Szkolenie: ISC2
ISC2 CISSP Certification Prep Course

DOSTĘPNE TERMINY

2025-04-28 | 5 dni | Warszawa / Wirtualna sala
2025-05-05 | 5 dni | Virtual Classroom
2025-05-12 | 5 dni | Kraków / Wirtualna sala *(Termin gwarantowany)*
2025-06-23 | 5 dni | Warszawa / Wirtualna sala *(Termin gwarantowany)*

Cel szkolenia:

Jest to oficjalne i autoryzowane seminarium ISC2 o pełnej nazwie:
Official ISC2 CBK Training Seminar for the CISSP (Certified Information Systems Security Professional)

Oferowane przez nas szkolenie ISC2 CISSP jest prowadzone przez autoryzowanego instruktora ISC2 posiadającego zarówno wymagane poświadczenia trenerskie wystawione przez ISC2 jak i zweryfikowaną wiedzę ekspercką z zakresu bezpieczeństwa informacji oraz aktualny certyfikat CISSP.

Seminarium jest prowadzone w dogodnej dla uczestników formie, czyli jako szkolenie stacjonarne w sali szkoleniowej lub szkolenie zdalne (online), czy też w formie hybrydowej.

Program kursu jest w pełni zgodny z aktualnie obowiązującym kanonem wiedzy wymaganej w czasie egzaminu CISSP.

Każdy uczestnik autoryzowanego szkolenia ISC2 CISSP Certification Prep Course realizowanego w Compendium CE, otrzymuje darmowy voucher egzaminacyjny CISSP Certification Exam.

Kurs ten jest przeznaczony dla specjalistów ds. bezpieczeństwa informacji posiadających już praktyczną wiedzę oraz doświadczenie zawodowe zarówno technologiczne jak i menedżerskie.

Szkolenie to zapewnia kompleksowy przegląd koncepcji bezpieczeństwa systemów informatycznych i najlepszych praktyk branżowych, obejmujących osiem domen wiedzy CISSP tzw. Common Body of Knowledge (CBK®):

- Domain 1: Security and Risk Management
- Domain 2: Asset Security
- Domain 3: Security Architecture and Engineering
- Domain 4: Communication and Network Security
- Domain 5: Identity and Access Management (IAM)

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Domain 6: Security Assessment Testing
- Domain 7: Security Operations
- Domain 8: Software Development Security

Po ukończeniu szkolenia, uczestnicy będą mogli:

- Stosować podstawowe koncepcje i metody związane z technologiami informacyjnymi oraz bezpieczeństwem informacji w organizacji.
- Dostosować funkcje bezpieczeństwa oraz implementować zabezpieczenia przystosowane do ogólnych celów operacyjnych organizacji.
- Definiować w jaki sposób efektywnie chronić aktywa organizacji podczas ich cyklu życia.
- Wykorzystać koncepcje, zasady, struktury i standardy używane do projektowania, wdrażania, monitorowania i zabezpieczania systemów operacyjnych, sprzętu, sieci, aplikacji oraz środków kontroli stosowanych do egzekwowania różnych poziomów poufności, integralności i dostępności w organizacji.
- Stosować zasady projektowania zabezpieczeń tak aby wybrać odpowiednie środki zaradcze dla podatności występujących powszechnie w systemach informatycznych.
- Rozumieć ważność kryptografii i usług bezpieczeństwa, w dzisiejszej rzeczywistości cyfrowej oraz informacyjnej.
- Prawidłowo oceniać fizyczne elementy bezpieczeństwa w odniesieniu do potrzeb zapewnienia bezpieczeństwa informacji.
- Poprawnie implementować elementy składające się na bezpieczeństwo komunikacji i sieci w odniesieniu do potrzeb zachowania bezpieczeństwa informacji.
- Wykorzystywać koncepcje i architekturę, która definiuje powiązane technologie z wdrożonymi systemami oraz protokołami w ramach modelu Open Systems Interconnection, tak aby spełniały one wymagania w zakresie bezpieczeństwa informacji.
- Wdrażać odpowiednie modele logicznej kontroli dostępu, aby zaspokoić wymagania bezpieczeństwa w organizacji.
- Umiejętnie stosować kontrolę dostępu fizycznego w organizacji.
- Rozróżniać podstawowe metody projektowania oraz walidacji strategii testów i audytów, które wspierają wymagania bezpieczeństwa informacji.
- Stosować odpowiednią kontrole bezpieczeństwa w celu optymalizacji funkcji w organizacji.
- Szacować ryzyko związane z systemami informatycznymi dla działań operacyjnych wewnątrz organizacji.
- Definiować odpowiednie zabezpieczenia w celu obniżenia poziomu określonego ryzyka lub podatności.
- Stosować koncepcje bezpieczeństwa systemów informatycznych w celu ograniczenia ryzyka związanego z lukami bezpieczeństwa w oprogramowaniu i systemach.

