Formation Implémenter et gérer un projet ISO 27001:2013

préparation aux certifications

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

La norme internationale de maîtrise du risque ISO/CEI 27001 lié à la sécurité de l'information décrit, sous forme d'exigences, les bonnes pratiques à mettre en place pour qu'une organisation puisse maîtriser efficacement les risques liés à l'information. Ce séminaire, vous présentera dans un premier temps l'ensemble des normes ISO traitant de la sécurité du système d'information puis vous apportera les éléments nécessaires pour mettre en place un système de management (SMSI) du risque de la sécurité de l'information.

Référence	ASE
Durée	3 jours (21h)
Tarif	2 950 €HT
Repas	repas inclus
Certification	- €HT

Objectifs

| Expliquer les composants d'un système de management de la sécurité de l'information (SMSI) conforme à ISO 27001
| Expliquer le contenu et la corrélation entre ISO 27001 et 27002 ainsi qu'avec d'autres normes et cadres réglementaires
| Adapter les exigences de la norme ISO 27001 au contexte spécifique d'un organisme
| Interpréter les exigences d'ISO 27001 dans le cadre de l'audit d'un SMSI

Public

| RSSI,
| Risk Managers,
| Directeurs ou responsables informatiques,
| MOE/ MOA,
| Ingénieurs ou correspondants Sécurité,
| Chefs de projets,
| Auditeurs internes et externes,
| Futurs "audités".

Prérequis

| Connaissances de base de la sécurité informatique.

Programme de la formation

Introduction
| Rappels. Terminologie ISO 27000 et ISO Guide 73.
| Définitions : menace, vulnérabilité, protection.
| La notion de risque (potentialité, impact, gravité).
| La classification CAID (Confidentialité, Auditabilité, Intégrité, Disponibilité).
| La gestion du risque (prévention, protection, report, externalisation).
| Analyse de la sinistralité. Tendances. Enjeux.
| Les réglementations SOX, PCI-DSS, COBIT. Pour qui ? Pourquoi ? Interaction avec l'ISO.
| Vers la gouvernance IT, les liens avec ITIL® et l'ISO 20000.
| L'apport de l'ISO pour les cadres réglementaires.
| L'alignement COBIT, ITIL® et ISO 27002.

Les normes ISO 2700x
| Historique des normes de sécurité vues par l'ISO.

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)

du 23 au 25 septembre 2025
du 14 au 16 octobre 2025
du 9 au 11 décembre 2025

PARIS

du 16 au 18 septembre 2025
du 7 au 9 octobre 2025
du 2 au 4 décembre 2025

VOIR TOUTES LES DATES

| Les standards BS 7799, leurs apports à l'ISO.
| Les normes actuelles (ISO 27001, 27002).
| Les normes complémentaires (ISO 27005, 27004, 27003...).
| La convergence avec les normes qualité 9001 et environnement 14001.
| L'apport des qualiticiens dans la sécurité.

La norme ISO 27001:2013
| Définition d'un Système de Gestion de la Sécurité des Systèmes (ISMS).
| Objectifs à atteindre par votre SMSI.
| L'approche "amélioration continue" comme principe fondateur, le modèle PDCA (roue de Deming).
| La norme ISO 27001 intégrée à une démarche qualité type SMQ.
| Détails des phases Plan-Do-Check-Act.
| De la spécification du périmètre SMSI au SoA (Statement of Applicability).
| Les recommandations de l'ISO 27001 pour le management des risques.
| De l'importance de l'appréciation des risques. Choix d'une méthode type ISO 27005:2011.
| L'apport des méthodes EBIOS, MEHARI dans sa démarche d'appréciation.
| L'adoption de mesures de sécurité techniques et organisationnelles efficientes.
| Les audits internes obligatoires du SMSI. Construction d'un programme.
| L'amélioration SMSI. La mise en oeuvre d'actions correctives et préventives.
| Les mesures et contre-mesures des actions correctives et préventives.
| L'annexe A en lien avec la norme 27002.

Les bonnes pratiques, référentiel ISO 27002:2013
| Objectifs de sécurité : Disponibilité, Intégrité et Confidentialité.
| Structuration en domaine/chapitres (niveau 1), objectifs de contrôles (niveau 2) et contrôles (niveau 3).
| Les nouvelles bonnes pratiques ISO 27002:2013, les mesures supprimées de la norme ISO 27001:2005. Les modifications.
| La norme ISO 27002:2013 : les 14 domaines et 113 bonnes pratiques.
| Exemples d'application du référentiel à son entreprise : les mesures de sécurité clés indispensables.

