Możliwość dofinansowania

ISACA CISA® – Certified Information Systems Auditor - akredytowane szkolenie z egzaminem

Numer usługi 2026/06/16/206646/3629391

10 209,00 PLN brutto
8 300,00 PLN netto
255,23 PLN brutto/h
207,50 PLN netto/h
261,33 PLN cena rynkowa

"CTS CUSTOMIZED TRAINING SOLUTIONS" SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

Brak ocen dla tego dostawcy

Usługa szkoleniowa
zdalna w czasie rzeczywistym
Zajęcia grupowe
40:00 h
24.08.2026 do 28.08.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	AKREDYTOWANE szkolenie skierowane głównie do specjalistów ds. bezpieczeństwa, audytorów systemów informatycznych. a także do; • Administratorów i oficerów bezpieczeństwa informatycznego. • Dyrektorów, managerów i , specjalistów odpowiedzialnych za ład korporacyjny, ryzyko i zgodność (Governance, Risk, Compliance) • Kkonsultantów ds. audytu IT • Kadry kierowniczej departamentów IT i departamentów bezpieczeństwa • Osób zainteresowanych tematyką cyberbezpieczeństwa i audytu IT, chcących podnieść swoje kwalifikacje i zdobyć międzynarodowy certyfikat "Certified Information Systems Auditor (CISA)"
Minimalna liczba uczestników	5
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	17-08-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Podstawa uzyskania wpisu do BUR	Certyfikat VCC Akademia Edukacyjna

Cel

Cel edukacyjny

Celem szkolenia jest przygotowanie rozwinięcie wiedzy i umiejętności niezbędnych do skutecznego prowadzenia audytu, kontroli i oceny systemów informatycznych w organizacji. Uczestnik po szkoleniu rozumie metodyki audytu IT, potrafi identyfikować ryzyka i słabości kontroli, a także przygotowywać rekomendacje usprawniające bezpieczeństwo i zgodność procesów IT.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
W1 – rozumie podstawy procesu audytu systemów informatycznych, jego cele, zakres i etapy (planowanie, wykonanie, raportowanie). W2 – zna standardy, metodyki i najlepsze praktyki audytu IT stosowane międzynarodowo (ISACA, ISO, inne). W3 – rozumie ład korporacyjny, role i odpowiedzialności w zarządzaniu IT oraz znaczenie polityk bezpieczeństwa informacji. W4 – zna procesy pozyskiwania, rozwoju i wdrażania systemów informatycznych oraz kluczowe kontrole w cyklu życia systemu. W5 – rozumie operacje, utrzymanie i wsparcie systemów informatycznych, zarządzanie incydentami i ciągłość działania. W6 – zna metody ochrony aktywów informacyjnych, kontrole dostępu, zabezpieczenia danych oraz mechanizmy monitorowania bezpieczeństwa. W7 – rozumie ryzyko IT, metody jego identyfikacji, oceny i zarządzania w kontekście audytu.	uczestnik uzyskuje co najmniej 70% poprawnych odpowiedzi w testach wiedzy po każdej z 5 domen szkolenia (planowanie audytu, ład korporacyjny, wdrażanie systemów, operacje, ochrona aktywów).	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
U1 – potrafi opracować plan audytu systemów informatycznych, określić cele, zakres, zasoby i harmonogram. U2 – potrafi stosować techniki zbierania dowodów audytowych (przegląd dokumentów, wywiady, testy, obserwacja). U3 – potrafi dokumentować wyniki audytu, tworzyć noty audytowe i przygotować raport z audytu wraz z rekomendacjami. U4 – potrafi identyfikować ryzyka i słabości kontroli w systemach informatycznych oraz oceniac ich wpływ na bezpieczeństwo i zgodność. U5 – potrafi formułować realistyczne i merytorycznie uzasadnione rekomendacje usprawniające bezpieczeństwo, kontrolę i efektywność procesów IT. U6 – potrafi wykorzystać wyniki audytu w procesie zarządzania ryzykiem i zgodnością w organizacji.	uczestnik uzyskuje co najmniej 70% poprawnych odpowiedzi w testach wiedzy po każdej z 5 domen szkolenia (planowanie audytu, ład korporacyjny, wdrażanie systemów, operacje, ochrona aktywów).	Test teoretyczny

