PROGRAMME DE FORMATION

ISO/CEI 27001 : mettre en œuvre un système de management de la sécurité de l'information (SMSI)

Cybersécurité & Protection des données

RÉFÉRENCE	VERSION	ÉDITION	DOMAINE
WF-0469	V2026-004	3 novembre 2026	Cybersécurité & Protection des données

DURÉE	MODALITÉ	PROGRAMME	SANCTION
35 h	Distanciel asynchrone (e-learning)	7 modules 30 leçons	Attestation et certificat de réalisation

Objectifs pédagogiques

- À l'issue de la formation, l'apprenant sera capable de :
- - Expliquer les principes de la sécurité de l'information et la place de la norme ISO/CEI 27001 dans la famille ISO/CEI 27000
- - Analyser le contexte de l'organisation et définir le périmètre d'un système de management de la sécurité de l'information (SMSI)
- - Conduire une appréciation des risques et établir un plan de traitement des risques
- - Sélectionner et justifier les mesures de sécurité de l'annexe A et rédiger une déclaration d'applicabilité
- - Produire et tenir à jour les informations documentées exigées par la norme
- - Organiser la surveillance du SMSI, l'audit interne, la revue de direction et l'amélioration continue

L'essentiel de la formation

Public visé

Responsables de la sécurité des systèmes d'information, responsables informatiques, qualité ou conformité, chefs de projet et consultants chargés de mettre en œuvre ou de faire évoluer un SMSI selon la norme ISO/CEI 27001

Prérequis

Connaissances générales du fonctionnement d'un système d'information ; aucune expérience préalable des normes de systèmes de management n'est exigée

Connaître les notions de base de l'informatique et des réseaux

Disposer d'un ordinateur ou d'une tablette

Disposer d'une connexion Internet

Disposer d'une adresse électronique

Modalités et déroulement

Formation à distance sur la plateforme WILL FORMATION, avec accès individuel aux contenus, exercices et quiz, en entrées et sorties permanentes. Un accompagnement pédagogique est assuré pendant toute la durée du parcours.

Méthodes pédagogiques

- Apports théoriques sous forme de contenus en ligne
- Analyse commentée des exigences de la norme
- Études de cas fil rouge sur une organisation fictive
- Exercices d'application (analyse de risques, déclaration d'applicabilité, plan d'audit)
- Quiz d'auto-évaluation
- Accompagnement pédagogique à distance

Répartition du temps de formation : **20 %** théorique · **53 %** pratique · **27 %** évaluation

Moyens pédagogiques et techniques

- Accès individuel à la plateforme WILL FORMATION
- Contenus pédagogiques consultables à distance
- Modèles de documents (politique de sécurité, registre des risques, déclaration d'applicabilité)
- Quiz et exercices en ligne
- Accompagnement pédagogique à distance pendant la durée du parcours

Modalités d'évaluation

- Positionnement initial au démarrage du parcours
- Évaluations formatives par quiz et exercices tout au long du parcours
- Évaluation finale des acquis en fin de parcours

Sanction

Une attestation de fin de formation et un certificat de réalisation sont remis au participant sous réserve de la réalisation du parcours.

Cette formation n'est pas présentée comme préparant à une certification enregistrée : elle ne comprend ni inscription ni présentation à des épreuves de certification, et n'ouvre droit à aucune délivrance de certification ni au financement par le CPF.

Modalités et délais d'accès

La demande d'inscription peut être effectuée par téléphone, par courrier électronique ou au moyen du formulaire en ligne.

Un entretien ou un questionnaire de positionnement permet de vérifier l'adéquation de la formation avec les besoins, le niveau initial et les prérequis du candidat.

L'inscription devient définitive après validation du dossier administratif, acceptation des documents contractuels et, le cas échéant, confirmation du financement.

Les accès à la plateforme sont généralement activés sous 48 à 72 heures ouvrées après validation complète du dossier.

Les formations à distance sont proposées en entrées et sorties permanentes, sous réserve des délais ou dates imposés par le financeur ou le certificateur.

Accessibilité aux personnes en situation de handicap

Les personnes en situation de handicap sont invitées à signaler leurs besoins lors de leur demande d'inscription. Une étude personnalisée est réalisée afin de définir les adaptations pédagogiques, techniques ou organisationnelles appropriées. Lorsque le besoin ne peut pas être satisfait directement, une orientation vers un partenaire ou une structure spécialisée est proposée.

Référent handicap : **handicap@will-formation.com**

Tarif de la formation

Prix : **3 060 €**

Financement : prise en charge possible par les organismes financeurs, selon les critères d'éligibilité applicables.

Qualiopi processus certifié

La certification qualité a été délivrée au titre de la catégorie d'action suivante : ACTIONS DE FORMATION. Certificat QUA25070009. WILL FORMATION — Société par actions simplifiée à associé unique au capital de 30 000 € — NDA 11757059675 (cet enregistrement ne vaut pas agrément de l'État) — SIRET 893 713 180 00014 — 01 85 09 25 99 — info@will-formation.com — www.will-formation.com

Programme détaillé

7 modules, 30 leçons — durée totale 35 h.

01 Sécurité de l'information et famille de normes ISO/CEI 27000

1. Disponibilité, intégrité et confidentialité de l'information
2. La famille ISO/CEI 27000 et la place de l'ISO/CEI 27001
3. La structure commune des normes de systèmes de management
4. Articuler le SMSI avec le RGPD et les exigences légales et contractuelles

02 Contexte, périmètre et leadership du SMSI

1. Analyser le contexte de l'organisation et les parties intéressées
2. Définir le périmètre du SMSI
3. Engagement de la direction, politique de sécurité et rôles
4. Planifier le projet de mise en œuvre

03 Appréciation et traitement des risques

1. Choisir une méthode d'appréciation des risques (repères ISO/CEI 27005)
2. Identifier les actifs, les menaces et les vulnérabilités
3. Analyser et évaluer les risques
4. Plan de traitement et acceptation des risques résiduels
5. Rédiger la déclaration d'applicabilité

04 Mesures de sécurité de l'annexe A et guide ISO/CEI 27002

1. Mesures organisationnelles
2. Mesures liées aux personnes
3. Mesures physiques
4. Mesures technologiques
5. Sélectionner et justifier les mesures retenues

05 Documentation et fonctionnement opérationnel du SMSI

1. Informations documentées : politiques, procédures et enregistrements
2. Sensibilisation, compétences et communication
3. Gestion des incidents de sécurité de l'information
4. Continuité d'activité et relations avec les fournisseurs

06 Surveillance, mesure et audit interne

1. Indicateurs et tableaux de bord de la sécurité
2. Construire un programme d'audit interne (repères ISO 19011)
3. Conduire un audit interne et formuler les constats
4. Préparer et tenir la revue de direction

07 Amélioration continue du SMSI

1. Traiter les non-conformités et les actions correctives
2. Faire vivre le SMSI dans la durée
3. Préparer le SMSI à une évaluation externe
4. Étude de cas récapitulative : feuille de route de mise en œuvre