

ISO 27001 Lead Auditor (examen inclus) Certification : ISO 27001

Programme (Mis à jour le 14/03/2025)

JOUR 1 : Introduction au système de management de la sécurité de l'information (SMSI) et à ISO/IEC 27001:2022

- Objectifs et structure de la formation
 - Cadres normatifs et réglementaires
 - Processus de certification
 - Principes fondamentaux du SMSI
 - SMSI
- Objectifs et structure de la formation
 - Introduction
 - À propos de PECB
 - Informations générales
 - Objectifs d'apprentissage
 - Approche éducative
 - Examen et certification
- Normes et cadres réglementaires
 - Qu'est-ce que l'ISO ?
 - La famille de normes ISO/IEC 27000
 - Avantages d'ISO/IEC 27001:2022
- Processus de certification
 - Processus de certification
 - Programme de certification
 - Organismes d'accréditation
 - Organismes de certification
- Concepts et principes fondamentaux de la sécurité de l'information
 - Information et actif
 - Sécurité de l'information
 - Confidentialité, intégrité et disponibilité
 - Vulnérabilité, menace et impact
 - Risque de sécurité de l'information
 - Mesures et objectifs des mesures de sécurité
 - Classification des mesures de sécurité
- Système de management de la sécurité de l'information (SMSI)
 - Définition de système de management
 - Définition de SMSI
 - Approche processus
 - Mise en œuvre du SMSI
 - Vue d'ensemble – articles 4 à 10
 - Vue d'ensemble – Annexe A
 - Déclaration d'applicabilité

JOUR 2 : Principes d'audit, préparation et initiation d'un audit

- Concepts et principes fondamentaux de l'audit
 - Normes d'audit
 - Qu'est-ce qu'un audit ?
 - Types d'audits
 - Parties impliquées
 - Objectifs et critères d'audit
 - Audit combiné
 - Principes d'audit
 - Compétence et évaluation des auditeurs

Référence

THIS3299

Durée

5 jours / 35 heures

Prix HT / stagiaire

3730€

Objectifs pédagogiques

- Expliquer les concepts et principes fondamentaux d'un système de management de la sécurité de l'information (SMSI) basé sur ISO/IEC 27001
- Interpréter les exigences d'ISO/IEC 27001 pour un SMSI du point de vue d'un auditeur
- Évaluer la conformité du SMSI aux exigences d'ISO/IEC 27001, en accord avec les concepts et principes fondamentaux d'audit
- Planifier, conduire et clore un audit de conformité à ISO/IEC 27001, conformément aux exigences d'ISO/IEC 17021-1, aux lignes directrices d'ISO 19011 et aux autres bonnes pratiques d'audit
- Gérer un programme d'audit ISO/IEC 27001

Niveau requis

- Une bonne connaissance de la norme ISO/CEI 27001 et des connaissances approfondies sur les principes de l'audit
- La formation est dispensée sur la version 2022 de la norme ISO/CEI 27001
- Il est conseillé aux participants de se munir d'un exemplaire de la norme pour suivre la formation et passer la certification dans des conditions optimales

Public concerné

- Auditeurs souhaitant réaliser et diriger des audits de certification du SMSI
- Responsables ou consultants désirant maîtriser le processus d'audit du SMSI
- Toute personne responsable du maintien de la conformité aux exigences du SMSI
- Experts techniques désirant préparer un audit du SMSI
- Conseillers spécialisés en MSI

Formateur

Les formateurs intervenants pour Themanis sont qualifiés par notre Responsable Technique Olivier Astre pour les formations informatiques et bureautiques et par Didier Payen pour les formations management.

Conditions d'accès à la formation

Délai : 3 mois à 1 semaine avant le démarrage de la formation dans la limite des effectifs indiqués

