Możliwość dofinansowania

Szkolenie Auditor Wewnętrzny Systemu Zarządzania Bezpieczeństwem Informacji wg. ISO/IEC 27001:2022

Numer usługi 2025/04/02/176271/2665583

1 451,40 PLN brutto
1 180,00 PLN netto
111,65 PLN brutto/h
90,77 PLN netto/h

OPEN HORIZON CONSULTING SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ SPÓŁKA KOMANDYTOWA

Brak ocen dla tego dostawcy

zdalna w czasie rzeczywistym
Usługa szkoleniowa
13 h
26.06.2025 do 27.06.2025

Informacje podstawowe

Kategoria	Biznes / Zarządzanie przedsiębiorstwem
Sposób dofinansowania	wsparcie dla osób indywidualnych wsparcie dla pracodawców i ich pracowników
Grupa docelowa usługi	• Dla osób odpowiedzialnych za bezpieczeństwo informacji w organizacjach. • Dla tych, którzy chcą rozpocząć karierę w audytowaniu systemów zarządzania bezpieczeństwem. • Dla wszystkich, którzy chcą poznać, jak działa system bezpieczeństwa informacji od podstaw.
Minimalna liczba uczestników	6
Maksymalna liczba uczestników	12
Data zakończenia rekrutacji	16-06-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	13
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

W dobie rosnących zagrożeń cybernetycznych, ochrona informacji stała się priorytetem każdej organizacji. Nasze szkolenie „Auditor Wewnętrzny Systemów Bezpieczeństwa Informacji” to unikalna okazja, by zdobyć praktyczną wiedzę i umiejętności, które pozwolą Ci stać się ekspertem w obszarze bezpieczeństwa informacji. Program łączy przystępne wyjaśnienie normy ISO 27001 z intensywnymi warsztatami , które przygotują Cię do pracy w roli auditora wewnętrznego.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnicy szkolenia zdobędą: Dogłębną znajomość normy ISO 27001 – fundamentu bezpieczeństwa informacji w organizacjach na całym świecie. Praktyczne umiejętności identyfikacji ryzyka, oceny zabezpieczeń i przeprowadzania audytów. Możliwość rozwijania kariery w dynamicznej dziedzinie zarządzania bezpieczeństwem informacji.	Ocena wyników ćwiczeń praktycznych podczas zajęć. Ocena aktywności uczestnika podczas symulacji. Ocena aktywności uczestnika podczas dyskusji.	Test teoretyczny Obserwacja w warunkach symulowanych Debata swobodna

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

Pytanie 1. Czy dokument potwierdzający uzyskanie kompetencji zawiera opis efektów uczenia się?

Certyfikat zawiera informację o ukończeniu szkolenia oraz zaliczeniu testu końcowego co jest równoznaczne z uzyskaniem kompetencji. Ukończenie szkolenia a nie zaliczenie testu oznacza brak certyfikatu i nie uzyskanie kompetencji.

Pytanie 2. Czy dokument potwierdza, że walidacja została przeprowadzona w oparciu o zdefiniowane w efektach uczenia się kryteria ich weryfikacji?

Certyfikat zawiera informację o ukończeniu szkolenia oraz zaliczeniu testu końcowego co jest równoznaczne z uzyskaniem kompetencji. Ukończenie szkolenia a nie zaliczenie testu oznacza brak certyfikatu i nie uzyskanie kompetencji.

Pytanie 3. Czy dokument potwierdza zastosowanie rozwiązań zapewniających rozdzielenie procesów kształcenia i szkolenia od walidacji?

Certyfikat zawiera informację o ukończeniu szkolenia oraz zaliczeniu testu końcowego co jest równoznaczne z uzyskaniem kompetencji. Ukończenie szkolenia a nie zaliczenie testu oznacza brak certyfikatu i nie uzyskanie kompetencji.

Program

Dzień 1: Podstawy bezpieczeństwa informacji

1. **Wprowadzenie do bezpieczeństwa informacji**
   - Znaczenie ochrony informacji w organizacji.
   - Omówienie aktualnych zagrożeń: cyberataki, błędy ludzkie, awarie techniczne.
   - Przykłady naruszeń bezpieczeństwa i ich konsekwencje.

