



LT MASTERY
SZKOLENIA DLA
BIZNESU PIOTR
SZYMCZYK

★★★★★ 4,9 / 5
76 ocen

Cyber Resilience Act (CRA) w praktyce producenta, importera i dystrybutora – klasyfikacja produktu, Załączniki I-VIII, SBOM, zgłoszenia do ENISA, ocena zgodności i oznakowanie CE, z blokiem poświęconym rozporządzeniu maszynowemu (UE) 2023/1230

Numer usługi 2026/10/15/204299/3881015

- 🏠 Usługa szkoleniowa
- 📺 zdalna w czasie rzeczywistym
- 👥 Zajęcia grupowe
- 🕒 08:00 h
- 📅 17.11.2026 do 17.11.2026

899,00 PLN brutto
899,00 PLN netto
112,38 PLN brutto/h
112,38 PLN netto/h
261,33 PLN cena rynkowa ⓘ

Informacje podstawowe

Kategoria

Informatyka i telekomunikacja / Bezpieczeństwo IT

Identyfikatory projektów

Kierunek - Rozwój, Akademia HR, FELB.06.03-IZ.00-0003/24 ZIPH,
FELB.06.08-IZ.00-0017/25, FELB.06.08-IZ.00-0083/24

Szkolenie skierowane jest do osób odpowiedzialnych za zgodność produktu z wymaganiami cyberbezpieczeństwa oraz relacje z dostawcami i odbiorcami produktów z elementami cyfrowymi. Obejmuje zarówno warstwę prawną-organizacyjną, jak i techniczną, ze szczególnym uwzględnieniem obowiązków producenta oraz momentu, w którym importer lub dystrybutor przejmuje pełny zakres tych obowiązków.

Usługa adresowana jest do:

Grupa docelowa usługi

- właścicieli produktu, kierowników i inżynierów rozwoju produktu w firmach wytwarzających sprzęt, oprogramowanie lub systemy wbudowane
- specjalistów ds. zgodności produktu, jakości i oznakowania CE (Product Compliance, Quality, Regulatory Affairs)
- inżynierów bezpieczeństwa produktu oraz osób odpowiedzialnych za obsługę zgłoszeń podatności i kontakt z badaczami bezpieczeństwa
- kadry zarządzającej podejmującej decyzje o priorytetach i budżecie zgodności – sankcje z art. 64 CRA sięgają 15 mln EUR albo 2,5 % rocznego światowego obrotu
- producentów, integratorów, importerów, dystrybutorów

Minimalna liczba uczestników

2

Maksymalna liczba uczestników

15

Data zakończenia rekrutacji	16-11-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym

Podstawa uzyskania wpisu do BUR	Certyfikat ICVC - SURE (Standard Usług Rozwojowych w Edukacji): Norma zarządzania jakością w zakresie świadczenia usług rozwojowych
---------------------------------	---

Cel

Cel edukacyjny

Wyposażenie uczestników w wiedzę i praktyczne narzędzia do wdrożenia i utrzymania zgodności z rozporządzeniem CRA: Cyber Resilience Act. Szkolenie umożliwia samodzielne przeprowadzenie analizy ryzyka, opracowanie dokumentacji (Technical File /SBOM), ustalenie statusu podmiotu i zaplanowanie działań audytowych, zarządzania łańcuchem dostaw, oraz reakcji na incydenty cyberbezpieczeństwa /podatności w produktach z elementami cyfrowymi, uwzględnia rozporządzenie maszynowe:(UE) 2023/1230- DigComp 2.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik rozróżnia zakres CRA i zakres dyrektywy NIS2 / ustawy o krajowym systemie cyberbezpieczeństwa oraz wskazuje, który reżim dotyczy jego organizacji i którego produktu.	Poprawnie przypisuje obowiązek do właściwego aktu prawnego: produktowy do rozporządzenia 2024/2847, organizacyjny do ustawy o KSC; wskazuje sytuację, w której jedno zdarzenie rodzi dwa niezależne obowiązki zgłoszeniowe.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik klasyfikuje produkt z elementami cyfrowymi do jednej z czterech kategorii i ustala rolę organizacji w łańcuchu dostaw.	Poprawnie stosuje Załączniki III i IV oraz rozporządzenie wykonawcze (UE) 2025/2392; prawidłowo rozstrzyga, kiedy importer lub dystrybutor jest traktowany jak producent zgodnie z art. 21.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik wskazuje wymagania zasadnicze z Załącznika I mające zastosowanie do produktu i identyfikuje luki wraz z wymaganym dowodem.	Poprawnie interpretuje 13 wymagań dotyczących cech produktu i 8 obowiązków obsługi podatności; wskazuje dowód zgodności dla każdego wymagania oraz uzasadnia pominięcie wymagania zgodnie z art. 13 ust. 4.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik przeprowadza ocenę ryzyka w cyberprzestrzeni zgodnie z art. 13 ust. 2–3 i wskazuje jej miejsce w dokumentacji technicznej.	Prawidłowo identyfikuje aktywa chronione, przeznaczenie i racjonalnie przewidywalne wykorzystanie produktu, zagrożenia dla interfejsów oraz środki łagodzące; wskazuje zdarzenia wymuszające aktualizację oceny.	Test teoretyczny z wynikiem generowanym automatycznie

