznane kwalifikacje

Pytanie 4. Czy dokument potwierdzający uzyskanie kwalifikacji jest rozpoznawalny i uznawalny w danej branży/sektorze (czy certyfikat otrzymał pozytywne rekomendacje od co najmniej 5 pracodawców danej branży/

sektorów lub związku branżowego, zrzeszającego pracodawców danej branży/sektorów)?

TAK

Informacje

Podstawa prawna dla Podmiotów / kategorii Podmiotów	uprawnione do realizacji procesów walidacji i certyfikowania na mocy innych przepisów prawa
Nazwa Podmiotu prowadzącego walidację	Design Center
Podmiot prowadzący walidację jest zarejestrowany w BUR	Nie
Nazwa Podmiotu certyfikującego	Design Center
Podmiot certyfikujący jest zarejestrowany w BUR	Nie

Program

Usługa prowadzona jest w godzinach dydaktycznych. Przerwy nie są wliczone w ogólny czas usługi rozwojowej. Harmonogram usługi może ulec nieznacznemu przesunięciu, ponieważ ilość przerw oraz długość ich trwania zostanie dostosowana indywidualnie do potrzeb uczestników szkolenia. Łączna długość przerw podczas szkolenia nie będzie dłuższa aniżeli zawarta w harmonogramie.

Szczegółowy harmonogram realizacji usługi zostanie dostosowany do potrzeb i możliwości uczestników a jego finalna wersja zostanie podana zgodnie z wymaganiami systemu BUR, przed rozpoczęciem realizacji usługi.

Zajęcia zostaną przeprowadzone przez ekspertów z wieloletnim doświadczeniem, którzy przekazuje nie tylko wiedzę teoretyczną, ale także praktyczne wskazówki i najlepsze praktyki. Uczestnicy mają możliwość czerpania z jego wiedzy i doświadczeń.

Szkolenie ma charakter **teoretyczny** i stanowi **część 1 (fundamenty)** w cyklu usług rozwijających kompetencje w zakresie systemów bezpieczeństwa informacji.

Moduł 1: Wprowadzenie do cyberbezpieczeństwa i zarządzania ryzykiem.

- Kluczowe pojęcia: zagrożenia, podatności, incydenty, ataki
- Modele bezpieczeństwa (CIA, STRIDE, DREAD)
- Wprowadzenie do zarządzania ryzykiem

Moduł 2: Dyrektywa NIS2 – nowe obowiązki organizacji.

- Zakres i cele NIS2
- Podmioty kluczowe i ważne – kto podlega?
- Wymogi w zakresie raportowania, środków bezpieczeństwa, odpowiedzialności
- Sankcje i nadzór

Moduł 3: System Zarządzania Bezpieczeństwem Informacji (ISMS) wg ISO/IEC 27001:2022.

- Struktura i podejście procesowe (PDCA)
- Rola polityki bezpieczeństwa, kontekstu i stron zainteresowanych
- Kluczowe wymagania normy i ich zastosowanie w organizacji

Moduł 4: Zarządzanie ryzykiem i środki kontroli (Annex A ISO 27001).

- Proces szacowania i traktowania ryzyka (wg ISO 27005)
- Kategorie środków bezpieczeństwa (organizacyjne, techniczne, fizyczne)
- Praktyczne przykłady zabezpieczeń dla systemów i sieci

- Integracja z kontrolami technicznymi i chmurowymi

Moduł 5: Zgodność i wdrażanie systemu bezpieczeństwa.

- Mapowanie wymagań NIS2 i ISO 27001
- Integracja z RODO, ISO 22301, ISO 31000
- Dobre praktyki i przygotowanie do certyfikacji
- Typowe błędy i zagrożenia przy wdrażaniu

Moduł 6: Walidacja efektów uczenia się.

Harmonogram

Liczba przedmiotów/zajęć: 9

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 9 Moduł 1: Wprowadzenie do cyberbezpieczeństwa i zarządzania ryzykiem	Paweł Pudo	19-01-2026	17:00	20:30	03:30
2 z 9 Moduł 2: Dyrektywa NIS2 – nowe obowiązki organizacji	Paweł Pudo	19-01-2026	17:00	20:30	03:30
3 z 9 Moduł 3: System Zarządzania Bezpieczeństwem Informacji (ISMS) wg ISO/IEC 27001:2022	Paweł Pudo	21-01-2026	17:00	20:15	03:15
4 z 9 oduł 4: Zarządzanie ryzykiem i środki kontroli (Annex A ISO 27001)	Paweł Pudo	21-01-2026	17:00	20:30	03:30
5 z 9 Przerwa	Paweł Pudo	21-01-2026	19:15	19:30	00:15
6 z 9 cd. Moduł 4: Zarządzanie ryzykiem i środki kontroli (Annex A ISO 27001)	Paweł Pudo	23-01-2026	19:30	21:00	01:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
7 z 9 Moduł 5: Zgodność i wdrażanie systemu bezpieczeństwa	Paweł Pudo	27-01-2026	17:00	20:30	03:30
8 z 9 Przerwa	Paweł Pudo	27-01-2026	19:15	19:30	00:15
9 z 9 Walidacja	-	27-01-2026	19:30	20:15	00:45

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	5 000,00 PLN
Koszt przypadający na 1 uczestnika netto	5 000,00 PLN
Koszt osobogodziny brutto	250,00 PLN
Koszt osobogodziny netto	250,00 PLN
W tym koszt walidacji brutto	0,00 PLN
W tym koszt walidacji netto	0,00 PLN
W tym koszt certyfikowania brutto	0,00 PLN
W tym koszt certyfikowania netto	0,00 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Paweł Pudo

Od ponad pięciu lat Paweł Pudo intensywnie rozwija kompetencje w obszarach cyberbezpieczeństwa, administracji IT oraz edukacji cyfrowej, z powodzeniem łącząc umiejętności techniczne z talentem do klarownego przekazywania wiedzy nietechnicznym odbiorcom.

