



Bezpieczeństwo cyfrowe - kompetencje w zakresie cyfryzacji

Numer usługi 2026/03/24/44943/3431434

5 166,00 PLN brutto
4 200,00 PLN netto
322,88 PLN brutto/h
262,50 PLN netto/h
261,33 PLN cena rynkowa ⓘ

RnD.Aero Spółka z
Ograniczoną
Odpowiedzialnością

★★★★★ 4,8 / 5

563 oceny

📍 Rzeszów

📄 Usługa szkoleniowa

📅 mieszana (stacjonarna połączona z usługą zdalną w czasie rzeczywistym)

🕒 16:00 h

📅 02.06.2026 do 16.06.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Usługa skierowana jest do całego personelu firm od kadry menadżerskiej i właścicielska/współwłaścicielska po pracowników biurowych. Osoby te powinny posiadać podstawowe kompetencje i wiedzę o obsłudze komputerów i Internetu oraz AI.
Minimalna liczba uczestników	5
Maksymalna liczba uczestników	20
Data zakończenia rekrutacji	01-06-2026
Forma prowadzenia usługi	mieszana (stacjonarna połączona z usługą zdalną w czasie rzeczywistym)
Liczba godzin usługi	16
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 podstawowego szkolenia jest przygotowanie do zidentyfikowania i zrozumienia przez uczestników różnicowanych źródeł zagrożeń ataków cyfrowych oraz umiejętność wyboru i stosowania zasad zabezpieczeń technicznych i organizacyjnych w celu przeciwdziałania atakom i/lub łagodzenia ich skutków.

Przygotowuje do: budowania świadomości osób przetwarzających informacje, opracowywania/weryfikowania zasad bezpieczeństwa danych, nadzorowania ustanawiania, wdrażania, utrzymania i ciągłego doskonalenia SZBI

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik posługuje się wiedzą, znajomością i interpretacją wymagań normy ISO 27001	Charakteryzuje i rozróżnia poszczególne punkty normy	Test teoretyczny z wynikiem generowanym automatycznie
	Omawia, uzasadnia i charakteryzuje cele i zasady Systemu Zarządzania Bezpieczeństwem Informacji	Test teoretyczny z wynikiem generowanym automatycznie

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 rozdzielanie procesów kształcenia i szkolenia od walidacji?

TAK

Program

Moduł 1. Wstęp i wprowadzenie do bezpieczeństwa informacji

- Źródła zagrożeń i ataków dotyczące cyberbezpieczeństwa w firmie (wynikających między innymi ze stosowania nowych rozwiązań cyfrowych, w tym algorytmów sztucznej inteligencji, przetwarzania w chmurze, rozwiązań mobilnych)
- Stosowanie odpowiednich zabezpieczeń przed atakami w tym podstawy zabezpieczania przesyłania danych w przedsiębiorstwie i w całym łańcuchu wartości
- Zarządzanie i szacowanie ryzyka w bezpieczeństwie informacji / bezpieczeństwie cyfrowym w oparciu o ISO/IEC 27005
- Modele zabezpieczeń oprogramowania
- Regulacje prawne z zakresu ochrony i przetwarzania danych oraz podstaw bezpieczeństwa cyfrowego w przedsiębiorstwie
- Cykl PDCA. Podejście procesowe. Nastawienie na osiągnięcie celów. Monitorowanie i doskonalenie w oparciu o uzyskane wyniki
- Norma ISO 9001 - podstawowe informacje
- Norma ISO/IEC 27005 Zarządzanie ryzykiem bezpieczeństwa informacji - wymagania, rola i charakterystyka

- Bezpieczeństwo pracy z AI

Moduł 2. Omówienie wymagań ISO/IEC 27001 w tym sposobów zapewnienia bezpieczeństwa informacji zgodnie z Załącznikiem A do ISO/IEC 27001:2022 oraz wymaganej dokumentacji.

- Kontekst Organizacyjny
- Przywództwo. Polityka Bezpieczeństwa Informacji. Role i Odpowiedzialność.
- Planowanie Systemu Zarządzania Bezpieczeństwem Informacji
- Wsparcie Systemu Zarządzania Bezpieczeństwem Informacji
- Realizacja Systemu Zarządzania Bezpieczeństwem Informacji
- Monitorowanie Systemu Zarządzania Bezpieczeństwem Informacji
- Ciągłe Doskonalenie
- Polityki Bezpieczeństwa Informacji
- Organizacja Zabezpieczenia Informacji
- Bezpieczeństwo Zasobów Ludzkich
- Zarządzanie
- Kontrola Dostępu
- Kryptografia
- Bezpieczeństwo fizyczne i środowiskowe
- Bezpieczeństwo operacji
- Bezpieczeństwo Komunikacji
- Uzyskanie dostępu, rozwój i utrzymanie systemu
- Relacje z dostawcami
- Zarządzanie incydentami związanymi z bezpieczeństwem informacji
- Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością biznesu
- Zgodność
- Polityki
- Procedury i instrukcje w tym przykład metodologii szacowania i zarządzania zidentyfikowanym ryzykiem
- Zapisy z realizacji Systemu Zarządzania Bezpieczeństwem Informacji w tym przykład analizy zabezpieczeń systemów teleinformatycznych

