Możliwość dofinansowania

ADN AKADEMIA spółka z ograniczoną odpowiedzialnością spółka komandytowa

4,6 / 5

316 ocen

Szkolenie: Cyberbezpieczeństwo organizacji – zgodność z NIS2 i normą ISO/IEC 27001:2022 (część 2: praktyczne wdrożenie wymagań i analiza przypadków).

Numer usługi 2025/11/17/47095/3153404

5 000,00 PLN brutto
5 000,00 PLN netto
333,33 PLN brutto/h
333,33 PLN netto/h

zdalna w czasie rzeczywistym
Usługa szkoleniowa
15 h
04.02.2026 do 13.02.2026

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	15

Data zakończenia rekrutacji	03-02-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	15
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
Identyfikuje etapy wdrożenia ISMS zgodnie z ISO/IEC 27001	Wskazuje poprawną kolejność działań: kontekst, ryzyko, środki, dokumentacja	Test teoretyczny
Rozróżnia środki bezpieczeństwa z Załącznika A ISO/IEC 27001	Dobiera środki do konkretnych obszarów ryzyka	Obserwacja w warunkach rzeczywistych
Przeprowadza analizę luk (gap analysis) w kontekście zgodności z ISO i NIS2	Wypełnia wzorzec gap analysis i uzasadnia wyniki	Test teoretyczny
Opracowuje uproszczoną ocenę ryzyka i proponuje działania zaradcze	Tworzy rejestr ryzyk i przypisuje do nich środki kontroli	Obserwacja w warunkach rzeczywistych
Tworzy podstawowe elementy dokumentacji ISMS	Przygotowuje szkic polityki, procedury lub zakres ISMS	Obserwacja w warunkach rzeczywistych
Przestrzega zasad odpowiedzialności i zgodności w zarządzaniu informacją	Wskazuje ryzyka niezgodności i proponuje działania zapobiegawcze	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 praktyczny i stanowi część 2 w cyklu usług rozwijających kompetencje w zakresie systemów bezpieczeństwa informacji.

Moduł 1: Diagnoza organizacji i analiza luk (gap analysis)(3 godz.)

Praca z arkuszem analizy luk ISO/IEC 27001 i dyrektywy NIS2

Identyfikacja słabych punktów i dobór priorytetów działań

Ćwiczenie: opracowanie uproszczonego planu wdrożeniowego

Moduł 2: Szacowanie ryzyka i dobór zabezpieczeń (risk treatment)(3 godz.)

Mapowanie aktywów i zagrożeń (ćwiczenie na case study)

Tworzenie rejestru ryzyka i wyboru środków zaradczych

Zastosowanie Annex A w doborze zabezpieczeń

Moduł 3: Dokumentacja systemu ISMS – warsztat(3 godz.)

Opracowywanie wzorcowej dokumentacji: polityka, procedury, zakres

Ćwiczenia w zespołach: opis dostępów, reagowanie na incydenty

Nadzór nad dokumentacją i działania zgodne z ISO 27001

Moduł 4: Monitoring, reagowanie i gotowość audytowa(5 godz.)

Planowanie audytów wewnętrznych i przeglądów zarządzania

Ćwiczenia z reagowania na incydenty (np. phishing, ransomware)

Opracowanie raportów zgodności i dowodów spełnienia wymagań

Symulacja audytu zgodności (checklista i pytania kontrolne)

Moduł 5: Walidacja efektów uczenia się(1 godz.)

Harmonogram

Liczba przedmiotów/zajęć: 9

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 9 Moduł 1: Diagnoza organizacji i analiza luk (gap analysis)	Paweł Pudo	04-02-2026	17:00	19:15	02:15
2 z 9 Moduł 2: Szacowanie ryzyka i dobór zabezpieczeń (risk treatment)	Paweł Pudo	06-02-2026	19:15	20:00	00:45
3 z 9 cd. Moduł 2: Szacowanie ryzyka i dobór zabezpieczeń (risk treatment)	Paweł Pudo	07-02-2026	17:00	18:30	01:30
4 z 9 Moduł 4: Monitoring, reagowanie i gotowość audytowa	Paweł Pudo	08-02-2026	17:00	19:15	02:15
5 z 9 Przerwa	Paweł Pudo	08-02-2026	18:30	18:45	00:15
6 z 9 Moduł 3: Dokumentacja systemu ISMS – warsztat	Paweł Pudo	08-02-2026	18:45	21:00	02:15

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
7 z 9 cd. Moduł 4: Monitoring, reagowanie i gotowość audytowa	Paweł Pudo	13-02-2026	17:00	18:30	01:30
8 z 9 Przerwa	Paweł Pudo	13-02-2026	18:30	18:45	00:15
9 z 9 Walidacja	-	13-02-2026	18:45	19:30	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	333,33 PLN
Koszt osobogodziny netto	333,33 PLN
W tym koszt walidacji brutto	120,00 PLN
W tym koszt walidacji netto	120,00 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 dot. szkolenia oraz materiały dydaktyczne- prezentację oraz zestaw ćwiczeń w formie elektronicznej

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 jest 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

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

Kontakt

Ariel Banaszewski

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