DAWAN

Plan de la formation

www.dawan.fr

Formation ISO 27001 – Lead Auditor (Certification PECB incluse)

Durée :	5 jours (35 heures)
Tarif inter-entreprises :	4 375,00 € HT (Présentiel) 3 500,00 € HT (Distanciel)
Public :	Auditeurs internes ou externes souhaitant réaliser ou diriger des audits SMSI - RSSI, responsables sécurité, consultants cybersécurité ou consultants systèmes de management - Responsables qualité, risques, conformité ou DPO impliqués dans la sécurité de l'information - Managers ou responsables informatiques devant préparer, accompagner ou piloter un audit ISO/IEC 27001 - Experts techniques souhaitant se préparer à un audit SMSI - Conseillers et consultants souhaitant renforcer leur expertise en audit de la sécurité de l'information
Pré-requis :	Compréhension de base de la norme ISO/IEC 27001 - Connaissance des principes d'audit - Expérience recommandée en sécurité de l'information, gestion des risques, conformité, qualité ou systèmes de management - Capacité à lire et exploiter une documentation normative et organisationnelle - Pour la validation de la certification RS7585 : avoir suivi l'ensemble de la formation PECB ou d'un partenaire habilité, selon les exigences France Compétences
Objectifs :	Comprendre les concepts et principes fondamentaux d'un SMSI basé sur ISO/IEC 27001 - Interpréter les exigences d'ISO/IEC 27001 dans une logique d'audit - Évaluer la conformité d'un SMSI aux exigences de la norme et aux bonnes pratiques d'audit - Planifier, conduire et clôturer un audit ISO/IEC 27001 conformément aux lignes directrices ISO 19011 et aux exigences applicables d'ISO/IEC 17021-1 - Diriger une équipe d'audit, communiquer avec les parties prenantes et gérer les situations d'audit - Rédiger des constats, des non-conformités et un rapport d'audit exploitable - Gérer un programme d'audit ISO/IEC 27001 - Se préparer au passage de l'examen PECB Certified ISO/IEC 27001 Lead Auditor

Modalités pédagogiques, techniques et d’encadrement :	• Formation synchrone en présentiel et distanciel. • Méthodologie basée sur l’Active Learning : 75 % de pratique minimum. • Un PC par participant en présentiel, possibilité de mettre à disposition en bureau à distance un PC et l’environnement adéquat. • Un formateur expert.
Modalité d'évaluation :	• Définition des besoins et attentes des apprenants en amont de la formation. • Auto-positionnement à l'entrée et la sortie de la formation. • Suivi continu par les formateurs durant les ateliers pratiques. • Évaluation à chaud de l'adéquation au besoin professionnel des apprenants le dernier jour de formation.
Sanction :	Parchemin de validation de la certification ou le cas échéant attestation de passage
Référence :	CYB103001-F
Note de satisfaction des participants :	Pas de données disponibles
Contacts :	commercial@dawan.fr - 09 72 37 73 73
Modalités d'accès :	Possibilité de faire un devis en ligne (www.dawan.fr, moncompteformation.gouv.fr, maformation.fr, etc.) ou en appelant au standard.
Délais d'accès :	Variable selon le type de financement.
Accessibilité :	Si vous êtes en situation de handicap, nous sommes en mesure de vous accueillir, n'hésitez pas à nous contacter à referenthandicap@dawan.fr, nous étudierons ensemble vos besoins

Comprendre le cadre ISO/IEC 27001 et le rôle de l’auditeur SMSI

Présentation de la formation, des objectifs de certification et du déroulement de l’examen PECB.
Principes fondamentaux de la sécurité de l’information : confidentialité, intégrité, disponibilité, gouvernance, risques et conformité.
Finalité d’un Système de Management de la Sécurité de l’Information et articulation avec la stratégie de l’organisation.
Structure de la norme ISO/IEC 27001, logique d’amélioration continue et exigences documentaires attendues.

Place d’ISO/IEC 27002, des contrôles de l’annexe A et des autres référentiels utiles à l’audit.
Rôle, responsabilités, posture et déontologie de l’auditeur ISO/IEC 27001.
Atelier fil rouge : analyse du contexte d’une organisation fictive et identification des enjeux SMSI à auditer.

Interpréter les exigences ISO/IEC 27001 dans une logique d’audit

Lecture orientée audit des clauses relatives au contexte, au leadership, à la planification, au support, aux opérations, à l’évaluation des performances et à l’amélioration.
Identification des informations documentées attendues et des preuves d’audit associées.
Analyse de la portée du SMSI, des parties intéressées, des objectifs de sécurité et des critères d’acceptation du risque.
Évaluation de la méthodologie d’appréciation et de traitement des risques de sécurité de l’information.
Analyse de la Déclaration d’Applicabilité, de la justification des exclusions et de la cohérence entre risques, traitements et mesures de sécurité.
Points de vigilance fréquents lors des audits ISO/IEC 27001 : gouvernance insuffisante, preuves incomplètes, objectifs non mesurés, plans d’action non suivis.
Atelier fil rouge : revue documentaire d’un SMSI et préparation d’une première liste de points d’audit.

