L'AKADÉMIE DU DIGITAL · PROGRAMME DE FORMATION Certification Qualiopi en cours de préparation

ISO 27001 : premiers pas (SMSI)

FOR-CYBER-M5-A · Cybersécurité & Conformité

Découvrir le système de management de la sécurité de l'information et amorcer sa démarche

DURÉE
7 h

TARIF
450 € HT

PUBLIC
Entreprises & particuliers

DÉLAI D'ACCÈS
Accès sous 2 jours ouvrés après validation du besoin et des prérequis.

Tarifs indiqués « à partir de », hors devis spécifique et promotions. Prix HT, à partir de 2 participants. TVA 20 %.

Objectifs pédagogiques

- Comprendre ce qu'est un SMSI (Système de Management de la Sécurité de l'Information) et la logique d'ISO/IEC 27001
- Situer ISO 27001 dans la famille ISO 27000 et par rapport aux autres cadres (NIST, ANSSI, RGPD)
- Comprendre les notions clés : périmètre, parties prenantes, appréciation et traitement des risques, déclaration d'applicabilité (SoA)
- Identifier les grandes étapes d'une démarche de certification (PDCA, audits, mesures de l'Annexe A)
- Réaliser une appréciation des risques simplifiée et amorcer une déclaration d'applicabilité
- Construire une feuille de route réaliste vers une démarche ISO 27001

Public concerné

- Référents sécurité, RSSI en prise de poste, DSI, responsables qualité et conformité
- Chefs de projet et responsables impliqués dans une démarche de certification
- Dirigeants de PME/ETI envisageant une démarche ISO 27001

Prérequis

- Savoir utiliser un ordinateur et les outils bureautiques courants.
- Avoir une sensibilisation à la cybersécurité (module Initiation conseillé) ou au pilotage (module Managers).
- Une expérience en qualité/conformité (ISO 9001, RGPD) facilite la compréhension (un atout).
- Disposer d'une motivation à amorcer une démarche structurée de sécurité de l'information.

Programme

THÉORIE Module Théorique — Comprendre l'ISO 27001 et le SMSI

Ce module explique les enjeux de la sécurité de l'information (confidentialité, intégrité, disponibilité), la famille ISO 27000 et le positionnement d'ISO 27001 par rapport à NIST, ANSSI et RGPD. Il présente l'esprit du SMSI (approche par les risques, amélioration continue PDCA, engagement de la direction), la structure de la norme, l'appréciation et le traitement des risques, le panorama des mesures de l'Annexe A, la déclaration d'applicabilité (SoA) et le parcours de certification.

Objectif : comprendre la logique et le vocabulaire d'ISO 27001 et du SMSI pour pouvoir amorcer une démarche structurée.

- Vulgarisation de la norme et de la logique SMSI (CID, PDCA).
- Positionnement clair par rapport aux autres cadres (NIST, ANSSI, RGPD).
- Compréhension de l'appréciation des risques, de l'Annexe A et de la SoA.

Évaluation : QCM sur la norme et le vocabulaire SMSI, exercice de positionnement des cadres de référence.

Accueil & présentation	15 min	Présenter le programme, les objectifs et le cadre (initiation non certifiante). Présentation orale, support visuel (slides), tour de table.	
Sécurité de l'information & CID	35 min	Enjeux ; confidentialité, intégrité, disponibilité ; pourquoi une norme. Exposé interactif, exemples, échanges.	Questions orales de compréhension.
Famille ISO 27000 & cadres	40 min	Positionnement d'ISO 27001 ; articulation NIST, ANSSI, RGPD. Exposé, tableau de positionnement, exercice.	Exercice de positionnement des cadres.
L'esprit du SMSI	50 min	Approche par les risques, PDCA, engagement de la direction, structure de la norme. Exposé structuré, schéma PDCA, exemples.	QCM sur la norme et le SMSI.
Risques, Annexe A & SoA	55 min	Appréciation/traitement des risques, mesures de l'Annexe A, déclaration d'applicabilité, certification. Exposé, panorama de l'Annexe A, exemple de SoA.	QCM intermédiaire sur le vocabulaire.
Synthèse	10 min	Résumer les points clés et préparer l'atelier. Récapitulatif, feedback des participants.	QCM rapide de fin de module.

ATELIER Atelier Pratique — Amorcer sa démarche SMSI

À partir d'un cas fil rouge ou de leur organisation, les participants définissent le périmètre d'un SMSI et identifient les parties prenantes, réalisent une appréciation des risques simplifiée (actifs, menaces, vulnérabilités, évaluation), choisissent des mesures de traitement et amorcent une déclaration d'applicabilité (SoA) sur un échantillon de l'Annexe A, puis construisent une feuille de route réaliste vers une démarche ISO 27001.

Objectif : amorcer concrètement une démarche SMSI : périmètre, appréciation des risques, ébauche de SoA et feuille de route.

- Travail possible directement sur le contexte réel de l'organisation.
- Appréciation des risques simplifiée et actionnable.
- Amorce d'une déclaration d'applicabilité (SoA) sur l'Annexe A.
- Feuille de route réaliste vers la certification.

Évaluation : production des livrables (périmètre, appréciation des risques, ébauche de SoA, feuille de route), restitution orale courte et revue collective.

Lancement de l'atelier	15 min	Présenter l'objectif et choisir son organisation ou un cas fil rouge. Présentation, constitution des groupes.	
Périmètre & parties prenantes	45 min	Définir le périmètre d'un SMSI et identifier les parties prenantes. TP guidé, gabarit de périmètre, accompagnement.	Livrable : périmètre + parties prenantes.
Appréciation des risques	1h00	Identifier actifs, menaces, vulnérabilités et évaluer les risques. TP collaboratif, grille d'appréciation des risques.	Livrable : appréciation des risques.
Traitement & ébauche de SoA	45 min	Choisir des mesures et amorcer une déclaration d'applicabilité (échantillon Annexe A). TP, extrait de l'Annexe A, modèle de SoA.	Livrable : ébauche de SoA.
Feuille de route & restitution	25 min	Construire une feuille de route vers ISO 27001 ; présenter. Modèle de feuille de route, présentations courtes, feedback.	Évaluation sommative : feuille de route + QCM final.
Enquête de satisfaction	10 min	Recueillir la satisfaction à chaud. Questionnaire de satisfaction.	Enquête de satisfaction.

Modalités et moyens pédagogiques

Formation en présentiel dans nos locaux ou dans vos locaux, en groupe restreint. Alternance d’apports théoriques, d’ateliers pratiques et de mises en situation.

Matériel requis :

8 Go de Ram

Modalités d’évaluation

Évaluation des acquis en cours et en fin de formation, attestation de fin de formation remise à chaque stagiaire.

Accessibilité

Formation accessible aux personnes en situation de handicap. Contactez-nous avant l’inscription pour étudier les aménagements nécessaires.

Financement

Devis ou convention de formation sur demande. La certification Qualiopi est en cours de préparation : l’éligibilité aux financements OPCO sera ouverte après son obtention.

Audit de certification prévu au T1 2027. Aucune éligibilité OPCO avant l’obtention.