CISSP, IS-beveiliging, voorbereiding op certificering

Praktijkcursus van 5 dagen - 35u
Ref : CIS - Prijs 2024 : € 3 690 excl. BTW

Deze cursus beschrijft de beveiligingsconcepten die nodig zijn voor het behalen van de CISSP certificering. De cursus bereidt u voor op het examen door de volledige Common Body of Knowledge (CBK) te behandelen, de kernkennis op het gebied van beveiliging zoals gedefinieerd door het International Information Systems Security Certification Consortium (ISC)².

PEDAGOGISCHE DOELSTELLINGEN

Na afloop van de opleiding kan de cursist:

Kennis van de Common Body of Knowledge van IT-beveiliging

Een globale visie ontwikkelen op IT-beveiligingsproblemen

Verdiep uw kennis van de acht CISSP-domeinen

Voorbereiding op het CISSP certificeringsexamen

CERTIFICERING

Om de certificering te behalen, moet u u registreren op de ISC2 website en een aanvraag indienen.

HET PROGRAMMA

laatste update: 10/2021

1) IS-beveiliging en de (ISC)² CBK

- Beveiliging van informatiesystemen.
- Waarom CISSP certificering?
- Presentatie van de reikwijdte van het CBK.

2) Veiligheidsbeheer en operationele veiligheid

- Praktijken voor veiligheidsbeheer. Opstellen van veiligheidsbeleid, richtlijnen, procedures en normen.
- Het programma voor veiligheidsbewustzijn, managementpraktijken, risicobeheer, enz.
- Operationele veiligheid: preventieve, detectie- en correctiemaatregelen, rollen en verantwoordelijkheden van alle betrokkenen.
- Beste praktijken, veiligheid bij het aannemen van personeel, enz.

3) Architectuur, beveiligingsmodellen en toegangscontrole

- Beveiligingsarchitectuur en -modellen: systeemarchitectuur, theoretische modellen van informatiebeveiliging.
- Methoden voor het beoordelen van systemen, operationele veiligheidsmodi, enz.
- Toegangscontrolesystemen en -methodologieën. Categorieën en soorten toegangscontrole.
- Toegang tot gegevens en systemen, inbraakpreventiesystemen (IPS) en inbraakdetectiesystemen (IDS).
- Auditlogs, bedreigingen en aanvallen met betrekking tot toegangscontrole, enz.

4) Cryptografie en ontwikkelingsbeveiliging

- Cryptografie. Concepten, symmetrische en asymmetrische cryptografie.
- Hashfuncties, openbare sleutelinfrastructuur, enz.
- Beveiliging van applicatie- en systeemontwikkeling. Databases en datawarehouses.

DEELNEMERS

IB-beveiligingsmanagers of andere personen met een rol in het IB-beveiligingsbeleid.

VOORAFGAANDE VEREISTEN

Basiskennis van netwerken en besturingssystemen en informatiebeveiliging. Basiskennis van audit- en bedrijfscontinuïteitsnormen.

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.

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.

- De ontwikkelcyclus, objectgeoriënteerd programmeren, expertsystemen, kunstmatige intelligentie, enz.

5) Telecom- en netwerkbeveiliging

- Netwerk- en telecombeveiliging. Basisbegrippen, TCP/IP-model, netwerk- en beveiligingsapparatuur.
- Beveiligingsprotocollen, aanvallen op netwerken, gegevensback-up, draadloze technologieën, VPN...

6) Bedrijfscontinuïteit, wetgeving, ethiek en fysieke beveiliging

- Planning van bedrijfscontinuïteit en noodherstel.
- Bedrijfscontinuïteitsplan, rampherstelplan.
- Noodmaatregelen, trainings- en bewustwordingsprogramma, crisiscommunicatie, oefeningen en tests.
- Recht, onderzoek en ethiek: burgerlijk, straf- en bestuursrecht, intellectueel eigendom.
- Het rechtskader voor onderzoeken, regels voor de toelaatbaarheid van bewijs, enz.
- Fysieke beveiliging. Bedreigingen en kwetsbaarheden gekoppeld aan de omgeving van een locatie, beveiligingsperimeter.
- Vereisten voor lay-out, bewaking van het terrein, bescherming van personeel, enz.

DATA

KLAS OP AFSTAND
2024 : 10 jun, 02 sep, 16 dec

BRUSSEL
2024 : 10 jun, 02 sep, 16 dec