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
Uczestnik ocenia kompletność zestawienia składników oprogramowania i opisuje proces zarządzania podatnościami oparty na SBOM.	Poprawnie wskazuje wymagany format i zakres SBOM zgodnie z Załącznikiem I cz. II pkt 1, rozpoznaje typowe defekty skanu automatycznego oraz właściwie kwalifikuje podatność jako aktywnie wykorzystywaną.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik stosuje kaskadę terminów zgłoszeniowych z art. 14 i wskazuje właściwych adresatów zgłoszenia.	Poprawnie identyfikuje moment powzięcia wiedzy, rozróżnia oba strumienie zgłoszeń, wskazuje terminy 24 h, 72 h oraz właściwy termin sprawozdania końcowego, a także CSIRT wyznaczony na koordynatora i ENISA.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik dobiera procedurę oceny zgodności do klasy produktu oraz wymienia elementy dokumentacji technicznej i deklaracji zgodności UE.	Poprawnie przyporządkowuje moduły A, B + C i H do klas produktu zgodnie z art. 32, wskazuje warunek zastosowania modułu A dla klasy ważnej I oraz obowiązkowe elementy Załączników V i VII.	Test teoretyczny z wynikiem generowanym automatycznie
Uczestnik wskazuje punkty styku CRA z rozporządzeniem maszynowym (UE) 2023/1230 i buduje harmonogram dojścia organizacji do zgodności.	Poprawnie wskazuje wymagania z Załącznika III pkt 1.1.9 i 1.2.1, datę rozpoczęcia stosowania rozporządzenia maszynowego oraz zasadę jednej deklaracji zgodności; buduje plan z produktem końcowym, właścicielem i datą dla każdej pozycji.	Test teoretyczny z wynikiem generowanym automatycznie

Kwalifikacje i kompetencje

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

Moduł I: Zakres CRA, klasyfikacja produktu i role w łańcuchu dostaw (08:00 – 09:15, 75 min; 1,5 godz. dyd.)

- Dlaczego powstał CRA – studium przypadku: udokumentowany przez CERT Polska atak destrukcyjny na polską energetykę z 29 grudnia 2025 r., obejrany od strony producenta urządzeń; sześć urządzeń i sześć wad po stronie produktu
- Rozporządzenie (UE) 2024/2847 – charakter aktu, cztery filary regulacji, struktura i mapa artykułów, do których wraca się w praktyce
- Ujednolicona oś czasu: przyjęcie 23.10.2024, wejście w życie 10.12.2024, rozdział IV od 11.06.2026, art. 14 od 11.09.2026, pełne stosowanie od 11.12.2027
- „Produkt z elementami cyfrowymi” – definicja z art. 3 pkt 1, granice zakresu (oprogramowanie samo w sobie, komponent sprzedawany osobno, rozwiązania zdalnego przetwarzania danych) oraz wyłączenia z art. 2
- CRA w ekosystemie regulacji: NIS2 i ustawa o KSC, rozporządzenie maszynowe (UE) 2023/1230, dyrektywa RED, dyrektywa o odpowiedzialności za produkt, akt o cyberbezpieczeństwie, akt o sztucznej inteligencji
- Role: producent (art. 13), importer (art. 19), dystrybutor (art. 20), upoważniony przedstawiciel (art. 18), opiekun oprogramowania open source (art. 24) oraz zasada substytucji roli z art. 21
- Cztery klasy produktów wg Załączników III i IV oraz rozporządzenia wykonawczego (UE) 2025/2392; klasa a minimalna procedura oceny zgodności (Ćwiczenie 1: klasyfikacja produktu i ustalenie roli)

Efekt modułu: uczestnik potrafi samodzielnie ustalić, czy produkt podlega CRA, do której klasy trafia i jaką rolę pełni wobec niego organizacja.

