

# Lead Implementer – Certification ISO 27001



## Description de la formation

Formation conforme à la norme internationale de maîtrise du risque ISO/CEI 27001 liée à la sécurité de l'information permettant d'acquérir l'expertise nécessaire pour accompagner une organisation lors de l'établissement, la mise en œuvre, la gestion et la tenue à jour d'un Système de management de la sécurité de l'information (SMSI) conforme à la norme ISO/CEI 27001.

Cette formation intègre les frais d'examen de la certification « Lead Implementer ISO 27001 » (PECB) attestant des connaissances et compétences nécessaires à la mise en place d'un SMSI suivant la norme ISO/IEC 27001. En étant titulaire d'une certification PECB, vous démontrerez que vous disposez des connaissances pratiques et des compétences professionnelles pour mettre en œuvre la norme ISO/CEI 27001 dans une organisation.

## Objectifs pédagogiques

- › Connaître et savoir interpréter les exigences de la norme ISO/CEI 27001.
- › Savoir planifier et mettre en place un SMSI : direction, pilotage, contrôles, gestion du risque, etc.
- › Acquérir les compétences nécessaires pour conseiller des structures dans la mise en place et la gestion d'un SMSI.
- › Préparer et passer la certification Lead Implementer ISO 27001 dans des conditions de succès.

## Prérequis

- › Connaître le guide sécurité de l'ANSSI.
- › Avoir suivi le parcours introductif à la cybersécurité ou posséder des connaissances équivalentes sur la sécurité des systèmes d'information.

## Modalités pédagogiques

- › **Modalité :** Formation réalisée en présentiel ou en distanciel selon la formule retenue.
- › **Méthode :** La formation se déroule entre 50% de théorie et 50% de pratique. Le formateur partage des points théoriques et des cas concrets, lance des discussions et échanges entre les stagiaires et propose des jeux / outils en relation avec le contenu et des mises en pratique.
- › **Support de formation :** Le support de formation (plus de 450 pages d'informations et d'exemples pratiques) est remis au stagiaire à l'issue de la formation.

## Modalités techniques

- › En format présentiel, le formateur dispose d'une présentation (support de formation), d'un vidéoprojecteur (ou TV), de tableaux blancs et de jeux / d'outils pédagogiques.
- › En format présentiel, le stagiaire a besoin d'un ordinateur pouvant être connecté à internet, équipé d'un micro et d'une webcam pour passer la certification.
- › En format distanciel, le formateur dispose d'une présentation (support de formation), d'une plateforme de visioconférence et d'outils collaboratifs numériques.
- › En format distanciel, le stagiaire a besoin d'avoir une bonne connexion internet et d'un ordinateur équipé d'une webcam et d'un micro.

## Code

CYB040

## Durée

5 jours (35 heures)

## Nombre de participants

Entre 4 (minimum) et 12 (maximum) participants.

## Profil des stagiaires

Chefs de projets, Consultants, Architectes Techniques, Responsables de la sécurité des systèmes d'information, Risk Managers ou tout acteur SI chargé de la sécurité de l'entreprise.

## Sanction de la formation

Attestation de fin de formation.

## Accessibilité

Accessible pour les personnes en situation de handicap et aménagement possible en fonction du type de handicap (prévenir avant le début de la formation).

## Modalités et délais d'accès

10 jours minimum avant la formation pour une demande de prise en charge.

## Modalités de suivi et d'évaluation

- › Evaluation préalable.
- › Autoévaluation des acquis au cours des exercices et mises en pratiques au cours de la formation.
- › Evaluation de fin de formation sous forme de test (QCM) afin de valider l'acquisition des compétences et des connaissances.
- › Examen « Lead Implementer ISO 27001 » (certificateur PECB).
- › Questionnaire d'évaluation de la satisfaction en fin de formation.
- › Feuille d'émargement signée par le(s) stagiaire(s) et le formateur, par demi-journée de formation.
- › Attestation de fin de formation.
- › Evaluation de suivi à froid (+ 1 mois).

## Intervenant

Corentin est **Consultant & Formateur en cybersécurité**. Il conseil les entreprises dans la gestion des risques liés à la sécurité de l'information, ainsi que l'implémentation et la certification d'un SMSI.

## Tarifs

- › Interentreprises : 2 200,00 € HT
- › Intra-entreprise : sur demande

## Contenu de la formation

### JOUR 01

#### INTRODUCTION A ISO/IEC 27001 ET INITIATION D'UN SMSI

- › Objectifs et structure de la formation
- › Normes et cadres réglementaires
- › Système de management de la sécurité de l'information (SMSI)
- › Concepts et principes fondamentaux de la sécurité de l'information
- › Initiation de la mise en œuvre du SMSI
- › Compréhension de l'organisme et de son contexte
- › Périmètre du SMSI

### JOUR 02

#### PLANIFICATION DE LA MISE EN ŒUVRE D'UN SMSI

- › Leadership et approbation du projet
- › Structure organisationnelle
- › Analyse du système existant
- › Politique de sécurité de l'information
- › Gestion des risques
- › Déclaration d'applicabilité

### JOUR 03

#### MISE EN ŒUVRE D'UN SMSI

- › Gestion de l'information documentée
- › Sélection et conception des mesures de sécurité
- › Mise en œuvre des mesures de sécurité
- › Tendances et technologies
- › Communication
- › Compétence et sensibilisation
- › Gestion des opérations de sécurité

### JOUR 04

#### SURVEILLANCE DU SMSI, AMELIORATION CONTINUE ET PREPARATION A L'AUDIT DE CERTIFICATION

- › Surveillance, mesure, analyse et évaluation
- › Audit interne
- › Revue de direction
- › Traitement des non-conformités
- › Amélioration continue
- › Préparation à l'audit de certification
- › Processus de certification et clôture de la formation

### JOUR 05

#### EXAMEN DE CERTIFICATION PECB

Passage de l'examen. L'examen porte sur les domaines 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

En cas d'échec à l'examen, le stagiaire pourra le repasser sans frais dans les 12 mois suivants.