Publicatiedatum : 25/02/2026

Opleiding : CISSP (Certified Information Systems Security Professional), voorbereiding op ISC2-certificering

Officiële ISC2-opleiding

Praktijkcursus - 5d - 35u00 - Ref. CIQ

Prijs : 4250 € V.B.

NEW

Deze cursus behandelt de volledige Common Body of Knowledge (CBK) gedefinieerd door ISC2 en bereidt je voor op het CISSP examen, de internationale standaard in de beveiliging van informatiesystemen.

Pedagogische doelstellingen

Aan het einde van de training is de deelnemer in staat om:

- Een wereldwijd informatiebeveiligingsprogramma ontwerpen en beheren dat is afgestemd op de bedrijfsdoelstellingen
- Cyberrisico's in een complexe organisatorische context identificeren, analyseren, beoordelen en aanpakken
- Beveiligingsbeheer definiëren en implementeren dat is geïntegreerd in de strategie van de organisatie
- Veiligheidscontroles selecteren en implementeren die zijn aangepast aan de operationele en wettelijke vereisten
- Toezicht houden op beveiligingsactiviteiten, incidentbeheer en bedrijfscontinuïteit
- Beveiliging integreren in IT-architecturen, netwerken en softwareontwikkelcycli
- De "manager/beslisser" redenering aan te nemen die door ISC2 wordt verwacht om te slagen voor het CISSP examen

Doelgroep

Managers, directeuren, architecten, ingenieurs, analisten, auditors en consultants die betrokken zijn bij de beveiliging van informatiesystemen en netwerkinfrastructuren. hier

DEELNEMERS

Managers, directeuren, architecten, ingenieurs, analisten, auditors en consultants die betrokken zijn bij de beveiliging van informatiesystemen en netwerkinfrastructuren. hier

VOORAFGAANDE VEREISTEN

Ten minste vijf jaar cumulatieve beroepservaring in ten minste twee van de acht gebieden van de ISC2 CISSP examensyllabus.

VAARDIGHEDEN VAN DE CURSUSLEIDER

De deskundigen die de cursus leiden zijn specialisten op het betreffende vakgebied. Zij werden geselecteerd door onze pedagogische teams zowel om hun vakkennis als hun pedagogische vaardigheden voor elke cursus die zij geven. Zij hebben minstens vijf tot tien jaar ervaring in hun vakgebied en oefenen of oefenden verantwoordelijke bedrijfsfuncties uit.

BEOORDELINGSMODALITEITEN

De cursusleider beoordeelt de pedagogische vooruitgang van de deelnemer gedurende de gehele cursus aan de hand van meerkeuzevragen, praktijksituaties, praktische opdrachten, ...
De deelnemer legt ook van tevoren en naderhand een test af ter bevestiging van de verworven kennis.

Voorafgaande vereisten

Ten minste vijf jaar cumulatieve beroepservaring in ten minste twee van de acht gebieden van de ISC2 CISSP examensyllabus.

Praktische modaliteiten

Voer hier de praktijkbeschrijving in

Opleidingsprogramma

1 Gebied 1: veiligheid en risicobeheer

- Beroepsethiek en SAI-gedragscode2.
- Fundamentele principes van informatiebeveiliging.
- Beveiligingsbeheer en organisatorische rollen.
- Naleving van regelgeving en wettelijke kaders.
- Juridische, regelgevende en contractuele kwesties.
- Soorten onderzoeken en bijbehorende processen.
- Veiligheidsbeleid, -normen, -procedures en -richtlijnen.
- Bedrijfscontinuïteit en bedrijfsimpactanalyse (BIA).
- Personeelsveiligheid.
- Risicobeheer: identificatie, analyse, behandeling.
- Dreigingsmodellering.
- Risicobeheer van de toeleveringsketen.
- Bewustzijn, training en veiligheidscultuur.

2 Gebied 2: Activabeveiliging

- Identificatie en classificatie van activa.
- Eigendom en verantwoordelijkheid voor informatie.
- Vereisten voor gegevensbescherming.
- Beheer van gegevenslevenscyclus.
- Veilige opslag, archivering en vernietiging.
- Beveiligingscontroles en naleving van gegevens.