Moduł II: Wymagania zasadnicze z Załącznika I, secure by design i ocena ryzyka (09:30 – 10:45, 75 min; 1,5 godz. dyd.)

- Architektura Załącznika I: część I – 13 wymagań dotyczących cech produktu (pkt 2 lit. a–m), część II – 8 obowiązków postępowania w przypadku wykrycia podatności
- Omówienie wszystkich trzynastu wymagań litera po literze, z przykładem dowodu zgodności dla każdego z nich
- Bezpieczna konfiguracja domyślna w praktyce urządzenia przemysłowego – zakaz poświadczeń fabrycznych, konta wbudowane, usługi zbędne, weryfikacja podpisu oprogramowania układowego
- Ocena ryzyka w cyberprzestrzeni (art. 13 ust. 2–4) – zakres, metodyka w sześciu krokach, aktualizacja w okresie wsparcia, uzasadnienie niestosowania wymagania
- Punkty styku z rozporządzeniem maszynowym: Załącznik III pkt 1.1.9 (zabezpieczenie przed uszkodzeniem) i pkt 1.2.1 (bezpieczeństwo i niezawodność układów sterowania), motyw 53 CRA
- Okres wsparcia – art. 13 ust. 8 i 9: minimum 5 lat, dostępność wydanych aktualizacji przez co najmniej 10 lat, publiczna deklaracja daty zakończenia wsparcia
- Informacje i instrukcje dla użytkownika wg Załącznika II oraz pięć błędów, które organ nadzoru rynku znajduje najszybciej (Ćwiczenie 2: analiza luk wobec Załącznika I)

Efekt modułu: uczestnik potrafi ocenić produkt wobec wymagań zasadniczych, wskazać dowód zgodności i udokumentować pominięcia wymagania.

Moduł III: Łańcuch dostaw, SBOM i zarządzanie podatnościami (11:00 – 12:30, 90 min; 2 godz. dyd.)

- Odpowiedzialność producenta za komponenty stron trzecich i open source – art. 13 ust. 5 i 6, w tym obowiązek zgłoszenia podatności podmiotowi utrzymującemu komponent
- Zestawienie składników oprogramowania (SBOM) – dokładne brzmienie wymagania z Załącznika I cz. II pkt 1: format powszechnie używany, odczyt maszynowy, co najmniej zależności najwyższego poziomu
- Formaty SPDX i CycloneDX, identyfikator komponentu PURL, dokumenty VEX i CBOM – funkcja każdego z narzędzi i kryteria wyboru
- Rodzaje SBOM (build-time, release, baseline) oraz pięć typowych defektów skanu automatycznego w systemach wbudowanych
- Proces zarządzania podatnościami w siedmiu krokach – od inwentarza wdrożeń po zapis dowodu (Ćwiczenie 3: budowa i ocena jakości SBOM)
- Polityka skoordynowanego ujawniania podatności (CVD) – wymagana zawartość, typowe błędy, powiązanie z terminem 24 h z art. 14
- Triage zgłoszenia: podatność niewykorzystywalna, wykorzystywalna i aktywnie wykorzystywana – konsekwencje każdej kwalifikacji (Ćwiczenie 4: obsługa zgłoszenia badacza)

- Aktualizacje bezpieczeństwa: bezpłatne, bezzwłoczne, oddzielone od funkcjonalnych, domyślnie automatyczne i bezpiecznie dystrybuowane; klauzule umowne wobec dostawców komponentów

Moduł rozszerzony do 2 godzin dydaktycznych ze względu na to, że zarządzanie łańcuchem dostaw i obsługa podatności są operacyjnie najtrudniejszą częścią regulacji.

Efekt modułu: uczestnik potrafi ocenić kompletność zestawienia składników i opisać proces obsługi podatności wymagany przez Załącznik I część II.

Moduł IV: Zgłoszenia do ENISA i CSIRT, nadzór rynkowy i sankcje (13:00 – 14:15, 75 min; 1,5 godz. dyd.)