Moyens pédagogiques et techniques

Salles de formation (les personnes en situation

- Impact des tendances et de la technologie en audit
 - Mégadonnées (Big data)
 - Les trois V des mégadonnées
 - L'utilisation de mégadonnées dans les audits
 - Intelligence artificielle
 - Apprentissage automatique (Machine learning)
 - Informatique en nuage (Cloud computing)
 - Audit des opérations externalisée
- Audit basé sur les preuves
 - Preuve d'audit
 - Types de preuves d'audit
 - Qualité et fiabilité des preuves d'audit
- Audit basé sur le risque
 - Approche d'audit basée sur les risques
 - Importance relative et planification de l'audit
 - Assurance raisonnable
- Initiation du processus d'audit
 - Offre d'audit
 - Responsable d'équipe d'audit
 - Équipe d'audit
 - La faisabilité de l'audit
 - Acceptation de l'audit
 - Prise de contact avec l'audité
 - Programme d'audit
- Étape 1 de l'audit
 - Objectifs de l'étape 1 de l'audit
 - Activités sur site préalables
 - Préparation des activités sur site
 - Réalisation des activités sur site
 - Documentation des résultats de l'étape 1

JOUR 3 : Activités d'audit sur site

- Préparation de l'étape 2 de l'audit
 - Détermination des objectifs de l'audit
 - Planification de l'audit
 - Attribution du travail à l'équipe d'audit
 - Préparation des plans de test d'audit
 - Préparation de l'information documentée en vue de l'audit
- Étape 2 de l'audit
 - Conduite de la réunion d'ouverture
 - Collecte d'information
 - Réalisation des tests d'audit
 - Définition des constatations d'audit et des rapports de non-conformité
 - Exécution de la revue de qualité
- Communication pendant l'audit
 - Comportement lors des visites sur site
 - Communication pendant l'audit
 - Réunions de l'équipe d'audit
 - Guides et observateurs
 - Gestion des conflits
 - Aspects culturels
 - Communication avec la direction générale
- Procédures d'audit
 - Vue d'ensemble du processus d'audit
 - Procédures de collecte et d'analyse des preuves
 - Entretien
 - Revue de l'information documentée
 - Observation
 - Analyse
 - Échantillonnage
 - Vérification technique
 - Corroboration
 - Évaluation
 - Audit des activités et sites virtuels
- Création de plans d'échantillonnage d'audit
 - Plans de tests d'audit
 - Exemples de plans de test d'audit
 - Lignes directrices pour les audits d'un SMSI

JOUR 4 : Clôture de l'audit

- Rédaction des rapports de constatations d'audit et de non-conformité
 - Constatations d'audit
 - Types de constatations d'audit possibles
 - Documenter les constatations de l'audit
 - Rédiger un rapport de non-conformité
 - Principe du bénéfice du doute
- Documentation d'audit et revue de la qualité
 - Documents de travail
 - Revue de qualité
- Clôture de l'audit
 - Détermination des conclusions d'audit
 - Discussion des conclusions d'audit
 - Réunion de clôture
 - Préparation du rapport d'audit
 - Diffusion du rapport d'audit
 - Décision de certification
 - Clôture de l'audit
- Évaluation des plans d'action par l'auditeur
 - Présentation des plans d'action par l'audité
 - Contenu des plans d'action
 - Évaluation des plans d'action
- Après l'audit initial
 - Activités de suivi d'audit
 - Activités de surveillance
 - Audit de renouvellement de la certification
 - Utilisation des marques déposées
- Gestion d'un programme d'audit interne
 - Gestion d'un programme d'audit
 - Rôle de la fonction d'audit interne
 - Principaux services et activités de l'audit interne
 - Ressources du programme d'audit
 - Enregistrements relatifs au programme d'audit
 - Suivi des non-conformités
 - Surveillance, évaluation, revue et amélioration du programme d'audit
- Clôture de la formation
 - Schéma de certification de PECB
 - Processus de certification PECB
 - Autres services PECB
 - Autres formations et certifications PECB

JOUR 5 : Préparation et Passage de la certification

- L'examen couvre les domaines de compétences suivants :
 - Domaine 1 : Principes et concepts fondamentaux du Système de management de la sécurité de l'information
 - Domaine 2 : Système de management de la sécurité de l'information
 - Domaine 3 : Planification de la mise en œuvre d'un SMSI selon la norme ISO/CEI 27001:2022
 - Domaine 4 : Mise en œuvre d'un SMSI conforme à la norme ISO/CEI 27001:2022
 - Domaine 5 : Évaluation de la performance, surveillance et mesure d'un SMSI selon la norme ISO/CEI 27001:2022
 - Domaine 6 : Amélioration continue d'un SMSI selon la norme ISO/CEI 27001:2022
 - Domaine 7 : Préparation de l'audit de certification d'un SMSI