Możliwość dofinansowania

ISACA CRISC® – Certified in Risk and Information Systems Control - akredytowane szkolenie

Numer usługi 2026/06/16/206646/3629540

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
- 14.09.2026 do 17.09.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	**Adresaci szkolenia CRISC** (Certified in Risk and Information Systems Control) to osoby pracujące w obszarach związanych z **zarządzaniem ryzykiem IT, bezpieczeństwem systemów informatycznych i kontrolą IT** w organizacji. Szkolenie CRISC jest przeznaczone dla: • Specjalistów i mangerów ryzyka IT • Pracowników działów zajmujących się bezpieczeństwem informacji i systemów • Audytorów i kontrolerów IT • Menedżerów i specjalistów IT • Osób pracujących w obszarach zgodności i regulacji
Minimalna liczba uczestników	5
Maksymalna liczba uczestników	15
Data zakończenia rekrutacji	07-09-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Podstawa uzyskania wpisu do BUR	Certyfikat VCC Akademia Edukacyjna

Cel

Cel edukacyjny

Celem szkolenia CRISC (Certified in Risk and Information Systems Control) jest przygotowanie uczestników do egzaminu certyfikującego oraz rozwinięcie wiedzy i umiejętności niezbędnych do skutecznego zarządzania ryzykiem IT i wdrażania kontroli systemów informatycznych w organizacji zgodnie ze globalnym standardem ISACA. Cel końcowy: uczestnik zdobywa praktyczne umiejętności zarządzania ryzykiem IT, potrafi identyfikować, analizować, reagować i raportować ryzyko w organizacji.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
1. W1 – rozumie ramy zarządzania i ład korporacyjny w kontekście zarządzania ryzykiem (np. COSO, COBIT, ERM, RMF) oraz role i odpowiedzialności w organizacji. 2. W2 – zna procesy identyfikacji, analizy i oceny ryzyka IT (kwalitatywnej i kwantytatywnej), wyceny zasobów IT oraz identyfikacji zagrożeń i wrażliwości. 3. W3 – rozumie strategie reagowania na ryzyko (unikanie, zmniejszanie, przekazywanie, akceptacja) oraz metody wyboru i implementacji kontroli. 4. W4 – zna zasady monitorowania, raportowania i komunikowania ryzyka, planowania reagowania na zdarzenia i zarządzania incydentami. 5. W5 – rozumie podstawy architektury IT, zasady zarządzania bezpieczeństwem informacji, kontroli bezpieczeństwa, polityk, standardów i procedur. 6. W6 – zna wpływ nowych technologii (chmura obliczeniowa, IoT, AI) na zarządzanie ryzykiem oraz podstawowe standardy i regulacje (np. NIS2, DORA, ISO 27001, GDPR). 7. W7 – zna strukturę i wymagania egzaminu CRISC oraz domeny egzaminacyjne.	uczestnik uzyskuje co najmniej 70% poprawnych odpowiedzi w testach wiedzy	Test teoretyczny

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
8. U1 – potrafi identyfikować ryzyka IT i związane z nimi zagrożenia oraz wrażliwości w środowisku organizacyjnym. 9. U2 – potrafi analizować i ocenić ryzyko IT metodami kwalitatywnymi i kwantytatywnymi. 10. U3 – potrafi wybrać odpowiednią strategię reagowania na ryzyko i dobrać skuteczne kontrole systemów informatycznych. 11. U4 – potrafi opracować plan monitorowania i raportowania ryzyka oraz komunikować ryzyko zainteresowanym (stakeholders). 12. U5 – potrafi wdrożyć i monitorować kontrole bezpieczeństwa informacji zgodne z politykami i standardami organizacji. 13. U6 – potrafi przygotować plan reagowania na zdarzenia i zarządzać incydentami IT.	uczestnik uzyskuje co najmniej 70% poprawnych odpowiedzi w testach wiedzy	Test teoretyczny

Cel biznesowy

Inwestycja w szkolenie CRISC (Certified in Risk and Information Systems Control) ma na celu wzmocnienie kompetencji organizacji w zakresie zarządzania ryzykiem IT i kontroli systemów informatycznych, co bezpośrednio przekłada się na:

Lepsze zarządzanie ryzykiem biznesowym związanym z technologią – organizacja zyskuje specjalistów zdolnych do identyfikacji, analizy, oceny i reagowania na ryzyka IT w sposób zgodny z globalnymi standardami ISACA.