- Art. 14 – dwa niezależne strumienie zgłoszeń: aktywnie wykorzystywana podatność (ust. 1–2) oraz poważny incydent mający wpływ na bezpieczeństwo produktu (ust. 3–5)
- Kaskada terminów: 24 h wczesne ostrzeżenie, 72 h zgłoszenie, sprawozdanie końcowe – 14 dni od udostępnienia środka naprawczego albo miesiąc od zgłoszenia 72-godzinnego
- Moment powzięcia wiedzy – pięć typowych źródeł informacji i rozstrzygnięcie dla każdego z nich; wymagana treść każdego ze zgłoszeń
- Pojedyncza platforma sprawozdawcza (art. 16), właściwość CSIRT wyznaczonego na koordynatora oraz kolejność ustalania właściwości dla producenta spoza Unii
- Obowiązek poinformowania użytkowników produktu (art. 14 ust. 8) i uprawnienie CSIRT do samodzielnego poinformowania w razie milczenia producenta
- Relacja do obowiązku zgłoszeniowego z ustawy o KSC – jedno zdarzenie, dwa niezależne obowiązki (Ćwiczenie 5: pierwsze 24 godziny)
- Nadzór rynkowy: uprawnienia organów, środki naprawcze, wycofanie i zakaz udostępniania. Sankcje z art. 64 – trzy progi do 15 mln EUR albo 2,5 % obrotu światowego oraz dwa wyłączenia z ust. 10

Efekt modułu: uczestnik potrafi zakwalifikować zdarzenie, wskazać moment startu terminu, adresata i treść zgłoszenia.

Moduł V: Ocena zgodności, CE, rozporządzenie maszynowe i plan wdrożenia (14:30 – 15:30, 50 min; 1 godz. dyd.)

- Moduły oceny zgodności A, B + C, H (art. 32 i Załącznik VIII) – zakres, czas, koszt i rozkład ryzyka każdej ze ścieżek
- Normy zharmonizowane: mandat M/606, seria EN 40000 opracowywana przez CEN/CENELEC JTC 13, normy ETSI serii EN 304 6xx; warunek domniemania zgodności z art. 27 i stan na dzień szkolenia
- Dokumentacja techniczna wg Załącznika VII, deklaracja zgodności UE wg Załącznika V, zasady nanoszenia oznakowania CE (art. 29–30)
- Rozporządzenie maszynowe (UE) 2023/1230 – zakres, definicja elementu bezpieczeństwa obejmująca oprogramowanie, kategorie z Załącznika I i procedury oceny zgodności z art. 25; stosowanie od 20 stycznia 2027 r.
- Co rozporządzenie maszynowe zmienia względem dyrektywy 2006/42/WE: cyberbezpieczeństwo w zasadniczych wymaganiach, maszyny o samozmieniającym się zachowaniu, istotna modyfikacja także cyfrowa, instrukcja w postaci cyfrowej
- Jeden projekt zgodności dla obu reżimów: wspólna ocena ryzyka (art. 13 ust. 4 CRA), jedna deklaracja zgodności UE i jedno oznakowanie CE (art. 21 ust. 3 rozporządzenia maszynowego), dwie dokumentacje techniczne
- Ścieżka wdrożenia w czterech horyzontach oraz decyzja o produktach, których nie da się doprowadzić do zgodności (Ćwiczenie 6: plan dojścia do zgodności na 11 grudnia 2027 r.)

Efekt modułu: uczestnik dobiera procedurę oceny zgodności, zna wymaganą dokumentację i wychodzi ze szkolenia z własnym harmonogramem wdrożenia.

Sesja końcowa (15:30 – 16:00, 30 min; 0,5 godz. dyd.)

- Podsumowanie, odpowiedzi na pytania zaparkowane w trakcie dnia, słowniczek pojęć, wskazanie źródeł i indywidualne rekomendacje wdrożeniowe (15:30 – 15:45)
- Walidacja: post-test wiedzy online, 20 pytań jednokrotnego wyboru, zaliczenie od 60 % (15:45 – 16:00)

Całkowity czas trwania szkolenia : 8 godzin zegarowych (5 godzin zegarowych przekazywania wiedzy + 1,5 godziny warsztatów + 15 min walidacji wiedzy + 75 min przerw)

Czas nauki oraz warsztatów: 6 godzin 30 minut

Czas walidacji wiedzy: 15 min

- Czas przerw: 3 x 15 minut + 1 x 30 minut (razem 75 min)
- Egzamin wewnętrzny / walidacja jest wliczona w czas trwania szkolenia.
 - Przerwy nie są wliczone w czas trwania szkolenia

