Możliwość dofinansowania

ISACA CISM® – Certified Information Security Manager - akredytowane szkolenie z egzaminem

Numer usługi 2026/06/15/206646/3627390

9 840,00 PLN brutto
8 000,00 PLN netto
307,50 PLN brutto/h
250,00 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
- 32:00 h
- 25.08.2026 do 28.08.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Osoby zajmujące się bezpieczeństwem informacji i zainteresowane tematyką cyberbezpieczeństwa w tym: • Osoby przygotowujące się do zdobycia certyfikatu Certified Information Security Manager (CISM) • CISO (Chief Information Security Officer) - Dyrektor ds. bezpieczeństwa informacji. • CSO (Chief Security Officer) - Dyrektor ds. bezpieczeństwa • Security Director/Manager/Consultant - Dyrektor/Menedżer/Konsultant ds. Bezpieczeństwa • IT Director/Manager/Consultant - Dyrektor/Menedżer/Konsultant IT • Compliance/Risk/Privacy Director/Manager (GRC)- Dyrektor/Manager ds. zgodności/ryzyka/ochrony danych osobowych
Minimalna liczba uczestników	5
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	20-08-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Podstawa uzyskania wpisu do BUR	Certyfikat VCC Akademia Edukacyjna

Cel

Cel edukacyjny

Usługa CISM® – Certified Information Security Manager na charakter usługi edukacyjnej, przygotowuje uczestników do praktycznego stosowania zasad zarządzania bezpieczeństwem informacji w organizacji zgodnie z obszarami kompetencji CISM. Celem szkolenia jest przygotowanie uczestników do skutecznego zarządzania bezpieczeństwem informacji w organizacji, ze szczególnym uwzględnieniem ładu korporacyjnego, zarządzania ryzykiem, budowy programu bezpieczeństwa oraz reagowania na incydenty.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
opisuje podstawowe zasady zarządzania bezpieczeństwem informacji w organizacji,	poprawnie definiuje kluczowe pojęcia związane z bezpieczeństwem informacj	Test teoretyczny
identyfikuje zagrożenia i ryzyka związane z bezpieczeństwem informacji,	wskazuje główne obszary odpowiedzialności w zarządzaniu bezpieczeństwem informacji,	Test teoretyczny
rozróżnia elementy ładu bezpieczeństwa, zarządzania ryzykiem, programu bezpieczeństwa informacji oraz reagowania na incydenty,	analizuje przykład sytuacji ryzyka i proponuje adekwatne działania ograniczające,	Test teoretyczny
stosuje podstawowe metody analizy i oceny ryzyka bezpieczeństwa informacji,	rozpoznaje właściwe działania w zakresie nadzoru, monitorowania i reakcji na incydent,	Test teoretyczny
dobiera działania wspierające ochronę informacji zgodnie z wymaganiami organizacyjnymi i regulacyjnymi.	analizuje przykłady działań dotyczących wspierania ochrony informacji zgodnie z przyjętymi standardami oraz ocenia skuteczność tych działań	Wywiad swobodny

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

Domena 1 – Zarządzanie bezpieczeństwem informacji (Information Security Governance) - 17%

- Rola i cele zarządzania bezpieczeństwem informacji w organizacji
- Ład bezpieczeństwa (security governance) i jego Relation do ładu korporacyjnego
- Strategie, polityki, standardy i procedury bezpieczeństwa
- Model ról i odpowiedzialności w obszarze bezpieczeństwa informacji
- Wskaźniki ryzyka i metryki bezpieczeństwa (KPI, KRIs)
- Zarządzanie zgodnością z wymaganiami regulacyjnymi i contractual
- Budżetowanie i alokacja zasobów w bezpieczeństwie informacji

Domena 2 – Zarządzanie ryzykiem informacyjnym i zgodność z przepisami (Information Risk Management and Compliance) - 20%

- Podstawy zarządzania ryzykiem informacyjnym
- Identyfikacja zagrożeń, słabości i ryzyk
- Analiza ryzyka: jakościowa i ilościowa
- Metody oceny i mapowania ryzyka
- Strategie zarządzania ryzykiem: unikanie, przenoszenie, ograniczanie, akceptacja
- Ocena i wybór środków kontroli ryzyka
- Monitorowanie i raportowanie ryzyka
- Zgodność z wymaganiami regulacyjnymi (RODO, ISO/IEC 27001, ISO 27002, NIST, krajowe uregulowania)
- Audyty ryzyka i przeglądy skuteczności kontroli

Domena 3 – Rozwój i zarządzanie programami bezpieczeństwa informacji (Information Security Program Development and Management) - 33%