Cel biznesowy

Uczestnik po szkoleniu będzie mógł zbudować wewnętrzną funkcję audytu IT – będzie pracownikiem zdolnym do planowania, wykonywania i raportowania audytów systemów informatycznych w swojego organizacji, zgodnie ze standardami ISACA.
Ukończenie szkolenia pozwoli zwiększyć poziom bezpieczeństwa i kontroli – zidentyfikować i ocenić słabe punkty w systemach IT, raportować zgodność oraz ustanawiać skuteczne kontrole w przedsiębiorstwie.
Organizacja w której pracuje osoba po szkoleniu CISA będzie mogła utrzymać międzynarodowy standard audytu – wdrożyć globalnie uznane praktyki audytu, kontroli i zabezpieczeń IS, co jest wymagane w wielu standardach i ustawach (np. audyty regulacyjne).
Organizacja zatrudniająca pracownika po szkoleniu CISA wzmocni wiarygodność i konkurencyjność w kontaktach z wewnętrznymi interesariuszami, regulatorami, zewnętrznymi audytorami i klientami oraz zwiększa przewagę pracownika potrzebną do awansu.
Certyfikat CISA pozwala zminimalizować ryzyka biznesowe związane z IT – zastosować podejście oparte na ryzyku w planowaniu i realizacji audytów, co pomaga chronić aktywa informacyjne i zapewnia ciągłość działania systemów biznesowych.

Efekt usługi

Po ukończeniu szkolenia CISA organizacja zyskuje przeszkolonych audytorów systemów informatycznych, którzy:

- potrafią samodzielnie planować i przeprowadzać audyty IT zgodnie ze standardami ISACA,
- identyfikują ryzyka i słabości kontroli w systemach informatycznych,
- formułują rekomendacje usprawniające bezpieczeństwo, zgodność i efektywność procesów IT,
- wspierają zarządzanie ryzykiem i ciągłość działania środowisk IT,
- zwiększają wiarygodność organizacji w relacjach z regulatorami, audytorami zewnętrznymi i klientami dzięki posiadaniu międzynarodowo uznanej certyfikacji wewnątrz firmy.

Efekt końcowy: **bardziej skuteczny audyt IT, lepsze zarządzanie ryzykiem, wyższa zgodność regulacyjna i wzrost bezpieczeństwa systemów biznesowych**, co przekłada się na mniejsze ryzyko incydentów, ograniczenie kosztów związanych z niezgodnością i zwiększoną konkurencyjność organizacji.

Efekt biznesowy można potwierdzić i zmierzyć poprzez następujące kryteria:

1. 1. **Certyfikacja uczestników**

- Liczba osób, które przeszły egzamin CISA i uzyskały certyfikat Certified Information Systems Auditor.
- Procent uczestników szkolenia, którzy uzyskali certyfikat w ciągu 3–6 miesięcy od zakończenia kursu.

1. **Zastosowanie kompetencji w praktyce**

- Liczba wewnętrznych audytów IT przeprowadzonych samodzielnie przez przeszkolonych audytorów w ciągu 6–12 miesięcy po szkoleniu.
- Zmiana liczby zidentyfikowanych i zgłoszonych ryzyk/defektów kontroli w systemach IT po szkoleniu.
- Liczba rekomendacji usprawniających przyjętych i wdrożonych w organizacji.

1. **Wpływ na bezpieczeństwo i zgodność**

- Zmiana liczby incydentów bezpieczeństwa IT związanych z niezgodnością lub słabymi kontrolami (przed vs. po szkoleniu).
- Liczba audytów regulacyjnych zewnętrznych, w których organizacja nie wykryła istotnych niezgodności w obszarach IT.
- Poziom zgodności z wymaganiami regulacyjnymi i standardami (np. ISO, CISM, CISA) w obszarze IT wyrażony procentowo w raportach z audytu.