Wzrost odporności biznesowej (business resilience) – szkolenie pozwala firmie budować skuteczne kontrole bezpieczeństwa, plany reagowania na zdarzenia i zarządzanie incydentami, co chroni przed cyberatakami i przestojami systemów.

Zgodność z wymaganiami regulacyjnymi – pracowników wyposaża się w wiedzę niezbędną do implementacji i utrzymania zgodności z regulacjami takimi jak NIS2, DORA, ISO 27001, GDPR.

Zmniejszenie kosztów związanych z incydentami i niezgodnością – efektywne zarządzanie ryzykiem IT ogranicza ryzyko cyberataków, które powodują ogromne przewód biznesowe, utratę funduszy i uszkodzenie reputacji organizacji.

Wzrost wiarygodności i konkurencyjności – certyfikacja CRISC daje natychmiastową wiarygodność w kontaktach z wewnętrznymi interesariuszami, regulatorami i klientami, zwiększając poziom zaufania klientów i reputację firmy.

Zatrudnienie ekspertów o wysokich kompetencjach – organizacja zyskuje możliwość zatrudnienia lub rozwoju pracowników z globalnie uznanej certyfikacją, co zwiększa przewagę w obszarze governance, risk i compliance (GRC).

Dla organizacji certyfikacja CRISC jest prewencją przed rzeczywistymi zagrożeniami w całej organizacji i pozwala być o krok przed zagrożeniami w zakresie zarządzania ryzykiem i bezpieczeństwem systemów informatycznych

Efekt usługi

Po ukończeniu szkolenia CRISC organizacja zyskuje przeszkolonych **specjalistów zarządzania ryzykiem IT**, którzy:

- **Identyfikują i analizują ryzyka IT** – potrafią stosować metodyki analizy ryzyka (kwalitatywnej i kwantytatywnej), ocenić wpływ na biznes i zidentyfikować zagrożenia oraz wrażliwości systemów.
- **Wybierają strategie reagowania na ryzyko** – dobierają odpowiednie kontrole (unikanie, zmniejszanie, przekazywanie, akceptacja) i wdrażają je skutecznie w organizacji.
- **Monitorują i raportują ryzyko** – tworzą metryki ryzyka, dashboards i raporty dla zainteresowanych (stakeholders), komunikując ryzyko w sposób zrozumiały dla biznesu.
- **Wdrażają i utrzymują kontrole bezpieczeństwa** – projektują, implementują, monitorują i utrzymują kontrole systemów informacyjnych zgodne z politykami i standardami organizacji.
- **Zarządzają incydentami i ciągłością działania** – planują reagowanie na zdarzenia, zarządają incydentami IT i wspierają Business Continuity Planning oraz Disaster Recovery.
- **Zrozumieją wpływ nowych technologii na ryzyko** – posiadają wiedzę o chmurze obliczeniowej, IoT, AI i innych emerging technologies oraz ich wpływie na zarządzanie ryzykiem IT.
- **Zyskują międzynarodowy certyfikat CRISC** – uzyskują Certified in Risk and Information Systems Control, który jest **złotym standardem dla profesjonalistów w dziedzinie bezpieczeństwa informacji i zarządzania ryzykiem**.

Efekt końcowy: **bardziej skuteczne zarządzanie ryzykiem IT, lepsza odporność biznesowa, wyższa zgodność regulacyjna i zwiększone bezpieczeństwo systemów biznesowych**, co przekłada się na:

- **Mniejsze ryzyko incydentów bezpieczeństwa** i cyberataków
- **Ograniczenie kosztów** związanych z niezgodnością i awaryjnością systemów
- **Wzrost konkurencyjności** organizacji w obszarze governance, risk i compliance (GRC)
- **Zwiększenie wiarygodności** wobec regulatorów, klientów i interesariuszy

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

Szkolenie CRISC to 4-dniowy kurs przygotowawczy Akredytowany przez ISACA, składający się z oficjalnych materiałów szkoleniowych ISACA International. Kurs obejmuje 4 domeny egzaminacyjne CRISC

- 4 dni (28 godzin dydaktycznych, 7 godzin dziennie)

- Godziny szkolenia: 9:00–17:00 z przerwami kawowymi i lunchem

DOMENA 1: Governance (Zarządzanie)

