Możliwość dofinansowania

STOWARZYSZENIE POLSKA PLATFORMA BEZPIECZEŃSTWA WEWNĘTRZNEGO

Brak ocen dla tego dostawcy

Zarząd wobec dyrektywy NIS2 i UKSC 2.0: Odpowiedzialność prawna, zarządzanie ryzykiem i ciągłość biznesowa

Numer usługi 2026/07/17/228055/3694947

750,00 PLN brutto
750,00 PLN netto
130,43 PLN brutto/h
130,43 PLN netto/h
128,21 PLN cena rynkowa

Usługa szkoleniowa
zdalna w czasie rzeczywistym
Zajęcia grupowe
05:45 h
23.11.2026 do 23.11.2026

Informacje podstawowe

Kategoria	Inne / Edukacja
Grupa docelowa usługi	• Zarząd • Kierownicy • Menadżerowie
Minimalna liczba uczestników	5
Maksymalna liczba uczestników	10
Data zakończenia rekrutacji	18-11-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Podstawa uzyskania wpisu do BUR	Standard Usług Szkoleniowo– Rozwojowych PIFS SUS 3.0

Cel

Cel edukacyjny

- Wymogi prawne: Zrozumienie dyrektywy NIS2 i nowelizacji UKSC 2.0.
Perspektywa biznesowa: Przełożenie zagrożeń technologicznych na strategiczne zarządzanie ryzykiem.
- Zarządzanie SZBI: Ugruntowanie wiedzy o wdrażaniu, budżetowaniu i nadzorze nad systemem bezpieczeństwa.
- Organizacja i role: Właściwe delegowanie uprawnień i mapowanie kluczowych stanowisk.
- Zarządzanie kryzysowe: Utrzymanie ciągłości działania (BCP) i zasady raportowania incydentów.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Wzrost świadomości zagrożenia atakiem hackerskim poprzez nabycie umiejętności rozróżniania rodzajów i sposobów ataku oraz rozpoznawanie podejrzanych wiadomości, stron, programów. Szkolenie umożliwi podjęcie działań profilaktycznych, których celem będzie wyeliminowanie ryzyka, które potencjalnie może wystąpić w związku z cyberprzestępczością. Uczestnik szkolenia będzie wiedzieć jak i gdzie zgłaszać próby np. ataku hakerskiego.	Uzyskanie pozytywnego wyniku testu - kryterium 60% poprawnych odpowiedzi.	Test teoretyczny

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 rozdzielenie procesów kształcenia i szkolenia od walidacji?

TAK

Program

I BLOK TEMATYCZNY 9:00- 9:40

Strategiczny kontekst prawny, nowy krajobraz cyberbezpieczeństwa i odpowiedzialność Zarządu w rozumieniu NIS2 i UKSC 2.0:

- Wprowadzenie do dyrektywy NIS2 i nowelizacji UKSC.
- Architektura Krajowego Systemu Cyberbezpieczeństwa i kwalifikacja podmiotu.
- Zarządzanie ryzykiem na poziomie strategicznym.
- Solidarna odpowiedzialność osobista i sankcje finansowe.
- Obowiązki decyzyjne, budżetowanie i edukacja (wymogi art. 8d i 8e UKSC).

WARSZTAT STRATEGICZNY - PANEL DYSKUSYJNY 9:40-9:50

II BLOK TEMATYCZNY 9:50:10:30

Architektura bezpieczeństwa i System Zarządzania Bezpieczeństwem Informacji (SZBI) z perspektywy Zarządu:

- Fundamenty SZBI i obowiązek ustawowy.
- Zarządzanie w oparciu o Cykl Deminga (PDCA) na szczeblu Zarządu.
- Przywództwo i Polityka Bezpieczeństwa Informacji.
- Zasoby, budżetowanie i priorytetyzacja.
- Struktura organizacyjna – podział ról, odpowiedzialności i uprawnień.

WARSZTAT STRATEGICZNY - PANEL DYSKUSYJNY 10:30-10:40

PRZERWA 10:40 -11:10

III BLOK TEMATYCZNY 11:10-11:50

Zarządzanie Ryzykiem, tolerancja na ryzyko i bezpieczeństwo Łańcucha Dostaw:

- Wielopoziomowe zarządzanie ryzykiem i rola Zarządu (Poziom 1).
- Definiowanie tolerancji na ryzyko i kultury organizacyjnej.
- Warianty postępowania z ryzykiem.
- Strategiczne wyzwanie NIS2 i UKSC 2.0 – Bezpieczeństwo Łańcucha Dostaw.

WARSZTAT STRATEGICZNY - PANEL DYSKUSYJNY 11:50-12:05

IV BLOK TEMATYCZNY 12:05-12:45

Reagowanie na incydenty, komunikacja kryzysowa i ciągłość działania:

- Ciągłość działania i Odtwarzanie po awarii jako wymóg prawny.
- Klasyfikacja incydentów i Zespoły Reagowania (CSIRT).
- Rygorystyczny system raportowania "24 – 72 – 1 miesiąc" (System S46).
- Współpraca z organami i komunikacja kryzysowa.