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

Grupa docelowa

Kurs ten jest przeznaczony dla osób planujących uzyskanie certyfikatu CISSP. Certyfikat CISSP jest przeznaczony dla profesjonalistów, którzy mają łącznie co najmniej 5 lat doświadczenia zawodowego w 2 lub więcej z 8 dziedzin CISSP Common Body of Knowledge (CBK). Ci uczestnicy szkolenia, który nie ma aktualnie wymaganego doświadczenia, a którzy mimo to podejdą i zdadzą egzamin CISSP, zostają Associate of ISC2. Osoby z tytułem Associate of ISC2 mają sześć lat na zdobycie wymaganego pięcioletniego doświadczenia i tym samym na uzyskanie tytułu CISSP.

Przed decyzją o udziale w tym seminarium, uczestnik powinien posiadać co najmniej kilkuletnie doświadczenie zawodowe oraz praktyczną wiedzę zdobytą w poniższych rolach zawodowych:

- Chief Information Officer
- Chief Information Security Officer
- Chief Technology Officer
- Compliance Manager/ Officer
- Director of Security
- Information Architect
- Information Manager / Information Risk Manager or Consultant
- IT Specialist/Director/Manager
- Network/System Administrator
- Security Administrator
- Security Architect / Security Analyst
- Security Consultant
- Security Manager
- Security Systems Engineer/ Security Engineer

Plan szkolenia:

- Środowisko bezpieczeństwa informacji
  - Kodeks etyki w organizacji.
  - Związek pomiędzy poufnością, integralnością, dostępnością, niezaprzeczalnością, autentycznością, prywatnością i bezpieczeństwem a należytą dbałością i starannością.
  - Związek pomiędzy ładem w bezpieczeństwie informacji a strategią biznesową, celem, misją i zadaniami w organizacji.
  - Cyberprzestępczości w powiązaniu z naruszeniem bezpieczeństwa danych i innymi naruszeniami bezpieczeństwa informacji.
  - Związek pomiędzy wymaganiami prawnymi, umowami i regulacjami dotyczącymi prywatności i ochrony danych a celami związanymi z bezpieczeństwem informacji.

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Związek pomiędzy transgranicznym przepływem danych oraz kwestiami importu i eksportu a ochroną danych, prywatnością i ochroną własności intelektualnej.

- Bezpieczeństwo zasobów informacyjnych
  - Powiązanie zarządzania zasobami IT i modeli cyklu życia danych z bezpieczeństwem informacji.
  - Wyjaśnienie zastosowania klasyfikacji i kategoryzacji informacji jako dwóch odrębnych, ale powiązanych ze sobą procesów.
  - Różne stany danych i związane z nimi względy bezpieczeństwa informacji.
  - Różne role związane z wykorzystaniem informacji oraz względy bezpieczeństwa związane z tymi rolami.
  - Różne rodzaje i kategorie środków kontroli bezpieczeństwa informacji oraz ich zastosowanie.
  - Wybór standardów bezpieczeństwa danych, w celu spełnienia wymagania zgodności organizacji.
- Zarządzanie tożsamością i dostępem (Identity and Access Management (IAM))
  - Porównanie modeli, mechanizmów i koncepcje kontroli dostępu.
  - Rola uwierzytelniania, autoryzacji i rozliczania w osiąganiu celów i zadań związanych z bezpieczeństwem informacji.
  - Wyjaśnienie w jaki sposób implementacje IAM muszą chronić zasoby fizyczne i logiczne.
  - Rola poświadczeń i magazynu tożsamości w systemach IAM.
- Architektura i inżynieria bezpieczeństwa
  - Główne elementy standardów inżynierii bezpieczeństwa.
  - Główne modele architektury bezpieczeństwa informacji.
  - Możliwości zabezpieczeń zaimplementowane w sprzęcie i oprogramowaniu sprzętowym.
  - Stosowanie odpowiednich zasad bezpieczeństwa w przypadku różnej architektury systemów informatycznych i ich środowisk.
  - Określanie najlepszego podejścia do procesów kryptograficznych w celu zaspokojenia potrzeb organizacji w zakresie bezpieczeństwa informacji.
  - Zarządzanie wykorzystaniem certyfikatów i podpisów elektronicznych w celu spełnienia potrzeb organizacji w zakresie bezpieczeństwa informacji.
  - Możliwe konsekwencje braku zastosowania technik kryptograficznych do ochrony łańcucha dostaw.
  - Zastosowanie różnych rozwiązań do zarządzania kryptografią, aby spełnić potrzeby organizacji w zakresie bezpieczeństwa informacji.
  - Weryfikacja czy rozwiązania kryptograficzne działają i odpowiadają na zmieniające się zagrożenia w świecie rzeczywistym.
  - Opis mechanizmów obronnych przed typowymi atakami kryptograficznymi.
- Komunikacja i bezpieczeństwo sieci
  - Charakterystyka architektury, stosowane technologie, protokoły i kwestie bezpieczeństwa każdej z warstw modelu OSI.

