Publicatiedatum : 29/08/2024

Opleiding : Lead Auditor - ISO 27001:2022 certificering

Een ISO 27001:2022-project implementeren en beheren

Praktijkcursus - 5d - 35u00 - Ref. PIS

Prijs : 3430 € V.B.

BEST

De internationale norm voor risicobeheer van informatiebeveiliging ISO/IEC 27001 beschrijft in de vorm van vereisten de best practices die moeten worden ingevoerd zodat een organisatie informatiegerelateerde risico's effectief kan beheren. Tijdens dit seminar maakt u eerst kennis met alle ISO-normen die te maken hebben met de beveiliging van informatiesystemen en krijgt u vervolgens de elementen aangereikt die u nodig hebt om een risicobeheersysteem voor informatiebeveiliging (ISMS) op te zetten.

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 eisen van ISO 27001 aanpassen aan de specifieke context van een organisatie
- Voorbereiding op en deelname aan het examen "Lead Auditor 27001:2022

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.

Certificatie

Om dit examen op afstand af te leggen, moeten kandidaten alle benodigde standaarden zelf op papier verwerven. Aan het eind van de sessie slagen voor het certificeringsexamen in het Frans. Dit examen certificeert dat u over de kennis en vaardigheden beschikt die nodig zijn om de conformiteit van een ISMS met de norm ISO/IEC 27001:2013 te controleren. Dit examen wordt afgenomen in samenwerking met de certificeringsinstantie LSTI (geaccrediteerd door COFRAC).

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.

Praktische modaliteiten

Praktisch werk

Voorbereiding voor de ISO 27001 Lead Implementer en Lead Auditor certificaten.

Composition de la formation

Een ISO 27001:2022-project implementeren en beheren

Ref. ASE - 3 dagen ★ 4 / 5

ISO 27001:2013 Lead Auditor, praktische toepassing, certificering

Ref. LAU - 2 dagen

Opleidingsprogramma

1 Inleiding

- Herinneringen. ISO 27000 en ISO Guide 73 terminologie.
- Definities: bedreiging, kwetsbaarheid, bescherming.
- Het begrip risico (gevolg, impact, waarschijnlijkheid).
- De minimale CID-classificatie (Vertrouwelijkheid, Integriteit, Beschikbaarheid).
- Risicobeheer (verminderen, onderhouden, weigeren, delen).
- Analyse van schade-ervaringen. Trends. De inzet.
- Beveiligingsvoorschriften (zakelijk, wettelijk, enz.) PCI-DSS, NIST, LPM/NIS. Voor wie is het? Voor wie? Interactie met ISO.
- ISO op één lijn met Governance / Protection / Defence / Resilience.
- Afstemming COBIT, ITIL® en ISO 27002.

2 ISO 2700x-normen

- Geschiedenis van ISO-veiligheidsnormen.
- BS 7799 normen en hun bijdrage aan ISO.
- Huidige normen (ISO 27001, 27002).
- Aanvullende normen (ISO 27005, 27004, 27003, etc.).
- Convergentie met 9001 kwaliteitsnormen en 14001 milieunormen.
- De bijdrage van kwaliteitsspecialisten aan veiligheid.

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.

3 De norm ISO 27001:2022

- Definitie van een beheersysteem voor systeembeveiliging (ISMS).
- Doelstellingen die moeten worden bereikt door uw ISMS.
- De aanpak van "voortdurende verbetering" als basisprincipe, het PDCA-model (Deming-wiel).
- ISO 27001 als onderdeel van een wereldwijde aanpak van IS-governance.
- Details van de Plan-Do-Check-Act fasen.
- Van specificatie van de ISMS-perimeter tot de SoA (Verklaring van Toepasselijkheid).
- ISO 27001 aanbevelingen voor risicobeheer.
- Het belang van risicobeoordeling. Het kiezen van een methode zoals ISO 27005:2022 / ISO 31000.
- De bijdrage van gepubliceerde methoden (bijv. EBIOS) aan hun beoordelingsproces.
- Het nemen van efficiënte technische en organisatorische beveiligingsmaatregelen.

