# ISO 27001 Lead Implementer

**Prix** : 3 890€ HT

**Durée** : 5 jours

**Code de Référence** : SELI27001

**4/5 Satisfaction globale - Moyenne des 24 derniers mois**

Cette formation certifiante vous permettra d'obtenir la certification ISO 27001 Lead Implementer. Elle vise à appréhender la corrélation entre la norme ISO 27001 et la ISO 27002, et d'autres normes et cadres réglementaires, et de maîtriser toutes les techniques, approches pour mettre en œuvre un SMSI (Système de Management de la Sécurité de l'Information). Cette formation permettra également d'accompagner et conseiller une structure quant au processus complet d'implémentation d'un SMSI efficace, de la planification à la maintenance.

## Objectifs de la formation

- Expliquer les concepts et principes fondamentaux d'un système de management SMSI basé sur ISO/IEC 27001
- Interpréter les exigences d'ISO/IEC 27001 pour un SMSI du point de vue d'un responsable de la mise en œuvre
- Initier et planifier la mise en œuvre d'un SMSI basé sur ISO/IEC 27001, en utilisant la méthodologie IMS2 de PECB et d'autres bonnes pratiques
- Soutenir un organisme dans le fonctionnement, le maintien et l'amélioration continue d'un SMSI basé sur ISO/IEC 27001

## Public

Cette formation s'adresse aux :

- 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

## Prérequis

La certification ISO 27001 Foundation ou des connaissances de base sur la norme ISO 27001 sont recommandées.

La formation est dispensée sur la version 2022 de la norme ISO/CEI 27001.
Il est conseillé aux participants de se munir d'un exemplaire de la norme pour suivre la formation et passer la certification dans des conditions optimales

## Certification

Cette formation inclut le passage de la certification ISO 27001 Lead Implementer.

## Programme de la formation

**JOUR 1 – Introduction à la norme ISO/IEC 27001:2022 et initiation d'un SMSI**

**Objectifs et structure de la formation**

- Introduction
- Informations générales
- Objectifs d'apprentissage
- Approche éducative
- Examen et certification
- À propos de PECB

**Normes et cadres réglementaires**

- Qu'est-ce que l'ISO ?
- La famille de normes ISO/IEC 27000
- Avantages d'ISO/IEC 27001:2022

**Système de management de la sécurité de l'information (SMSI)**

- Définition de système de management
- Normes relatives aux systèmes de management
- Systèmes de management intégrés
- Définition d'un SMSI
- Approche processus
- Vue d'ensemble – articles 4 à 10
- Vue d'ensemble – Annexe A

**Concepts et principes fondamentaux de la sécurité de l'information**

- Information et actif
- Sécurité de l'information
- Confidentialité, intégrité et disponibilité
- Vulnérabilité, menace et impact
- Risque de sécurité de l'information
- Classification des mesures de sécurité

**Initiation de la mise en oeuvre du SMSI**

- Définition de l’approche de la mise en œuvre du SMSI
- Approches de mise en œuvre proposées
- Application des approches de mise en œuvre proposées
- Choisir un cadre méthodologique pour gérer la mise en œuvre d’un SMSI
- Approche et méthodologie
- Alignement sur les bonnes pratiques

**Compréhension de l’organisation et de son contexte**

- Mission, objectifs, valeurs et stratégies de l’organisation
- Objectifs du SMSI
- Définition préliminaire du périmètre
- Environnement interne et externe
- Principaux processus et activités
- Parties intéressées
- Exigences métier

**Domaine d’application du SMSI**

- Limites du SMSI
- Limites organisationnelles
- Limites de la sécurité de l’information
- Limites physiques
- Énoncé du périmètre du SMSI

**JOUR 2 – Planification de la mise en oeuvre d’un SMSI**

**Leadership et approbation du projet**

- Étude de faisabilité
- Exigences relatives aux ressources
- Plan du projet SMSI
- Équipe de projet SMSI
- Approbation de la direction

**Structure organisationnelle**

- Structure organisationnelle
- Coordinateur de la sécurité de l’information
- Rôles et responsabilités des parties intéressées
- Rôles et responsabilités des principaux comités

**Analyse du système existant**

- Détermination de l’état actuel
- Réalisation de l’analyse des écarts
- Établissement des objectifs de maturité

- Publication d’un rapport d’analyse des écarts

**Politique de sécurité de l’information**

- Types de politiques
- Modèles de politiques
- Politique de sécurité de l’information
- Politiques de sécurité spécifiques
- Approbation de la politique de management
- Publication et diffusion
- Sessions de formation et de sensibilisation
- Contrôle, évaluation et revue

**Gestion des risques**

- ISO 31000
- ISO/IEC 27005
- Établissement du contexte
- Identification des risques
- Analyse des risques
- Évaluation des risques
- Traitement des risques
- Communication et consultation
- Enregistrement et élaboration de rapports
- Surveillance et revue

