Możliwość dofinansowania

CRISC® – Certified in Risk and Information Systems Control - akredytowane szkolenie (S_52187)

Numer usługi 2026/03/07/7629/3387912

5 768,70 PLN brutto
4 690,00 PLN netto
180,27 PLN brutto/h
146,56 PLN netto/h
196,00 PLN cena rynkowa

ASSECO DATA SYSTEMS SPÓŁKA AKCYJNA

4,4 / 5

152 oceny

zdalna w czasie rzeczywistym
Usługa szkoleniowa
32 h
22.06.2026 do 25.06.2026

Informacje podstawowe

Kategoria	Informatyka i telekomunikacja / Bezpieczeństwo IT
Grupa docelowa usługi	Specjaliści, menadżerzy i konsultanci ds. ryzyka i bezpieczeństwa informacji Audytorzy IT Analitycy Ryzyka - Risk Analysts Specjaliści ds. Kontroli Ryzyka - Risk Control Specialists Inspektorzy ds. ryzyka/zgodności - Risk/Compliance Investigators
Minimalna liczba uczestników	3
Maksymalna liczba uczestników	20
Data zakończenia rekrutacji	15-06-2026
Forma prowadzenia usługi	zdalna w czasie rzeczywistym
Liczba godzin usługi	32
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

Szkolenie rozwija kompetencje w zakresie zarządzania ryzykiem w systemach informacyjnych, obejmujące identyfikację, analizę i ocenę ryzyka IT, projektowanie mechanizmów kontrolnych oraz monitorowanie skuteczności zarządzania ryzykiem. Program łączy perspektywę biznesową i technologiczną w obszarze bezpieczeństwa informacji oraz przygotowuje uczestników do egzaminu certyfikacyjnego CRISC®.

Efekty uczenia się oraz kryteria weryfikacji ich osiągnięcia i Metody walidacji

Efekty uczenia się	Kryteria weryfikacji	Metoda walidacji
WIEDZA: Uczestnik wyjaśnia podstawowe pojęcia i zasady zarządzania ryzykiem w systemach informacyjnych.	Definiuje pojęcie ryzyka w kontekście systemów informacyjnych Rozróżnia zagrożenie, podatność i kontrolę Wskazuje elementy procesu zarządzania ryzykiem	Test teoretyczny
WIEDZA: Uczestnik opisuje metody identyfikacji i oceny ryzyka w organizacji.	dentyfikuje etapy analizy ryzyka Rozróżnia jakościowe i ilościowe metody oceny ryzyka Określa rolę właściciela ryzyka	Test teoretyczny
UMIEJĘTNOŚCI: Uczestnik potrafi przeprowadzić analizę ryzyka dla systemów informacyjnych.	Identyfikuje aktywa i zagrożenia Ocenia poziom ryzyka Proponuje działania ograniczające ryzyko	Test teoretyczny
UMIEJĘTNOŚCI: Uczestnik potrafi zaprojektować i ocenić mechanizmy kontroli ograniczające ryzyko IT.	Dobiera kontrolę adekwatną do poziomu ryzyka Oceni skuteczność mechanizmów kontrolnych Rozróżnia kontrolę prewencyjną i detekcyjną	Test teoretyczny
KOMPETECJE SPOŁECZNE: Uczestnik przyjmuje odpowiedzialną postawę w zarządzaniu ryzykiem organizacji.	Rozumie znaczenie zarządzania ryzykiem dla organizacji Wspiera kulturę bezpieczeństwa Podejmuje decyzje uwzględniające ryzyko biznesowe	Test teoretyczny
KOMPETECJE SPOŁECZNE: Uczestnik komunikuje ryzyko w sposób zrozumiały dla interesariuszy.	Przedstawia ryzyko w kontekście biznesowym Stosuje jasną komunikację dotyczącą zagrożeń Wspiera podejmowanie decyzji przez kierownictwo	Test teoretyczny

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

Ramowy program szkolenia:

Wprowadzenie do kursu (*Course Introduction*)

Informacje o egzaminie CRISC (*CRISC Exam Prep*)

Obszar 1: Ład korporacyjny (*Governance*)

- Organizational Governance:
- Organizational Strategy, Goals, and Objectives
- Organizational Structure, Roles and Responsibilities
- Organizational Culture
- Policies and Standards
- Business Processes
- Organizational Assets
- Risk Governance:
- Enterprise Risk Management and Risk Management Framework
- Three Lines of Defense
- Risk Profile
- Risk Appetite and Risk Tolerance
- Legal, Regulatory and Contractual Requirements
- Professional Ethics of Risk Management

Obszar 2: Ocena ryzyka IT (*IT Risk Assessment*)