1.1 Ramy i Zasady Zarządzania

- - Zrozumienie różnych ram zarządzania (np. COSO, COBIT, ERM, RMF)
  - Zasady efektywnego zarządzania
  - Organizational governance i risk governance

1.2 Struktura i Kultura Organizacyjna

- - Rola i odpowiedzialności wewnątrz organizacji
  - Czynniki kulturowe wpływające na zarządzanie ryzykiem
  - Integracja zarządzania ryzykiem w procesy organizacyjne

1.3 Prewencja Prawna i Regulacyjna

- - Wymagania dotyczące zgodności z prawem w zakresie zarządzania ryzykiem IT
  - Prawne konsekwencje niezgodności
  - Standardy branżowe i najlepsze praktyki

1.4 Ramy Zarządzania Ryzykiem

- - Komponenty ramy zarządzania ryzykiem (ERM, RMF)
  - Integracja zarządzania ryzykiem w procesy organizacyjne
  - Polityki, standardy i procesy biznesowe związane z ryzykiem IT

1.5 Etyka i Kody Postępowania

- - Etyczne aspekty zarządzania ryzykiem
  - Ważność przestrzegania kodów postępowania
  - Kodeks Etyki Zawodowej ISACA

DOMENA 2: IT Risk Assessment (Ocena Ryzyka IT)

2.1 Techniki Identyfikacji Ryzyka

- - Metody identyfikacji ryzyka IT
  - Narzędzia i metodologie do identyfikacji ryzyka
  - Identifikacja ryzyk i scenariuszy ryzykowych

2.2 Analiza i Ocena Ryzyka

- - Techniki analizy ryzyka kwalitatywnej i kwantytatywnej
  - Ocena scenariuszy ryzykowych i ich wpływu
  - Analiza wpływu na biznes (Business Impact Analysis)

2.3 Wycenianie Zasobów IT

- - Wycena zasobów IT i ich wartości dla organizacji
  - Krytyczność zasobów w kontekście ryzyka
  - Mapa krytycznych procesów biznesowych

2.4 Identyfikacja Zagrożeń i Wrażliwości

- - Threat modeling i analiza wrażliwości
  - Identyfikacja zagrożeń wewnętrznych i zewnętrznych
  - Ocena podatności systemów na zagrożenia

2.5 Inherent Risk i Residual Risk

- - Zarządzanie ryzykiem pierwotnym (inherent risk)
  - Zarządzanie ryzykiem pozostałym (residual risk)
  - Metody obniżania ryzyka

DOMENA 3: Risk Response and Reporting (Reagowanie na Ryzyko i Raportowanie)

3.1 Strategie Reagowania na Ryzyko

- Unikanie ryzyka (risk avoidance)
- Zmniejszanie ryzyka (risk mitigation)
- Przekazywanie ryzyka (risk transfer)
- Akceptacja ryzyka (risk acceptance)

3.2 Własność Ryzyka i Kontroli

- Ownership ryzyka i kontroli w organizacji
- Role i odpowiedzialności w zarządzaniu ryzykiem
- Delegowanie odpowiedzialności

3.3 Zarządzanie Ryzykiem Trzeciej Strony

- Third-party risk management
- Ocena ryzyka dostawców i partnerów
- Kontrole w umowach i SLA

3.4 Raportowanie i Komunikacja Ryzyka

- Metody raportowania ryzyka
- Komunikacja ryzyka zainteresowanym (stakeholders)
- Metryki i dashboards ryzyka

3.5 Planowanie Reagowania na Zdarzenia

- Plan reagowania na zdarzenia (incident response plan)
- Zarządzanie incydentami IT
- Business Continuity Planning i Disaster Recovery

DOMENA 4: Information Technology and Security (Technologia i Bezpieczeństwo)

4.1 Ramy i Standardy IT i Bezpieczeństwa

- IT i security frameworks (ISO 27001, NIST, COBIT)
- Standardy branżowe i regulacje (NIS2, DORA, GDPR)
- Polityki bezpieczeństwa informacji

4.2 Projektowanie i Wdrażanie Kontroli Systemów Informacyjnych

- Design kontroli systemów informatycznych
- Implementacja kontroli bezpieczeństwa
- Kontrola dostępu, kontrola danych, kontrola procesów