**Déclaration d’applicabilité**

- Rédaction de la Déclaration d’applicabilité
- Approbation de la direction
- Revue et sélection des mesures de sécurité de l’information applicables
- Justification des mesures de sécurité sélectionnées
- Justification des mesures de sécurité exclues

**JOUR 3 – Mise en oeuvre du SMSI**

**Gestion des informations documentées**

- Valeur et types d’informations documentées
- Liste maîtresse des informations documentées
- Création de modèles
- Processus de gestion de l’information documentée
- Mise en œuvre d’un système de management de l’information documentée
- Gestion des enregistrements

**Sélection et conception des mesures**

- Architecture de sécurité de l’organisation
- Préparation de la mise en œuvre des mesures
- Conception et description des mesures

**Mise en oeuvre des mesures**

- Mise en œuvre des processus et des mesures de sécurité
- Introduction des mesures de l’Annexe A

**Tendances et technologies**

- Mégadonnées (Big data)
- Les trois V des mégadonnées
- Intelligence artificielle
- Apprentissage automatique (Machine learning)
- Externalisation des opérations
- Impact des nouvelles technologies en sécurité de l’information

**Communication**

- Principes d’une stratégie de communication efficace
- Processus de communication de sécurité de l’information
- Définition des objectifs de communication
- Identification des parties intéressées
- Planification des activités de communication
- Réalisation d’une activité de communication
- Évaluation de la communication

**Compétence et sensibilisation**

- Compétences et développement du personnel
- Différence entre formation, sensibilisation et communication
- Détermination des besoins en compétences
- Planification des activités de développement des compétences
- Définition du type et de la structure du programme de développement des compétences
- Programmes de formation et de sensibilisation
- Organisation des formations
- Évaluation des résultats des formations

**Gestion des opérations de sécurité**

- Planification de la gestion du changement
- Gestion des opérations
- Gestion des ressources
- ISO/IEC 27035-1 et ISO/IEC 27035-2
- ISO/IEC 27032
- Politique de gestion des incidents en sécurité de l’information
- Processus et procédure de gestion des incidents
- Équipe de réponse aux incidents
- Mesures de sécurité pour la gestion des incidents
- Processus forensiques
- Enregistrement des incidents de sécurité de l’information
- Mesure et revue du processus de gestion des incidents

**JOUR 4 – Suivi, amélioration continue et préparation de l’audit**

**Suivi, mesure, analyse et évaluation**

- Détermination des objectifs de mesure

- Définition de ce qui doit être surveillé et mesuré
- Établissement des indicateurs de performance du SMSI
- Rapport de résultats

**Audit interne**

- Qu’est-ce qu’un audit ?
- Types d’audits
- Création d’un programme d’audit interne
- Désignation d’une personne responsable
- Établissement de l’indépendance, de l’objectivité et de l’impartialité
- Planification des activités d’audit
- Réalisation des activités d’audit
- Suivi des non-conformités

**Revue de direction**

- Préparation d’une revue de direction
- Conduite d’une revue de direction
- Résultats de la revue de direction
- Activités de suivi de la revue de direction

**Traitement des non-conformités**

- Processus d’analyse des causes fondamentales
- Outils d’analyse des causes fondamentales
- Procédure d’actions correctives
- Procédure d’actions préventives

**Amélioration continue**

- Processus de surveillance continue
- Maintien et amélioration du SMSI
- Mise à jour continue des informations documentées
- Documentation des améliorations

**Préparation à l’audit de certification**

- Sélection de l’organisme de certification
- Préparation à l’audit de certification
- Étape 1 de l’audit
- Étape 2 de l’audit
- Suivi d’audit
- Décision de certification

**Clôture de la formation**

- Schéma de certification de PECB
- Processus de certification PECB
- Autres services PECB
- Autres formations et certifications PECB

**JOUR 5 – Préparation et passage de la certification ISO 27001 Lead Implementer**

- Matin : Révision en autonomie. Les moyens pédagogiques nécessaires (support de cours, salles de formations) seront à votre disposition
- Après-midi : Passage de 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 27001:2022
- Domaine 4 : Mise en œuvre d'un SMSI conforme à la la norme ISO/CEI 27001:2022
- 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

## Méthodes pédagogiques

La formation est constituée d'apports théoriques, d'exercices pratiques et de réflexions.

Remise d'une documentation pédagogique papier ou numérique pendant le stage.

## Méthodes d'évaluation des acquis

Afin d'évaluer l'acquisition de vos connaissances et compétences, il vous sera envoyé un formulaire d'auto-évaluation, qui sera à compléter en amont et à l'issue de la formation.
Un certificat de réalisation de fin de formation est remis au stagiaire lui permettant de faire valoir le suivi de la formation.