

Opleiding : Chief Information Security Officer (CISO), PECB-certificering

Praktijkcursus - 5d - 35u00 - Ref. CSO

Prijs : 3810 € V.B.

★★★★☆ 4,6 / 5

Deze cursus geeft je de vaardigheden die je nodig hebt om informatiebeveiliging te overzien en te beheren, waarbij je zorgt voor de implementatie van robuuste beveiligingsmaatregelen, de identificatie en beperking van risico's voor informatiebeveiliging en de ontwikkeling van beveiligingsstrategieën die zijn afgestemd op de specifieke behoeften van de organisatie.

Pedagogische doelstellingen

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

- ✓ De fundamentele principes en concepten van informatiebeveiliging uitleggen
- ✓ De rollen en verantwoordelijkheden van de CISO en de bijbehorende ethische overwegingen begrijpen
- ✓ Een effectief informatiebeveiligingsprogramma ontwerpen en ontwikkelen dat is afgestemd op de behoeften van de organisatie
- ✓ Toepasselijke kaders en wet- en regelgeving aannemen
- ✓ Effectief beleid communiceren en implementeren om naleving van informatiebeveiliging te garanderen
- ✓ Informatiebeveiligingsrisico's identificeren, analyseren, beoordelen en aanpakken

Doelgroep

Professionals die betrokken zijn bij het beheer van informatiebeveiliging, IT-managers, analisten, beveiligingsauditors, CIO's, CEO's en COO's.

Voorafgaande vereisten

Inzicht in de fundamentele principes en concepten van informatiebeveiliging.

DEELNEMERS

Professionals die betrokken zijn bij het beheer van informatiebeveiliging, IT-managers, analisten, beveiligingsauditors, CIO's, CEO's en COO's.

VOORAFGAANDE VEREISTEN

Inzicht in de fundamentele principes en concepten van informatiebeveiliging.

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.

Certificatie

L'examen consiste à répondre à 80 questions, en 3h00 à livre ouvert. À l'issue du cours, une attestation de suivi de la formation de 31 crédits de FPC (Formation professionnelle continue) sera délivrée. Les candidats ayant suivi la formation mais échoué à l'examen peuvent le repasser gratuitement une seule fois dans un délai de 12 mois à compter de la date initiale de l'examen. L'examen se passe en distanciel et différé.

Overgang naar certificaties op afstand

[Raadpleeg de officiële documentatie van de certificerende instantie](#) om de voorafgaande vereisten voor het afleggen van het online certificatie-examen te raadplegen.

Opleidingsprogramma

1 Grondbeginselen van informatiebeveiliging en de rol van een CISO

- Doelstellingen en structuur van de cursus.
- Grondbeginselen van informatiebeveiliging.
- Beveiligingsmanager informatiesysteem (ISSM).
- Programma voor informatiebeveiliging.

2 Beveiliging, risicobeheer, beveiligingsarchitectuur en -ontwerp

- Nalevingsprogramma voor informatiebeveiliging.
- Analyse van bestaande informatiebeveiligingscapaciteiten.
- Risicobeheer van informatiebeveiliging.
- Beveiligingsontwerp en -architectuur.

3 Beveiligingsmaatregelen, incidentbeheer en wijzigingsbeheer

- Informatiebeveiligingsmaatregelen.
- Beheer van informatiebeveiligingsincidenten.
- Veranderingsbeheer.

4 Informatiebeveiligingsbewustzijn, bewaking en meting, voortdurende verbetering

- Bewustwordings- en trainingsprogramma's.
- Monitoren en meten.
- Garantieprogramma.
- Voortdurende verbetering.

5 Competentiegebieden die onder het examen vallen

- Domein 1: Fundamentele concepten van informatiebeveiliging.
- Domein 2: de rol van de CISO in een informatiebeveiligingsprogramma.
- Domein 3: het selecteren van een beveiligingscomplianceprogramma, risicomanagement, architectuur en ontwerp.
- Gebied 4: Informatiebeveiligingsmaatregelen, incidentbeheer en wijzigingsbeheer.
- Gebied 5: Bevordering van een cultuur van informatiebeveiliging, bewaking en verbetering van een beveiligingsprogramma.

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.

Data en plaats

KLAS OP AFSTAND

2026 : 13 apr., 22 juni, 5 okt., 14 dec.

PARIS LA DÉFENSE

2026 : 30 maa., 15 juni, 28 sep., 7 dec.