



Cyberbezpieczeństwo w organizacji

Numer usługi 2025/07/09/10919/2867612

1 574,40 PLN brutto

1 280,00 PLN netto

104,96 PLN brutto/h

85,33 PLN netto/h

Polski Instytut
KontroliWewnętrznej Sp. z
o.o.

★★★★☆ 4,3 / 5

2 oceny

📍 zdalna w czasie rzeczywistym

🏠 Usługa szkoleniowa

🕒 15 h

📅 03.12.2025 do 11.12.2025

Informacje podstawowe

Kategoria	Inne / Edukacja
Grupa docelowa usługi	Szkolenie przeznaczone jest dla osób, które chcą zdobyć praktyczną wiedzę i umiejętności w zakresie zapobiegania zagrożeniom cybernetycznym.
Minimalna liczba uczestników	6
Maksymalna liczba uczestników	20
Data zakończenia rekrutacji	24-11-2025
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	15
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

Podniesienie świadomości i rozwój kompetencji pracowników w zakresie identyfikacji zagrożeń cybernetycznych oraz skutecznej ochrony danych i systemów informatycznych organizacji przed incydentami bezpieczeństwa.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik rozumie standardy, przepisy prawa i dobre praktyki w zakresie cyberbezpieczeństwa i umie je dopasować do organizacji. Ocenia prawidłowość przygotowania planu BCP w zakresie IT. Ocenia zagrożenia i dobiera odpowiednie środki/zachowania, zabezpieczające dane i systemy informatyczne organizacji przed incydentami bezpieczeństwa, w tym przy wykorzystaniu systemów informatycznych. Potrafi zbudować skuteczny system bezpieczeństwa informacji w organizacji w oparciu o analizę ryzyka w zakresie cyberbezpieczeństwa, analizę zagrożeń i zarządzanie incydentami bezpieczeństwa informacji.	Uczestnik zna standardy, przepisy prawa i dobre praktyki w zakresie cyberbezpieczeństwa. Zna podstawowe zasady dotyczące: OSINT, bezpieczeństwa webaplikacji, bezpieczeństwa przemysłowych systemów sterowania (ICS/OT), wytwarzania oprogramowania, w tym DevSecOps. Zna podstawowe zasady dotyczące bezpieczeństwa w procesie nabywania, rozwoju i utrzymania sieci i systemów informatycznych oraz łańcucha dostaw, poddostawców/podwykonawców. Rozumie szanse i zagrożenia dotyczące nowych technologii i wyzwania na przyszłość w zakresie cyberbezpieczeństwa – w tym sztucznej inteligencji (AI) i technologii kwantowej.	Test teoretyczny z wynikiem generowanym automatycznie

Kwalifikacje

Kompetencje

Usługa prowadzi do nabycia kompetencji.

Warunki uznania kompetencji

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

TAK

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

TAK

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

TAK

Program

Budowa skutecznego systemu bezpieczeństwa informacji.	1 h
Standardy, przepisy prawa i dobre praktyki w zakresie cyberbezpieczeństwa.	1 h

Identyfikacja aktywów i analiza ryzyka w zakresie cyberbezpieczeństwa.	1 h
Analiza zagrożeń w cyberprzestrzeni (<i>Cyber Threat Intelligence</i>).	1 h
OSINT. Rekonesans pasywny w zakresie IT i ICS/OT.	0,5 h
Zarządzanie incydentami.	1 h
Autoryzacja i uwierzytelnianie (zasady tworzenia haseł i narzędzia do „łamania” haseł).	0,5 h
BCP w IT (Business Continuity Plan, czyli Plan Ciągłości Działania).	1 h
Bezpieczeństwo webaplikacji.	1 h
Bezpieczeństwo przemysłowych systemów sterowania (ICS/OT).	1 h
Wytwarzanie oprogramowania, w tym DevSecOps.	1 h
Narzędzia IT m.in. typu SIEM, DLP, NAC, EDR/XDR, PAM.	1 h
Łącuch dostaw, poddostawcy, podwykonawcy w aspekcie cyberbezpieczeństwa.	0,5 h
Bezpieczeństwo w procesie nabywania, rozwoju i utrzymania sieci i systemów informatycznych.	0,5 h
Kryptografia i kryptoanaliza, w tym funkcje skrótu i hashe.	1 h
Nowe technologie i wyzwania na przyszłość w zakresie cyberbezpieczeństwa – w tym AI i technologia kwantowa.	1 h
Egzamin	1 h

Harmonogram

Liczba przedmiotów/zajęć: 0

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
Brak wyników.					

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	1 574,40 PLN
Koszt przypadający na 1 uczestnika netto	1 280,00 PLN
Koszt osobogodziny brutto	104,96 PLN
Koszt osobogodziny netto	85,33 PLN

Prowadzący

Liczba prowadzących: 1



1 z 1

Rafał Nikodym

Ekspert PIKW w zakresie cyberbezpieczeństwa, certyfikowany audytor: CRISC (Certified in Risk and Information Systems Control), ITIL 4 (Information Technology Infrastructure Library), CRMA (Certification in Risk Management Assurance), CISCO - Cybersecurity, audytor wiodący systemów zarządzania bezpieczeństwem informacji wg ISO 27001 oraz zarządzania ciągłości działania wg ISO 22301, Agile Project Management Practitioner Examination, Agile Project Management Foundation Examination, certyfikowany audytor Ministerstwa Finansów, CGAP, Internal Quality Assessment/Validator. Członek zespołu GK PGZ w zakresie CyberExpertGame (blue team).

Posiada doświadczenie audytora wewnętrznego w sektorze finansowym i przemyśle zbrojeniowym, koordynatora zadań audytowych IT oraz cyberbezpieczeństwa, w tym w obszarze OT oraz deweloperów w PGZ.

Prelegent, moderator i trener z zakresu IT, cyberbezpieczeństwa, zarządzania ryzykiem IT, sztucznej inteligencji, kryptografii, komputerów kwantowych, audytu wewnętrznego.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

Materiały w formie elektronicznej uczestnicy otrzymają po zakończeniu szkolenia.

Warunki uczestnictwa

Uczestnictwo w szkoleniu

Cena i warunki udziału zawarte są w formularzu zgłoszeniowym.

Pobierz: Formularz_zgłoszeniowy

Jeśli spełniają Państwo ustawowe wymogi, dotyczące zwolnienia z podatku VAT,

prosimy o wypełnienie i dołączenie do zgłoszenia, załącznika zamieszczonego poniżej:

Pobierz: Oświadczenie VAT

Zgłoszenie należy przesłać w formie skanu na adres **eszkolenia@pikw.pl**

Warunki techniczne

Opisane są na stronie https://www.pikw.pl/jak-dolaczyc-do-szkolenia-online-instrukcja,art_668.html

Kontakt



Gabriela Szalkowska

E-mail g.szalkowska@pikw.pl

Telefon (+48) 533 795 400