

ISO 27001 LEAD IMPLEMENTER

Cette formation de 5 jours offre aux participants l'occasion de monter en compétence sur la fonction de pilotage d'un projet de mise en œuvre de la gestion de la sécurité de l'information et de se préparer par la pratique à diriger des équipes opérationnelles sur base de principes, de procédures et de techniques de management de projets largement appliquées dans le monde de l'entreprise. Au cours de cette formation, le stagiaire acquerra les bases de connaissance et les aptitudes l'autorisant à planifier, mettre en œuvre, évaluer et garantir l'intégrité du SMSI dans le respect des exigences de la norme ISO 27001 ainsi que le processus d'assurance qualité requis par les guides de pratiques associés. Sur base d'exemples réels et d'exercices concrets, le stagiaire sera amené durant la formation à mener à bien un projet d'implémentation de SMSI en développant des capacités en gestion de programmes et de techniques de mise en œuvre et de suivi ainsi qu'en gestion d'équipe, à travers la communication avec les différentes parties intéressées.



OBJECTIFS

- Comprendre les principes de fonctionnement d'un SMSI selon ISO 27001
- Développer les aptitudes nécessaires pour mener à bien un projet d'implémentation ISO 27001 dans le respect des exigences de la norme et les lignes directrices des normes ISO 27002, 27003, 27004 et 27005
- Acquérir la compétence de gestion d'une équipe projets pour lancer et maintenir un SMSI
- Réussir l'examen de CERTI-TRUST™
- Solliciter la qualification de Certified ISO 27001 Lead Implementer selon le niveau d'expérience.

CONTENU PEDAGOGIQUE

- **Jour 1 : Le SMSI tel qu'exigé par la norme ISO/CEI 27001:2013**
 - Système de Management de la Sécurité de l'Information – concepts de base
 - Principes fondamentaux de la sécurité de l'information
 - Les clauses 4 à 10 de l'ISO 27001 et l'Annexe A d'ISO 27001
 - Le contexte du SMSI au sein de l'entreprise et son champ d'application
 - Aspects de leadership et engagement managérial
 - Planification d'un SMSI (gestion des risques, mesures de sécurité, applicabilité, etc.)
- Support des opérations d'un SMSI (documentation, ressources, etc.)



👉 Jour 2 : Fonctionnement du SMSI

- Gestion des opérations d'un SMSI
- Surveillance du SMSI (journalisation, audit et revue de direction)
- Évaluation de l'efficacité des opérations et gestion des métriques
- Actions correctives et amélioration continue
- Processus de certification ISO 27001
- Présentation de la documentation nécessaire aux opérations du SMSI (toolbox)

Examen certifiant
« ISO 27001 Foundation »
(1h – 50 questions QCM à livre fermé)

👉 Jour 3 : Préparation et démarrage d'un projet SMSI

- Les jalons et le calendrier d'un projet de SMSI
- Planification d'un projet SMSI
- Périmètre du projet et définition du champ d'application du SMSI
- Les acteurs du projet – Rôles et responsabilités des parties prenantes
- Business Case et méthodologie de gestion de projet
- Obtenir le soutien des parties prenantes et de la direction
- Gestion des relations avec les parties intéressées durant le projet d'implémentation
- Documentation du SMSI
- Politiques et procédures du SMSI
- Présentation et utilisation des outils de préparation au projet (via étude de cas)

👉 Jour 4 : Les opérations et la performance d'un SMSI

- Gestion des risques en Sécurité de l'Information
- Mesures de sécurité et sélection des contrôles applicables
- Déclaration d'Applicabilité (DdA) et Plan de traitement des risques (PTR)
- Rôles et responsabilités des opérateurs et des parties intéressées
- Communication, sensibilisation et formation
- Gestion des incidents de sécurité
- Surveillance, mesure, analyse et évaluation du SMSI
- Présentation et utilisation des outils de réalisation et de suivi du projet (via étude de cas)

👉 Jour 5 : Cycle de vie et pérennité du SMSI

- Audit interne du SMSI, gestion de la conformité
- Revue de Direction
- Gestion de l'amélioration continue & actions correctives et préventives
- Processus de certification
- Présentation et utilisation des outils de suivi du cycle de vie du SMSI (via étude de cas)

Examen certifiant
« ISO 27001 Lead Implementer »
(2h – 100 questions QCM à livre fermé)



Pour s'inscrire :

02 99 23 46 51
formation@sodifrance.fr

Public : Security Officers, Gestionnaires de risques, Responsables du traitement des données en entreprise, Chefs de projets ou consultants souhaitant maîtriser la mise en œuvre d'un système de management de la Sécurité de l'Information, CxO et managers responsables de la gestion TI d'une entreprise ainsi que la gestion des risques, Membres d'une équipe de sécurité de l'information, Conseillers experts en technologie de l'information, Experts techniques voulant se préparer pour un poste en sécurité de l'information.

Pré-requis : Une connaissance de base de la Sécurité de l'Information et de la norme ISO 27001 est nécessaire pour participer à ce cours.

Méthodes et moyens pédagogiques : 1 poste/stagiaire, alternance théorie/pratique, 8 stagiaires maximum (plus de détails p5)

Durée : 5 jours - 40 heures

Evaluation des acquis : Cette formation est certifiante

👉 Cette formation est aussi disponible en intra entreprise, nous consulter pour plus d'informations.