WARSZTAT STRATEGICZNY - PANEL DYSKUSYJNY 12:45-12:55

PRZERWA 12:55-13:25

V BLOK TEMATYCZNY 13:25-14:15

Struktura personalna, Pełnomocnik, Świadomość i Audyt Zewnętrzny:

- Rola i zadania Pełnomocnika ds. Cyberbezpieczeństwa.
- Niezawodność kadr – rygorystyczny wymóg weryfikacji.
- Kultura organizacyjna i obowiązkowe szkolenia.
- Niezależny Audyt Bezpieczeństwa Systemu Informacyjnego.

WARSZTAT STRATEGICZNY - PANEL DYSKUSYJNY 14:15-14:30

Harmonogram

Liczba pozycji harmonogramu: 13

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 13 I BLOK TEMATYCZNY	Zajęcia	Dawid Rachmajda	23-11-2026	09:00	09:40	00:40

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
2 z 13 WARSZTAT STRATEGICZNY - PANEL DYSKUSYJNY	Zajęcia	Dawid Rachmajda	23-11-2026	09:40	09:50	00:10
3 z 13 II BLOK TEMATYCZNY	Zajęcia	Dawid Rachmajda	23-11-2026	09:50	10:30	00:40
4 z 13 WARSZTAT STRATEGICZNY - PANEL DYSKUSYJNY	Zajęcia	Dawid Rachmajda	23-11-2026	10:30	10:40	00:10
5 z 13 -	Przerwa	-	23-11-2026	10:40	11:10	00:30
6 z 13 III BLOK TEMATYCZNY	Zajęcia	Dawid Rachmajda	23-11-2026	11:10	11:50	00:40
7 z 13 WARSZTAT STRATEGICZNY - PANEL DYSKUSYJNY	Zajęcia	Dawid Rachmajda	23-11-2026	11:50	12:05	00:15
8 z 13 IV BLOK TEMATYCZNY	Zajęcia	Dawid Rachmajda	23-11-2026	12:05	12:45	00:40
9 z 13 WARSZTAT STRATEGICZNY - PANEL DYSKUSYJNY	Zajęcia	Dawid Rachmajda	23-11-2026	12:45	12:55	00:10
10 z 13 -	Przerwa	-	23-11-2026	12:55	13:25	00:30
11 z 13 V BLOK TEMATYCZNY	Zajęcia	Dawid Rachmajda	23-11-2026	13:25	14:15	00:50
12 z 13 WARSZTAT STRATEGICZNY - PANEL DYSKUSYJNY	Zajęcia	Dawid Rachmajda	23-11-2026	14:15	14:30	00:15
13 z 13 -	Walidacja	-	23-11-2026	14:30	14:45	00:15

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	05:45
w tym suma godzin zajęć	04:30
w tym suma godzin walidacji	00:15
w tym suma przerw	01:00
Suma godzin dydaktycznych bez przerw	06:15

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	750,00 PLN
Podmiot uprawniony do zwolnienia z VAT na podstawie art. 43 ust. 1 ustawy o VAT	
Koszt przypadający na 1 uczestnika netto	750,00 PLN
Koszt osobogodziny brutto	130,43 PLN
Koszt osobogodziny netto	130,43 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	05:45

Prowadzący

Liczba prowadzących: 1

1 z 1

Dawid Rachmajda

Dawid Rachmajda - ekspert PPBW z zakresu cyberbezpieczeństwa, analityk kryminalny i certyfikowany ekspert w dziedzinie białego wywiadu (OSINT) od ponad 15 lat związany z organami ścigania. Specjalizuje się w zwalczaniu zaawansowanej przestępczości cyfrowej, identyfikowaniu

schematów oszust gospodarczych oraz prowadzeniu dochodzeń w środowiskach trudno dostępnych, takich jak sieć Darknet. ego kompetencje potwierdzają liczne certyfikaty z zakresu analizy śledczej i
bezpieczeństwa IT, w tym specjalistyczne szkolenia organizowane przez United States Secret Service. Posiada formalne uprawnienia Pełnomocnika ds. cyberbezpieczeństwa zgodne z nowelizacją ustawy UKSC 2.0 (dyrektywa NIS2). Prelegent na największych wydarzeniach technologicznych, takich jak konferencja Oh My Hack. Wykształcenie
zdobył na Wyższej Szkole Bezpieczeństwa, gdzie ukończył specjalność z zakresu cyberterroryzmu, cyberbezpieczeństwa i bezpieczeństwa publicznego.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały dydaktyczne zostaną udostępnione w formie elektronicznej w dniu szkolenia, przed rozpoczęciem zajęć.

Warunki techniczne

Spotkanie będzie przeprowadzone za pośrednictwem aplikacji Microsoft Teams. Link do spotkania uczestniczy otrzymają na 5 dni przed szkoleniem.

Uczestnik musi posiadać:

- dostęp do komputera ze sprawnym systemem operacyjnym i kamerą internetową, mikrofon
- stabilne łącze internetowe
- dostęp do przeglądarki internetowej lub zainstalowaną aplikację Microsoft Teams
- zaleca się zalogowanie do platformy Microsoft Teams na 10-15 minut przed rozpoczęciem zajęć w celu przetestowania warunków technicznych połączenia

Kontakt

Aneta Jabłońska

E-mail aneta.jablonska@ppbw.pl
Telefon (+48) 695 386 963