Préparer et déclencher un audit ISO/IEC 27001

Principes d’audit selon ISO 19011 : intégrité, présentation impartiale, diligence professionnelle, confidentialité, indépendance, approche fondée sur les preuves et approche par les risques.
Différences entre audit interne, audit fournisseur, audit de certification, audit initial, audit de surveillance et audit de renouvellement.
Définition des objectifs, du périmètre, des critères, des méthodes et du calendrier d’audit.
Analyse préalable de la documentation, identification des risques d’audit et préparation de la stratégie d’échantillonnage.
Élaboration du plan d’audit, constitution de l’équipe d’audit et répartition des responsabilités.
Préparation des guides d’entretien, check-lists, matrices de preuves et documents de travail.
Communication avec le client audité, confirmation logistique et préparation de la

réunion d’ouverture.
Atelier fil rouge : construction d’un plan d’audit ISO/IEC 27001 et préparation des documents de travail associés.

Conduire les activités d’audit sur site ou à distance

Animation de la réunion d’ouverture et rappel des objectifs, du périmètre, des méthodes et des règles de communication.
Conduite des entretiens d’audit auprès de la direction, des responsables sécurité, des équipes IT, métiers, conformité et support.
Collecte et vérification des preuves : observations, entretiens, documents, enregistrements, indicateurs, tests et échantillonnages.
Audit des processus clés du SMSI : gestion des risques, gestion des actifs, contrôle des accès, continuité, incidents, fournisseurs, sensibilisation, surveillance et amélioration.
Techniques de questionnement, reformulation, écoute active et gestion des situations difficiles.
Traitement des écarts entre pratiques observées, exigences normatives, procédures internes et objectifs du SMSI.
Communication quotidienne avec l’audité et coordination de l’équipe d’audit.
Atelier fil rouge : simulation d’entretiens d’audit, collecte de preuves et qualification de constats.

Formuler les constats, non-conformités et conclusions d’audit

Distinction entre conformité, opportunité d’amélioration, point sensible, non-conformité mineure et non-conformité majeure.
Rédaction factuelle des constats à partir de preuves vérifiables et traçables.
Qualification des écarts selon leur impact sur la conformité, l’efficacité du SMSI et la maîtrise des risques.
Lien entre exigence ISO/IEC 27001, preuve collectée, écart observé et conséquence potentielle.
Préparation des conclusions d’audit et consolidation des constats avec l’équipe d’audit.
Animation de la réunion de clôture, présentation des constats et gestion des objections.
Évaluation de la pertinence des corrections, actions correctives et plans d’action proposés par l’organisation auditée.
Atelier fil rouge : rédaction de fiches de non-conformité et préparation d’une réunion de clôture.

Rédiger le rapport et assurer le suivi de l’audit ISO/IEC 27001

Structure attendue d’un rapport d’audit : contexte, objectifs, périmètre, critères, méthode, personnes rencontrées, constats, conclusions et recommandations.
Règles de qualité d’un rapport : clarté, traçabilité, neutralité, proportionnalité, confidentialité et exploitabilité.
Validation interne du rapport, revue qualité et diffusion aux parties prenantes autorisées.
Suivi des non-conformités, analyse des causes, vérification des actions correctives et décision de clôture.
Contribution de l’audit à l’amélioration continue du SMSI et à la préparation des audits ultérieurs.
Gestion documentaire et conservation des enregistrements d’audit.
Atelier fil rouge : production d’un rapport synthétique d’audit et évaluation d’un plan d’actions correctives.

Gérer un programme d’audit ISO/IEC 27001

Objectifs et gouvernance d’un programme d’audit SMSI.
Planification pluriannuelle des audits selon les risques, les exigences réglementaires, les changements organisationnels et les résultats précédents.
Sélection, compétence, évaluation et amélioration des auditeurs.
Gestion des ressources, priorités, indicateurs et tableaux de bord d’un programme d’audit.
Coordination entre audits internes, audits fournisseurs, audits de certification et audits réglementaires.
Traitement des conflits, arbitrages, contraintes de disponibilité et exigences de confidentialité.
Amélioration continue du programme d’audit et capitalisation des retours d’expérience.
Atelier fil rouge : construction d’un programme annuel d’audit SMSI fondé sur les risques.

Se préparer à l’examen PECB Certified ISO/IEC 27001 Lead Auditor

Présentation des domaines de compétences évalués : principes du SMSI, exigences ISO/IEC 27001, principes d’audit, préparation, réalisation, clôture et gestion d’un programme d’audit.
Méthodologie de réponse aux questions d’examen et gestion du temps.
Révision des notions clés : exigences normatives, approche par les risques, preuves

d’audit, non-conformités, rapport d’audit et suivi des actions correctives.
Entraînement sur des questions représentatives et correction commentée.
Identification des points de vigilance individuels et consolidation des acquis.
Rappel des modalités de passage, des règles de certification et des exigences du certificateur.
Atelier fil rouge : examen blanc, correction collective et plan de révision personnalisé.