

## Formation « ISO 27001 Lead Implementer »

Réf : ISO27LI

### Objectifs

- Apprendre à mettre en œuvre la norme ISO27001 et les guides associés
- Apprendre à utiliser concrètement les normes, avec des exemples pour que chacun puisse les utiliser chez lui ou chez ses clients : les processus à mettre en place, le dimensionnement et l'organisation du projet, etc

### Durée & horaires

- 5 jours soit 35 heures réparties en 31h00 de cours, 1h00 de travail individuel sur les exercices le soir et 3h00 d'examen. L'heure de travail individuel correspond à des exercices donnés aux participants par les formateurs à réaliser le soir et qui sont corrigés le lendemain pendant la formation.
- Du lundi au jeudi : de 9h30 à 12h00 et de 13h30 à 17h30/18h00.
- Le vendredi : de 09h30 à 12h00 et de 13h30/14h00 à 17h00/17h30.

### Nombre de participant

- Minimum 6 participants – Maximum 24 participants

### Public visé

- Personnes devant mettre en œuvre un SMSI à tous les niveaux, du management à l'opérationnel :
  - RSSI et à leurs équipes
  - Personnes responsables de services opérationnels
  - DSI et leurs équipes
  - Responsables méthodes et qualité
  - Consultants et aux personnes en reconversion souhaitant mettre en œuvre l'ISO27001
- Personnes devant participer à l'implémentation de la norme en vue d'une certification ISO27001 ou une certification HDS (Hébergeur de Données de Santé)

### Pré-requis

- Aucun pré-requis n'est demandé. Toutefois, avoir une expérience en informatique et en sécurité est un plus.

### Méthode pédagogique

La formation peut être suivie en mode présentiel ou en mode distanciel via ZOOM.

La méthode pédagogique se base sur les quatre points suivants :

- Cours magistral basé sur la norme ISO27001:2022, et plus succinctement les normes ISO27002/2022, ISO27003, ISO2004 et ISO27005.
- Exercices de contrôle des connaissances sur les concepts à connaître et sur les normes.
- Exemples concrets illustrant les notions explicitées profitant du partage d'expérience des instructeurs HS2 tous implémenteurs de SMSI
- Exercices pratiques individuels et collectifs effectués par les stagiaires, basés sur des études de cas : périmètre, politique, procédures, plan projet, suivi et réunions, traitement des risques, surveillance et indicateurs. Ces exercices permettent également de se préparer à l'examen de certification.
- Formation nécessitant 1 heure de travail personnel et ce quotidiennement durant la session.

### Supports

- Support de cours en français au format papier en mode présentiel et au format numérique en mode distanciel (après signature d'une attestation de non diffusion)
- Cahier d'exercices et corrections des exercices
- Tous les documents nécessaires à la formation en français ou anglais
- Certificat attestant de la participation à la formation

### Modalité d'évaluation de la formation

- Fiche d'évaluation remise aux stagiaires à l'issue de la formation afin de recueillir leurs impressions et identifier d'éventuels axes d'amélioration
- Evaluation de pré-formation envoyée avant le début de la formation
- Evaluation de mi-formation effectuée en session par le formateur au moyen de QCM et de travaux pratiques
- Examen final à la fin de la formation (cf certification)
- Ces évaluations ont pour but de valider les compétences acquises.

### Certification

- Cette formation prépare à l'examen de certification HS2 ISO 27001 Lead Implementer. A l'issue de cette formation, le stagiaire passe l'examen d'une durée de 3h00 en français. L'examen est constitué d'une partie QCM sur les notions de cours et d'une partie rédactionnelle sous forme d'étude de cas. En option, nous proposons également à la vente (à commander exclusivement simultanément avec la formation) avec la formation les examens suivants :
  - ISO 27001 Lead Auditor de l'organisme de certification Best Certif éligible au CPF
  - ISO 27001 Lead Auditor de l'organisme de certification Certi-TrustTous ces examens en option se déroulent à distance à un horaire à choisir avec l'organisme certificateur

### Programme

#### Accueil des participants et tour de table

#### Introduction à la sécurité des systèmes d'information

#### Introduction au système de management

- Notion de SMSI (Système de Management de la Sécurité de l'Information)
- Modèle PDCA (Plan-Do-Check-Act)

#### Présentation détaillée de la norme ISO 27001

- Contexte de l'organisation
- Leadership
- Planification
- Support
- Fonctionnement
- Évaluation des performances
- Amélioration

#### Présentation de la norme ISO 27002

- Différentes catégories de mesures de sécurité
- Mesures d'ordre organisationnel / technique
- Implémentation d'une mesure de sécurité selon le modèle PDCA

#### Panorama des normes complémentaires

- ISO27017, ISO27018, ISO27025

#### Processus dans un SMSI

- Processus support
- Gestion des exigences légales et réglementaires
- Gestion des risques
- Implémentation et suivi des mesures de sécurité
- Gestion des incidents
- Gestion documentaire
- Évaluation de la performance

#### La gestion des risques et la norme ISO 27005

- Vocabulaire : risque, menace, vulnérabilité, etc.
- Critères de gestion de risque
- Appréciation des risques, acceptation du risque, communication du risque
- Déclaration d'applicabilité (DdA/SoA)
- Réexamen du processus de gestion de risques et suivi des facteurs de risques

#### Gestion des exigences légales et réglementaires

- Protéger les données à caractère personnelles

- Outils de veille juridique
- Gestion des engagements contractuels
- Gestion des fournisseurs et prestataires
- Contractualiser la sécurité

### **L'évaluation des performances**

- Surveillance au quotidien
- Indicateurs et norme ISO 27004
- Audit interne
- Revue de Direction

### **Projet SMSI**

- Conviction la direction
- Étapes du projet
- Acteurs
- Facteurs clés de réussite et d'échec
- Processus de certification ISO27001

### **Certification ISO27001**

- Accréditation
- Normes ISO19011 et ISO27007
- Normes ISO17021 et ISO27006
- Règlement de certification

### **Examen de certification HS2**

## Pour aller plus loin

**Nous vous recommandons de suivre les formations suivantes :**

- **ISO27RM – ISO 27005 Risk Manager**
- **ISO 27004 – Indicateurs et tableaux de bord de la cybersécurité**
- **ISO27035 – Gestion des incidents de sécurité**
- **SECUPKI – Principe et mise en œuvre des PKI**