Moduł 3. Bezpieczeństwo Informacji na co dzień - GEMBA WALK

Moduł 4. Egzamin

Harmonogram

Liczba pozycji harmonogramu: 1

Przedmiot / temat	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin	Forma stacjonarna
1 z 1 Moduł 4. Egzamin	-	16-06-2026	11:00	11:30	00:30	Nie

Cennik

Jeżeli korzystasz z dofinansowania w wysokości co najmniej 70% przysługuje Tobie zwolnienie z podatku VAT

Cennik

Rodzaj ceny	Cena
-------------	------

Koszt przypadający na 1 uczestnika brutto	5 166,00 PLN
Koszt przypadający na 1 uczestnika netto	4 200,00 PLN
Koszt osobogodziny brutto	322,88 PLN
Koszt osobogodziny netto	262,50 PLN

Prowadzący

Liczba prowadzących: 3



1 z 3

KAROL URBAN

Posiadam 12 letnie doświadczenie na stanowiskach kierowniczych w branży lotniczej:

- Pełnomocnik ds. ZSZ ISO 900,ISO/IEC 27001, AS 9100
- Kierownik Jakości w Part 21 G POA
- Head of ISM a Part 21J DOA
- Doświadczenie w pracy w Organizacjach obsługowych EASA Part M/F, EASA Part 145
- Znajomość przepisów technicznych z dziedziny lotnictwa CS-25/FAR-25, CS-23/FAR-25, CS-P
- Znajomość wymagań technicznych dla cyfrowych urządzeń awioniki, w szczególności wymagania w zakresie odporności środowiskowej RTCA DO-160 oraz wymagania dla oprogramowania cyfrowych urządzeń awioniki zgodnie z RTCA DO-178C.
- Doświadczenie w projektach związanych modyfikacją floty (od strony projektowania i produkcji) dla wiodących linii lotniczych, w zakresie schematów malowań oraz wyposażenia kabiny pasażerskiej i kokpitu

W trakcie pracy zawodowej zdobyłem unikalne w skali kraju doświadczenie w projektach w branży lotniczej, w szczególności w obszarze zarządzania jakością oraz certyfikacji wyrobów lotniczych.

Swoje doświadczenie wykorzystałem w świadczeniu usług rozwojowych dla firm z branży lotniczej oraz dla innych przedsiębiorstw, co pozwala mi na dostosowanie prowadzonych szkoleń i realizowanych usług doradczych dokładnie do profilu Państwa przedsiębiorstwa.



2 z 3

ŁUKASZ RACHWAŁ

Absolwent studiów inżynierskich i magisterskich Politechniki Rzeszowskiej na kierunku Zarządzanie i Inżynieria Produkcji, o specjalności Systemy Zapewnienia Jakości Produkcji.

Odbyte szkolenia Audytora wewnętrznego ISO9001 oraz lotniczej normy z serii AS9110. Praktyczna wiedza i doświadczenie zdobyte podczas audytów wewnętrznych, zewnętrznych oraz klientów.

Doświadczenie praktyczne zdobyte w licznych projektach realizowanych dla firm z branży lotniczej, medycznej oraz informatycznej. Doświadczenie w pracy z firmami projektującymi, produkcyjnymi oraz handlowymi.

Udział w wielu projektach:

- cyfryzacji procesów technologicznych i wdrożenie technologii Przemysłu 4.0
- wdrożeń ISO 9001 i ISO 27001

- utrzymanie Systemów Zarządzania Jakością wg ISO9001 oraz AS9100 i AS9120
- utrzymanie Systemów Zarządzania Bezpieczeństwem Informacji wg ISO27001
- przeprowadzanie szkoleń z zakresu Systemów Jakości oraz Kontroli Jakości

Wiedza i umiejętności z zakresu objętym szkoleniem oraz ocena umiejętności instruktora została pozytywnie zweryfikowane przez Kierownictwo zgodnie z procedurami wdrożonego Systemu Zarządzania Jakości ISO9001. Trener posiada co najmniej 120 godzin doświadczenia w prowadzeniu szkoleń o podobnej tematyce dla osób dorosłych w ostatnich dwóch latach (24 miesiącach) wstecz od dnia rozpoczęcia szkolenia.