4 Bijlage A als referentiehulpmiddel - koppeling met norm 27002.

- Beveiligingsdoelstellen: Beschikbaarheid, Integriteit en Vertrouwelijkheid.
- 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 113 goede praktijken.
- Voorbeelden van de toepassing van de norm op uw onderneming: noodzakelijke essentiële beveiligingsmaatregelen.

5 Beste praktijken, ISO 27002:2022-norm

- Structurering op het eerste niveau: organisatorische, persoonlijke, fysieke en technologische maatregelen.
- Thema's en kenmerken (#Preventie, #Opsporing, #Correctie).
- Cyberbeveiligingsconcepten (#Identificatie, #Bescherming, #Opsporing, #Verwerking, #Herstel).
- Operationele capaciteiten (#Governance, #Asset_Management, Informatie_Bescherming...).
- Veiligheidsdomeinen ((#Governance_and_ecosystem, #Protection, #Defence, #Resilience).
- ISO 27002:2022: een overzicht van 93 best practices.
- De nieuwe ISO 27002:2022 good practices, de maatregelen verwijderd uit ISO 27001:2017. De wijzigingen.

6
- Continu en compleet proces. Stappen, prioriteiten.
- De auditcategorieën: organisatorisch, technisch enz.
- Interne, externe audits en door derden, de auditor kiezen.
- Het typische ISO-auditproces, de belangrijkste stappen.
- De doelstellingen van een audit, de kwaliteit van een audit.
- Organisatorische audit: aanpak, methoden.
- Vergeleken bijdragen, menselijke implicaties.
- Intellectuele eigendom van software, aansprakelijkheid uit onrechtmatige daad en contractuele aansprakelijkheid.
- Strafrechtelijke aansprakelijkheid, de aansprakelijkheid van leidinggevenden, delegatie van bevoegdheden, sancties. De LCEN-wet.
- ISO-conformiteit en juridische conformiteit: het nieuwe domein 18 van ISO 27002:2013.
- Deze opleiding biedt een interactieve lesmethode met oefeningen via rollenspellen.
- Kennistests via meerkeuzevragenlijsten en gespreksimulaties auditor/gecontroleerde.

7 **Auditcategorieën: organisatorisch, technisch, enz.**

- Interne en externe audits en audits door derden.
- De typische ISO-auditprocedure en de belangrijkste stappen.
- Controledoelstellingen en controlekwaliteit.
- Het opbouwen van het interne auditprogramma.
- De verbeteraanpak voor de audit.

8 **De benodigde normen: ISO 27000, ISO 27001, ISO 27002, ISO 27005, ISO 19011, ISO 17021, ISO 27006.**

- De procedure voor het online examen wordt op de eerste trainingsdag uitgelegd: inhoud en te volgen regels.
- Technische vereisten voor het online examen (webcam geactiveerd, internetverbinding).
- 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.

9 **Examen**

- Het schriftelijke examen duurt 3,5 uur en bestaat uit zes onderdelen.
- Een meerkeuzevragenlijst over de ISO/IEC 19011-norm en bijbehorende gidsen op 20 punten.
- Een meerkeuzevragenlijst over de ISO/IEC 27001-norm en bijbehorende gidsen op 20 punten.
- Een oefening om een normatieve referentie te vinden op basis van de auditbevindingen op 5 punten.
- Een oefening in verband met de PDCA-cyclus op 5 punten.
- Een oefening "feiten en gevolgtrekkingen" op basis van een persartikel op 10 punten.
- Een casestudie op 35 punten.
- Voorts een beoordeling door de trainer van de houding en aanpak van de auditor op 5 punten.
- De resultaten van het examen zullen u 4 tot 6 weken later per post worden toegestuurd.

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.