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

- Zastosowanie bezpiecznych praktyk projektowych w rozwoju infrastruktury sieciowej.
- Ewolucja metod zabezpieczania protokołów komunikacyjnych IP.
- Implikacje dla bezpieczeństwa wynikające ze stosowania przewodowych i bezprzewodowych środowisk sieciowych.
- Ewolucja i rozwój kluczowych urządzeń sieciowych i ich wpływ na bezpieczeństwo.
- Porównanie i ocena bezpieczeństwa związanego z komunikacją głosową w infrastrukturze tradycyjnej oraz VoIP.
- Porównanie i ocena bezpieczeństwa dla kluczowych technologii zdalnego dostępu.
- Implikacje dla bezpieczeństwa wynikające ze stosowania rozwiązań software-defined networking (SDN) i technologii wirtualizacji sieci.

- Bezpieczeństwo procesu wytwarzania oprogramowania
  - Rozpoznanie elementów oprogramowania, które mogą zagrażać bezpieczeństwu systemów informatycznych.
  - Identyfikacja i zobrazowanie głównych przyczyny występowania luk bezpieczeństwa w kodzie źródłowym.
  - Zobrazowanie głównych przyczyny występowania luk bezpieczeństwa w systemach baz danych i hurtowniach danych.
  - Stosowanie OWASP framework przy ocenie bezpieczeństwa różnorodnych aplikacji internetowych.
  - Wybór strategii łagodzenia skutków działania szkodliwego oprogramowania właściwej do potrzeb danej organizacji w zakresie jej polityki bezpieczeństwa informacji.
  - Porównanie sposobów w jakie różne metodyki wytworzenia oprogramowania, ramy i wytyczne, przyczyniają się do bezpieczeństwa systemów.
  - Wdrażanie kontroli bezpieczeństwa dla ekosystemów programistycznych.
  - Wybór właściwej kombinacji stosowanych testów bezpieczeństwa, oceny, kontroli i metod zarządzania bezpieczeństwem dla różnych systemów i środowisk aplikacji.
- Ocena i testowanie bezpieczeństwa
  - Procesy i cele formalnej i nieformalnej oceny w testowaniu bezpieczeństwa organizacji.
  - Etyka zawodowa i organizacyjna w procesie oceny i testowania bezpieczeństwa.
  - Ocena i testowanie bezpieczeństwa wykonywane wewnętrznie, zewnętrznie i przez strony trzecie.
  - Kwestie związane z planowaniem i zarządzaniem przeprowadzaną oceną bezpieczeństwa.
  - Rola oceny ryzyka w podejmowaniu decyzji dotyczących bezpieczeństwa w oparciu o dane.
- Monitorowanie bezpieczeństwa
  - Wydajnie i skuteczne sposoby gromadzenia i oceny danych dotyczących bezpieczeństwa.
  - Korzyści dla bezpieczeństwa wynikające ze skutecznego zarządzania zmianami i kontroli zmian w organizacji.
  - Zasady i plany reagowania na incydenty.
  - Połączenie reakcji na incydenty z potrzebami w zakresie kontroli bezpieczeństwa i ich

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

wykorzystania operacyjnego.
    - Powiązanie środków kontroli bezpieczeństwa z poprawą i osiągnięciem wymaganej dostępności zasobów i systemów informacyjnych.
    - Bezpieczeństwo i konsekwencje związane z bezpieczeństwem dla różnych obiektów, systemów i infrastruktury.
- Łącząc wszystko razem
    - Wyjaśnienie, w jaki sposób ramy i procesy zarządzania odnoszą się do operacyjnego wykorzystania kontroli bezpieczeństwa informacji.
    - Powiązanie procesów prowadzenia dochodzeń informatyki śledczej z operacjami związanymi z bezpieczeństwem informacji.
    - Powiązanie ciągłość biznesowej i gotowość do odzyskiwania zasobów po awarii z operacjami związanymi z bezpieczeństwem informacji.
    - Wyjaśnienie, jak wykorzystać edukację, szkolenia, świadomość i zaangażowanie wszystkich członków organizacji jako sposobu na wzmocnienie i egzekwowanie procesów bezpieczeństwa informacji.
    - Systemy informatyczne, a zarządzanie ryzykiem w łańcuchu dostaw IT.