2. **Kluczowe pojęcia i terminologia**
   - Definicje podstawowe: poufność, integralność, dostępność.
   - Rozróżnienie między zagrożeniem, podatnością i ryzykiem.
   - Wprowadzenie do norm ISO 27000 i ich zakresu.

3. **Model bezpieczeństwa informacji**
   - Wielopoziomowa ochrona: organizacyjna, techniczna, fizyczna, personalna.
   - Zasady zarządzania bezpieczeństwem informacji.
   - Jak wdrożyć model w praktyce organizacyjnej.

4. **Norma ISO/IEC 27001:2022 – struktura i cele**
   - Omówienie punktów 0-3: wprowadzenie, zakres i kontekst organizacji.
   - Punkty 4-10: planowanie, wsparcie, operacje, ocena i doskonalenie.
   - Ćwiczenie: praktyczne zastosowanie normy w wybranym scenariuszu.

5. **Zarządzanie ryzykiem w bezpieczeństwie informacji**
   - Zasady oceny ryzyka zgodnie z ISO 27005.
   - Identyfikacja zagrożeń i analiza potencjalnych skutków.
   - Opracowanie matrycy ryzyka dla przykładowego przypadku.

6. **Dokumentacja bezpieczeństwa informacji**
   - Wymagania dokumentacyjne normy ISO 27001.
   - Przykłady: polityka bezpieczeństwa, procedury, deklaracja stosowania.
   - Tworzenie prostego szablonu dokumentacji.

7. **Zabezpieczenia organizacyjne**
   - Tworzenie struktury organizacyjnej wspierającej bezpieczeństwo.
   - Rola zarządu i pracowników w zapewnianiu ochrony danych.
   - Polityki i procedury organizacyjne.

8. **Zabezpieczenia personalne**
   - Szkolenie pracowników jako element ochrony danych.
   - Weryfikacja kompetencji i dostępności do informacji.
   - Monitorowanie zgodności działań personelu z zasadami bezpieczeństwa.

9. **Zabezpieczenia techniczne**
   - Ochrona systemów IT: firewalle, antywirusy, systemy szyfrowania.
   - Zarządzanie dostępem: autoryzacja i uwierzytelnianie użytkowników.
   - Tworzenie kopii zapasowych i odzyskiwanie danych.

10. **Podsumowanie dnia – pytania i odpowiedzi**
    - Omówienie kluczowych zagadnień.
    - Dyskusja o zastosowaniach wiedzy w praktyce uczestników.
    - Przygotowanie do dnia 2.

Dzień 2: Audyt systemów bezpieczeństwa informacji

1. **Kim jest auditor?**
   - Rola auditora w organizacji.
   - Wymagania kompetencyjne zgodnie z ISO 19011.
   - Jak auditor wspiera rozwój systemu zarządzania bezpieczeństwem informacji.

2. **Różnice między audytem a kontrolą**
   - Cele audytu i kontroli.
   - Korzyści z prowadzenia audytów w organizacji.

- Wskazówki, kiedy stosować audyt, a kiedy kontrolę.

3. **Proces audytowania w oparciu o ISO 19011**
   - Cykl PDCA jako podstawa organizacji audytu.
   - Zasady audytowania: niezależność, obiektywizm, przejrzystość.
   - Kryteria audytu i ich zastosowanie.

4. **Planowanie audytów**
   - Przygotowanie harmonogramu i zakresu audytów.
   - Dobór zespołu audytowego i przypisanie odpowiedzialności.
   - Ćwiczenie: opracowanie planu audytu dla wybranej organizacji.

5. **Przygotowanie działań audytowych**
   - Analiza dokumentacji organizacji przed audytem.
   - Tworzenie listy pytań audytowych i matrycy zgodności.
   - Wybór metod zbierania danych podczas audytu.

6. **Przeprowadzenie audytu**
   - Spotkanie otwierające: cele i zasady audytu.
   - Zbieranie dowodów: rozmowy, dokumentacja, obserwacje.
   - Rozpoznawanie niezgodności i formułowanie wniosków.