1. **Efektywność kosztowa i organizacyjna**

- Ograniczenie kosztów związanych z zewnętrznymi audytorami IT (np. zmniejszenie liczby zleceń zewnętrznych).
- Skrócenie czasu trwania audytów IT w organizacji dzięki wewnętrznej funkcji audytowej.
- Zmniejszenie liczby zaległości i raportowanych niezgodności w systemach IT w raportach z okresowego nadzoru.

1. **Wzrost wiarygodności i reputacji**

- Liczba potwierdzeń, rekomendacji lub pozytywnych ocen z audytów zewnętrznych regulacyjnych w obszarze IT.
- Zmiana oceny interesariuszy (kierownictwo, regulator, Klienci) wobec jakości zarządzania IT w organizacji.
- Liczba organizacji lub partnerów biznesowych, którzy wymagają certyfikacji audytora IT i uznają posiadanie CISA jako warunek współpracy.

1. **Kryteria jakościowe**

- Ocena jakości raportów z audytu (np. przez kierownictwo, audytorów zewnętrznych) – mniej błędów, lepsza struktura, bardziej precyzyjne rekomendacje.
- Poziom satysfakcji uczestników szkolenia i menedżerów z zastosowania nowych kompetencji w praktyce (np. ankiety, wywiady).

Metoda potwierdzenia osiągnięcia efektu usługi

1. Plan działania po szkoleniu (post-training action plan) - wykonany przez uczestnika
2. Ankiety, testy
3. Obserwacja wykonywania symulowanych zadań audytowych

Kwalifikacje

Kwalifikacje niewłączone do ZSK

Uznane kwalifikacje

Pytanie 3. Czy dokument jest certyfikatem wydawanym przez międzynarodowe instytucje?

TAK

Strona internetowa Instytucji Certyfikującej: https://www.isaca.org

Strona internetowa Instytucji Walidującej: https://www.isaca.org

Informacje

Nazwa Podmiotu prowadzącego walidację	ISACA

Nazwa Podmiotu certyfikującego	ISACA

Program

Obszar 1: Proces audytu systemów informatycznych (Information System Auditing Process)

- - Planowanie:
  - Standardy, wytyczne, funkcje i kodeksy etyczne dotyczące audytu systemów informatycznych
  - Rodzaje audytów, ocen i przeglądów
  - Planowanie audytu oparte na ryzyku
  - Rodzaje środków kontroli i kwestie do rozważenia
  - Realizacja:
  - Zarządzanie projektem audytowym
  - Metodologia testowania i pobierania próbek w audycie
  - Techniki gromadzenia dowodów audytowych
  - Analiza danych audytowych
  - Techniki raportowania i komunikacji
  - Zapewnienie jakości i doskonalenie procesu audytu
  - Pytania egzaminacyjne i podsumowanie rozdziału (Practice Questions & Review)

Obszar 2: Ład i zarządzanie IT (Governance and Management of IT)

- - Ład w IT:
  - Przepisy prawne, regulacje i standardy branżowe
  - Struktura organizacyjna, ład w IT i strategia IT
  - Polityki, standardy, procedury i wytyczne dotyczące IT
  - Architektura korporacyjna i kwestie do rozważenia
  - Zarządzanie ryzykiem w przedsiębiorstwie (ERM)
  - Program i zasady ochrony danych
  - Zarządzanie danymi i ich klasyfikacja
  - Zarządzanie IT:
  - Zarządzanie zasobami IT
  - Zarządzanie dostawcami IT
  - Monitorowanie wydajności IT i raportowanie
  - Zapewnienie jakości i zarządzanie jakością IT
  - Pytania egzaminacyjne i podsumowanie rozdziału (Practice Questions & Review)

Obszar 3: Pozyskiwanie, rozwój i wdrażanie systemów informatycznych (Information Systems Acquisition, Development and Implementation)

- - Pozyskiwanie i rozwój systemów informatycznych:
  - Zarządzanie projektami i kierowanie nimi
  - Analiza biznesowa i analiza wykonalności
  - Metodologie tworzenia systemów
  - Identyfikacja i projektowanie mechanizmów kontroli
  - Wdrażanie systemów informatycznych:
  - Gotowość systemu i testy wdrożeniowe
  - Konfiguracja wdrożeniowa i zarządzanie wydaniami
  - Migracja systemu, wdrażanie infrastruktury i konwersja danych
  - Przegląd po wdrożeniu
  - Przykładowe pytania egzaminacyjne i podsumowanie rozdziału (Practice Questions & Review)

