

# ISO/IEC 27001 - Management de la Sécurité de l'Information - Lead implementer

Référence : **SECLI27001A**

Durée : **5 jours (35 heures)**

Certification : **ISO/IEC 27001Lead Implementer de PECB**

## Connaissances préalables

- Avoir une connaissance générale des concepts du SMSI et des exigences de la norme ISO/IEC 27001

## Profil des stagiaires

- RSSI, Risk manager, auditeurs ou futurs audités, chefs de projet, consultants, toute personne souhaitant maîtriser la mise en œuvre d'un SMSI ou responsable du maintien de la conformité aux exigences d'un SMSI

## Objectifs

- Connaître et savoir interpréter les exigences de la norme ISO/CEI 27001 pour la mise en œuvre d'un SMSI
- Comprendre la relation entre la norme ISO/IEC 27001 et les autres normes (ISO/IEC 27002, ISO 31000, ISO/IEC 27005 par exemple)
- 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

## Certification préparée

- Durée de l'examen : 3 heures. Format : un QCM de 80 questions en français. Modalité : passage en-dehors du temps de formation, via Internet, sous e-surveillance, à livre ouvert. Le support de cours contient les extraits de norme(s) nécessaires au passage de l'examen. Un deuxième passage est offert dans un délai d'un an si la première tentative n'est pas couronnée de succès. Taux de réussite constaté chez EduGroupe pour cette certification en 2024 : 94%

## Méthodes pédagogiques

- Groupes de 4 à 12 personnes
- Apports théoriques illustrés d'exemples concrets
- Exercices pratiques
- Etude de cas fil rouge
- Remise d'une documentation pédagogique numérique (PDF accessible)
- Utilisation d'outils collaboratifs (Miro, Wooclap) pour la co-construction
- Signature d'une feuille d'émargement pour attester de la présence à chaque demi-journée de formation

## Formateur

- Consultant-formateur expert en management de la sécurité et conformité réglementaire (certification ISO 27001 Lead Implementer/Auditor)

## Méthodes d'évaluation des acquis

- Participation et réalisation d'exercices tout au long de la formation
- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestations des compétences acquises et de fin de stage adressée à chaque participant

## Contenu du cours

### **JOUR 1 - Introduction à la norme ISO/IEC 27001 et lancement de la mise en œuvre d'un SMSI (7h)**

#### **Section 1 : Programme et objectifs de la formation (0h20)**

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

#### **Section 2 : Normes et cadres réglementaires (0h50)**

- La famille de normes ISO/IEC 27000
- Élaboration de la famille de normes ISO/IEC 27000
- Avantages d'un SMSI conformément à la norme ISO/IEC 27001
- Quiz

#### **Section 3 : Système de management de la sécurité de l'information (SMSI) (1h20)**

- Définition d'un système de management
- Définition d'un SMSI
- Systèmes de management intégrés
- Aperçu des articles 4 à 10
- Aperçu de l'Annexe A
- Approche processus
- Quiz
- Exercice

#### **Section 4 : Concepts et principes fondamentaux de la sécurité de l'information (1h)**

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

#### **Section 5 : Lancement de la mise en œuvre du SMSI (1h)**

- Définition d'une approche pour la mise en œuvre du SMSI
- Proposition d'approches de mise en œuvre
- Application des approches de mise en œuvre proposées
- Préparation d'une analyse de rentabilité
- Choix d'un cadre méthodologique pour la gestion de la mise en œuvre du SMSI
- Arrimage aux bonnes pratiques
- Quiz

## Section 6 : Compréhension de l'organisation et de son contexte (1h)

- Mission, objectifs, valeurs, stratégies de l'organisation
- Objectifs du SMSI
- Domaine d'application préliminaire
- Environnement interne et externe
- Principaux processus et activités
- Impact du changement climatique
- Parties intéressées
- Exigences métier
-  Quiz

## Section 7 : Domaine d'application du SMSI (1h30)

- Limites du SMSI
- Limites organisationnelles
- Limites de la sécurité de l'information
- Limites physiques
- Déclaration du domaine d'application du SMSI
-  Quiz
-  Réflexion commune sur le Scénario 1

## JOUR 2 - Plan de mise en œuvre d'un SMSI (7h)

### Section 8 : Leadership et approbation du projet (1h)

- Leadership et engagement
- Plan du projet SMSI
- Équipe de projet SMSI
- Chef de projet SMSI
- Approbation de la direction générale pour le projet de mise en œuvre du SMSI
-  Quiz

### Section 9 : Structure organisationnelle (0h40)

- Structure organisationnelle
- Coordonnateur de la sécurité de l'information
- Rôles et responsabilités des parties intéressées
- Rôles et responsabilités des principaux comités
-  Quiz

### Section 10 : Analyse du système existant (1h)

- Détermination de l'état actuel
- Réalisation d'une analyse des écarts
- Établissement des objectifs de maturité
- Présentation d'un rapport d'analyse des écarts
-  Quiz

### Section 11 : Politique de sécurité de l'information (1h)

- Types de politiques
- Modèles de politiques
- Politique de sécurité de l'information
- Politiques de sécurité spécifiques
- Approbation des politiques par la direction générale
- Publication et diffusion des politiques
- Contrôle, évaluation et revue des politiques
-  Quiz