- Budowa programu bezpieczeństwa informacji zgodnego z celami biznesowymi
- Klasyfikacja i ochrona danych
- Zarządzanie dostępem i kontrola dostępu
- Bezpieczeństwo fizyczne i środowiskowe
- Kryptografia i zarządzanie kluczami
- Bezpieczeństwo sieci i komunikacji
- Bezpieczeństwo aplikacji i systemów
- Szkolenia i podnoszenie świadomości w organizacji
- Zarządzanie bezpieczeństwem w procesach transformacji
- Programy ciągłości działania (BCP) i odbudowy po incydencie (ITDR)

Domena 4 – Zarządzanie incydentami związanymi z bezpieczeństwem informacji (Information Security Incident Management) - 30%

- Definicje i klasyfikacja incydentów bezpieczeństwa
- Procesy zarządzania incydentami: wykrywanie, raportowanie, reagowanie, investigated

- Planowanie i przygotowanie na incydenty (incident response planning)
- Budowa zespołu reagowania na incydenty (CSIRT)
- Komunikacja podczas incydentu (wewnętrzna i zewnętrzna)
- Analiza po-incydentalna (post-incident review)
- Weryfikacja i testowanie planów reagowania
- Zarządzanie kryminalistyką komputerową w organizacji
- Powiązanie między reakcją na incydent i ciągłością działania

Harmonogram

Liczba pozycji harmonogramu: 35

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 35 Wprowadzenie - zapozanaie z harmonogramem, celem szkolenia	Zajęcia	Piotr Dzwonkowski	25-08-2026	09:00	09:30	00:30
2 z 35 Informacje o egzaminie CISM	Zajęcia	Piotr Dzwonkowski	25-08-2026	09:30	09:45	00:15
3 z 35 Nadzór nad bezpieczeństwem informacji - Zarządzanie bezpieczeństwem informacji (Information Security Governance)	Zajęcia	Piotr Dzwonkowski	25-08-2026	09:45	10:30	00:45
4 z 35 -	Przerwa	-	25-08-2026	10:30	10:45	00:15
5 z 35 Rola i cele zarządzania bezpieczeństwem informacji w organizacji	Zajęcia	Piotr Dzwonkowski	25-08-2026	10:45	12:15	01:30
6 z 35 -	Przerwa	-	25-08-2026	12:15	12:45	00:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
7 z 35 Ład bezpieczeństwa (security governance) i jego Relation do ładu korporacyjnego	Zajęcia	Piotr Dzwonkowski	25-08-2026	12:45	14:15	01:30
8 z 35 -	Przerwa	-	25-08-2026	14:15	14:30	00:15
9 z 35 Strategie, polityki, standardy i procedury bezpieczeństwa. Model ról i odpowiedzialności w obszarze bezpieczeństwa informacji	Zajęcia	Piotr Dzwonkowski	25-08-2026	14:30	15:30	01:00
10 z 35 Wskaźniki ryzyka i metryki bezpieczeństwa (KPI, KRIs), Zarządzanie zgodnością z wymaganiami . Budżetowanie i alokacja zasobów w bezpieczeństwie informacji	Zajęcia	Piotr Dzwonkowski	25-08-2026	15:30	17:00	01:30
11 z 35 Zarządzanie ryzykiem informacyjnym i zgodność z przepisami (Information Risk Management and Compliance) - wprowadzenie	Zajęcia	Piotr Dzwonkowski	26-08-2026	09:00	10:30	01:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
12 z 35 -	Przerwa	-	26-08-2026	10:30	10:45	00:15
13 z 35 Identyfikacja zagrożeń, słabości i ryzyk. Analiza ryzyka: jakościowa i ilościowa	Zajęcia	Piotr Dzwonkowski	26-08-2026	10:45	12:15	01:30
14 z 35 -	Przerwa	-	26-08-2026	12:15	12:45	00:30
15 z 35 Metody oceny i mapowania ryzyka. Strategie zarządzania ryzykiem: unikanie, przenoszenie, ograniczanie, akceptacja	Zajęcia	Piotr Dzwonkowski	26-08-2026	12:45	14:15	01:30
16 z 35 -	Przerwa	-	26-08-2026	14:15	14:30	00:15
17 z 35 Ocena i wybór środków kontroli ryzyka. Monitorowanie i raportowanie ryzyka.	Zajęcia	Piotr Dzwonkowski	26-08-2026	14:30	15:30	01:00
18 z 35 Zgodność z wymaganiami regulacyjnymi (RODO, ISO/IEC 27001, ISO 27002, NIST, krajowe uregulowania). Audyty ryzyka i przeglądy skuteczności kontroli	Zajęcia	Piotr Dzwonkowski	26-08-2026	15:30	17:00	01:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
19 z 35 Rozwój i zarządzanie programami bezpieczeństwa informacji (Information Security Program Development and Management) - Budowa programu bezpieczeństwa informacji zgodnego z celami biznesowymi	Zajęcia	Piotr Dzwonkowski	27-08-2026	09:00	10:30	01:30
20 z 35 -	Przerwa	-	27-08-2026	10:30	10:45	00:15
21 z 35 Klasyfikacja i ochrona danych. Zarządzanie dostępem i kontrola dostępu	Zajęcia	Piotr Dzwonkowski	27-08-2026	10:45	12:15	01:30
22 z 35 -	Przerwa	-	27-08-2026	12:15	12:45	00:30
23 z 35 Bezpieczeństwo fizyczne i środowiskowe.	Zajęcia	Piotr Dzwonkowski	27-08-2026	12:45	14:15	01:30
24 z 35 -	Przerwa	-	27-08-2026	14:15	14:30	00:15
25 z 35 Kryptografia i zarządzanie kluczami. Bezpieczeństwo sieci i komunikacji. Bezpieczeństwo aplikacji i systemów	Zajęcia	Piotr Dzwonkowski	27-08-2026	14:30	15:30	01:00