Obszar 4: Eksploatacja systemów informatycznych i odporność biznesowa (Information Systems Operations and Business Resilience)

- - Eksploatacja systemów informatycznych:
  - Komponenty IT
  - Zarządzanie zasobami IT
  - Planowanie zadań i automatyzacja procesów produkcyjnych
  - Interfejsy systemowe

- Komputery użytkowników końcowych i „shadow IT”
- Dostępność systemów i zarządzanie wydajnością
- Zarządzanie problemami i incydentami
- Zarządzanie zmianami, konfiguracją i poprawkami w IT
- Zarządzanie logami operacyjnymi
- Zarządzanie poziomem usług IT
- Zarządzanie bazami danych
- Odporność biznesowa:
- Analiza wpływu na działalność
- Odporność systemowa i operacyjna
- Tworzenie kopii zapasowych, przechowywanie i przywracanie danych
- Plan ciągłości działania
- Plany odzyskiwania po awarii
- Pytania egzaminacyjne do ćwiczeń i podsumowanie rozdziału (Practice Questions & Review)

Obszar 5: Ochrona zasobów informacyjnych

- - Bezpieczeństwo i kontrola zasobów informacyjnych:
  - Polityki, ramy, standardy i wytyczne dotyczące bezpieczeństwa zasobów informacyjnych
  - Kontrole fizyczne i środowiskowe
  - Zarządzanie tożsamością i dostępem
  - Bezpieczeństwo sieci i punktów końcowych
  - Zapobieganie utracie danych
  - Szyfrowanie danych
  - Infrastruktura klucza publicznego (PKI)
  - Środowiska chmurowe i wirtualne
  - Urządzenia mobilne, bezprzewodowe i urządzenia Internetu rzeczy
  - Zarządzanie zdarzeniami bezpieczeństwa:
  - Szkolenia i programy z zakresu świadomości bezpieczeństwa
  - Metody i techniki ataków na systemy informatyczne
  - Narzędzia i techniki testowania bezpieczeństwa
  - Dzienniki, narzędzia i techniki monitorowania bezpieczeństwa
  - Zarządzanie reagowaniem na incydenty bezpieczeństwa
  - Gromadzenie dowodów i analiza kryminalistyczna
  - Pytania egzaminacyjne i podsumowanie rozdziału (Practice Questions & Review)

Szkolenie CISA trwa 5 dni, łącznie 40 godzin zegarowych.

- - **Przerwy:** Każdego dnia szkoleniowego przewidziano jedną 30-minutową przerwę lunchową oraz dwie krótsze przerwy po 15 minut.
  - **Program obejmuje 5 głównych obszarów tematycznych CISA**, z których każdy realizowany jest w formule łączącej część teoretyczną i praktyczną, w tym pracę na przykładach, analizę scenariuszy audytowych oraz przygotowanie do egzaminu certyfikacyjnego.
  - **Część teoretyczna** szkolenia obejmuje 30 godzin lekcyjnych (45 min), a **część praktyczna** 10 godzin lekcyjnych.(45 min)
  - **Walidacja efektów uczenia się** obejmuje 15-minutowy pre-test diagnostyczny realizowany na początku szkolenia oraz 15-minutowy post-test walidacyjny przeprowadzany po zakończeniu szkolenia.