- IT Risk Identification:
  - Risk Events (e.g., contributing conditions, loss result)
  - Threat Modelling and Threat Landscape
  - Vulnerability and Control Deficiency Analysis (e.g., root cause analysis)
  - Risk Scenario Development
- IT Risk Analysis and Evaluation:
  - Risk Assessment Concepts, Standards and Frameworks
  - Risk Register
  - Risk Analysis Methodologies
  - Business Impact Analysis
  - Inherent and Residual Risk

Obszar 3: Reagowanie na ryzyko i raportowanie (*Risk Response and Reporting*)

- Risk Response:
  - Risk Treatment / Risk Response Options
  - Risk and Control Ownership
  - Third-Party Risk Management
  - Issue, Finding and Exception Management
  - Management of Emerging Risk

- Control Design and Implementation:
  - Control Types, Standards and Frameworks
  - Control Design, Selection and Analysis
  - Control Implementation
  - Control Testing and Effectiveness Evaluation

- Risk Monitoring and Reporting:
  - Risk Treatment Plans
  - Data Collection, Aggregation, Analysis and Validation
  - Risk and Control Monitoring Techniques
  - Risk and Control Reporting Techniques (heatmap, scorecards, dashboards)
  - Key Performance Indicators
  - Key Risk Indicators (KRIs)
  - Key Control Indicators (KCIs)

Obszar 4: Technologie informacyjne i bezpieczeństwo (*Information Technology and Security*)

- Information Technology Principles:
  - Enterprise Architecture
  - IT Operations Management (e.g., change management, IT assets, problems, incidents)
  - Project Management
  - Disaster Recovery Management (DRM)
  - Data Lifecycle Management
  - System Development Life Cycle (SDLC)
  - Emerging Technologies

- Information Security Principles:
  - Information Security Concepts, Frameworks and Standards
  - Information Security Awareness Training
  - Business Continuity Management
  - Data Privacy and Data Protection Principles

Próbne pytania egzaminacyjne i podsumowanie (*Practice Questions & Review*)

Wskazówki i porady przed egzaminem CRISC (*CRISC Exam Prep*)

Harmonogram

Liczba przedmiotów/zajęć: 8

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
1 z 8 Wprowadzenie do kursu (Course Introduction)	academy@assecods.pl	22-06-2026	09:00	09:30	00:30

Przedmiot / temat zajęć	Prowadzący	Data realizacji zajęć	Godzina rozpoczęcia	Godzina zakończenia	Liczba godzin
2 z 8 Informacje o egzaminie CRISC (CRISC Exam Prep)	academy@assecods.pl	22-06-2026	09:30	10:00	00:30
3 z 8 Obszar 1: Ład korporacyjny (Governance)	academy@assecods.pl	22-06-2026	10:00	15:30	05:30
4 z 8 Obszar 2: Ocena ryzyka IT (IT Risk Assessment)	academy@assecods.pl	23-06-2026	09:00	15:30	06:30
5 z 8 Obszar 3: Reagowanie na ryzyko i raportowanie (Risk Response and Reporting)	academy@assecods.pl	24-06-2026	09:00	15:30	06:30
6 z 8 Obszar 4: Technologie informacyjne i bezpieczeństwo (Information Technology and Security)	academy@assecods.pl	25-06-2026	09:00	14:30	05:30
7 z 8 Próbne pytania egzaminacyjne i podsumowanie (Practice Questions & Review)	academy@assecods.pl	25-06-2026	14:30	15:00	00:30
8 z 8 Wskazówki i porady przed egzaminem CRISC (CRISC Exam Prep)	academy@assecods.pl	25-06-2026	15:00	15:30	00:30

Cennik

Cennik

Rodzaj ceny	Cena
Koszt przypadający na 1 uczestnika brutto	5 768,70 PLN

Koszt przypadający na 1 uczestnika netto	4 690,00 PLN
Koszt osobogodziny brutto	180,27 PLN
Koszt osobogodziny netto	146,56 PLN

Prowadzący

Liczba prowadzących: 2

1 z 2

academy@assecods.pl

Trener z co najmniej 5 letnim doświadczeniem w prowadzeniu szkoleń, w tym z obszaru merytorycznego, którego dotyczy. W przypadku szkoleń akredytowanych i autoryzowanych nasi trenerzy posiadają stosowne uprawnienia do ich prowadzenia.

2 z 2

Koordynator walidacji efektów uczenia się

Pracownik Asseco Academy, który przeprowadza i zarządza procesem walidacji efektów uczenia w oparciu o przygotowane narzędzia diagnostyczne

Informacje dodatkowe

Informacje o materiałach dla uczestników usługi

W cenie uczestnik otrzymuje

- Udział w 4-dniowym akredytowanym szkoleniu Certified in Risk and Information Systems Control® (CRISC®) prowadzonym na żywo przez trenera eksperta ds. cyberbezpieczeństwa
- Oficjalny podręcznik CRISC przygotowujący do egzaminu (eBook CRISC Official Review Manual, 7th Edition Revised)
- 12-miesięczną subskrypcję bazy pytań egzaminacyjnych i odpowiedzi (CRISC Exam Question, Answer and Explanation)
- Zaświadczenie Asseco Academy o ukończeniu szkolenia.

