Publicatiedatum : 16/05/2024

Opleiding : Een ISO 27001:2022-project implementeren en beheren

Voorbereiding LSTI certificering

seminarie - 3d - 21u00 - Ref. ASE

Prijs : 2550 € V.B.

4,3 / 5

BEST

De internationale norm ISO/IEC 27001 voor risicobeheer van informatiebeveiliging beschrijft de best practices die moeten worden toegepast zodat een organisatie informatiegerelateerde risico's effectief kan beheren. Deze cursus presenteert de ISO-normen voor de beveiliging van informatiesystemen en vervolgens de elementen voor het opzetten van een risicobeheersysteem voor informatiebeveiliging (ISMS).

Pedagogische doelstellingen

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

- De onderdelen van een ISO 27001-conform beheersysteem voor informatiebeveiliging (ISMS) uitleggen.
- De inhoud van en correlatie tussen ISO 27001 en 27002 en andere normen en regelgevende kaders uitleggen
- De eisen van ISO 27001 aanpassen aan de specifieke context van een organisatie
- De vereisten van ISO 27001 interpreteren in de context van een ISMS-audit
- De verschillende benaderingen van IS-governance (ISO, LPM, NIS, etc.) op elkaar afstemmen.

Doelgroep

CISO's, risicomanagers, IT-directeuren of -managers, projectmanagers, beveiligingsengineers of -correspondenten, projectmanagers, interne en externe auditors, toekomstige "auditees".

Voorafgaande vereisten

Basiskennis van IT-beveiliging.

DEELNEMERS

CISO's, risicomanagers, IT-directeuren of -managers, projectmanagers, beveiligingsengineers of -correspondenten, projectmanagers, interne en externe auditors, toekomstige "auditees".

VOORAFGAANDE VEREISTEN

Basiskennis van IT-beveiliging.

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

In de remote modus moeten kandidaten alle benodigde standaarden zelf aanschaffen (ISO 27000, ISO 27001, ISO 27002, ISO 27005, ISO 27006, ISO 19011, ISO 17021, ISO 27006). In de face-to-face modus bij Orsys worden de standaarden op papier uitgeleend tijdens de training.

Praktische modaliteiten

Certificaat

Voorbereiding voor ISO 27001 Implementer en Lead Auditor certificaten.

Opleidingsprogramma

1 Inleiding

- Herinneringen. ISO 27000 en ISO Guide 73 terminologie.
- Het begrip risico (gevolg, waarschijnlijkheid).
- De minimale CID-classificatie (Vertrouwelijkheid, Integriteit, Beschikbaarheid).
- Risicobeheer (verminderen, onderhouden, weigeren, delen).
- Analyse van schade-ervaringen. Trends. De inzet.
- Beveiligingsvoorschriften (zakelijk, wettelijk, enz.) bijv. PCI-DSS, NIST, LPM/NIS.
- Voor wie is het? Voor wie? Interactie met ISO.
- ISO op één lijn met Governance / Protection / Defence / Resilience.
- Afstemming ISO – NIS/LPM: op weg naar convergentie?

2 ISO 2700x-normen

- Geschiedenis van ISO-veiligheidsnormen.
- De basisnormen (ISO 27001, 27002).
- De essentiële standaarden (ISO 27005, 27004, 27003, etc.).
- Convergentie met andere "Management System" standaarden.
- Convergentie met andere "Management System"-normen.

3 De norm ISO 27001:2022

- Definitie van een beheersysteem voor informatiebeveiliging (ISMS).
- Doelstellingen die moeten worden bereikt door uw ISMS.
- De aanpak van "voortdurende verbetering" als basisprincipe, het PDCA-model (Deming-wiel).
- ISO 27001 geïntegreerd in een wereldwijde aanpak van risicobeheer.
- Van specificatie van de ISMS-perimeter tot het in kaart brengen van bedrijfsmiddelen.
- ISO 27005 aanbevelingen voor risicobeheer.
- Het belang van risicobeoordeling. Het kiezen van een methode zoals ISO 27005:2022 / ISO 31000.
- Advies over het opstellen van een risicomanagementplan.
- De bijdrage van gepubliceerde methoden (bijv. EBIOS RM) aan de beoordeling van cyberrisico's.
- Het nemen van efficiënte technische en organisatorische beveiligingsmaatregelen.
- De verklaring van toepasselijkheid is gebaseerd op bijlage A.
- Verplichte interne ISMS-audits. Een auditprogramma opstellen.
- Implementatie van corrigerende en preventieve maatregelen.