La mise en oeuvre de la sécurité dans un projet SMSI
| Des spécifications sécurité à la recette sécurité.
| Comment respecter la PSSI et les exigences de sécurité du client/MOA ?
| De l'analyse de risques à la construction de la déclaration d'applicabilité.
| Les normes ISO 27003, 15408 comme aide à la mise en oeuvre.
| Intégration de mesures de sécurité au sein des développements spécifiques.
| Les règles à respecter pour l'externalisation.
| Assurer un suivi du projet dans sa mise en oeuvre puis sa mise en exploitation.
| Les rendez-vous "Sécurité" avant la recette.
| Intégrer le cycle PDCA dans le cycle de vie du projet.
| La recette du projet ; comment la réaliser : test d'intrusion et/ou audit technique ?
| Préparer les indicateurs. L'amélioration continue.
| Mettre en place un tableau de bord. Exemples.
| L'apport de la norme 27004.
| La gestion des vulnérabilités dans un SMSI : scans réguliers, Patch Management...

Les audits de sécurité ISO 19011:2011
| Processus continu et complet. Etapes, priorités.
| Les catégories d'audits, organisationnel, technique...
| L'audit interne, externe, tierce partie, choisir son auditeur.
| Le déroulement type ISO de l'audit, les étapes clés.
| Les objectifs d'audit, la qualité d'un audit.
| La démarche d'amélioration pour l'audit.
| Les qualités des auditeurs, leur évaluation.
| L'audit organisationnel : démarche, méthodes.
| Apports comparés, les implications humaines.

Les bonnes pratiques juridiques
| La propriété intellectuelle des logiciels, la responsabilité civile délictuelle et contractuelle.
| La responsabilité pénale, les responsabilités des dirigeants, la délégation de pouvoir, les sanctions. La loi LCEN.
| Conformité ISO et conformité juridique : le nouveau domaine 18 de la norme ISO 27002:2013.

La certification ISO de la sécurité du SI - La relation auditeur-audité
| Intérêt de cette démarche, la recherche du "label".
| Les critères de choix du périmètre. Domaine d'application. Implication des parties prenantes.
| L'ISO : complément indispensable des cadres réglementaires et standard (SOX, ITIL®...).
| Les enjeux économiques escomptés.

| Organismes certificateurs, choix en France et en Europe.
| Démarche d'audit, étapes et charges de travail.
| Norme ISO 27006, obligations pour les certificateurs.
| Coûts récurrents et non récurrents de la certification.

Méthode pédagogique

Préparation aux certificats ISO 27001 Lead Implementer et Lead Auditor.

Certification

Cette formation prépare au passage de la certification suivante.
N'hésitez pas à nous contacter pour toute information complémentaire.

PECB ISO/IEC 27001:2013
L'examen a lieu lors de la dernière demi-journée de formation.
Cet examen certifie que vous possédez les connaissances et les compétences nécessaires pour mettre en oeuvre un SMSI suivant la norme ISO/IEC 27001:2013.

| Durée : 3h30
| Format : questions et études de cas
| Résultats transmis 4 à 6 semaines plus tard

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Suivre cette formation à distance

Voici les prérequis techniques pour pouvoir suivre le cours à distance :

| Un ordinateur avec webcam, micro, haut-parleur et un navigateur (de préférence Chrome ou Firefox). Un casque n'est pas nécessaire suivant l'environnement.
| Une connexion Internet de type ADSL ou supérieure. Attention, une connexion Internet ne permettant pas, par exemple, de recevoir la télévision par Internet, ne sera pas suffisante, cela engendrera des déconnexions intempestives du stagiaire et dérangera toute la classe.
| Privilégier une connexion filaire plutôt que le Wifi.
| Avoir accès au poste depuis lequel vous suivrez le cours à distance au moins 2 jours avant la formation pour effectuer les tests de connexion préalables.
| Votre numéro de téléphone portable (pour l'envoi du mot de passe d'accès aux supports de cours et pour une messagerie instantanée autre que celle intégrée à la classe virtuelle).
| Selon la formation, une configuration spécifique de votre machine peut être attendue, merci de nous contacter.
| Pour les formations incluant le passage d'une certification la dernière journée, un voucher vous est fourni pour passer l'examen en ligne.
| Pour les formations logiciel (Adobe, Microsoft Office...), il est nécessaire d'avoir le logiciel installé sur votre machine, nous ne fournissons pas de licence ou de version test.
| Horaires identiques au présentiel.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.