Harmonogram

Liczba pozycji harmonogramu: 43

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 43 Wprowadzenie do szkolenia - harmonogram	Zajęcia	Piotr Dzwonkowski	24-08-2026	09:00	09:30	00:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
2 z 43 Pre-Test	Zajęcia	Piotr Dzwonkowski	24-08-2026	09:30	09:45	00:15
3 z 43 Proces audytu systemów informatycznych (Information System Auditing Process)	Zajęcia	Piotr Dzwonkowski	24-08-2026	09:45	10:30	00:45
4 z 43 -	Przerwa	-	24-08-2026	10:30	10:45	00:15
5 z 43 Standardy, wytyczne, funkcje i kodeksy etyczne dotyczące audytu systemów informatycznych, Rodzaje audytów, ocen i przeglądów	Zajęcia	Piotr Dzwonkowski	24-08-2026	10:45	12:15	01:30
6 z 43 -	Przerwa	-	24-08-2026	12:15	12:45	00:30
7 z 43 Planowanie audytu oparte na ryzyku. Rodzaje środków kontroli i kwestie do rozważenia	Zajęcia	Piotr Dzwonkowski	24-08-2026	12:45	14:15	01:30
8 z 43 -	Przerwa	-	24-08-2026	14:15	14:30	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
9 z 43 Zarządzanie projektem audytowym. Metodologia testowania i pobierania próbek w audycie. Techniki gromadzenia dowodów audytowych	Zajęcia	Piotr Dzwonkowski	24-08-2026	14:30	15:30	01:00
10 z 43 Analiza danych audytowych, Techniki raportowania i komunikacji, Zapewnienie jakości i doskonalenie procesu audytu	Zajęcia	Piotr Dzwonkowski	24-08-2026	15:30	17:00	01:30
11 z 43 Ład i zarządzanie IT (Governance and Management of IT), Przepisy prawne, regulacje i standardy branżowe. Struktura organizacyjna, ład w IT i strategia IT	Zajęcia	Piotr Dzwonkowski	25-08-2026	09:00	10:30	01:30
12 z 43 -	Przerwa	-	25-08-2026	10:30	10:45	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
13 z 43 Polityki, standardy, procedury i wytyczne dotyczące IT. Architektura korporacyjna. Zarządzanie ryzykiem (ERM), Program i zasady ochrony danych. Zarządzanie danymi i ich klasyfikacja	Zajęcia	Piotr Dzwonkowski	25-08-2026	10:45	12:15	01:30
14 z 43 -	Przerwa	-	25-08-2026	12:15	12:45	00:30
15 z 43 Zarządzanie zasobami IT, dostawcami IT, Monitorowanie wydajności IT i raportowanie, Zapewnienie jakości i zarządzanie jakością IT	Zajęcia	Piotr Dzwonkowski	25-08-2026	12:45	14:15	01:30
16 z 43 -	Przerwa	-	25-08-2026	14:15	14:30	00:15
17 z 43 Pozyskiwanie, rozwój i wdrażanie systemów informatycznych (Information Systems Acquisition, Development and Implementation)	Zajęcia	Piotr Dzwonkowski	25-08-2026	14:30	15:30	01:00

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
18 z 43 Pozyskiwanie i rozwój systemów informatycznych: Zarządzanie projektami i kierowanie nimi	Zajęcia	Piotr Dzwonkowski	25-08-2026	15:30	17:00	01:30
19 z 43 Analiza biznesowa i analiza wykonalności. Metodologie tworzenia systemów	Zajęcia	Piotr Dzwonkowski	26-08-2026	09:00	10:30	01:30
20 z 43 -	Przerwa	-	26-08-2026	10:30	10:45	00:15
21 z 43 Identyfikacja i projektowanie mechanizmów kontroli. Gotowość systemu i testy wdrożeniowe. Konfiguracja wdrożeniowa i zarządzanie wydaniami	Zajęcia	Piotr Dzwonkowski	26-08-2026	10:45	12:15	01:30
22 z 43 -	Przerwa	-	26-08-2026	12:15	12:45	00:30
23 z 43 Migracja systemu, wdrażanie infrastruktury i konwersja danych	Zajęcia	Piotr Dzwonkowski	26-08-2026	12:45	14:15	01:30
24 z 43 -	Przerwa	-	26-08-2026	14:15	14:30	00:15
25 z 43 Przegląd po wdrożeniu	Zajęcia	Piotr Dzwonkowski	26-08-2026	14:30	15:30	01:00