4.3 Monitorowanie i Utrzymanie Kontroli

- Control monitoring i maintenance
- Audyt kontroli bezpieczeństwa
- Ocena skuteczności kontroli

4.4 Nowe technologie i Trends w IT Risk i Control

- Cloud computing i ryzyko IT
- IoT i ryzyko bezpieczeństwa
- AI i automatyzacja w zarządzaniu ryzykiem
- Emerging technologies i ich wpływ na ryzyko

Harmonogram

Liczba pozycji harmonogramu: 36

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 36 Wprowadzenie do szkolenia - harmonogram	Zajęcia	Piotr Dzwonkowski	14-09-2026	09:00	09:30	00:30
2 z 36 Pre-Test	Zajęcia	Piotr Dzwonkowski	14-09-2026	09:30	09:45	00:15
3 z 36 DOMENA 1: Governance (Zarządzanie). Ramy i Zasady Zarządzania. Zrozumienie różnych ram zarządzania (np. COSO, COBIT, ERM, RMF). Organizational governance i risk governance	Zajęcia	Piotr Dzwonkowski	14-09-2026	09:45	10:30	00:45
4 z 36 -	Przerwa	-	14-09-2026	10:30	10:45	00:15
5 z 36 1.2 Struktura i Kultura Organizacyjna. Rola i odpowiedzialności wewnątrz organizacji. Czynniki kulturowe wpływające na zarządzanie ryzykiem. Integracja zarządzania ryzykiem w procesy organizacyjne	Zajęcia	Piotr Dzwonkowski	14-09-2026	10:45	12:15	01:30
6 z 36 -	Przerwa	-	14-09-2026	12:15	12:45	00:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
7 z 36 1.3 Prewencja Prawna i Regulacyjna. Wymagania dotyczące zgodności z prawem w zakresie zarządzania ryzykiem IT. Prawne konsekwencje niezgodności. Standardy branżowe i najlepsze praktyki	Zajęcia	Piotr Dzwonkowski	14-09-2026	12:45	14:15	01:30
8 z 36 -	Przerwa	-	14-09-2026	14:15	14:30	00:15
9 z 36 1.4 Ramy Zarządzania Ryzykiem. Komponenty ramy zarządzania ryzykiem (ERM, RMF). Integracja zarządzania ryzykiem w procesy organizacyjne. Polityki, standardy i procesy biznesowe związane z ryzykiem IT	Zajęcia	Piotr Dzwonkowski	14-09-2026	14:30	15:30	01:00
10 z 36 1.5 Etyka Postępowania. Etyczne aspekty zarządzania ryzykiem. Ważność przestrzegania kodeksów postępowania. Kodeks Etyki Zawodowej ISACA	Zajęcia	Piotr Dzwonkowski	14-09-2026	15:30	17:00	01:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
11 z 36 DOMENA 2: IT Risk Assessment (Ocena Ryzyka IT) Techniki i metody Identyfikacji Ryzyka. Narzędzia i metodologie	Zajęcia	Piotr Dzwonkowski	15-09-2026	09:00	10:30	01:30
12 z 36 -	Przerwa	-	15-09-2026	10:30	10:45	00:15
13 z 36 2.2 Analiza i Ocena Ryzyka. Techniki analizy ryzyka. Analiza wpływu na biznes (Business Impact Analysis)	Zajęcia	Piotr Dzwonkowski	15-09-2026	10:45	12:15	01:30
14 z 36 -	Przerwa	-	15-09-2026	12:15	12:45	00:30
15 z 36 2.3 Wycenianie Zasobów IT. Krytyczność zasobów w kontekście ryzyka. Mapa krytycznych procesów biznesowych	Zajęcia	Piotr Dzwonkowski	15-09-2026	12:45	14:15	01:30
16 z 36 -	Przerwa	-	15-09-2026	14:15	14:30	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
17 z 36 2.4 Identyfikacja Zagrożeń i Wrażliwości, analiza wrażliwości. Identyfikacja zagrożeń wewnętrznych i zewnętrznych. Ocena podatności systemów na zagrożenia	Zajęcia	Piotr Dzwonkowski	15-09-2026	14:30	15:30	01:00
18 z 36 2.5 Zarządzanie ryzykiem. Metody obniżania ryzyka	Zajęcia	Piotr Dzwonkowski	15-09-2026	15:30	17:00	01:30
19 z 36 DOMENA 3: Reagowanie na Ryzyko i Raportowanie. Strategie Reagowania na Ryzyko. Unikanie ryzyka Zmniejszanie ryzyka. Przekazywanie ryzyka. Akceptacja ryzyka.	Zajęcia	Piotr Dzwonkowski	16-09-2026	09:00	10:30	01:30
20 z 36 -	Przerwa	-	16-09-2026	10:30	10:45	00:15

