

Certifiante

Formation ISO/IEC 27701 Lead Auditor, avec certification PECB

Réf. SF34708

Préparez et obtenez la certification PECB Certified ISO/IEC 27701 Lead Auditor pour planifier et diriger des audits de systèmes de management de la protection de la vie privée.

5 j
Durée

4 000 € HT
Inter / participant

0
Sessions à venir

Objectifs pédagogiques

- ✓ Comprendre un PIMS et ses processus fondés sur ISO/IEC 27701
- ✓ Identifier la relation entre ISO/IEC 27701, ISO/IEC 27001, ISO/IEC 27002 et les autres normes et cadres réglementaires
- ✓ Maîtriser les concepts et principes fondamentaux de l'audit selon ISO 19011
- ✓ Préparer un audit ISO/IEC 27701 (revue documentaire, plan d'audit, audit de phase 1)
- ✓ Réaliser un audit sur site (collecte de preuves, techniques et procédures d'audit, plans de test)
- ✓ Clôturer un audit (constats, rapports de non-conformité, évaluation des plans d'action)
- ✓ Gérer un programme d'audit ISO/IEC 27701 et la relation avec l'audité
- ✓ Réussir l'examen de certification PECB Certified ISO/IEC 27701 Lead Auditor

Public visé & prérequis

Public visé Auditeurs

Prérequis- Une compréhension fondamentale de la sécurité de l'information et de la protection de la vie privée, et une connaissance des principes d'audit (recommandé par PECB) - Prérequis implicite : connaissance d'ISO/IEC 27001 (le PIMS est une extension du SMSI 27001) et notions de techniques d'audit (ISO 19011) ; un parcours Lead Auditor ISO/IEC 27001 en amont facilite fortement le suivi - Aucun prérequis officiel n'est exigé pour passer l'examen (la qualification obtenue dépend ensuite de l'expérience d'audit — voir schéma de certification)

Programme détaillé

Introduction au PIMS et à la norme ISO/IEC 27701

- Objectifs, structure de la formation et processus de certification PECB
- Normes et cadres réglementaires : articulation ISO/IEC 27701, ISO/IEC 27001, ISO/IEC 27002 et lien avec le RGPD
- Principes et concepts fondamentaux de la sécurité de l'information et de la protection de la vie privée
- Système de management de la protection de la vie privée (PIMS) : exigences, processus et documentation attendue
- Interprétation des exigences d'ISO/IEC 27701 dans une perspective d'audit

Activités pratiques :

- Étude de cas fil rouge : prise en main du contexte d'un organisme à auditer
- Quiz sur les exigences du PIMS et leur traçabilité vers les preuves d'audit
- Analyse de scénario : identifier les processus clés d'un PIMS à examiner en audit

Principes d'audit, préparation et ouverture d'un audit

- Concepts et principes fondamentaux de l'audit selon ISO 19011
- Impact des tendances et de la technologie sur l'audit
- Audit fondé sur des éléments probants et audit fondé sur le risque
- Lancement du processus d'audit : prise de contact, revue documentaire, plan d'audit

- Audit de phase 1 : revue de la documentation et préparation de l'audit sur site

Activités pratiques :

- Atelier : construire un plan d'audit à partir de l'étude de cas
- Jeu de rôle : conduire une réunion d'ouverture d'audit
- Exercice : évaluer la maturité documentaire d'un PIMS en audit de phase 1

Activités d'audit sur site

- Préparation de l'audit de phase 2 (audit sur site)
- Réalisation de l'audit de phase 2 : collecte et évaluation des preuves
- Communication pendant l'audit : entretiens, gestion de l'équipe et de l'audité
- Procédures d'audit et techniques d'échantillonnage
- Création et exploitation de plans de test d'audit

Activités pratiques :

- Jeu de rôle : mener un entretien d'audit et recueillir des preuves
- Atelier : rédiger un plan de test d'audit pour une mesure du PIMS
- Mise en situation : qualifier un écart en constat d'audit

Clôture de l'audit et gestion du programme d'audit

- Rédaction des constats d'audit et des rapports de non-conformité
- Documentation d'audit et revue de la qualité
- Clôture de l'audit : réunion de clôture et restitution
- Évaluation des plans d'action correctifs par l'auditeur
- Au-delà de l'audit initial : audits de suivi et cycle de certification
- Gestion d'un programme d'audit, communication avec les clients et résolution des conflits

Activités pratiques :

- Atelier : rédiger un rapport de non-conformité argumenté et priorisé
- Jeu de rôle : animer une réunion de clôture et gérer un désaccord avec l'audité
- Mise en situation : évaluer la pertinence d'un plan d'action correctif

Préparation à la certification

- Modalités de l'examen : 3 heures, distanciel en différé (format et seuil de réussite à confirmer avec PECB)
- Examen blanc en conditions réelles
- Stratégies de réponse : gestion du temps, lecture des questions, appui sur la norme
- Révision ciblée : synthèse des points clés par domaine d'examen (7 domaines)
- Planification : inscription à l'examen et conseils de préparation post-formation

Activités pratiques :

- Examen blanc chronométré avec correction commentée
- Atelier de révision par domaine avec quiz

Pourquoi choisir Sparks Formation ?

20 ans d'expertise IT, des formateurs experts et des sessions garanties contre l'annulation.

20 ans
d'expertise

1 068+
formations

11 178
apprenants formés/an

+67
Net Promoter Score

Avis des participants

Note moyenne des participants de la filière Cybersécurité et Protection des Données : 4,9/5 — 13 avis

William B. — Prévoir l'envoi à chaque participant du livre de CISS au moins un mois avant la formation.

Mickael L. — il est top Romain GARCIA

Ils nous font confiance

Cette année notre filière Gouvernance, Risques & Conformité (GRC) a accompagné plus de 30 entreprises dont :

AVEM MÉTROPOLE DE LYON ADISTA ALSTOM ASTEK FRANCE AXA ASSISTANCE FRANCE COMMUNAUTÉ DE COMMUNES DES HAUTS DE FLANDRE CONSORT FRANCE ECONOCOM SERVICES & SOLUTION EGIS +20 autres

Financement & certifications

Cette formation est éligible aux financements OPCO et FNE-Formation. Nos équipes vous accompagnent dans le montage de votre dossier.



Réservez votre place dès maintenant

20 ans d'expertise · 1 000+ formations · NPS +67 · réponse sous 24h ouvrées

0 805 950 800

demande@sparks-formation.com