ISO 27001 : Lead auditor

Ce cours intensif de cinq jours permet aux participants d'acquérir les connaissances nécessaires et de développer l'expertise pour :

- planifier et effectuer des audits de la conformité d'un système de management de la sécurité de l'information par rapport aux exigences de la norme ISO 27001;
- manager une équipe d'auditeurs en appliquant les principes, procédures et techniques d'audits communément reconnus.

A partir d'exercices pratiques basés sur un cas d'étude, le stagiaire sera mis en situation de développer les compétences (maîtrise des techniques d'audit) et les aptitudes (gestion d'équipes et d'un programme d'audit, communication avec les clients, résolution de conflits, etc.) nécessaires à la conduite d'un audit.

La formation est basée sur les lignes directrices d'audit de système de management (ISO 19011 :2002) ainsi que les meilleures pratiques internationales d'audit. Elle se compose de :

- Cours magistraux illustrés de cas concrets,
- Exercices pratiques, réalisés seul ou en groupe (jeux de rôles), tirés de missions réelles, en lien direct avec la préparation à l'examen.

Objectifs :

- Comprendre les principes d'application de l'ISO 27 001 :2005 dans la construction d'un système de management de la sécurité de l'information,
- Comprendre la relation entre le système de management de la sécurité de l'information, le management des risques, les mesures, et les différentes parties prenantes,
- Comprendre les principes, procédures et techniques d'audit de l'ISO 19011 :2002, et comment les appliquer dans le cadre d'un audit selon l'ISO 27001,
- Comprendre l'application des obligations légales, statutaires, réglementaires ou contractuelles pertinentes lors de l'audit d'un SMSI,
- Acquérir les compétences nécessaires pour effectuer un audit de façon efficace, et les techniques de gestion d'une équipe d'audit, préparer et compléter un rapport d'audit ISO 27001.

Prérequis :

Une connaissance préalable des normes ISO 27001 et ISO 27002 est recommandée.

Participants :

- Personnes désirant diriger des audits de certification ISO 27001 en tant que responsable d'une équipe d'audit,
- Consultants désirant préparer et accompagner une organisation lors d'un audi t de certification ISO 27001,
- Auditeurs internes désirant préparer et accompagner leur organisation vers l'audit de certification ISO 27001,
- Responsables de la sécurité de l'information ou de la conformité,
- Conseillers experts en technologies de l'inform ation.

Programme :

Jour 1 : Introduction à la gestion d'un système de management de la sécurité de l'information selon ISO 27001

- Objectifs et structure du cours
- Cadre normatif et réglementaire
- Processus de certification ISO 27001
- Principes fondamentaux de la sécurité de l'information et de la gestion du risque
- Système de management de la sécurité de l'information (SMSI)
- Présentation des clauses 4 à 8 de l'ISO 27001

Jour 2 : Démarrer un audit ISO 27001

- Concepts et principes fondamentaux d'audit
- Éthique et déontologie de l'audit
- L'approche d'audit fondée sur la preuve et sur le risque
- Préparation d'un audit de certification ISO 27001
- L'audit documentaire
- Préparation du plan d'audit
- Conduite d'une réunion d'ouverture

Jour 3 : Conduire un audit ISO 27001

- Communication durant l'audit
- Les procédures d'audit (observation, entrevue, techniques d'échantillonnage)
- Rédaction des conclusions d'audit et des rapports de non -conformité

Jour 4 : Conclure un audit ISO 27001

- Documentation de l'audit
- Revue des notes d'audit
- Conclusion d'un audit ISO 27001
- Gestion d'un programme d'audit
- La compétence et l'évaluation des auditeurs
- Clôture de la formation

Jour 5 : Examen

- Examen

Examen et certification :

L'examen ISMS - ISO 27001 Lead Auditor est certifié par le RABQSA et répond aux critères du 'RABQSA Training Provider Examination Certification Scheme' (TPECS), dont il couvre les unités de compétence :

- RABQSA – IS (sécurité de l'information),
- RABQSA – AU (Techniques d'audit),
- RABQSA –TL (Techniques d'auditeur pr incipal).

L'examen ISMS - ISO 27001 Lead Auditor est disponible en français, en anglais et en espagnol.

Un certificat est remis aux participants ayant réussi l'examen.

Le certificat de réussite d'examen RABQSA est reconnu par l'IRCA et répond aux critè res de certification IRCA/2016.

Le participant ayant réussi l'examen pourra s'inscrire auprès de l'IRCA ou du RABQSA, et prétendre, selon son expérience de l'audit, au titre d'auditeur provisoire ISO 27001, d'auditeur ISO 27001, d'auditeur principal ISO 2 7001, ou de Lead Auditor ISO 27001.

Documentation fournie aux participants :

- Une copie papier de la norme ISO/CEI 27001 :2005
- Une attestation de participation de 35 CPE (Continuing Professional Education),
- Une trousse à outils d'audit ainsi qu'un manuel de l'étudiant (plus de 400 pages d'informations et d'exemples pratiques)

Durée :

La durée de la session est de 5 jours : 4 jours de cours et une demi-journée d'examen, soit un stage de 40 heures réparties en 32 heures de cours, 5 heures de travail individuel à réaliser le soir après les cours, et 3 heures d'examen.

Cette durée de 40 heures répond à une exigence de la norme ISO 19011 :2002.

Coût :

Le coût de l'examen est **inclus** dans le tarif spécifique de cette formation.

Référence : FCS001