Wymagania:

Kandydaci do tytułu CISSP muszą posiadać łącznie co najmniej pięć lat doświadczenia zawodowego zdobytego w płatnej pracy w zakresie co najmniej dwóch z ośmiu niżej wymienionych obszarów wiedzy CISSP CBK (CISSP Common Body of Knowledge). Ukończone 4-letnie studia (posiadanie dyplomu) lub ich regionalnego odpowiednika lub posiadanie dodatkowego poświadczenia z zatwierdzonej listy ISC2 mogą być ekwiwalentem dla jednego rok wymaganego doświadczenia. Z pomocą poświadczeń edukacyjnych można zastąpić maksymalnie tylko jeden rok wymaganego doświadczenia.

Kandydat, który nie ma aktualnie wymaganego doświadczenia, aby zostać CISSP, może zostać Associate of ISC2 po pomyślnym zdaniu egzaminu CISSP. Associate of ISC2 będzie miał wówczas sześć lat na zdobycie wymaganego pięcioletniego doświadczenia.

Wymagane doświadczenie zawodowe musi mieścić się w dwóch lub więcej z ośmiu domen ISC2 CISSP CBK:

- Domain 1. Security and Risk Management
- Domain 2. Asset Security
- Domain 3. Security Architecture and Engineering
- Domain 4. Communication and Network Security
- Domain 5. Identity and Access Management (IAM)
- Domain 6. Security Assessment and Testing
- Domain 7. Security Operations
- Domain 8. Software Development Security

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

Więcej informacji https://www.isc2.org/Certifications/CISSP/experience-requirements

Poziom trudności

Certyfikaty:

Uczestnicy szkolenia otrzymują certyfikat ukończenia szkolenia sygnowany przez ISC2 (ukończenie szkolenia).

Aby otrzymać certyfikat ukończenia szkolenia i zdobyć punkty kształcenia zawodowego ISC2 (Continuing Professional Education (CPE)), uczestnicy muszą:

- Ukończ wszystkie zajęcia edukacyjne w ramach kursu
- Wypełnić ankietę poszkoleniową
- Uzyskać wynik 70% lub wyższy podczas końcowego testu sprawdzającego

Certyfikat ukończenia zostanie dostarczony przez instruktora po ukończeniu kursu i spełnieniu wszystkich wymagań. Prosimy zachować świadectwo ukończenia jako dowód zdobytych punktów CPE.

Ponadto kurs ten przygotowuje uczestników do **egzaminu certyfikacyjnego** prowadzącego do uzyskania tytuły **CISSP (Certified Information Systems Security Professional)**, który jest realizowany za pośrednictwem centrów testowych **Pearson VUE**.

This course will help prepare you also for the CISSP certification exam available at Pearson VUE test centers.

Każdy uczestnik autoryzowanego szkolenia ISC2 CISSP Certification Prep Course realizowanego w Compendium CE, otrzymuje darmowy voucher egzaminacyjny CISSP Certification Exam.

Prowadzący:

Autoryzowany instruktor ISC2

Informacje dodatkowe:

Uczestnicząc w tym szkoleniu otrzymujesz 40 punktów CPE (Continuing Professional Education).

Punkty CPE zdobyte podczas szkolenia należy zagościć samodzielnie za pośrednictwem portalu ISC2 CPE Portal dostępnego pod adresem www.isc2.org logując się za pomocą swoich danych członkowskich ISC2.

Punkty CPE zdobyte podczas tego szkolenia mogą również kwalifikować się jako punkty kontynuacji kształcenia zawodowego CPE w innych programach certyfikacyjnych niż tych od ISC2. Aby skorzystać

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70
BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001

z tej możliwości należy zapoznaj się z wymaganiami dotyczącymi kontynuacji kształcenia zawodowego ustanowionymi przez inne organizację których certyfikacje posiada uczestnik.

W przypadku konkretnych pytań związanych z punktami CPE lub portalem CPE należy skontaktować się z działem wsparcia dla członków społeczności ISC2 - membersupport@isc2.org

Autoryzowane szkolenie ISC2 CISSP Certification Prep Course pozwala zdobyć również ACE CREDIT. Jest to ważne dla studentów amerykańskich uniwersytetów i uczelni. Więcej informacji https://www.acenet.edu/national-guide/Pages/default.aspx

Compendium Centrum Edukacyjne Spółka z o.o.
ul. Tatarska 5, 30-103 Kraków, tel.: (12) 298 47 77
ul. Bielska 17, 02-394 Warszawa, tel.: (22) 417 41 70

BNP Paribas Bank Polska S.A.
Oddział w Warszawie
Nr konta: PL 20 1600 1462 1853 6451 3000 0001