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
21 z 36 3.2 Własność Ryzyka i Kontroli. Ownership ryzyka i kontroli w organizacji. Role i odpowiedzialności w zarządzaniu ryzykiem. Delegowanie odpowiedzialności.	Zajęcia	Piotr Dzwonkowski	16-09-2026	10:45	12:15	01:30
22 z 36 -	Przerwa	-	16-09-2026	12:15	12:45	00:30
23 z 36 3.3 Zarządzanie Ryzykiem Trzeciej Strony. Third-party risk management. Ocena ryzyka dostawców i partnerów. Kontrole w umowach i SLA	Zajęcia	Piotr Dzwonkowski	16-09-2026	12:45	14:15	01:30
24 z 36 -	Przerwa	-	16-09-2026	14:15	14:30	00:15
25 z 36 3.4 Raportowanie i Komunikacja Ryzyka Metody raportowania ryzyka. Komunikacja ryzyka zainteresowanym (stakeholders). Metryki i dashboards ryzyka	Zajęcia	Piotr Dzwonkowski	16-09-2026	14:30	15:30	01:00

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
26 z 36 3.5 Planowanie Reagowania na Zdarzenia. Plan reagowania na zdarzenia (incident response plan). Zarządzanie incydentami IT. Business Continuity Planning i Disaster Recovery	Zajęcia	Piotr Dzwonkowski	16-09-2026	15:30	17:00	01:30
27 z 36 DOMENA 4:Technologia i Bezpieczeństwo. Ramy i Standardy IT i Bezpieczeństwa. IT i security frameworks (ISO 27001, NIST, COBIT). Polityki bezpieczeństwa informacji	Zajęcia	Piotr Dzwonkowski	17-09-2026	09:00	10:30	01:30
28 z 36 -	Przerwa	-	17-09-2026	10:30	10:45	00:15
29 z 36 Standardy branżowe i regulacje (NIS2, DORA, GDPR)	Zajęcia	Piotr Dzwonkowski	17-09-2026	10:45	12:15	01:30
30 z 36 -	Przerwa	-	17-09-2026	12:15	12:45	00:30

Przedmiot / temat	Typ aktywności	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
31 z 36 4.2 Projektowanie i Wdrażanie Kontroli Systemów Informacyjnych. Planowanie i implementacja kontroli systemów informatycznych	Zajęcia	Piotr Dzwonkowski	17-09-2026	12:45	14:15	01:30
32 z 36 -	Przerwa	-	17-09-2026	14:15	14:30	00:15
33 z 36 4.3 Monitorowanie i Utrzymanie Kontroli. Audyt kontroli bezpieczeństwa. Ocena skuteczności kontroli	Zajęcia	Piotr Dzwonkowski	17-09-2026	14:30	15:30	01:00
34 z 36 4.4 Nowe technologie i Trends w IT Risk i Control. AI i automatyzacja w zarządzaniu ryzykiem	Zajęcia	Piotr Dzwonkowski	17-09-2026	15:30	16:00	00:30
35 z 36 -	Walidacja	-	17-09-2026	16:00	16:30	00:30
36 z 36 Podsumowanie zakończenie szkolenia	Zajęcia	Piotr Dzwonkowski	17-09-2026	16:30	17:00	00:30

Podsumowanie

Rodzaj godzin	Liczba godzin
Suma godzin zegarowych usługi	32:00
w tym suma godzin zajęć	27:30

Rodzaj godzin	Liczba godzin
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	3 690,00 PLN
W tym koszt certyfikowania netto	3 000,00 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 CRISC (eBook CISA Official Review Manual) w jezyku angielskim
- 6-miesięczna subskrypcja bazy pytań i odpowiedzi (CRISC Exam Question, Answer and Explanations Database) w języku angielskim
- Voucher na egzamin online CRISC 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: 5- 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.

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