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
26 z 43 Eksploatacja systemów informatycznych i odporność biznesowa (Information Systems Operations and Business Resilience)	Zajęcia	Piotr Dzwonkowski	26-08-2026	15:30	17:00	01:30
27 z 43 Komponenty IT, Zarządzanie zasobami IT	Zajęcia	Piotr Dzwonkowski	27-08-2026	09:00	10:30	01:30
28 z 43 -	Przerwa	-	27-08-2026	10:30	10:45	00:15
29 z 43 Planowanie zadań i automatyzacja procesów produkcyjnych, Interfejsy systemowe	Zajęcia	Piotr Dzwonkowski	27-08-2026	10:45	12:15	01:30
30 z 43 -	Przerwa	-	27-08-2026	12:15	12:45	00:30
31 z 43 Komputery użytkowników końcowych i „shadow IT”, Dostępność systemów i zarządzanie wydajnością, Zarządzanie problemami i incydentami	Zajęcia	Piotr Dzwonkowski	27-08-2026	12:45	14:15	01:30
32 z 43 -	Przerwa	-	27-08-2026	14:15	14:30	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
33 z 43 Zarządzanie zmianami, konfiguracją i poprawkami w IT, Zarządzanie logami operacyjnymi, Zarządzanie poziomem usług IT, Zarządzanie bazami danych	Zajęcia	Piotr Dzwonkowski	27-08-2026	14:30	15:30	01:00
34 z 43 Odporność biznesowa: Analiza wpływu na działalność. Odporność systemowa i operacyjna. Tworzenie kopii zapasowych, przechowywanie i przywracanie danych	Zajęcia	Piotr Dzwonkowski	27-08-2026	15:30	17:00	01:30
35 z 43 Plan ciągłości działania, Plany odzyskiwania po awarii. Metody i techniki ataków na systemy informatyczne. Narzędzia i techniki testowania bezpieczeństwa	Zajęcia	Piotr Dzwonkowski	28-08-2026	09:00	10:30	01:30
36 z 43 -	Przerwa	-	28-08-2026	10:30	10:45	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
37 z 43 Ochrona zasobów informacyjnych. Bezpieczeństwo i kontrola zasobów informacyjnych: Polityki, ramy, standardy i wytyczne dotyczące bezpieczeństwa zasobów informacyjnych	Zajęcia	Piotr Dzwonkowski	28-08-2026	10:45	12:15	01:30
38 z 43 -	Przerwa	-	28-08-2026	12:15	12:45	00:30
39 z 43 Kontrole fizyczne i środowiskowe. Zarządzanie tożsamością i dostępem. Bezpieczeństwo sieci i punktów końcowych. Zapobieganie utracie danych	Zajęcia	Piotr Dzwonkowski	28-08-2026	12:45	14:15	01:30
40 z 43 -	Przerwa	-	28-08-2026	14:15	14:30	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
41 z 43 Szyfrowanie danych. Infrastruktura PKI. Środowiska chmurowe i wirtualne. Urządzenia mobilne, bezprzewodowe. Gromadzenie dowodów i analiza kryminalistyczna. Zarządzanie reagowaniem na incydenty.	Zajęcia	Piotr Dzwonkowski	28-08-2026	14:30	15:30	01:00
42 z 43 -	Walidacja	-	28-08-2026	15:30	16:30	01:00
43 z 43 Zakończenie szkolenia rozdanie certyfikatów	Zajęcia	Piotr Dzwonkowski	28-08-2026	16:30	17:00	00:30

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	40:00
w tym suma godzin zajęć	34:00
w tym suma godzin walidacji	01:00
w tym suma przerw	05:00
Suma godzin dydaktycznych bez przerw	46:30

Cennik

Jeżeli korzystasz z dofinansowania i usługa stanowi usługę kształcenia zawodowego lub przekwalifikowania zawodowego wraz z usługą lub dostawą towarów ściśle związaną z usługami kształcenia zawodowego lub przekwalifikowania zawodowego to możesz mieć możliwość skorzystania za zwolnienia z podatku VAT na podstawie art. 43 ust. 1 pkt 29 lit. c ustawy z dnia 11 marca 2024 r. o podatku od towarów i usług, jeśli usługa w

całości jest finansowana ze środków publicznych lub § 3 ust. 1 pkt 14 rozporządzenia Ministra Finansów z dnia 20 grudnia 2013 r. w sprawie zwolnień od podatku od towarów i usług oraz warunków stosowania tych zwolnień w przypadku, gdy usługa jest finansowana w co najmniej 70% ze środków publicznych.