## Section 12 : Gestion des risques (1h50)

- ISO 31000
- ISO/IEC 27005
- Établissement du contexte
- Appréciation des risques
- Traitement du risque
- Communication et concertation
- Enregistrement et élaboration de rapports
- Surveillance et revue
-  Quiz
-  Exercice

## Section 13 : Déclaration d'applicabilité (1h30)

- Revue et sélection des mesures de sécurité de l'information applicables
- Justification des mesures de sécurité sélectionnées
- Justification des mesures de sécurité exclues
- Finalisation de la déclaration d'applicabilité
- Approbation par la direction générale
-  Quiz
-  Réflexion commune sur le Scénario 2

## JOUR 3 - Mise en œuvre du SMSI (7h)

### Section 14 : Sélection et conception des mesures de sécurité (1h)

- Analyse de l'architecture de sécurité de l'organisation
- Préparation de la mise en œuvre des mesures
- Conception et description des mesures
- Quiz

### Section 15 : Mise en œuvre des mesures de sécurité (1h30)

- Mise en œuvre des processus et des mesures de sécurité
- Introduction des mesures de l'Annexe A
-  Quiz
-  Exercice

### Section 16 : Gestion des informations documentées (1h)

- Types d'informations documentées
- Approche de documentation
- Création de modèles
- Processus de gestion des informations documentées
- Système de management des informations documentées
- Gestion des enregistrements
-  Quiz

### Section 17 : Tendances et technologies (0h40)

- Big data
- Les trois V du big data
- Intelligence artificielle
- Apprentissage automatique
- Cloud computing
- Externalisation des opérations
- Impact des nouvelles technologies dans la sécurité de l'information
-  Quiz

## Section 18 : Communication (0h40)

- Principes d'une communication efficace
- Processus de communication de la sécurité de l'information
- Objectifs de communication
- Identification des parties intéressées
- Activités de communication
- Évaluation du processus de communication
- Quiz

## Section 19 : Compétence et sensibilisation (0h40)

- Compétence et développement du personnel
- Formation et sensibilisation
- Besoins en compétences
- Activités de développement des compétences
- Programmes de développement des compétences
- Programmes de formation et de sensibilisation
- Évaluation des résultats de la formation
-  Quiz

## Section 20 : Gestion des opérations de sécurité (1h30)

- Planification de la gestion du changement
- Gestion des opérations
- Gestion des ressources
- Processus et procédure de gestion des incidents
- Politique de gestion des incidents de sécurité de l'information
- Équipe de réponse aux incidents
- Mesures de sécurité de gestion des incidents
- Processus de criminalistique numérique
- Enregistrement des incidents de sécurité de l'information
- Mesurage et revue du processus de gestion des incidents
-  Quiz
-  Réflexion commune sur le Scénario 3

## JOUR 4 - Surveillance, amélioration continue et préparation à l'audit de certification du (7h)

### Section 21 : Surveillance, mesurage, analyse et évaluation (1h10)

- Déterminer les objectifs de mesurage
- Définir ce qui doit être surveillé et mesuré
- Définir les indicateurs de performance du SMSI
- Déterminer la fréquence et la méthode de surveillance et de mesurage
- Rapport de résultats
-  Quiz
-  Exercice

### Section 22 : Audit interne (0h50)

- Qu'est-ce qu'un audit ?
- Types d'audits
- Programme d'audit interne
- Indépendance, objectivité et impartialité
- Affectation et gestion des ressources pour le programme d'audit
- Non-conformités
- Suivi des non-conformités
-  Quiz

## Section 23 : Revue de direction (0h40)

- Préparation de la revue de direction
- Réalisation de la revue de direction
- Détermination des résultats de la revue de direction
- Suivi de la revue de direction
-  Quiz

## Section 24 : Traitement des non-conformités (0h40)

- Résolution des problèmes et des non-conformités
- Analyse des causes fondamentales
- Actions correctives
- Actions préventives
- Plans d'action
- Quiz

## Section 25 : Amélioration continue (0h40)

- Surveillance continue des facteurs de changement
- Mise à jour et amélioration du SMSI
- Mise à jour continue des informations documentées
- Documentation des améliorations
-  Quiz

## Section 26 : Préparation de l'audit de certification (1h50)

- Organismes d'accréditation et de certification
- Sélection de l'organisme de certification
- Étape 1 de l'audit
- Étape 2 de l'audit
- Suivi de l'audit
- Recommandation et décision de certification
- Audit de renouvellement de la certification
-  Quiz
-  Réflexion commune sur le Scénario 4

## Section 27 : Clôture de la formation (0h30)

- Programme de certification de PECB
- Processus de certification PECB

## JOUR 5 - Révisions encadrées (7h)

- Rappel structuré des acquis des Jours 1 à 4
-  Quiz de réactivation global
-  Étude de cas intégrative
-  Audit blanc
-  Élaboration d'un plan d'amélioration
-  Simulation d'examen
- Synthèse finale et projection

Notre référent handicap se tient à votre disposition au [01.71.19.70.30](tel:01.71.19.70.30) ou par mail à <mailto:referent.handicap@edugroupe.com> pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.