Mis à jour le 22/08/2025

S'inscrire

Formation ISO/IEC 27001 -Management de la Sécurité de l'Information -Lead Auditor

ALL-IN-ONE : EXAMEN INCLUS AU TARIF

5 jours (35 heures)

PRÉSENTATION

La formation « ISO/IEC 27001 Lead Auditor – Management de la Sécurité de l'Information » vise à donner aux participants une compréhension solide des concepts et principes d'un Système de Management de la Sécurité de l'Information (SMSI) fondé sur la norme ISO/IEC 27001. Elle aborde la finalité d'un SMSI, sa structure, ses liens avec les autres référentiels et son rôle dans la gouvernance de la sécurité de l'information. Cette première étape permet d'expliquer le cadre conceptuel et d'en saisir la portée dans un contexte d'audit.

Les stagiaires apprennent ensuite à interpréter les exigences d'ISO/IEC 27001 dans une perspective d'audit. Chaque clause est étudiée avec un angle pratique : identification du périmètre, leadership, planification, gouvernance, mise en œuvre opérationnelle et revue de performance. L'accent est mis sur la capacité de l'auditeur à relier les exigences normatives aux pratiques de l'organisation et à comprendre comment en évaluer la conformité sur le terrain.

Un volet central de la formation est consacré à l'évaluation de la conformité d'un SMSI. Les participants découvrent comment apprécier l'efficacité des contrôles et mesurer la robustesse du système à travers des preuves documentaires, des entretiens et des observations. L'approche est guidée par les principes fondamentaux de l'audit définis dans ISO 19011, garantissant une méthodologie professionnelle, rigoureuse et conforme aux bonnes pratiques internationales.

La formation couvre également toutes les étapes nécessaires pour planifier, réaliser et clôturer un audit ISO/IEC 27001. Les stagiaires s'entraînent à préparer un plan d'audit, conduire les entretiens, collecter et analyser les preuves, formuler et classer les constats, rédiger un rapport clair et restituer les résultats devant une direction. Des mises en situation concrètes permettent de développer à la fois les compétences techniques et la posture de l'auditeur.

À l'issue de ces cinq jours, les participants sont capables de conduire de bout en bout un audit

de conformité ISO/IEC 27001, en respectant les exigences normatives et les meilleures pratiques d'audit. Ils maîtrisent les outils et méthodes pour expliquer, interpréter, évaluer et auditer efficacement un SMSI, et peuvent ainsi garantir la valeur et la crédibilité de leurs missions auprès des organisations auditées.

Objectifs

- Expliquer les concepts et principes d'un SMSI basé sur la norme ISO/IEC 27001
- Interpréter les exigences d'ISO/CEI 27001 dans le contexte d'un audit du SMSI
- Evaluer la conformité d'un SMSI aux exigences de la norme ISO/IEC 27001 selon les concepts et principes fondamentaux d'un audit
- Planifier, réaliser et clôturer un audit de conformité à la norme ISO/IEC 27001 et conformément aux exigences et bonnes pratiques d'audit

Public visé

- Chefs de projet
- Consultants
- Architectes techniques
- Toutes personnes souhaitant conduire des audits de conformité ISO/IEC 27001...

Pré-requis

- Connaître les principes de bases de la sécurité de l'information

Programme de notre Formation ISO/IEC 27001 - Management de la Sécurité de l'Information - Lead Auditor

[Jour 1 - Matin]

Concepts clés d'un SMSI

- Définitions : information asset, confidentialité-intégrité-disponibilité, parties intéressées
- Structure « High-Level Structure » des clauses 4 à 10 (2022)
- Relations ISO 27001 avec ISO 27002, ISO 27005, ISO 31000
- Vision d'ensemble des bonnes pratiques de gouvernance SSI
- Lien entre les concepts fondamentaux et leur rôle dans un audit de conformité
- Atelier pédagogique : Cartographier les actifs et visualiser les flux de données prioritaires.

[Jour 1 - Après-midi]

Principe et objectifs d'un audit ISO 27001

- Différences audit interne / tierce partie / certification
- Principes ISO 19011 : éthique, présentation fidèle, approche basée risques
- Notions de conformité vs efficacité, types de preuves (documentaire, observation, entretien)
- Cycle de vie d'un programme d'audit : planification ? exécution ? suivi
- Mise en relation avec les attendus d'un auditeur de certification
- Atelier pédagogique : Analyser un extrait de rapport pour distinguer constats, preuves et conclusions.

Interpréter les exigences des clauses 4 et 5

- Contexte de l'organisme & parties prenantes
- Définition du périmètre et de la Politique SSI
- Leadership, engagement et rôles (Top Management, CISO, auditeur)
- Gestion documentaire et niveaux de preuve attendus
- Exercice d'interprétation des exigences en se plaçant dans le rôle d'auditeur
- Atelier pédagogique : Évaluer la pertinence d'un périmètre SMSI proposé par un client.

[Jour 2 - Matin]

Planification du SMSI (clause 6)

- Objectifs de sécurité alignés stratégie business
- Appréciation et traitement du risque : méthode ISO 27005 / EBIOS RM
- Statement of Applicability : choix et justification des contrôles
- Plans d'action, ressources et délais
- Approche audit : évaluer la cohérence et la pertinence du SoA lors d'un audit
- Atelier pédagogique : Construire un SoA simplifié pour une startup SaaS.

