

ISO 27001 - Certification Lead Implementer

5 j (35 heures)

Ref : ISO27001

Public

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

Pré-requis

Connaissance de base de la sécurité des systèmes d'information

Moyens pédagogiques

Formation réalisée en présentiel ou à distance selon la formule retenue
Exposés, cas pratiques, synthèse, assistance post-formation pendant un mois
Un poste par stagiaire, vidéoprojecteur ou écran interactif tactile, support de cours fourni à chaque stagiaire

Modalités de suivi et d'évaluation

Feuille de présence émargée par demi-journée par les stagiaires et le formateur
Exercices de mise en pratique ou quiz de connaissances tout au long de la formation permettant de mesurer la progression des stagiaires
Questionnaire d'évaluation de la satisfaction en fin de stage
Auto-évaluation des acquis de la formation par les stagiaires
Passage de l'examen de certification ISO 27001 Lead Implementer en fin de formation (durée : 3h)
Attestation de fin de formation

Objectifs

- Comprendre la corrélation entre la norme ISO/CEI 27001 et la norme ISO/CEI 27002
- Maîtriser les techniques nécessaires pour mettre en œuvre et gérer efficacement un SMSI
- Savoir interpréter les exigences de la norme ISO/CEI 27001
- Savoir accompagner une organisation dans la planification et la gestion du SMSI
- Savoir accompagner une organisation dans la surveillance et la tenue à jour du SMSI
- Se préparer et passer la certification ISO 27001 Lead Implementer

Programme détaillé

INTRODUCTION A LA NORME ISO/CEI 27001 ET INITIALISATION D'UN SMSI

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

PLANIFICATION DE LA MISE EN ŒUVRE 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 œuvre du SMSI
Définition de la structure organisationnelle de la sécurité de l'information

MISE EN ŒUVRE 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 œuvre des mesures de sécurité
Gestion des incidents
Gestion des activités opérationnelles

SURVEILLANCE, MESURE, AMELIORATION CONTINUE ET PREPARATION 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 »
Clôture de la formation

PASSAGE DE LA CERTIFICATION PECB ISO 27001 LEAD IMPLEMENTER

L'examen couvre les domaines de compétences suivants :
Domaine 1 : Principes et concepts fondamentaux du Système de management de la sécurité de l'information
Domaine 2 : Système de management de la sécurité de l'information
Domaine 3 : Planification de la mise en œuvre d'un SMSI selon la norme ISO/CEI 27001

Domaine 4 : Mise en œuvre d'un SMSI conforme à la norme ISO/CEI 27001

Domaine 5 : Évaluation de la performance, surveillance et mesure d'un SMSI selon la norme ISO/CEI 27001

Domaine 6 : Amélioration continue d'un SMSI selon la norme ISO/CEI 27001

Domaine 7 : Préparation de l'audit de certification d'un SMSI
