Formation « ISO 27001 Lead Auditor »

Réf : ISO27LA

Objectifs

- Apprendre à auditer sur la norme ISO27001 et les guides associés
- Devenir auditeur ou responsable d'équipe d'audit pour les systèmes de management de la sécurité de l'information (SMSI)
- Disposer de la vision auditeur vis-à-vis de la norme ISO 27001,
- Intégrer le modèle PDCA lors des activités d'audits,
- Auditer les différentes catégories de mesures de sécurité (Annexe A de l'ISO27001 / ISO27002) et conduire un audit de SMSI et ses entretiens en maîtrisant les notions de non-conformités majeures ou mineures.

Durée & horaires

- 5 jours soit 35 heures réparties en 31h30 de cours, 1h00 de travail individuel sur les exercices le soir et 2h30 d'examen.
- Du lundi au jeudi : de 9h30 à 12h00 et de 13h30 à 17h30/18h00.
- Le vendredi : de 09h30 à 12h00 et de 13h30/14h00 à 17h00/17h30.

Nombre de participant

- Minimum 6 participants – Maximum 24 participants

Public visé

- La formation s'adresse à tous ceux amenés à conduire des audits d'un SMSI et plus généralement un audit dans le domaine de la cybersécurité, donc :
  - les membres des équipes de contrôle interne,
  - des équipes sécurité ou des équipes d'audit,
  - les auditeurs d'autres systèmes de management comme les qualiticiens,
  - les auditeurs externes réalisant des audits conseil (appelés également pré-audits ou audit à blanc) pour leurs clients,
  - ceux souhaitant devenir auditeur de conformité ISO27001, et ceux devant être audités et devant comprendre l'état d'esprit de l'auditeur.

Pré-requis

- Aucun pré-requis n'est demandé. Toutefois, la connaissance des systèmes de management dans un autre domaine, la qualité par exemple, est un plus. La notion de SMSI (ISO 27001) et la réalisation d'audits de systèmes de management (ISO 19011) seront explicitées lors de la formation. Cependant la lecture des normes ISO 27001 et ISO 19011 avant la formation est recommandée. Les 133 mesures de sécurité sont rapidement survolées et ne seront pas acquises à l'issue de cette formation, leur maîtrise demandant des bases solides en informatique.

Méthode pédagogique

La méthode pédagogique se base sur les quatre points suivants :

- Cours magistral basé sur les normes ISO27001, ISO19011, et plus succinctement les normes ISO27002, ISO17021, ISO27006 et ISO27007.
- Exercices de contrôle des connaissances sur les concepts à connaître et sur les normes.

- **Exemples concrets illustrant les notions explicitées profitant du partage d'expérience des instructeurs HS2 tous auditeurs de SMSI**
- **Exercices pratiques individuels et collectifs effectués par les stagiaires, basés sur des cas réels d'audit anonymisés et un jeu de rôle auditeur / audité.**
- **Formation nécessitant 1 heure de travail personnel et ce quotidiennement durant la session.**

Supports

- **Support de cours au format papier en français en mode présentiel, au format numérique en mode distanciel**
- **Cahier d'exercices et corrections des exercices**
- **Tous les documents nécessaires à la formation en français ou anglais**
- **Certificat attestant de la participation à la formation**

Modalité d'évaluation de la formation

- **Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration**

Certification

Cette formation prépare à un examen de certification HS2 ISO 27001 Lead Auditor. Une attestation de stage nominative est envoyée au service formation du client à l'issue de la formation. En option, nous proposons également à la vente (à commander exclusivement simultanément avec la formation) avec la formation les examens suivants :

- ISO 27001 Lead Auditor de l'organisme de certification Best Certif éligible au CPF
- ISO 27001 Lead Auditor de l'organisme de certification Best Certif accrédité COFRAC
- ISO 27001 Lead Auditor de l'organisme de certification Certi-Trust

Tous ces examens en option se déroulent à distance à un horaire à choisir avec l'organisme certificateur

Programme

Accueil des participants et tour de table

Introduction à la sécurité des systèmes d'information

Introduction au système de management

- Notion de SMSI (Système de Management de la Sécurité de l'Information)
- Modèle PDCA (Plan-Do-Check-Act)

Présentation détaillée de la norme ISO 27001 pour l'auditeur

- Contexte de l'organisation
- Leadership
- Planification
- Support
- Fonctionnement
- Évaluation des performances
- Amélioration

Relations entre les éléments structurants du SMSI

- Principaux processus d'un SMSI

Processus de certification ISO27001

- Certification et accréditation
- Autorités d'accréditation
- Organismes de certification
- Normes ISO17021 et ISO27006
- Règlement de certification

Présentation de la norme ISO 27002

- Objectifs et usage de la norme
- Exigences de l'ISO 27001
- Auditer une mesure de sécurité
- Présentation des mesures de sécurité
- Exemple d'audit de mesures de sécurité

Présentation de la démarche d'audit de la norme ISO19011

- Principes de l'audit
- Types d'audit
- Programme d'audit
- Démarche d'audit
- Avant l'audit
- Audit d'étape 1
- Audit d'étape 2
- Après l'audit
- Auditeur et Responsable d'équipe d'audit

Présentation de la démarche d'audit SMSI

- Application ISO17021, ISO27006 et ISO19001 à un SMSI
- Critères d'audit
- Déroulement d'un audit
- Constats d'audit et fiches d'écart
- Conduite d'entretiens
- Réunion de clôture
- Rapport d'audit

Examen de certification HS2