# ISO/CEI 27001 Lead Implementer : piloter la mise en œuvre d'un système de management de la sécurité de l'information

## Date et durée

Code formation : ISO27001LI-RS
Durée : 4,5 jours
Nombre d'heures : 31 heures

## Description

L'objectif d'un système de gestion de la sécurité de l'information (SMSI) est d'implémenter des mesures qui permettent une réduction, voire une suppression des différentes menaces dans une organisation afin de **favoriser la continuité de l'activité**, la protection des actifs informationnels et la confiance du client. La norme ISO 27001 version 2022 décrit sous forme d'exigences, un ensemble de bonnes pratiques organisationnelles, techniques et des points de contrôle à mettre en place pour s'assurer de la pertinence du SMSI. L'objectif étant qu'une organisation puisse **maîtriser efficacement les risques** liés à l'information.
Cette formation ISO 27001:2022 Lead Implementer a pour objectif de vous donner les connaissances et les compétences nécessaires pour **la mise en place, le management et la mise à jour d'un SMSI** au sein d'une organisation. Ces acquis permettront aux organisations de se doter d'une maîtrise des meilleures pratiques en matière de système de management de la sécurité de l'information pour sécuriser les informations sensibles, améliorer l'efficacité et la performance globale de l'organisation. La norme ISO 27001 peut s'appliquer aux organisations de toute taille, quel que soit le domaine d'activité.
À la fin de cette formation, **vous passerez l'examen de certification ISO 27001 Lead Implementer**. La réussite de celui-ci vous permettra d'attester de vos capacités professionnelles à mettre en place et gérer un SMSI.

*Skills4All est un organisme certificateur spécialisé dans le développement des compétences numériques et la transformation digitale.*

## Objectifs

**Objectifs pédagogiques :**

- Collecter et analyser les données existantes (Gap Analysis).
- Définir les objectifs du système de management de la sécurité de l'information (SMSI).
- Formaliser le domaine d'application et le business case.
- Constituer une équipe projet en définissant les rôles et responsabilités.
- Concevoir un plan de projet d'implémentation du SMSI.
- Élaborer la Politique de sécurité de l'information et la Déclaration d'applicabilité.
- Exécuter le plan de projet.
- Faciliter l'appropriation du SMSI en s'appuyant sur une démarche d'accompagnement au changement

- Mettre en œuvre une démarche de contrôle et d'amélioration continue du SMSI.

## Points forts

Certification internationalement reconnue. Travaux pratiques basés sur des cas réels avec une documentation de 450 pages ; Examens de certification compris dans le prix de la formation.

## Certification

Passage de la certification « **Piloter la mise en œuvre d'un système de management de la sécurité de l'information (ISO/CEI 27001 Lead Implementer)** » inscrite au Répertoire Spécifique n° 6244 (SKILLS4ALL). Examen officiel passé après la formation et vos révisions personnelles.
L'évaluation dure 3h00 et se fait à travers **une mise en situation professionnelle** fictive sous forme d'une étude de cas depuis une plateforme d'apprentissage. Le candidat devra préparer une présentation de son **projet d'implémentation d'un SMSI selon ISO 27001** pour une organisation fictive dont le contexte spécifique, les particularités, les enjeux et le SI de l'entreprise seront décrits dans la notice d'examen.
**Le candidat devra pour cela :**

- Répondre à un QCM (questions fermées)
- Présenter son projet d'implémentation d'un SMSI par écrit et par vidéo (voir explications ci-dessous) en 3 parties :
    - Partie 1 : justification du choix du périmètre ;
    - Partie 2 : description du projet d'implémentation (politique et principales mesures) ;
    - Partie 3 : formalisation de sa démarche d'accompagnement à la mise en place (principaux enjeux humains et actions/positionnement envisagées).

A noter que comme le candidat passe son examen en toute autonomie, il sera également demandé au candidat d'enregistrer 4 capsules vidéo aux fins de présentation et de justification de :

- Vidéo 1 : son identité (le candidat se présente)
- Vidéo 2 : la partie 1 ;
- Vidéo 3 : la partie 2 ;
- Vidéo 4 : la partie 3.

