Cyberbeveiliging, ISO 27032, certificering

Praktijkcursus van 5 dagen - 35u
Ref : CYB - Prijs 2024 : € 3 990 excl. BTW

Met deze intensieve opleiding kunt u zich de kennis en vaardigheden eigen maken die nodig zijn voor de implementatie en het beheer van een cyberbeveiligingsprogramma op basis van de ISO 27032-norm. U kunt via de opleiding de ISO 27032-certificering behalen.

PEDAGOGISCHE DOELSTELLINGEN

Na afloop van de opleiding kan de cursist:

De onderdelen en de werking kennen van een cyberbeveiligingsprogramma in overeenstemming met de ISO 27032-norm

De doelstelling, de inhoud en de correlatie tussen ISO 27032 en andere normen en raamwerken uitleggen

De concepten, methoden, normen en technieken voor het beheer van een cyberbeveiligingsprogramma onder de knie krijgen

Een cyberbeveiligingsprogramma beheren, zoals wordt gespecificeerd in de ISO 27032-norm

PEDAGOGISCHE METHODEN

Theoretische cursus, ondersteund door een met concrete voorbeelden geïllustreerde presentatie die wordt afgewisseld met besprekingen, vragen en uitwisselingen over theorie en praktijk.

CASE STUDY

Ontleding van een aanval op een internationaal telecommunicatiebedrijf. Oefeningen om afwijkingen te identificeren, en de kernconcepten te bewerken.

CERTIFICERING

De PECB-certificering “Certified ISO 27032 Lead Cybersecurity Manager” wordt behaald door te slagen voor het certificeringsexamen.

DEELNEMERS

Cyberbeveiligingsprofessionals, informatiebeveiligingsexperts, projectleiders en IT-beveiligingsconsultants.

VOORAFGAANDE VEREISTEN

Kennis 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.

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.

HET PROGRAMMA

laatste update: 10/2021

1) Cyberbeveiligingsconcepten en de ISO 27032-norm

- Doelstellingen en structuur van de cursus.
- Regelgevend en normatief kader.
- Definitie van de basisconcepten van cyberbeveiliging.
- Planning van een cyberbeveiligingsprogramma.

2) Een cyberbeveiligingsprogramma initiëren

- Organisatiestructuur.
- De rollen en verantwoordelijkheden van belanghebbenden op het gebied van cyberbeveiliging bepalen.
- Beleid en principes voor cyberbeveiliging vaststellen.
- Beheer van cyberbeveiligingsrisico's binnen het bedrijfsrisicobeheer.
- Beoordeling van cyberbeveiligingsrisico's.

3) Een cyberbeveiligingsprogramma implementeren

- Implementatie van een kader voor documentenbeheer.
- Informatie delen en coördinatie van de hoofdrolspelers.
- Ontwikkeling van een opleidings- en sensibiliseringsprogramma voor personeel en hoofdrolspelers.
- Implementatie van specifieke cyberbeveiligingscontroles.

- Beheer van cyberbeveiligingsincidenten en integratie ervan in het routinematige incidentenbeheer.
- Bedrijfscontinuïteitsbeheer.

4) Evaluatie van de prestaties van het cyberbeveiligingsprogramma

- Bepaling van het rendement van ondernomen acties.
- Zelfevaluatie van controles.
- Implementatie van een verzekeringsomgeving.
- Evaluatie van het niveau van paraatheid voor cyberdreigingen.
- Adequate implementatie van voortdurende verbetering.
- Meting van de mate van integratie van cyberbeveiligingscontroles in de informatiebeveiligingscontroles.
- Voorstelling van het PECB-certificeringssysteem.

5) Het certificeringsexamen afleggen

- Gebied 1: cyberbeveiligingsbasisconcepten.
- Gebied 2: gids voor het starten, implementeren en beheren van een cyberbeveiligingsprogramma.
- Gebied 3: richtlijnen voor de rollen en verantwoordelijkheden van belanghebbenden op het gebied van cyberbeveiliging.
- Gebied 4: beheer van cyberbeveiligingsrisico's.
- Gebied 5: controle van activiteiten die verband houden met het cyberbeveiligingsprogramma.

Examen op papier dat uit 12 open vragen bestaat, en binnen de 3 u in het Frans dient te worden afgelegd. "Open boek"-formaat (toegestaan met ondersteuning en tijdens de sessie gemaakte persoonlijke aantekeningen).

DATA

KLAS OP AFSTAND
2024 : 02 sep, 25 nov

BRUSSEL
2024 : 02 sep, 25 nov