Een ISO 27001:2013-project implementeren en beheren, Lead Implementer-certificering

Cycle van 5 dags - 35h
Ref : PIZ - Prijs 2025 : € 4 140 excl. BTW

De internationale norm ISO/IEC 27001 voor risicomanagement in verband met informatiebeveiliging beschrijft de beste praktijken die een organisatie moet invoeren om de risico's in verband met informatie doeltreffend te beheren. In dit seminarie komen in eerste instantie alle ISO-normen aan bod in verband met de beveiliging van informatiesystemen en vervolgens de elementen die nodig zijn om een managementsysteem voor informatiebeveiliging (ISMS) op te zetten.

Deze cyclus bestaat uit:

- Een ISO 27001:2022-project implementeren en beheren (Ref ASE, 3 dags)
- ISO 27001:2013 Lead Implementer, praktische toepassing, certificering (Ref LED, 2 dags)

PEDAGOGISCHE DOELSTELLINGEN

Na afloop van de opleiding kan de cursist:

De componenten van een ISO 27001-conform managementsysteem voor informatiebeveiliging (ISMS) uitleggen

De eisen van de norm ISO 27001 aanpassen aan de specifieke context van een organisatie

Het examen "Lead Implementer 27001:2013" voorbereiden en afleggen

HANDS-ON WORK

Voorbereiding op de ISO 27001 Lead Implementer- en Lead Auditor-certificaten.

CERTIFICERING

Het eindexamen certificeert dat u over de nodige kennis en competenties beschikt om een ISMS te implementeren volgens de norm ISO/IEC 27001:2013. Het examen vindt plaats tijdens de laatste halve dag. Het wordt afgenomen in samenwerking met de certificeringsinstantie LSTI (erkend door COFRAC).

HET PROGRAMMA

laatste update: 02/2024

1) Inleiding

- Herhalingen. Terminologie ISO 27000 en ISO Guide 73.
- Definities: bedreiging, kwetsbaarheid, bescherming.
- Het begrip risico (mogelijkheid, impact, ernst).
- De CAID-classificatie (Vertrouwelijkheid, Controleerbaarheid, Integriteit, Beschikbaarheid).
- Risicobeheer (preventie, bescherming, uitstel, uitbesteding).
- SOX-, PCI-DSS- en COBIT-voorschriften. Voor wie? Waarom? Interactie met ISO.
- Naar IT-governance, samenhang met ITIL® en ISO 20000.
- Afstemming COBIT, ITIL® en ISO 27002.

2) ISO 2700x-normen

- Geschiedenis van de beveiligingsnormen door de ogen van de ISO.
- BS 7799-normen, hun bijdrage aan de ISO.

DEELNEMERS

CISO's, risicobeheerders, IT-directeuren of -verantwoordelijken, projectmanagers, beveiligingsingenieurs of -correspondenten, projectleiders, interne en externe auditors, toekomstige 'gecontroleerden'.

VOORAFGAANDE VEREISTEN

Basiskennis van computerbeveiliging.

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.

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.

- De huidige normen (ISO 27001, 27002).
- De aanvullende normen (ISO 27005, 27004, 27003.)).
- Overeenstemming met de kwaliteitsnormen 9001 en de milieunormen 14001.
- De bijdrage van kwaliteitsbewakers aan de veiligheid.

3) De norm ISO 27001:2013

- Definitie van een managementsysteem voor informatiebeveiliging (ISMS).
- 'Continue verbetering' als basisprincipe, het PDCA-model (wiel van Deming).
- De ISO 27001-norm geïntegreerd in een kwaliteitsbeleid van het type KMS.
- Specificatie van de Plan-Do-Check-Act-fasen.
- Van specificatie van de ISMS-perimeter tot SoA (Statement of Applicability).
- Inbreng van de methoden EBIOS, MEHARI in uw beoordelingsproces.
- Verplichte interne audits van het ISMS.
- Verbetering van het ISMS. Uitvoering van corrigerende en preventieve maatregelen.

4) Goede praktijken, norm ISO 27002:2013

- 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 113 goede praktijken.
- Voorbeelden van de toepassing van de norm op uw onderneming: noodzakelijke essentiële beveiligingsmaatregelen.

5) Implementatie van de beveiliging in een ISMS-project

- Van de beveiligingsspecificaties tot de goedkeuring van de beveiliging.
- De normen ISO 27003, 15408 als hulpmiddel bij de uitvoering.
- De PDCA-cyclus integreren in de levenscyclus van het project.
- Oplevering van het project, hoe uitvoeren: inbraaktest en/of technische audit?
- Indicatoren voorbereiden. Continue verbetering.
- Een dashboard installeren. Voorbeelden.
- De bijdrage van de norm 27004.
- Beheer van zwakke plekken in een ISMS: regelmatige scans, Patch Management...

6) Beveiligingsaudits volgens ISO 19011:2011

- 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.
- Het verbeteringsproces voor de audit.
- Organisatorische audit: aanpak, methoden.

7) Goede juridische praktijken.

- 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.

8) ISO-certificering van de beveiliging van het IS, de relatie tussen auditor en gecontroleerde

- Het belang van deze aanpak, het streven naar het 'label'.
- Criteria voor de keuze van de perimeter. Toepassingsgebied. Betrokkenheid van de stakeholders.
- ISO: essentiële aanvulling op de regelgevende kaders en normen (SOX, ITIL®, ...).
- Certificerende instanties, aanbod in Frankrijk en in Europa.

- Norm ISO 27006, verplichtingen voor certificerende instanties.
- Terugkerende en eenmalige kosten van de certificering.

9) Oefeningen - practica

- Er zullen typische beveiligingsprojecten worden aangeboden om te ervaring op te doen door de praktijk.
- De toepassing van een PDCA-aanpak en goede praktijken volgens ISO 27001 en ISO 27002.
- U zult een toepasselijkheidsverklaring opstellen op basis van een risicoanalyse van het type ISO 27001 of 27005.
- U leert de belangrijkste indicatoren van een ISSP en een beveiligingsproject bepalen.
- Schriftelijke en mondelinge oefeningen in rollenspellen, kennistests via meerkeuzevragen.

10) Laatste herhaling en examen

- Het schriftelijk examen duurt 3,5 uur.
- Het verloop van het schriftelijk examen wordt op de eerste dag van de opleiding uiteengezet door de trainer.
- Inhoud van het examen, in acht te nemen regels. Normen of andere documenten die ter beschikking worden gesteld aan de kandidaten.
- Procedures die worden ingevoerd om de vertrouwelijkheid van kopieën te respecteren.
- Minimaal vereiste punten om te slagen voor het schriftelijk examen.
- Het examen bevat een meerkeuzevragenlijst met betrekking tot de norm ISO/IEC 2018.
- Het examen omvat ook praktische oefeningen en een casestudie.
- De resultaten van het examen zullen u 4 tot 6 weken later per post worden toegestuurd.
- Ter afsluiting van de voorbereiding is er een laatste herhaling.
- Tips, trucs en te vermijden valkuilen om u beter voor te bereiden om de certificering te behalen.

DATA

Neem contact met ons op