Harmonogram

Liczba pozycji harmonogramu: 16

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 16 Wprowadzenie, pre-test i studium przypadku: atak na polską energetykę z 29.12.2025 z perspektywy producenta. Ramy prawne CRA i oś czasu 2024-2027	Zajęcia	Piotr Szymczyk	17-11-2026	08:00	08:45	00:45
2 z 16 Zakres CRA, role w łańcuchu dostaw, cztery klasy produktów wg Załączników III i IV i zasada substytucji roli - Ćwiczenie 1	Zajęcia	Piotr Szymczyk	17-11-2026	08:45	09:15	00:30
3 z 16 -	Przerwa	-	17-11-2026	09:15	09:30	00:15
4 z 16 Wymagania zasadnicze z Załącznika I: 13 cech produktu i 8 obowiązków obsługi podatności; bezpieczna konfiguracja domyślna	Zajęcia	Piotr Szymczyk	17-11-2026	09:30	10:15	00:45

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
5 z 16 Ocena ryzyka w cyberprzestrzeni (art. 13), okres wsparcia, informacje dla użytkownika - Ćwiczenie 2 (analiza luk)	Zajęcia	Piotr Szymczyk	17-11-2026	10:15	10:45	00:30
6 z 16 -	Przerwa	-	17-11-2026	10:45	11:00	00:15
7 z 16 Łańcuch dostaw i odpowiedzialność za komponenty stron trzecich. SBOM: formaty, PURL, VEX, jakość zestawienia - Ćwiczenie 3	Zajęcia	Piotr Szymczyk	17-11-2026	11:00	11:45	00:45
8 z 16 Proces zarządzania podatnościami, polityka CVD i triage zgłoszenia. Aktualizacje bezpieczeństwa - Ćwiczenie 4	Zajęcia	Piotr Szymczyk	17-11-2026	11:45	12:30	00:45
9 z 16 -	Przerwa	-	17-11-2026	12:30	13:00	00:30
10 z 16 Zgłoszenia z art. 14: dwa strumienie, terminy 24 h / 72 h i sprawozdanie końcowe, platforma ENISA i CSIRT - Ćwiczenie 5	Zajęcia	Piotr Szymczyk	17-11-2026	13:00	14:00	01:00

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
11 z 16 Nadzór rynkowy, sankcje z art. 64 oraz relacja CRA - NIS2 / UoKSC przy jednym zdarzeniu	Zajęcia	Piotr Szymczyk	17-11-2026	14:00	14:15	00:15
12 z 16 -	Przerwa	-	17-11-2026	14:15	14:30	00:15
13 z 16 Ocena zgodności (moduły A, B+C, H), normy zharmonizowane, dokumentacja techniczna, deklaracja zgodności UE i CE	Zajęcia	Piotr Szymczyk	17-11-2026	14:30	15:00	00:30
14 z 16 Rozporządzenie maszynowe (UE) 2023/1230 a CRA: zał. III pkt 1.1.9 i 1.2.1, jedno CE. Plan wdrożenia - Ćwiczenie 6	Zajęcia	Piotr Szymczyk	17-11-2026	15:00	15:30	00:30
15 z 16 Podsumowanie, Q&A i indywidualne rekomendacje wdrożeniowe	Zajęcia	Piotr Szymczyk	17-11-2026	15:30	15:45	00:15
16 z 16 -	Walidacja	Piotr Szymczyk	17-11-2026	15:45	16:00	00:15

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	08:00

Rodzaj godzin	Liczba godzin
w tym suma godzin zajęć	06:30
w tym suma godzin walidacji	00:15
w tym suma przerw	01:15
Suma godzin dydaktycznych bez przerw	09:00

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	899,00 PLN
Podmiot uprawniony do zwolnienia z VAT na podstawie art. 113 ust. 1 ustawy o VAT ze względu na wartość sprzedaży	
Koszt przypadający na 1 uczestnika netto	899,00 PLN
Koszt osobogodziny brutto	112,38 PLN
Koszt osobogodziny netto	112,38 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	08:00

