Publicatiedatum : 05/03/2025

Opleiding : ISO 27005:2022 Risicobeheer, voorbereiding en LSTI-certificering

Praktijkcursus - 3d - 21u00 - Ref. RMG
Prijs : 2290 € V.B.

4,2 / 5

BEST

Na afronding van de cursus zijn studenten in staat om risico's voor informatiebeveiliging te beoordelen en te beheren, met het oog op het definiëren en implementeren van passend beleid en passende procedures. Ze zijn ook in staat om de certificering "Risk Manager ISO 27005" te behalen die gekoppeld is aan risicomanagement als onderdeel van een ISMS.

Pedagogische doelstellingen

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

- De vereisten van ISO 27005 voor risicobeheer van informatiebeveiliging begrijpen
- Een risicobeoordeling beheren als onderdeel van een ISMS
- Een ISO 27005-conform risicobeheerproces opzetten
- Voorbereiden op en succesvol afronden van de ISO 27005-certificering voor risicobeheerders

Doelgroep

Projectmanagers, consultants, technische architecten, IS security managers, iedereen die verantwoordelijk is voor informatiebeveiliging, compliance en risico's binnen een organisatie.

Voorafgaande vereisten

Bekendheid met een gids met best practices (ANSSI-hygiëne, ISO 27002 of gelijkwaardig), afronding van de introductiecursus in cyberbeveiliging of gelijkwaardige kennis.

DEELNEMERS

Projectmanagers, consultants, technische architecten, IS security managers, iedereen die verantwoordelijk is voor informatiebeveiliging, compliance en risico's binnen een organisatie.

VOORAFGAANDE VEREISTEN

Bekendheid met een gids met best practices (ANSSI-hygiëne, ISO 27002 of gelijkwaardig), afronding van de introductiecursus in cyberbeveiliging of gelijkwaardige kennis.

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 de certification est dirigé en partenariat avec l'organisme de certification LSTI. Il se déroule pendant la dernière demi-journée. Ce diplôme international officiel ISO vous apportera la plus grande crédibilité dans la conduite de vos projets d'analyse de risques. Il est à noter qu'un travail personnel important est à prévoir pour se préparer au mieux à l'examen.

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 Inleiding

- ISO 27000-terminologie, definities van bedreiging. Kwetsbaarheid. Risico...
- Beschikbaarheid, integriteit en vertrouwelijkheid.
- Rekening houden met traceerbaarheid/bewijs.
- Herinnering aan regelgevende en normatieve beperkingen (RGPD, LPM/NIS, PCI DSS, enz.).
- De rol van de CISO versus de risicomanager.
- De 31000-norm, de waarde van de "overkoepelende" norm als universele benchmark.

2 Het concept "IS-risico

- Risico-identificatie en -classificatie.
- Oorsprong van bedreigingen (per ongeluk, opzettelijk, milieu).
- De gevolgen van het risico (financieel, juridisch, menselijk, enz.).
- Risicobeheer (verminderen/verminderen, risico's vermijden, delen).
- Het speciale geval van digitaal risico in "persistentie" (APT).
- Hoe te handelen naar aanleiding van het risico (voor, tijdens en na het incident).

3 Risicobeheer volgens ISO

- De 27001:2022-methode en het bijbehorende proces voor risicobeheer.
- De initiële beoordeling in de planfase van hoofdstuk 6 - Planning.
- De belangrijkste evolutie van de norm 27005:2022: Risicomanagement voor informatiebeveiliging.
- Een PDCA-risicobeheerproces implementeren.
- De context, beoordeling, behandeling, acceptatie en herziening van risico's.
- De fasen van risicobeoordeling (identificatie, analyse en evaluatie).
- Opstellen van een behandelplan gebaseerd op ISO 27002 maatregelen.
- Het proces van het selecteren van maatregelen op basis van eigenschappen (preventief, detectief of correctief).
- De keuze van beveiligingsmaatregelen voor de verklaring van toepasselijkheid (SoA).

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.

4 De norm ISO 27005:2022

- Inleiding tot de nieuwe ISO 27005:2022-norm, de invloed van EBIOS RM.
- Het verband tussen risicomanagementprocessen en ISMS-processen.
- Gerichte analyse van cyberrisico's, hoe APT's te analyseren.
- De cyber kill chain, nieuwe risicobronnen en hun doelstellingen.
- Voorbeeld van een schaal voor het berekenen van waarschijnlijkheid en gevolgen.
- De event-based versus asset-based benadering van risicomanagement.
- Beschrijving van strategische en operationele scenario's.
- Rekening houden met risico's via het ecosysteem.

5 Voorbereiding en eindbeoordeling

- Rollenspel, multiple-choice kennistests, casestudies.
- Inventarisatie van bedrijfsmiddelen en beoordeling van bedreigingen en kwetsbaarheden.
- Risicobeheerplannen opstellen, enz.
- Proefexamen en interactieve antwoordsleutel.
- Tips om de valkuilen te vermijden.

6 Examen doen

- De procedure voor het online examen wordt op de eerste trainingsdag uitgelegd: inhoud en regels die in acht moeten worden genomen.
- Technische vereisten voor het online examen (webcam geactiveerd, internetverbinding).
- Administratorrechten om anti-cheatsoftware te installeren, enz.
- Dit examen vindt plaats op het TESTWE online examenplatform (testwe.eu).
- Als het examen op locatie van Orsys wordt afgenomen, zorgt Orsys voor de voorbereiding van de werkplek van de kandidaat.
- Wanneer je examen doet bij Orsys, ontvang je ook een papieren exemplaar van de standaarden die tijdens de cursus zijn beschreven.
- Om dit examen voor afstandsonderwijs te kunnen afleggen, moeten kandidaten alle standaarden zelf op papier verwerven.

Data en plaats

KLAS OP AFSTAND
2026 : 27 mei, 29 juni, 9 sep., 14 okt., 2 dec., 16 dec.

PARIS LA DÉFENSE
2026 : 20 mei, 17 juni, 2 sep., 7 okt., 25 nov., 16 dec.