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	10 209,00 PLN
Koszt przypadający na 1 uczestnika netto	8 300,00 PLN
Koszt osobogodziny brutto	255,23 PLN
Koszt osobogodziny netto	207,50 PLN
W tym koszt walidacji brutto	123,00 PLN
W tym koszt walidacji netto	100,00 PLN
W tym koszt certyfikowania brutto	3 690,00 PLN
W tym koszt certyfikowania netto	3 000,00 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	40:00

Prowadzący

Liczba prowadzących: 1

1 z 1

Piotr Dzwonkowski

Akredytowany Trener CTS Customized Training Solutions, Audytor, członek ISACA Warsaw Chapter oraz członek ISSA Polska. Piotr zawodowo zajmuje się różnymi obszarami związanymi z przetwarzaniem informacji: zarządzaniem, ryzykiem, ciągłością działania, bezpieczeństwem, audytem oraz spełnieniem wymagań prawnych, regulacyjnych lub normatywnych. Jest akredytowanym trenerem ISACA i prowadzi szkolenia przygotowujące do egzaminu na certyfikacje CISA, CISM, CRISC i AAIA, a także warsztaty z obszaru zarządzania ryzykiem IT, COBIT, ISO/IEC 27001, ISO 22301, RODO i z Cyberbezpieczeństwa. Jest czynnym audytorem wiodącym ISO/IEC

27001 oraz ISO 22301. Posiada certyfikaty m.in. CISA, CISM, CRISC, CDPSE, AAIA oraz ISO/IEC 27001 i ISO 22301 Lead Auditor.

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

W cenie szkolenia uczestnik otrzymuje

- Dostęp do platformy do komunikacji na żywo przez czas trwania szkolenia - 5-dni
- Prezentacja trenerska
- Oficjalny podręcznik CISA (eBook CISA Official Review Manual) w jezyku angielskim
- 6-miesięczna subskrypcja bazy pytań i odpowiedzi (CISA Exam Question, Answer and Explanations Database) w języku angielskim
- Voucher na egzamin online CISA ważny 6 miesięcy.
- Certyfikat CTS ukończenia szkolenia.

Informacje dodatkowe

Organizacja szkolenia

- Rodzaj szkolenia: szkolenie on-line grupa otwarta
- Forma realizacji: zdalnie prowadzone na żywo przez akredytowanego trenera
- Język szkolenia: polski
- Język materiałów: angielski
- Wielkość grupy: 6- 15 uczestników
- Szkolenie jest realizowane w godz. 9:00-17:00 w tym 3 przerwy

Wymagana frekwencja:

- **min. 80% obecności**. Podstawą weryfikacji są listy obecności tworzona na podstawie rzeczywistego czasu zalogowania w sesji szkoleniowej. Brak wymaganej frekwencji skutkuje nieuznaniem usługi za zrealizowaną i brakiem możliwości rozliczenia dofinansowania w systemie BUR.

Finasowanie:

Dla usług szkoleniowych z dofinansowaniem powyżej 70% z środków publicznych istnieje możliwość wystawienia faktury VAT zw.

Warunki techniczne

Szkolenie prowadzone jest w formie zdalnej na żywo za pośrednictwem aplikacji MS TEAMS. Aby dołączyć do szkolenia, konieczne jest posiadanie urządzenia takiego jak komputer stacjonarny/ laptop wyposażonego w stabilne łącze internetowe oraz mikrofon i kamerę.

- **Szkolenie realizowane jest w formie zdalnej (on-line) na żywo**. Uczestnik powinien dysponować komputerem z dostępem do Internetu wyposażonym w kamerę i mikrofon,
- **Szkolenie jest realizowane w formule otwartej**, uczestnik uczestniczy w szkoleniu wraz z całą grupą szkoleniową, zarówno w części teoretycznej, jak i praktycznej, zgodnie z programem.

Kontakt

Iwona Kwiatkowska

E-mail iwona@cts.com.pl

Telefon (+48) 222 082 861