Prowadzący

Liczba prowadzących: 1



1 z 1

Piotr Szymczyk

Dynamiczny menedżer i trener z wieloletnim doświadczeniem w sektorze IT oraz usługach bezpieczeństwa dla globalnych korporacji (blue-chip). Specjalizuje się w budowaniu odporności cyfrowej organizacji, optymalizacji procesów serwisowych oraz wdrażaniu standardów zgodnych z najnowszymi dyrektywami unijnymi (w tym NIS2). Jako praktyk biznesu, Piotr nie tylko przekazuje wiedzę teoretyczną, ale uczy, jak zarządzać zmianą w środowisku wysokiej zmienności i niepewności (VUCA). Jego szkolenia charakteryzują się wysokim poziomem merytorycznym, ścisłą

orientacją na cele biznesowe oraz praktycznym podejściem do technologii, co pozwala uczestnikom na natychmiastowe wdrożenie zdobytych umiejętności.

OBSZARY EKSPERTYZY SZKOLENIOWEJ

- Cyberbezpieczeństwo i Zgodność: Kompleksowe wdrażanie dyrektywy NIS2, nowelizacja UoKSC, implementacja SZBI, audyt systemów informatycznych zgodnie z normami ISO 27001
- Zarządzanie Usługami IT (ITIL): Optymalizacja procesów dostarczania usług, zarządzanie incydentami oraz planowanie ciągłości działania (BCP/DRP)
- Change Management: Prowadzenie organizacji przez procesy transformacji cyfrowej i przełamywanie oporu wobec zmian technologicznych
- Przywództwo w IT: Budowanie i szkolenie wielokulturowych zespołów technicznych, coaching menedżerski oraz strategiczne zarządzanie talentami

Certyfikaty: AgilePM® Foundation & Practitioner, Change Management® Foundation, ISO 27001

Audytor Wewnętrzny, Akademia Bezpieczeństwa Informacji (EITCA/IS), ITIL® 4 Foundation

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

- **Prezentacja za szkolenia** – pełna prezentacja szkoleniowa w formacie PDF
- **kompendium** – kompendium wiedzy CRA z rozszerzonym omówieniem każdego zagadnienia i odwołaniami do przepisów źródłowych,
- **pakiet ćwiczeń** – karta scenariusza wykorzystywanego przez cały dzień, sześć szablonów do wypełnienia (po jednym na ćwiczenie) oraz sześć ściągawek z odpowiedziami wzorcowymi,
- **narzędzia wdrożeniowe** – checklista audytowa CRA oraz roadmapa wdrożenia ze spisem dokumentów do przygotowania, w formie arkusza kalkulacyjnego,
- **wzory dokumentów** – cztery edytowalne wzory na start wdrożenia: polityka skoordynowanego ujawniania podatności, procedura zgłaszania zgodnie z art. 14 CRA, szablon komunikatu dotyczącego bezpieczeństwa produktu (security advisory) oraz deklaracja zgodności UE wg Załącznika V,

Warunki uczestnictwa

- Podstawowa wiedza w zakresie kompetencji cyfrowych
- Logowanie się pełnym imieniem i nazwiskiem
- Warunkiem uzyskania zaświadczenia jest uczestnictwo w co najmniej 80%–100% zajęć usługi rozwojowej (w zależności od programu dofinansowania i podpisanej umowy z Operatorem)
- W ramach realizacji usług szkoleniowych Organizator utrzuca wizerunek Uczestników w formie nagrań wideo, fotografii lub innych materiałów audiowizualnych wyłącznie w celach archiwizacyjnych, kontrolnych oraz dokumentacyjnych związanych z projektem dofinansowanym
- Uczestnik zapisując się na szkolenie wyraża zgodę na utrwalenie i wykorzystanie jego wizerunku w wyżej wymienionych celach

Informacje dodatkowe

Usługa jest zwolniona z podatku VAT w przypadku, kiedy przedsiębiorstwo zwolnione jest z podatku VAT lub dofinansowanie wynosi co najmniej 70%. W innej sytuacji do ceny netto doliczany jest podatek VAT w wysokości 23%.

Podstawa: §3 ust. 1 pkt. 14 rozporządzenia Ministra Finansów z dnia 20.12.2013 r. w sprawie zwolnień od podatku od towarów i usług oraz szczegółowych warunków stosowania tych zwolnień (Dz.U. z 2018 r., poz. 701).

Całe szkolenie jest rejestrowane w celach kontroli oraz audytu.

Wykorzystanie nagrania w innym celu niż kontrola czy audyt wymaga zgody trenera oraz uczestników.