Opcjonalnie do szkolenia można zakupić voucher na międzynarodowy egzamin online CRISC.

Organizacja szkolenia

- Rodzaj szkolenia: otwarte lub dla grup zamkniętych
- Forma realizacji: stacjonarnie lub zdalnie; więcej informacji: Formy Szkoleń Asseco Academy
- Język szkolenia: polski
- Język materiałów: angielski
- Wielkość grupy: do 20 uczestników
- Uczestnik szkolenia musi założyć konto w systemie MyISACA https://www.isaca.org/myisaca
- Materiały szkoleniowe, baza próbnych pytań egzaminacyjnych oraz voucher na egzamin zostaną udostępnione na koncie MyISACA kandydata.

Organizacja szkolenia w Wirtualnej Klasie

- Szkolenie jest realizowane w godz. 9:00-15:30

- Każdy uczestnik powinien dokonać rejestracji do zdalnej sesji szkoleniowej w godz. 8:30-8:50
- W trakcie dnia szkoleniowego przewidujemy kilka przerw, w tym 60-minutową na lunch, a także po każdej godzinie szkolenia 10-minutowe przerwy; szczegółowy rozkład przerw każdy trener ustala indywidualnie z grupą
- Jedna godzina lekcyjna to 45 minut
- Komplet akredytowanych materiałów szkoleniowych dystrybuowany jest w formie elektronicznej.

Warunki uczestnictwa

Prosimy o zapisanie się na szkolenie przez naszą stronę internetową https://academy.asseco.pl/szkolenie/crisc-certified-in-risk-and-information-systems-control/ w celu rezerwacji miejsca.

UWAGA! Dla usług z dofinansowaniem powyżej 70% istnieje możliwość wystawienia faktury ZW VAT. Prosimy o kontakt z Biurem Asseco Academy academy@assecods.pl Natomiast w przypadku dofinansowania usługi poniżej 70% ze środków publicznych, usługa nie jest zwolniona z podatku VAT. Należy wówczas doliczyć do usługi szkoleniowej należny VAT w wysokości 23%.

Warunki techniczne

Szkolenie prowadzone jest w formie zdalnej na żywo za pośrednictwem aplikacji Webex Meeting. Aby wziąć udział, konieczne jest posiadanie urządzenia takiego jak komputer stacjonarny, laptop wyposażonego w stabilne połączenie internetowe oraz mikrofon i kamerę. Przed rozpoczęciem szkolenia uczestnicy będą mieli możliwość przetestowania swojego sprzętu podczas sesji próbnej, aby upewnić się, że połączenie internetowe, mikrofon i kamera/słuchawki działają poprawnie.

Minimalne wymagania sprzętowo-systemowe:

- Komputer PC z systemem Windows 7 lub nowszym, Max OX 10.13 lub nowszym. Istnieje możliwość korzystania z innych systemów, w tym Linux. Szczegółowe informacje można uzyskać pod adresem: https://help.webex.com/en-us/nki3xrq/Webex-Meetings-Suite-SystemRequirements.
- Przeglądarka internetowa (zalecamy korzystanie z Chrome lub Firefox).
- Karta LAN: min. 100 MBPS lub stabilne połączenie WiFi (zalecamy połączenie do sieci „kablem”). Nie dopuszcza się udziału w szkoleniu za pośrednictwem łączy GSM/LTE. Zalecane pasmo, to przynajmniej 2 MB/s (download i upload). W przypadku spadku przepustowości łącza poniżej 1,2 MB/s należy liczyć się z istotnym obniżeniem jakości połączenia.
- Mikrofon i głośniki (zalecamy korzystanie z zestawu typu headset).
- Kamera internetowa.

Przed szkoleniem każdy uczestnik otrzyma na podany adres email link do platformy, gdzie odbędzie się szkolenie. Uczestnictwo w szkoleniu umożliwia aktywne uczestnictwo w zajęciach, w tym komunikację z trenerem oraz pozostałymi uczestnikami. Umożliwia to wymianę doświadczeń oraz aktywny kontakt zarówno z grupą, jak i prowadzącym. Dodatkowo, uczestnicy mają dostęp do funkcji czatu online, co jeszcze bardziej ułatwia interakcję.

Kontakt

Alicja Kozłowska

E-mail bur-szkolenia@assecods.pl

Telefon (+48) 801 303 030