Lead Auditor ISO 27001

Objectifs

Maîtriser la conduite d'un audit relatif à un système de management de la sécurité de l'information.
Appréhender les exigences de l'ISO 27001 et acquérir les connaissances nécessaires à l'évaluation d'un système de management de la sécurité de l'information.
Connaître les notions et principes spécifiques à la gestion de la sécurité de l'information (ISO 27002).
Identifier les objectifs de l'audit interne ou de l'audit de certification.
Savoir préparer, conduire et conclure un audit de façon pertinente et efficace, conformément à l'ISO 19011.
Maîtriser les techniques de communication propres à l'audit.
Gérer l'après-audit.

PUBLIC VISÉ :

L'ensemble des professionnels de la Sécurité, souhaitant maîtriser la conduite de l'audit et la démarche de certification afin de préparer ou réaliser des audits internes ou de conformité ISO 27001 :

- Membres des équipes de contrôle et d'audit interne.
- Consultants et auditeurs.
- Responsables de la sécurité des systèmes d'information.

PRÉ-REQUIS :

Connaissances générales de la sécurité des systèmes d'information ou expérience des audits.
La formation peut être préalable ou complémentaire à la certification « Lead Implementer ISO 27001 ».

PÉDAGOGIE & SUPPORTS :

Des phases pratiques et théoriques sont organisées en alternance, avec pour supports, les outils pédagogiques suivants :

- Cours théoriques : définitions, notions clés, acquisitions méthodologiques.
- Étude de cas.
- Exercices théoriques et pratiques.
- Supports visuels et documentaires.
- Prêt de normes ISO.

FORMATION DISPONIBLE en FRANCAIS / ANGLAIS

DURÉE :

5 JOURS (35H)

FORMATION + EXAMEN : 3 060 € HT
FORMATION SEULE : 2 460 € HT
DATES DE SESSION P. 12-13.

Programme

1. Accueil des participants et présentation de la formation « Lead Auditor ISO 27001 ».
2. Présentation de la famille des normes ISO 2700X.
3. Exposé sur les exigences de l'ISO 27001, description de la notion de Système de Management de la Sécurité de l'Information (SMSI), présentation du modèle Plan, Do, Check, Act (PDCA), définition de la notion de risque et des objectifs à atteindre.
4. Présentation du référentiel d'audit ISO 27001, description des points de contrôles et des éléments techniques à apprécier conformément à l'Annexe A de l'ISO 27001.
5. Exposé des lignes directrices de l'audit définies dans l'ISO 19011.
6. Présentation du déroulement d'un audit : différentes phases pour la réalisation d'un audit (de la programmation à l'après-audit) et supports documentaires accompagnant chaque phase (programme, plan, rapport, fiches d'écarts).
7. Ateliers personnalisés : mise en pratique avec l'étude de documents, la réalisation d'exercices, l'élaboration de supports, la correction de cas pratiques.
8. Exposé sur la communication, clé du succès de l'audit : différentes attitudes, déontologie, conduite d'un entretien, gestion de la communication orale et recueil écrit des informations, animation d'une réunion de clôture.
9. Entraînement à la pratique de l'audit autour des thèmes : audit de procédures (conduite de l'audit, prise de notes, gestion du temps) , réunion d'ouverture (présentation du plan d'audit, organisation), réunion de clôture (élaboration de conclusions d'audit, restitution des résultats de l'évaluation, présentation des écarts et accompagnement dans la décision d'actions).
10. Entraînement pour corriger l'attitude de l'auditeur (autour des 3 items : savoir, savoir-faire, savoir-être, et/ou avec une appréciation de ce qui est acquis, à compléter, à approfondir), comprendre les difficultés rencontrées lors de l'audit, éviter les pièges, maîtriser la communication, être efficace.
11. Présentation de l'audit tierce partie : environnement normatif et procédure de certification.
12. Conclusion et bilan de la formation (appréciation et positionnement des participants sur leurs acquis initialement, en cours et en fin de formation).

Examen en vue de la certification Lead Auditor ISO 27001