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
26 z 35 Programy ciągłości działania (BCP) i odbudowy po incydencie (ITDR)	Zajęcia	Piotr Dzwonkowski	27-08-2026	15:30	17:00	01:30
27 z 35 Zarządzanie incydentami związanymi z bezpieczeństwem informacji (Information Security Incident Management)	Zajęcia	Piotr Dzwonkowski	28-08-2026	09:00	10:30	01:30
28 z 35 -	Przerwa	-	28-08-2026	10:30	10:45	00:15
29 z 35 Definicje i klasyfikacja incydentów bezpieczeństwa. Procesy zarządzania incydentami: wykrywanie, raportowanie, reagowanie.	Zajęcia	Piotr Dzwonkowski	28-08-2026	10:45	12:15	01:30
30 z 35 -	Przerwa	-	28-08-2026	12:15	12:45	00:30
31 z 35 Planowanie i przygotowanie na incydenty (incident response planning). Budowa zespołu reagowania na incydenty (CSIRT). Komunikacja podczas incydentu (wewnętrzna i zewnętrzna)	Zajęcia	Piotr Dzwonkowski	28-08-2026	12:45	14:15	01:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
32 z 35 -	Przerwa	-	28-08-2026	14:15	14:30	00:15
33 z 35 Analiza po-incydentalna (post-incident review). Weryfikacja i testowanie planów reagowania.	Zajęcia	Piotr Dzwonkowski	28-08-2026	14:30	15:30	01:00
34 z 35 Podsumowanie szkolenia - rozdanie certyfikatów	Zajęcia	Piotr Dzwonkowski	28-08-2026	15:30	16:30	01:00
35 z 35 -	Walidacja	-	28-08-2026	16:30	17:00	00:30

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	32:00
w tym suma godzin zajęć	27:30
w tym suma godzin walidacji	00:30
w tym suma przerw	04:00
Suma godzin dydaktycznych bez przerw	37:15

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

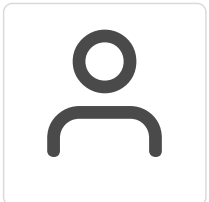
Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	9 840,00 PLN
Koszt przypadający na 1 uczestnika netto	8 000,00 PLN
Koszt osobogodziny brutto	307,50 PLN
Koszt osobogodziny netto	250,00 PLN
W tym koszt walidacji brutto	123,00 PLN
W tym koszt walidacji netto	100,00 PLN
W tym koszt certyfikowania brutto	3 321,00 PLN
W tym koszt certyfikowania netto	2 700,00 PLN

Liczba godzin usługi

Rodzaj godzin	Liczba godzin
Liczba godzin zegarowych usługi	32:00

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 - 4-dni
  - Prezentacja trenerska
  - Oficjalny podręcznik CISM (eBook CISM Official Review Manual) w jezyku angielskim
  - 6-miesięczna subskrypcja bazy pytań i odpowiedzi (CISM Exam Question, Answer and Explanations Database) w języku angielskim
  - Voucher na egzamin online CISM ważny 6 miesięcy.
  - Certyfikat CTS ukończenia szkolenia.

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

Informacje dodatkowe

Warunki organizacyjne:

- **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.

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.

Minimalne wymagania sprzętowo-systemowe:

- - Komputer PC/ laptop / tablet /smartfon
  - Przeglądarka internetowa lub zainstalowana aplikacja MS TEAMS.

Kontakt

Iwona Kwiatkowska

E-mail iwona@cts.com.pl
Telefon (+48) 222 082 861