ISO 27001 Lead Auditor /Sécurité de l'information

★★★★★

SII-422 **5 Jours (35 Heures)**

Description

La formation "ISO/IEC 27001 Lead Auditor" vous permettra de développer l'expertise requise pour mener un audit du système de management de la sécurité de l'information (SMSI) en utilisant des principes, procédures et techniques largement reconnus en audit.

Grâce à cette formation, vous serez en mesure de planifier et de réaliser des audits internes et externes conformément aux processus de certification ISO 19011 et ISO/IEC 17021-1, tout en acquérant les connaissances et les compétences nécessaires.

À qui s'adresse cette formation ?

Pour qui

- Responsables ou consultants impliqués dans le management de la sécurité de l'information.
- Conseillers spécialisés désirant maîtriser la mise en œuvre d'un Système de management de la sécurité de l'information.
- Toute personne responsable du maintien de la conformité aux exigences du SMSI . Membres d'une équipe du SMSI .

Prérequis

Bonne connaissance de la norme ISO/IEC 27001 et connaissance approfondie des principes de mise en œuvre.

Les objectifs de la formation

- Comprendre la relation entre la norme ISO/CEI 27001, la norme ISO/CEI 27002, ainsi que d'autres normes et cadres réglementaires
- Maîtriser les concepts, les approches, les méthodes et les techniques nécessaires pour mettre en place et gérer efficacement un SMSI
- Interpréter les exigences de la norme ISO/CEI 27001 dans un contexte spécifique à l'organisation
- Accompagner une organisation dans la planification, la mise en œuvre, la gestion, la surveillance et la tenue à jour du SMSI

- Acquérir l'expertise nécessaire pour conseiller une organisation sur la mise en œuvre des meilleures pratiques en matière de système de management de la sécurité de l'information

Programme de la formation

Jour 1: introduction au système de management de la sécurité de l'information (SMSI) et la norme ISO/IEC 27001

- Tirer parti de la formation pour acquérir de nouvelles connaissances et compétences sur la sécurité de l'information et le système de management de la sécurité de l'information (SMSI).
- Se familiariser avec les normes et cadres réglementaires pertinents pour le domaine de la sécurité de l'information en suivant la formation.
- Comprendre le processus de certification en sécurité de l'information grâce à la formation.
- Apprendre les concepts et principes fondamentaux de la sécurité de l'information en suivant la formation.
- Acquérir des connaissances sur la mise en place et la gestion d'un système de management de la sécurité de l'information (SMSI) grâce à la formation.

Jour 2 : Les fondements, la planification et l'initiation de l'audit

- Les concepts et principes fondamentaux de l'audit sont les fondements du processus d'audit, incluant l'intégrité, l'objectivité, la compétence, la confidentialité, la planification et la supervision.
- L'impact des tendances et de la technologie en audit est de plus en plus important, avec l'utilisation de l'IA, de la blockchain et d'autres outils qui améliorent l'efficacité et la qualité de l'audit.
- L'audit basé sur les preuves consiste à collecter des preuves tangibles et vérifiables pour évaluer la conformité aux normes et procédures internes, ainsi que pour identifier les non-conformités et les opportunités d'amélioration.
- L'audit basé sur les risques implique l'évaluation des risques associés aux activités de l'entreprise et la planification de l'audit en conséquence, afin de couvrir les zones les plus à risque.
- L'initiation du processus d'audit implique la notification de l'audit aux parties prenantes concernées, la planification des activités d'audit et la collecte des informations nécessaires.
- L'étape 1 de l'audit consiste à définir les objectifs de l'audit, à sélectionner l'équipe d'audit et à identifier les domaines à auditer. C'est une étape importante pour assurer la réussite de l'audit.

Jour 3 : Les activités d’audit sur site

- La préparation de la deuxième étape de l'audit consiste à planifier les activités et à recueillir les informations nécessaires pour mener à bien cette étape.
- L'étape 2 de l'audit est la phase durant laquelle les informations collectées sont évaluées et vérifiées afin de confirmer la conformité aux normes et aux procédures internes.
- La communication pendant l'audit est une étape importante pour assurer la transparence et la collaboration entre les parties prenantes impliquées dans l'audit.
- Les procédures d'audit sont des instructions détaillées qui guident l'auditeur tout au long du processus d'audit.
- La création de plans de test d'audit est une étape clé pour garantir que toutes les zones à risque sont couvertes lors de l'audit et que les résultats sont fiables.

Jour 4 : Clôture de l’audit

- Les rapports de constatations d'audit et de non-conformité sont rédigés à l'issue de l'audit.
- La documentation d'audit est examinée ainsi que la revue de qualité.
- La clôture de l'audit est la dernière étape du processus d'audit au cours de laquelle les résultats sont présentés et les actions correctives éventuelles sont identifiées.
- L'évaluateur vérifie l'efficacité des plans d'action mis en place suite à l'audit.
- Après l'audit initial, les mesures correctives sont mises en place pour améliorer les processus.
- La gestion d'un programme d'audit interne est nécessaire pour garantir la conformité aux normes et aux réglementations.
- La clôture de la formation marque la fin de la session de formation.

Jour 5 : Révision pour préparer les candidats à passer l'examen de certification

- Révision des concepts en vue de la certification et examen blanc
- Un voucher permettant le passage du test de certification est adressé à l'issue de la session