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 Beveiligingsdoelstellen: Beschikbaarheid, Integriteit en Vertrouwelijkheid.

- Indeling in domeinen/hoofdstukken (niveau 1), controledoelstellingen (niveau 2) en controles (niveau 3).
- De nieuwe goede praktijken van ISO 27002:2013, de maatregelen verwijderd uit ISO 27001:2005. De wijzigingen.
- De norm ISO 27002:2013: de 14 domeinen en 114 goede praktijken.
- Voorbeelden van de toepassing van de norm op uw onderneming: noodzakelijke essentiële beveiligingsmaatregelen.
- Risicobeperkende maatregelen voor ondersteunende activa zoals mensen, eigendom en IT.
- De maatregelen die nodig zijn voor het delen via domein 15.

5 **Risicomanagement (#Preventie, #Opsporing, #Correctie).**

- Cyberbeveiligingsconcepten: #Identificatie, #Bescherming, #Opsporing, #Verwerking, #Herstel.
- Operationele capaciteiten: #Governance, #Asset_Management, #Information_Protection, #HR_Security.
- #Physical_security, #System_and_network_security, #Application_security, #Secure_configuration.
- #Identiteit_en_toegang_beheer.
- Veiligheidsdomeinen (#Governance_and_ecosystem, #Protection, #Defence, #Resilience)
- ISO 27002:2022: een overzicht van 93 best practices.
- Nieuwe ISO 27002:2022 praktijken, maatregelen verwijderd uit ISO 27002:2017. Wijzigingen en goedkeuringen.
- Voorbeelden van hoe u de nieuwe standaarden kunt toepassen op uw organisatie: de belangrijkste beveiligingsmaatregelen die essentieel zijn.
- Oplevering van het project, hoe uitvoeren? Inbraaktest en/of technische audit?
- Indicatoren voorbereiden. Voortdurende verbetering.
- Een dashboard installeren. Voorbeelden.
- De bijdrage van de norm 27004:2016 bij het opstellen van conformiteits- en efficiëntiecriteria.
- Beheer van zwakke plekken in een ISMS: regelmatige scans, Patch Management...

6 **Beveiliging implementeren in een ISMS-project**

- Van beveiligingsspecificaties tot beveiligingsacceptatie.
- Hoe voldoet u aan de PSSI en de beveiligingsvereisten van de klant/MOA?
- Van risicoanalyse tot de constructie van de verklaring van toepasselijkheid.
- Beveiligingsmaatregelen integreren in specifieke ontwikkelingen.
- De regels voor uitbesteding.
- Houd toezicht op het project terwijl het wordt geïmplementeerd en in werking wordt gesteld.
- Veiligheidsbijeenkomsten voor het recept.
- De PDCA-cyclus integreren in de projectlevenscyclus.
- Projectacceptatie: hoe pakt u dat aan? Welke soorten audits?

7 De bijdrage van norm 27004:2016 aan de constructie van metrieken.

- Het belang van deze aanpak, het streven naar het "label".
- Criteria voor de keuze van de perimeter. Toepassingsgebied. Betrokkenheid van de belanghebbenden.
- ISO: essentiële aanvulling op de regelgevende kaders en normen?
- De verwachte zakelijke en/of regelgevende uitdagingen.
- Certificerende instanties, aanbod in Frankrijk en in de wereld.
- Auditproces, stappen en werklast.
- Normen ISO 17021 en ISO 27006, verplichtingen voor certificerende instanties.
- Kosten van de certificering, ROI.

Data en plaats

KLAS OP AFSTAND
2026 : 14 apr., 27 mei, 22 juni, 29 juni, 22 sep., 28 sep., 5 okt., 9 nov., 30 nov., 1 dec., 7 dec.

PARIS LA DÉFENSE
2026 : 18 mei, 22 juni, 28 sep., 2 nov., 30 nov.