Publicatiedatum : 17/06/2024

Opleiding : IS-beveiliging, praktische uitvoering van een risicoanalyse

Praktijkcursus - 2d - 14u00 - Ref. CUR
Prijs : 1480 € V.B.

4,5 / 5

In deze cursus leer je hoe je bedreigingen en risico's voor je informatiesysteem en hun mogelijke impact op je bedrijf kunt identificeren en analyseren. Je werkt aan een casestudy "fil rouge" waarin je de belangrijkste stappen van een risicoanalyse leert beheersen.

Pedagogische doelstellingen

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

- De bedreigingen en risico's voor een IS identificeren en analyseren
- Inzicht in de fundamentele concepten van risicoanalyse voor de beveiliging van IS
- Kennis van de beschikbare analysemethoden om IS-risico's te beheersen
- Risico's identificeren en prioriteren met behulp van een risicomatrix
- De inhoud van een risicomanagementplan begrijpen

Doelgroep

CIO of hoofd van IT-afdeling. ISSM (Information System Security Manager). IT-projectmanager die de leiding heeft over het beveiligingsproject.

Voorafgaande vereisten

Basiskennis van de beveiliging van informatiesystemen.

DEELNEMERS

CIO of hoofd van IT-afdeling. ISSM (Information System Security Manager). IT-projectmanager die de leiding heeft over het beveiligingsproject.

VOORAFGAANDE VEREISTEN

Basiskennis van de 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.

Praktische modaliteiten

Casestudy

Een casestudy zal als rode draad door de twee dagen lopen en de hele praktische risicoanalysemethode behandelen.

Leer methodes

Afwisselend theorie, voorbeelden en praktische oefeningen uitgevoerd door de deelnemers op basis van de casestudy aan het einde van elk thema.

Opleidingsprogramma

1 Het begrip risico in informatiebeveiliging

- Waarschijnlijkheid en waarschijnlijkheid.
- Impact op de IB en op het bedrijf.
- De mate van ernst kwantificeren.
- Soorten risico's.
- Risicogebaseerd management. De principes. De voordelen.

Praktisch werk

Vragenlijst over IB-risico's en risicomanagement.

2 Informatie-assets identificeren

- Inventariseer de activa: informatie en de media (primair, secundair).
- De organisatie, de reikwijdte.
- DICT-classificatie.
- Rente en methode.

Casestudy

Inventarisatie en classificatie van informatie en informatiedragers.

3 Risicoanalyse

- Identificatie van bedreigingen en kwetsbaarheden.
- Risicobeoordeling.
- Prioritering: de risicomatrix, het begrip scenario.

Praktisch werk

Risico's identificeren en prioriteren met behulp van de matrix.

4 Nuttige methoden

- Franse methoden: EBIOS, MEHARI.
- Internationale methoden: OCTAVE.
- De voordelen, voor- en nadelen van elke methode.
- Adequate keuze van methode en personalisatie.

Praktisch werk

Groepsdiscussie over de keuzecriteria en de voor- en nadelen van de verschillende methoden.

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 Normen

- De verschillende standaarden die worden gebruikt voor risicoanalyse.
- De 27001-benadering voor risicoanalyse.
- De PDCA-aanpak (Plan - Do - Check - Act).
- De bijdragen van ISO 27002, BS25999 en ISO 31000.

Praktisch werk
Voorbeelden van de toepassing van een standaard.

6 Een risicobeheerplan opstellen

- Het scala aan acties: preventie, bescherming, risico-overdracht, uitbesteding, verzekering.
- Een risicomanagementplan opstellen op basis van de risicomatrix en andere bronnen (audits, enz.).
- Wat het plan bevat: doelstellingen en maatregelen, voortgangs- en kwaliteitsindicatoren.
- Restrisico's.
- Beheer en gebruik van het risicomanagementplan.

Casestudy
Een risicomanagementplan opstellen.

Data en plaats

KLAS OP AFSTAND
2026 : 21 mei, 8 okt., 17 dec.

PARIS LA DÉFENSE
2026 : 21 mei, 8 okt., 17 dec.