3 Gebied 3: Beveiligingsarchitectuur en -techniek

- Principes van veilig ontwerp en engineering.
- Veiligheidsmodus en fundamentele concepten.
- Selectie van systeembeveiligingscontroles.
- Beveiliging van hardware- en softwarecomponenten.
- Kwetsbaarheid van architecturen en ontwerpen.
- Cryptografie: principes, gebruik en beheer.
- Bedreigingen en cryptografische aanvallen.
- Fysieke beveiliging van locaties en infrastructuren.

4 Gebied 4: communicatie- en netwerkbeveiliging

- Principes van veilig netwerkontwerp.
- Netwerkapparatuur en -infrastructuur beveiligen.
- Segmentatie, isolatie en verdediging in de diepte.
- Veilige communicatiekanalen.

PEDAGOGISCHE EN TECHNISCHE MIDDELEN

• De gebruikte pedagogische middelen en cursusmethoden zijn voornamelijk: audiovisuele hulpmiddelen, documentatie en cursusmateriaal, praktische oefeningen en correcties van de oefeningen voor praktijkstages, casestudies of reële voorbeelden voor de seminars.
• Na afloop van de stages of seminars verstrekt ORSYS de deelnemers een evaluatievragenlijst over de cursus die vervolgens door onze pedagogische teams wordt geanalyseerd.
• Na afloop van de cursus wordt een presentielijst per halve dag verstrekt, evenals een verklaring van de afronding van de cursus indien de stagiair alle sessies heeft bijgewoond.

TOEGANGSMODALITEITEN EN TERMIJNEN

De inschrijving dient 24 uur voor aanvang van de cursus plaatsgevonden te hebben.

TOEGANKELIJKHEID VOOR MINDERVALIDEN

Is voor u speciale toegankelijkheid vereist? Neem contact op met mevr. FOSSE, contactpersoon voor mindervaliden, via het adres psh-accueil@ORSYS.fr om uw verzoek en de haalbaarheid daarvan zo goed mogelijk te bestuderen.

5 Gebied 5: Identiteits- en toegangsbeheer (IAM)

- Fysieke en logische toegangscontrole.
- Identificatie en authenticatie.
- Identiteitsfederaties en diensten van derden.
- Autorisatie en rechtenbeheer.
- Levenscyclus van identiteit en toegang.
- Authenticatiemechanismen.

6 Gebied 6: Beveiligingsbeoordeling en -testen

- Strategieën voor beveiligingstests en -audits.
- Technische en organisatorische tests.
- Resultaten verzamelen en analyseren.
- Veiligheidsrapporten opstellen.
- Interne en externe audits.

7 Gebied 7: Veiligheidsactiviteiten

- Onderzoeken en enquêtes.
- Registratie en bewaking.
- Configuratiebeheer.
- Dagelijkse veiligheidsactiviteiten.
- Hulpbronnen beschermen.
- Beheer van beveiligingsincidenten.
- Detectie en preventie.
- Beheer van kwetsbaarheden en patches.
- Veranderingsbeheer.
- Bedrijfscontinuïteit en noodherstel.
- Fysieke en omgevingsveiligheid.
- Veiligheid van personeel.

8 CISSP examenvoorbereiding

- Presentatie van het CISSP (CAT) examen.
- Methodologie voor het beantwoorden van vragen.
- Tijdmanagement en veelvoorkomende valkuilen.
- Quiz en examenvragen.
- Advies van CISSP-gecertificeerde experts.

Opties

: 750 € HT

Het officiële examen vindt plaats in het Engels, zowel online als offline, in de vorm van een 3 uur durende MCQ, bestaande uit 100 tot 150 vragen, met een minimumscore van 700/1000.

Data en plaats

KLAS OP AFSTAND
2026 : 15 juni, 31 aug., 2 nov.

PARIS LA DÉFENSE
2026 : 15 juni, 31 aug., 2 nov.