Publicatiedatum : 14/10/2024

Opleiding : DORA (Digital Operational Resilience Act), implementatie van een digitale veerkrachtstrategie

seminarie - 2d - 14u00 - Ref. DRA
Prijs : 1810 € V.B.

4,3 / 5

Het DORA-kader is een Europees regelgevingskader dat is ontworpen om de operationele weerbaarheid van financiële entiteiten tegen IT- en cyberbeveiligingsrisico's te versterken. Het stelt strenge eisen aan IT-risicobeheer, cyberbeveiligingstests, incidentbeheer en veerkracht van kritieke infrastructuur. Door de normen in de hele EU te harmoniseren, zorgt DORA voor een betere bescherming tegen cyberdreigingen, waardoor de verstoring van de financiële dienstverlening wordt beperkt en het digitale vertrouwen wordt versterkt.

Pedagogische doelstellingen

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

- De belangrijkste doelstellingen en begrippen van de DORA-verordening begrijpen
- De verschillende soorten cyberrisico's begrijpen
- Gegevensbeveiliging en wettelijke nalevingsverplichtingen identificeren
- Leer meer over goede digitale beveiligingspraktijken en verhoog het bewustzijn onder werknemers
- Een digitale veerkrachtstrategie opzetten en implementeren

Doelgroep

ISSM's en beveiligingsadviseurs, beveiligingsarchitecten, IT-directeuren en -managers, IT-ingenieurs, projectmanagers, beveiligingsauditors en juristen op het gebied van IT-regelgeving.

Voorafgaande vereisten

Basiskennis van cyberbeveiliging en beveiliging van informatiesystemen.

Opleidingsprogramma

DEELNEMERS

ISSM's en beveiligingsadviseurs, beveiligingsarchitecten, IT-directeuren en -managers, IT-ingenieurs, projectmanagers, beveiligingsauditors en juristen op het gebied van IT-regelgeving.

VOORAFGAANDE VEREISTEN

Basiskennis van cyberbeveiliging en beveiliging van informatiesystemen.

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.

1 Risicobeheer van informatie- en communicatietechnologie (ICT)

- DORA-bepalingen die de noodzaak herhalen om een ICT-risicobeheersysteem te implementeren.
- Basisprincipes en vereisten voor risicobeheer in financiële entiteiten.
- Verplichtingen met betrekking tot het ICT-raamwerk voor risicobeheer.

2 Beheer, classificatie en rapportage van ICT-incidenten

- Bepalingen van de DORA-verordening gericht op het harmoniseren en rationaliseren van het melden van ICT-incidenten.
- Classificatie en rapportage van ICT-incidenten.
- Kennisgeving aan de bevoegde ESA (Europese toezichthoudende autoriteiten) van grote ICT-gerelateerde incidenten.
- Vrijwillige melding van grote cyberdreigingen aan autoriteiten zoals EBA, EIOPA en ESMA.

3 Testen van digitale operationele veerkracht

- Digitale operationele veerkrachttesten op de meest kritieke onderdelen van hun informatiesystemen.
- Geavanceerde tests op basis van TLPT (Threat-Led Penetration Testing).
- Grootschalige live tests van bedreigingen, uitgevoerd door onafhankelijke testinstanties.

4 De risico's van externe dienstverleners beheren

- Principes voor het beheren van risico's van derden als onderdeel van ICT-risicobeheer.
- Bepalingen waarmee rekening moet worden gehouden in de relatie met externe dienstverleners die ICT-diensten leveren.
- Europawijd toezichtskader voor kritische externe ICT-dienstverleners.

5 Bepalingen betreffende de uitwisseling van informatie

- De digitale operationele weerbaarheid van financiële entiteiten versterken.
- Vrijwillige uitwisseling van informatie en inlichtingen over cyberdreigingen tussen verschillende financiële entiteiten.

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 : 17 maa., 28 mei, 13 okt., 26 nov.

PARIS LA DÉFENSE
2026 : 10 maa., 21 mei, 6 okt., 19 nov.