



<b>Objectifs</b>	Apporter aux participants une compréhension approfondie de la norme ISO/IEC 27001, de ses exigences, de son application concrète au sein d'une organisation, ainsi que des méthodes pour mettre en oeuvre, piloter et auditer un Système de Management de la Sécurité de l'Information (SMSI).
<b>Participants</b>	RSSI (Responsables Sécurité des SI) - Chefs de projet sécurité ou conformité - Auditeurs internes / externes - DSI - Consultants cybersécurité - DPO - Responsables qualité / gestion des risques - Responsables de la gouvernance IT
<b>Prérequis</b>	Compréhension des concepts de management de la sécurité - notions de conformité et réglementation - capacité à documenter et mettre en place des processus - connaissance du cycle PDCA.
<b>Moyens pédagogiques</b>	1 poste par participant - 1 vidéo projecteur - Support de cours fourni à chaque participant - Ateliers individuels - Modalités d'évaluation : Ateliers (TP) pendant tout au long de la formation et évaluation des acquis tout au long de la formation.
<b>Méthodes pédagogiques</b>	Exposés interactifs et démonstrations - Travaux pratiques individuels et en groupe - Échanges d'expériences et de bonnes pratiques
<b>Type de formation</b>	Formation présentielle ou distancielle, selon les besoins et les contraintes des participants
<b>Tarif inter-entreprise</b>	2670 € HT
<b>Durée</b>	3 jour(s) - 21 heure(s)
<b>Modalités et délais d'accès</b>	Formations accessibles sous 15 à 20 jours suite à votre demande. Un entretien initial doit être prévu avant votre entrée en formation.

**Code : NCI\_K4LH400B**

**Mis à jour le : 25 mars 2026**

### Programme :

#### Introduction à la norme ISO/IEC 27001

Historique, objectifs et champ d'application  
Concepts clés : sécurité, disponibilité, intégrité, confidentialité  
ISO 27001 vs ISO 27002, 27005, 27701  
Vocabulaire fondamental et principes du SMSI

#### Exigences de la norme ISO 27001

Contexte de l'organisation et parties intéressées  
Leadership, politique de sécurité, rôles et responsabilités  
Planification du SMSI : analyse de risques, objectifs, plans d'action  
Support documentaire et ressources

#### Mise en oeuvre d'un SMSI

Identification et traitement des risques liés à la sécurité de l'information  
Définition des actifs, menaces, vulnérabilités  
Choix des mesures de sécurité (référentiel Annexe A)  
Intégration dans les processus existants

#### Pilotage et fonctionnement du SMSI

Surveillance, revue de direction et amélioration continue  
Indicateurs et tableaux de bord  
Réaction aux incidents de sécurité  
Gestion des non-conformités

#### Audit interne du SMSI

Préparation et planification d'un audit ISO 27001  
Conduite de l'audit (checklist, entretien, preuves)  
Rapport d'audit et actions correctives  
Exemples d'écarts fréquents et retours d'expérience

#### Certification ISO 27001

Processus de certification et rôle des organismes accrédités  
Étapes clés : audit initial, surveillance, renouvellement  
Conditions de succès et pièges à éviter  
Maintien et amélioration du SMSI après certification

#### Cas pratiques & exercices

Cartographie des risques sécurité d'un service IT  
Atelier : construire une politique de sécurité conforme  
Étude de cas : identifier les écarts d'un SMSI existant  
Simulation d'un audit interne ISO 27001  
Analyse d'incident de sécurité et mise en place d'actions

#### Clôture

Résumé des exigences clés  
Questions / réponses  
Ressources utiles (normes, guides, outils gratuits)  
Évaluation des acquis