*Pour rappel, en suivant cette formation éligible au CPF, vous vous engagez à passer l'examen de certification.*

## Modalités d'évaluation

Quiz / QCM
Travaux Pratiques
Etude de cas

## Pré-requis

Suivre cette formation ISO 27001 Lead Implementer nécessite les prérequis suivants :

- avoir une bonne connaissance des systèmes d'information des organisations ;
- être impliqué dans la sécurité des systèmes d'information.

## Public

**Cette formation s'adresse aux publics suivants :**

- les responsables ou consultants impliqués dans le management de la sécurité de l'information ;

- les conseillers spécialisés désirant maîtriser la mise en œuvre d’un SMSI ;
- les membres d’une équipe d'un SMSI ;
- toute personne responsable du maintien de la conformité aux exigences du SMSI.

Cette formation s'adresse aux profils suivants

Administrateur système
Architecte informatique / SI
Ingénieur système
Auditeur interne / externe
Chef de projet / Responsable de projet
Contrôleur de gestion
Directeur des Systèmes d'Information (DSI)

Programme

### Tour de table :

- Introduction individuelle des participants.
- Exploration des attentes et des objectifs de chaque participant.
- Introduction au cadre de la formation.
- Alignement avec les objectifs et enjeux spécifiques de la formation ISO 27001.
- Identification des attentes et des perspectives individuelles des participants.

### Partie 1 : introduction au SMSI tel que défini par l’ISO 27001 et Gap Analysis

- Introduction à la norme ISO 27001 :
    - expliquer le contexte et les principes fondamentaux de la sécurité de l’information et en particulier de la norme ISO 27001.
    - comprendre l’approche processus.
    - présentation des normes ISO 27001:2022, ISO 27002:2013 et ISO 27003:2017.
- Analyser et collecter les données :
    - réaliser une analyse des écarts en appliquant des méthodologies de collecte de données basées sur des études de cas.
    - organiser des ateliers pour simuler des scénarios de collecte et d'analyse de données de sécurité, en illustrant les meilleures pratiques et les pièges à éviter.

### Partie 2 : planification du SMSI

- Formaliser le domaine d'application :
    - utiliser des outils interactifs pour apprendre à délimiter le périmètre de son propre SMSI.
    - conduire des discussions en groupe pour explorer les implications stratégiques de la formalisation du domaine d'application.
- Élaborer le plan de projet :
    - créer des plans de projet basés sur des templates personnalisables.
    - réaliser des jeux de rôle pour simuler la mise en place d'un plan de projet, incluant la gestion des risques et la planification des ressources.

### Partie 3 : mise en œuvre du SMSI

- Former l'équipe projet :
    - identifier les compétences et les rôles clés nécessaires au sein d'une équipe SMSI efficace.
    - mener des exercices de team building pour renforcer la cohésion et la collaboration inter-fonctionnelle.

- Développer la politique de sécurité et la déclaration d'applicabilité :
    - apprendre à rédiger une ébauche de politique de sécurité. Analyser des exemples de Déclarations d’Applicabilité pour comprendre leur importance et leur contenu.

### Partie 4 : exécution et gestion du changement

- Mettre en œuvre le plan de projet :
    - suivre des études de cas réels pour comprendre les défis de l'implémentation du SMSI.
    - utiliser des logiciels de gestion de projet pour simuler la mise en œuvre du plan de projet.
- Encourager l'adoption d'un SMSI :
    - discuter des stratégies de changement organisationnel et de leur impact sur l'adoption d'un SMSI.
    - évaluer l'efficacité des techniques de communication et de formation pour faciliter cette adoption.

### Partie 5 : contrôle et amélioration

- Implémenter les processus de contrôle et d'amélioration du SMSI :
    - apprendre à utiliser des outils de surveillance et de reporting pour mesurer l'efficacité du SMSI.
    - effectuer un audit interne du SMSI.
    - discuter des cas où des améliorations qui sont nécessaires et comment les intégrer.
    - mettre en œuvre un programme d’amélioration continue.

### Partie 6 : révisions et préparation à la certification (***Dernier jour – Matinée***)

- Réviser les principaux concepts et termes de la norme ISO 27001.
- Répondre aux questions sur des points qui n’auraient pas été bien compris.
- Fournir des conseils et des stratégies pour réussir l'examen de certification, incluant des pratiques d'examen et des questions types.