Uczestnicy otrzymają zaświadczenie / certyfikat, potwierdzające ukończenie szkolenia.

Usługa zdalna w czasie rzeczywistym - prowadzona na żywo.

Uczestnik ma możliwość złożenia reklamacji po zrealizowanej usłudze, sporządzając ją w formie pisemnej na formularzu reklamacji i odsyłając na adres: biuro@legacyturn.com

Warunki techniczne

Poniżej opisane są minimalne wymagania techniczne dotyczące uczestnictwa w szkoleniu przy pomocy platformy TEAMS:

1. Parametry urządzenia: komputer / laptop / tablet

- Procesor dwurdzeniowy 1–2 GHz minimalnie; zalecany dual-core 2 GHz lub lepszy (Intel i3/i5 lub równoważny)
- 2 GB pamięci RAM (zalecane 4 GB lub więcej).
- System operacyjny: Windows 10/11, macOS 10.13+ (lub nowsze), Linux (nowsze dystrybucje wspierane), iOS 13+/Android 8+
 - • • • zainstalowany TEAMS (najświeższa wersja) oraz najnowsza wersja Chrome/Edge/Firefox;

1. Kamera i mikrofon

- TEAMS współpracuje z wbudowanymi kamerami w laptopach oraz większością kamer internetowych.
 - słuchawki z mikrofonem zalecane dla lepszej jakości dźwięku.
 - zaawansowane lub profesjonalne kamery/mikrofony, mogą wymagać zainstalowanie dodatkowego oprogramowania .

1. Urządzenia mobilne

- Jeżeli łączysz się z urządzenia mobilnego, pobierz i zainstaluj aplikację TEAMS z App Store (Apple) lub Google Play
- Aby korzystać z dźwięku i obrazu, użyj zestawu słuchawkowego z mikrofonem lub głośników podłączonych do urządzenia.
- Przed rozpoczęciem szkolenia sprawdź, czy urządzenie rozpoznaje wybrane urządzenie audio oraz czy nie jest ono jednocześnie zajęte przez inną aplikację
- Upewnij się, że aplikacja ma przyznane uprawnienia do korzystania z mikrofonu i kamery.

1. Wymagania dla łącza internetowego:

- *min. 1,5 Mbps download i upload* dla podstawowego udziału
- zalecane 3 Mbps+ dla stabilnego wideo HD i udostępniania ekranu
- najnowsza wersja używanej przeglądarki internetowej

1. Link do szkolenia oraz warunki / wymagania dodatkowe:

- • • • • Link do szkolenia zostanie dostany drogą elektroniczną przed rozpoczęciem usługi na adres email podany przez uczestnika szkolenia.
- Link do szkolenia będzie ważny w dniach i godzinach określonych w harmonogramie usługi.

1. Podczas szkolenia online zapewniamy:

- • Wygodną formę szkolenia, gdzie wystarczy dostęp do urządzenia z internetem (komputer, tablet, telefon), słuchawki lub głośniki.
- Szkolenie zdalne w czasie rzeczywistym w wirtualnym pokoju konferencyjnym, w niewielkiej grupie uczestników.
- Możliwość pełnej interakcji z trenerem, który prowadzi zajęcia "na żywo" z włączoną kamerą w czasie trwania całego szkolenia.
- Możliwości zadawania pytań, omawiania indywidualnych zagadnień oraz aktywny udział w ćwiczeniach.

Przed szkoleniem:

- Upewnij się, że masz stabilne połączenie internetowe, które spełnia minimalne wymagane prędkości dla transmisji audio oraz wideo.
- Przetestuj dostęp i uruchomienie aplikacji TEAMS w wykorzystaniu kamery oraz mikrofonu.
- Rekomenduje się przygotowanie zapasowego zestawu awaryjnego sprzętu w celu zapewnienia ciągłości realizacji szkolenia. Powinien on obejmować kluczowe komponenty: komputer, kamerę, mikrofon/głośnik, klawiaturę, myszkę oraz alternatywne źródło dostępu do Internetu (np. modem Hot-Spot).

Podstawą do rozliczenia usługi jest wygenerowanie z systemu raportu, umożliwiającego identyfikację wszystkich uczestników oraz zastosowanego narzędzia.

Kontakt



PIOTR SZYMCZYK

E-mail szyplodz@yahoo.com

Telefon (+48) 501 435 131