7. **Techniki audytowe**
   - Audyt pionowy: szczegółowa analiza jednego procesu.
   - Audyt poziomy: przegląd szerokiego zakresu procesów.
   - Praktyka: symulacja wybranego rodzaju audytu.

8. **Raportowanie wyników audytu**
   - Tworzenie raportu z audytu: kluczowe elementy i format.
   - Identyfikacja niezgodności i propozycje działań korygujących.
   - Prezentacja wyników na spotkaniu zamykającym.

9. **Działania poaudytowe**
   - Planowanie i wdrażanie działań korygujących.
   - Monitorowanie skuteczności podjętych działań.
   - Zamknięcie audytu i przygotowanie na kolejny cykl.

10. **Ćwiczenia praktyczne z audytowania**
    - Przeprowadzenie symulacji audytu w grupach.
    - Analiza wyników i tworzenie raportów.
    - Dyskusja na temat doświadczeń uczestników i wniosków z warsztatów.

11. Test końcowy (podsumowanie i weryfikacja wiedzy)

Harmonogram

Liczba przedmiotów/zajęć: 9

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 9 Wprowadzenie do bezpieczeństwa informacji; Kluczowe pojęcia i terminologia; Model bezpieczeństwa informacji	Daniel Lampart	26-06-2025	09:00	10:30	01:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
2 z 9 Norma ISO/IEC 27001:2022 – struktura i cele; Zarządzanie ryzykiem w bezpieczeństwie informacji; Dokumentacja bezpieczeństwa informacji	Daniel Lampart	26-06-2025	10:45	12:15	01:30
3 z 9 Zabezpieczenia organizacyjne, personalne i techniczne	Daniel Lampart	26-06-2025	13:00	15:15	02:15
4 z 9 Podsumowanie dnia – pytania i odpowiedzi	Daniel Lampart	26-06-2025	15:30	17:00	01:30
5 z 9 Kim jest auditor? Różnice między audytem a kontrolą; Proces audytowania w oparciu o ISO 19011	Daniel Lampart	27-06-2025	09:00	10:30	01:30
6 z 9 Planowanie audytów; Przygotowanie działań audytowych; Przeprowadzenie audytu	Daniel Lampart	27-06-2025	10:15	12:30	02:15
7 z 9 Techniki audytowe; Raportowanie wyników audytu; Działania poaudytowe	Daniel Lampart	27-06-2025	13:15	15:00	01:45
8 z 9 Ćwiczenia praktyczne z audytowania	Daniel Lampart	27-06-2025	15:30	16:30	01:00
9 z 9 Test końcowy.Walidacja	-	27-06-2025	16:30	17:00	00:30

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	1 451,40 PLN
Koszt przypadający na 1 uczestnika netto	1 180,00 PLN
Koszt osobogodziny brutto	111,65 PLN
Koszt osobogodziny netto	90,77 PLN

Prowadzący

Liczba prowadzących: 1

1 z 1

Daniel Lampart

Ekspert w zakresie Systemów Zarządzania Bezpieczeństwem Informacji wg. ISO/IEC 27001 oraz Zintegrowanych systemów Zarządzania Jakością, Bezpieczeństwem i Środowiskiem wg ISO 9001, 45001 oraz 14001, trener, konsultant, auditor

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Uczestnicy otrzymują materiały szkoleniowe w formie wydrukowanej i dodatkowe materiały do ćwiczeń i symulacji.

Informacje dodatkowe

Szkolenie jest realizowana w godzinach zegarowych .

Przerwy nie wliczają się do czasu usługi rozwojowej.

Warunki techniczne

Szkolenie odbywa się na platformie ZOOM. Wymagania :zalecane procesor 2-rdzeniowy 2GHz, RAM 4Gb, łącze min. 5Mb/s. Potrzebne oprogramowanie Windows 10 lub nowszy, Microsoft Office.

Kontakt

Andrzej Jóźwiak

E-mail biuro@openhorizon.com.pl
Telefon (+48) 616 661 374