Obecnie odpowiada za całość infrastruktury IT w jednostce edukacyjnej, gdzie zarządza m.in. środowiskiem sieciowym, Azure Active Directory, pakietem Office 365, drukiem 3D i administracją stron internetowych. Równocześnie prowadzi audyty zgodne z normami ISO/IEC 27001:2017-06, ISO 22301:2020-04 oraz RODO, wspierając instytucje w budowaniu bezpiecznych i zgodnych z przepisami systemów informatycznych. Ukończył kurs audytora wiodącego SZBI (ISO 27001).

Paweł od lat prowadzi szkolenia z zakresu cyberbezpieczeństwa dla szkół, samorządów i przedsiębiorstw, dzieląc się praktyczną wiedzą i doświadczeniem. Znany z wyjątkowej umiejętności tłumaczenia skomplikowanych zagadnień technicznych w prosty i przystępny sposób, co czyni go niezwykle skutecznym edukatorem i konsultantem.

W 2021 roku ukończył studia podyplomowe "Bezpieczeństwo i ochrona cyberprzestrzeni" na Uniwersytecie Ekonomicznym w Katowicach.

W ostatnim czasie intensywnie szkoli się również w zakresie zastosowań sztucznej inteligencji w edukacji i biznesie, wykorzystując AI m.in. do budowania narzędzi szkoleniowych. Regularnie występuje jako prelegent na wydarzeniach branżowych, dzieląc się wiedzą jako członek społeczności cybersec.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Informacje o materiałach dla uczestników usługi

Uczestnik otrzyma skrypt, materiały dydaktyczne w formie prezentacji oraz zestaw ćwiczeń w formie cyfrowej- pdf.

Warunki uczestnictwa

- Uczestnik powinien posiadać podstawową wiedzę o funkcjonowaniu organizacji oraz przepływie informacji w jej strukturze.
- Zalecana jest znajomość podstawowych pojęć z zakresu bezpieczeństwa informacji, przepisów RODO lub zarządzania ryzykiem (mile widziane doświadczenie zawodowe w działach IT, compliance, administracji lub audytu).
- Uczestnictwo nie wymaga wiedzy technicznej ani doświadczenia w normach ISO – szkolenie obejmuje wprowadzenie do ISO/IEC 27001:2022 i dyrektywy NIS2.

Ponadto:

Wymagana jest obecność min 80% lub ze wskazaniami Operatora

Uczestnicy przyjmują do wiadomości, że usługa może być poddana monitoringowi z ramienia Operatora lub PARP i wyrażają na to zgodę. Uczestnik ma obowiązek zapisania się na usługę przez BUR co najmniej na 1 dzień przed rozpoczęciem szkolenia.

Informacje dodatkowe

Przed zapisaniem się na usługę, w celu potwierdzenia dostępności miejsca w grupie szkoleniowej prosimy o kontakt pod numerem telefonu

34 387 16 73 lub 530 642 270

Podstawa zwolnienia z VAT:

1) art. 43 ust. 1 pkt 29 lit. c Ustawy z dnia 11 marca 2024 o podatku od towarów i usług - w przypadku dofinansowania w wysokości 100%

2) § 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 dofinansowania w co najmniej 70%

3) W przypadku braku uzyskania dofinansowania lub uzyskania dofinansowania poniżej 70%, do ceny usługi należy doliczyć 23% VAT

Warunki techniczne

Szkolenie realizowane będzie w formule zdalnej (online) w czasie rzeczywistym, z wykorzystaniem platformy wideokonferencyjnej (Click Meeting).

Minimalne wymagania techniczne po stronie uczestnika:

- komputer lub laptop z dostępem do internetu o minimalnej prędkości 10 Mb/s,
- aktualna wersja przeglądarki internetowej (Google Chrome, Firefox, Edge lub Safari),
- działający mikrofon i głośniki (lub słuchawki)- **WARUNEK KONIECZY**
- kamera – **WARUNEK KONIECZNY**
- możliwość korzystania z linków i dokumentów udostępnianych podczas zajęć.

Minimalne wymagania dotyczące parametrów łącza sieciowego, jakim musi dysponować Uczestnik - minimalna prędkość łącza: 512 KB/sek

Platforma, na której zostanie przeprowadzone szkolenie to Click Meeting

Okres ważności linku: 1h przed rozpoczęciem szkolenia w pierwszym dniu do ostatniej godziny w dniu zakończenia

Kontakt

Ariel Banaszewski

E-mail ariel.banaszewski@adn.pl
Telefon (+48) 22 1627 981