

Formation **ISO 27001 Lead Implementer** (avec certification)

Notre formation ISO 27001 Lead Implementer est conçue pour vous permettre d'acquérir les connaissances et compétences nécessaires pour accompagner votre organisation dans la mise en œuvre d'un Système de Management de la Sécurité de l'Information (SMSI). Vous maîtriserez les bonnes pratiques relatives à l'établissement, l'implémentation, la gestion et le suivi du SMSI conformément aux dispositions de la norme ISO/IEC 27001:2022. Sécurisez les informations sensibles, améliorez l'efficacité et in fine la performance globale de votre organisation grâce à ce stage intensif de 5 jours. A l'issue de notre formation, les participants passeront la certification ISO 27001 Lead Implementer. L'examen s'effectuera durant la dernière journée de formation, sous la supervision d'un formateur accrédité. Le coût de l'examen est inclus dans le prix de la formation.

Durée

5 jours

Objectifs pédagogiques

- ❖ Maîtriser les concepts, approches et méthodes de mise en œuvre et de gestion d'un SMSI.
- ❖ Comprendre les liens entre ISO/IEC 27001, ISO/IEC 27002 et d'autres cadres réglementaires.
- ❖ Appréhender le fonctionnement d'un SMSI et ses processus selon ISO/IEC 27001.
- ❖ Interpréter et appliquer les exigences de la norme dans un contexte organisationnel.
- ❖ Acquérir les compétences nécessaires pour planifier, gérer et maintenir un SMSI efficace.

Public

MOA, MOE, Risk managers, RSSI,
Auditeurs...

Prérequis

Connaissances basiques des concepts
de la sécurité des système
d'information

Programme de formation

Phase d'inclusion

Accueil des participants, présentation des objectifs et contextes professionnels de chacun.

Introduction à la norme ISO/IEC 27001 et démarrage de la mise en œuvre d'un SMSI

- Objectifs et structure de la formation
- Normes et cadres réglementaires
- Système de gestion de la sécurité de l'information basé sur la norme ISO/IEC 27001
- Concepts et principes fondamentaux de la sécurité de l'information
- Lancement de la mise en œuvre du SMSI
- Comprendre l'organisation et son contexte
- Champ d'application du SMSI

Plan de mise en œuvre d'un SMSI

- Leadership et approbation du projet
- Structure organisationnelle
- Analyse du système existant
- Politique de sécurité de l'information

- Management du risque
- Déclaration de conformité

Mise en œuvre du SMSI

- Sélection et conception des mesures de sécurité
- Mise en œuvre des mesures de sécurité
- Gestion des informations documentées
- Tendances et technologies
- Communication
- Compétence et sensibilisation
- Gestion des opérations de sécurité

Suivi, amélioration continue et préparation à l'audit de certification du SMSI

- Surveillance, mesurage, analyse et évaluation
- Audit interne
- Revue de direction
- Traitement des non-conformités
- Amélioration continue
- Préparation de l'audit de certification
- Clôture de la formation

Examen de certification

Moyens et méthodes pédagogiques

- La formation alterne entre présentations des concepts théoriques et mises en application à travers d'ateliers et exercices pratiques (hors formation de type séminaire).
- Les participants bénéficient des retours d'expérience terrains du formateur ou de la formatrice
- Un support de cours numérique est fourni aux stagiaires

Modalités d'évaluation

- **En amont de la session de formation**, un questionnaire d'auto-positionnement est remis aux participants, afin qu'ils situent leurs connaissances et compétences déjà acquises par rapport au thème de la formation.
- **En cours de formation**, l'évaluation se fait sous forme d'ateliers, exercices et travaux pratiques de validation, de retour d'observation et/ou de partage d'expérience, en cohérence avec les objectifs pédagogiques visés.
- **En fin de session**, le formateur évalue les compétences et connaissances acquises par les apprenants grâce à un questionnaire reprenant les mêmes éléments que l'auto-positionnement, permettant ainsi une analyse détaillée de leur progression.