3 z 3

KAROLINA DERYŁO

Posiadam wieloletnie doświadczenie w obszarze bezpieczeństwa informacji oraz audytów systemów zarządzania bezpieczeństwem informacji. Od 5 lat jestem certyfikowanym audytorem wiodącym ISO 27001, specjalizującym się w ocenie zgodności organizacji z wymaganiami norm oraz przepisów dotyczących cyberbezpieczeństwa. W swojej praktyce przeprowadziłam około 150 audytów związanych z bezpieczeństwem informacji, w tym audyty dotyczące zgodności z wymaganiami cyberbezpieczeństwa oraz rozporządzeniem Krajowych Ram Interoperacyjności.

Wspieram organizacje w identyfikacji zagrożeń, ocenie ryzyka oraz doskonaleniu procesów związanych z ochroną informacji. Posiadam doświadczenie we współpracy z małymi i średnimi przedsiębiorstwami, pomagając im w budowaniu skutecznych i praktycznych rozwiązań w zakresie bezpieczeństwa IT.

Prowadzę również szkolenia dotyczące bezpieczeństwa w sieci, aktualnych zagrożeń informatycznych oraz budowania świadomości cyberbezpieczeństwa wśród pracowników. W trakcie szkoleń skupiam się na praktycznym podejściu do ochrony danych i systemów informatycznych w codziennej pracy. Moim celem jest zwiększanie świadomości zagrożeń oraz wspieranie organizacji w tworzeniu kultury bezpieczeństwa informacji. Dzięki połączeniu doświadczenia audytorskiego i szkoleniowego przekazuję wiedzę w sposób zrozumiały i dostosowany do potrzeb uczestników.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Każdy uczestnik pierwszego dnia otrzyma komplet materiałów w postaci elektronicznej.

Każdy z uczestników będzie miał dostęp do materiałów ćwiczeniowych

Informacje dodatkowe

Bezpieczeństwo cyfrowe - kompetencje w zakresie cyfryzacji to 16 godzin lekcyjnych, w tym ponad 15 godzin lekcyjnych na zdobywanie wiedzy, umiejętności i kompetencji oraz 30 minut przeznaczonych na egzamin w formie testu wiedzy na temat podstawowych zagadnień dotyczących cyberbezpieczeństwa.

1 godzina lekcyjna to 45 minut, 16 godzin lekcyjnych (16 godzin lekcyjnych x 45minut = 720 minut = 12 godzin zegarowych).

Warunkiem uzyskania zaświadczenia jest uczestnictwo, w co najmniej 80% zajęć usługi rozwojowej oraz pozytywna ocena z egzaminu sprawdzającego osiągnięte efekty usługi rozwojowej.

Warunki techniczne

Usługi wykonywane przez naszą firmę są realizowane za pomocą narzędzi Google Meet lub Jitsi Meet

Dla Google Meet wymagany jest komputer z systemem w najnowszych(i 2 poprzednich) wersjach:

Mac OS X

Windows

Google Chrome

Ubuntu

Linuks dystrybucje oparte na Debianie

Do działania Google Meet wymaga aktualnej wersji jednej z wymienionych niżej przeglądarek:

- Chrome
- Mozilla Firefox
- Microsoft Edge
- Apple Safari.

Microsoft Internet Explorer nie zapewnia obsługi Google Meet i Jitsi Meet.

Do korzystania z Jitsi Meet wymagana jest jedna z najnowszych przeglądarek:

- Chrome
- Firefox
- Safari

Wymagane jest również stabilne połączenie z siecią internet. Zalecana prędkość minimalna to 2MB/s. Wymagane jest

posiadanie mikrofonu i słuchawek(głośników). Wymagane jest posiadanie kamery.

Każdy z uczestników przed usługą otrzyma link umożliwiający połączenie się. Link będzie ważny podczas trwania usługi zgodnie z harmonogramem.

Do przeglądania materiałów wymagany jest oprogramowanie Adobe Acrobat Reader lub inne pozwalające na otwarcie pliku PDF.

Każdy uczestnik musi posiadać adres e-mail.

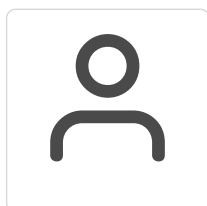
Adres

ul. Henryka Jakuba Kreczmera 4/4

35-065 Rzeszów

woj. podkarpackie

Kontakt



Piotr Mróz

E-mail biuro@rndaero.com

Telefon (+48) 502 704 605