[Jour 2 - Après-midi]

Support et gouvernance (clause 7)

- Compétences & sensibilisation sécurité (plan annuel de formation)
- Communication interne / externe, canaux et responsabilités
- Information documentée : politique, procédures, registres, preuves d'audit
- Maîtrise des ressources et de la chaîne d'approvisionnement
- Point de vue auditeur : comment vérifier la maîtrise documentaire et les preuves
- Atelier pédagogique : Analyser un kit documentaire et détecter les manques critiques.

Interpréter l'Annexe A 2022 (93 contrôles)

- Nouvelle structure : 4 thèmes + attributs
- Contrôles organisationnels, humains, technologiques, physiques
- Focus cloud & DevSecOps
- Lien risques-contrôles : priorisation & justification

- Application audit : vérifier la mise en œuvre des contrôles par des entretiens et revues documentaires
- Atelier pédagogique : Sélectionner 20 contrôles pour un environnement multcloud.

[Jour 3 - Matin]

Fonctionnement opérationnel (clause 8)

- Processus d'exploitation : change, backup, journalisation, accès
- Gestion des incidents : détection, réponse, apprentissage
- Critères d'acceptation du risque & traitement résiduel
- Exigences de preuves légales / forensics
- Positionnement auditeur : quelles preuves rechercher pour évaluer la conformité opérationnelle.
- Atelier pédagogique : Jeu de rôle « incident ransomware » et collecte d'évidences.

[Jour 3 - Après-midi]

Évaluer la conformité et la performance d'un SMSI (clause 9)

- Indicateurs KPI/KRI, tableaux de bord SMSI
- Évaluer l'efficacité des mesures par rapport aux exigences de la norme
- Audit interne : objectifs, portée, critères, méthodes
- Revue de direction : entrées / sorties obligatoires
- Satisfaction des parties intéressées & amélioration participative
- Mise en situation d'audit croisé entre stagiaires (auditeurs/audités)
- Atelier pédagogique : Définir trois indicateurs pertinents pour un hôpital.

Amélioration continue (clause 10)

- Non-conformités, actions correctives (CAPA) et boucles d'amélioration
- Capitalisation des incidents et retours d'expérience
- Intégration avec d'autres systèmes de management (ISO 9001, 22301)
- Culture sécurité : programmes de sensibilisation avancés
- Analyse d'un cas d'audit avec non-conformités réelles et proposition de CAPA
- Atelier pédagogique : Construire un plan CAPA à partir de constats d'audit fictifs.

[Jour 4 - Matin]

Plan d'audit détaillé et préparation logistique

- Définir objectifs, portée, critères, méthodes
- Allocation de l'équipe : compétences, indépendance, man-days
- Check-list & guides d'entretien basés sur ISO 27001
- Lettre de mission, communication avec l'audit, gestion documentaire préalable
- Atelier pédagogique : Élaborer un agenda d'audit sur deux sites distants.

[Jour 4 - Après-midi]

Techniques de collecte d'évidences

- Observation, entretiens, revue de documents, tests techniques
- Échantillonnage et représentativité
- Gestion du temps et adaptation in situ
- Outils digitaux : audit à distance, enregistrement sécurisé des preuves
- Atelier pédagogique : Simulation d'entretien auditeur-audité sur la gestion des accès.

Analyse des constats et rédaction du rapport

- Classification : non-conformité majeure / mineure, opportunités d'amélioration
- Formulation SMART et traçabilité des preuves
- Structure du rapport ISO 27001 pour un organisme certificateur
- Réunion de clôture : techniques de communication assertive
- Mise en situation : restitution orale des résultats d'audit devant un comité de direction fictif
- Atelier pédagogique : Rédiger la synthèse exécutive en 15 minutes.

[Jour 5 - Matin]

Processus de certification ISO 27001

- Étapes : revue de candidature, Stage 1, Stage 2, audits de surveillance, recertification
- Critères d'accréditation et rôle de l'organisme certificateur
- Gestion des écarts post-audit et suivi
- Stratégies multi-sites & échantillonnage
- Atelier pédagogique : Planifier la feuille de route de certification d'une PME européenne.

[Jour 5 - Après-midi]

Conseil et accompagnement des organisations

- Positionnement du rôle Lead Auditor / consultant
- Argumentaire de valeur et retour sur investissement sécurité
- Gestion du changement et conduite de projet SMSI
- Alignement ISO 27001 avec cadres NIS 2, DORA, NIST CSF
- Atelier pédagogique : Construire un pitch conseil « ISO 27001 ROI » pour la direction générale.

Préparation à l'examen final

- Structure type de l'examen
- Techniques de gestion du temps et décryptage des pièges

- Conseils administratifs : inscription, identification, surveillance à distance
- Atelier pédagogique : Passage de l'examen blanc et correction.

Sociétés concernées

Cette formation s'adresse à la fois aux particuliers ainsi qu'aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d'auto-évaluation nous permettant d'apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d'anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l'acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.