Développez vos talents
Certifiez vos compétences

Gouvernance et Juridique

ISO 27001 - Lead Auditor - Avec certification

5 jours (35h00) | ★★★★½ 4,6/5 | ISO-27LA | Code Certif Info : 104041 | Certification PECB 27001 Lead Auditor (incluse) | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel [1]

Formations Informatique › Cybersécurité › Gouvernance et Juridique

À l'issue de ce stage vous serez capable de :

- Comprendre le fonctionnement d'un Système de Management de la Sécurité de l'Information (SMSI) conforme à la norme ISO/CEI 27001
- Expliquer la corrélation entre la norme ISO/CEI 27001 et la norme ISO/CEI 27002, ainsi qu'avec d'autres normes et cadres réglementaires
- Comprendre le rôle d'un auditeur : planifier, diriger et assurer le suivi d'un audit de système de management conformément à la norme ISO 19011
- Diriger un audit et une équipe d'audit
- Interpréter les exigences d'ISO/CEI 27001 dans le contexte d'un audit du SMSI
- Acquérir les compétences d'un auditeur dans le but de : planifier un audit, diriger un audit, rédiger des rapports et assurer le suivi d'un audit, en conformité avec la norme ISO 19011.

Niveau requis

Avoir une bonne connaissance de la norme ISO/CEI 27001 et des connaissances approfondies sur les principes de l'audit.

Public concerné

Auditeurs SMSI, responsables ou consultants SMSI, experts techniques désirant préparer un audit du SMSI, conseillers spécialisés SMSI ou toute personne responsable du maintien de la conformité aux exigences du SMSI.

(1) Modalité et moyens pédagogique :

Formation délivrée en présentiel ou distanciel * (e-learning, classe virtuelle, présentiel à distance). Le formateur alterne entre méthodes ** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation). La validation des acquis peut se faire via des études de cas, des quiz et/ou une certification.

Les moyens pédagogiques mis en oeuvre (variables suivant les formations) sont : ordinateurs Mac ou PC (sauf pour les cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel). Environnements de formation installés sur les postes de travail ou en ligne. Supports de cours et exercices.

* Nous consulter pour la faisabilité en distanciel. ** Ratio variable selon le cours suivi.

Cette formation :

- Est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par M2i Formation
- Bénéficie d'un suivi de son exécution par une feuille de présence émargée par demi-journée par les stagiaires et le formateur.

Programme

Jour 1

Introduction à la norme ISO/CEI 27001 et initialisation d'un SMSI

- Objectifs et structure de la formation
- Cadres normatifs et règlementaires
- Etude du SMSI
- Principes et concepts fondamentaux du SMSI
- Initialisation de la mise en oeuvre du SMSI
- Compréhension de l'organisation et clarification des objectifs de sécurité de l'information
- Analyse du système de management existant

Jour 2

Planification de la mise en oeuvre d'un SMSI

- Leadership et approbation du projet du SMSI
- Périmètre du SMSI
- Politiques de sécurité de l'information
- Appréciation du risque
- Déclaration d'applicabilité et décision de la direction pour la mise en oeuvre du SMSI
- Définition de la structure organisationnelle de la sécurité de l'information

Jour 3

Mise en oeuvre d'un SMSI

- Définition d'un processus de gestion de la documentation
- Conception des mesures de sécurité et rédaction des procédures et des politiques spécifiques
- Plan de communication
- Plan de formation et de sensibilisation
- Mise en oeuvre des mesures de sécurité
- Gestion des incidents
- Gestion des activités opérationnelles

Jour 4

Surveillance, mesure, amélioration continue et préparation de l'audit de certification du SMSI

- Surveillance, mesure, analyse et évaluation
- Audit interne
- Revue de direction
- Traitement des non-conformités
- Amélioration continue
- Préparation de l'audit de certification
- Compétence et évaluation des "implementers"

Jour 5

Passage de la certification

- Le prix et le passage de l'examen sont inclus dans la formation
- L'examen (en français) a lieu le dernier jour, à l'issue de la formation et s'effectue en ligne ou sur papier, pour une durée moyenne de 3h00
- Examen papier composé de 12 questions ouvertes pour un total de 75 points
- Un score minimum de 70% est requis pour réussir l'examen

- Déroulement à "livre ouvert" (autorisé avec support et notes personnelles prises durant la session)

Modalités d'évaluation des acquis

L'évaluation des acquis se fait :

- En cours de formation, par des études de cas ou des travaux pratiques
- Et, en fin de formation, par un questionnaire d'auto-évaluation ou une certification (M2i ou éditeur)

Les + de la formation

Ce cours est animé par un formateur certifié PECB.

Compétences visées

- Décrire les éléments et le fonctionnement d'un système de management de la sécurité de l'information à l'intention des responsables de l'entreprise, en vue de les impliquer dans l'élaboration d'un programme d'audit de celui-ci
- Préparer et planifier un audit du système de management de la sécurité de l'information conformément à la norme ISO / IEC 27001, afin d'assurer la fiabilité des résultats de celui-ci
- Diriger un audit du système de management de la sécurité de l'information conformément à la norme ISO 19011, afin d'assurer un encadrement de l'équipe d'auditeurs adapté aux objectifs
- Clôturer un audit du système de management de la sécurité de l'information, en vue d'assurer des activités de suivi conformes à la norme ISO / IEC 27001
- Rédiger un rapport d'audit du système de management de la sécurité de l'information, en vue de conseiller une entreprise sur les meilleures pratiques en matière de sécurité de l'information et de renforcer ainsi l'efficacité du système de management de la sécurité de l'information.