Smartfuture
Certifications | Training | Technology solutions

Formation

Mettre en œuvre un Système de Management de la Sécurité de l'Information (SMSI)

Formation intensive de 5 jours pour maîtriser la mise en œuvre d'un SMSI ISO/IEC 27001:2022, de l'analyse de risque à la préparation à la certification.

Formateurs certifiés

5 jours (35 h)	**Format** Présentiel / En ligne
Examen ISO/IEC 27001 Lead Implementer	**Niveau** Intermédiaire à avancé

INSCRIPTION / RÉSERVATION

Je m'inscris maintenant

OBJECTIFS PÉDAGOGIQUES

- Comprendre en profondeur les 8 domaines du CBK CISSP.
- Concevoir, mettre en œuvre et maintenir un SMSI.
- Maîtriser l'appréciation et le traitement des risques SSI.
- Préparer un projet ISO/IEC 27001 et collaborer avec les auditeurs.

PUBLIC CIBLE

- Responsables sécurité de l'information / RSSI.
- Chefs de projet SMSI, responsables qualité ou risques.
- DSI, responsables IT, consultants et membres d'équipe impliqués dans la mise en conformité ISO 27001.

PRÉREQUIS

- Connaissances de base en sécurité de l'information ou expérience dans les systèmes de management (ISO 9001, ISO 20000, etc.) recommandées.
- Une familiarité avec l'IT et les risques SI est un atout pour profiter pleinement de la formation.

PROGRAMME DE LA FORMATION – DÉTAILLÉ

Introduction à la sécurité de l'information et à ISO/IEC 27001

Contexte de la sécurité de l'information

- Concepts clés : confidentialité, intégrité, disponibilité, traçabilité, authenticité.
- Menaces, vulnérabilités, incidents de sécurité, cybercriminalité et enjeux de conformité.
- Rôle d'un Système de Management de la Sécurité de l'Information (SMSI) dans l'organisation.

Cadre normatif et famille ISO/IEC 27000

- Présentation de la série ISO/IEC 27000 (27001, 27002, 27005, 27017, 27018, etc.).
- Structure de haut niveau (HLS) des normes de management ISO.
- Positionnement d'ISO/IEC 27001 par rapport aux autres normes (qualité, continuité, services IT…).

Vocabulaire et principes de la norme ISO/IEC 27001:2022

- Termes et définitions clés de la norme.
- Principes de management (PDCA, amélioration continue, approche risque).

Comprendre le contexte de l'organisme (Clausse 4)

- Analyse du contexte interne et externe.
- Identification des parties intéressées et de leurs exigences.
- Définition du périmètre du SMSI et de ses limites.

Gouvernance, leadership et gestion des risques du SMSI

Leadership et gouvernance (Clausse 5)

- Engagement de la direction et rôles / responsabilités.
- Politique de sécurité de l'information : contenu, diffusion, revue.
- Organisation de la sécurité : comité, RSSI, sponsors, pilotes.

Planification du SMSI (Clausse 6)

- Objectifs de sécurité de l'information et planification pour les atteindre.
- Intégration de la sécurité de l'information dans les processus métier.

PROGRAMME DE LA FORMATION – DÉTAILLÉ

Appréciation et traitement des risques (ISO/IEC 27005)

- Méthodologie d'appréciation du risque (identification, analyse, évaluation).
- Identification des actifs, des menaces, des vulnérabilités et des impacts.
- Choix des options de traitement du risque (accepter, éviter, réduire…).
- Élaboration du plan de traitement des risques et articulation avec les contrôles de l'Annexe A.

Déclaration d'applicabilité (SoA)

- Rôle et structure de la SoA.
- Justification de l'inclusion / exclusion des contrôles de l'Annexe A (ISO/IEC 27001:2022)

Mise en œuvre opérationnelle du SMSI et contrôles ISO/IEC 27002

Support (Clausse 7)

- Ressources, compétences et plan de formation / sensibilisation.
- Communication interne et externe sur la sécurité de l'information.
- Documentation du SMSI : politiques, procédures, enregistrements, preuves.

Fonctionnement du SMSI (Clausse 8)

- Mise en œuvre et maîtrise opérationnelle des processus sécurité.
- Gestion des fournisseurs et de la chaîne de sous-traitance.
- Gestion des changements impactant la sécurité de l'information.

Contrôles de l'Annexe A / ISO/IEC 27002 (vue pratique)

- Organisation de la sécurité de l'information.
- Gestion des actifs, classification de l'information et manipulation sécurisée.
- Contrôles d'accès, identités, authentification, droits.
- Sécurité physique et environnementale.
- Sécurité des opérations, sauvegardes, journalisation, protection contre les malwares.
- Sécurité des communications et des réseaux.
- Acquisition, développement et maintenance des systèmes d'information..

PROGRAMME DE LA FORMATION – DÉTAILLÉ

Surveillance, audit, amélioration continue et préparation à la certification

Évaluation des performances (Clausse 9)

- Indicateurs de performance du SMSI (KPI, KRI, tableaux de bord).
- Surveillance, mesure, analyse et évaluation.
- Revue de direction : préparation, contenu, décisions, actions.

Audits internes du SMSI

- Planification, réalisation et rapport d'audit interne ISO 27001.
- Techniques d'entretien, collecte de preuves, constats et conclusions.

Amélioration continue (Clausse 10)

- Gestion des non-conformités et actions correctives.
- Cycle PDCA appliqué au SMSI : maintien, revue et amélioration dans la durée.

Préparation à l'audit de certification ISO/IEC 27001

- Processus de certification : phases, acteurs, documents attendus.
- Bonnes pratiques pour interagir avec les auditeurs externes et répondre aux constats.

Atelier pratique de mise en œuvre & préparation à l'examen Lead Implementer

Étude de cas complète de mise en œuvre d'un SMSI

- Analyse d'un contexte organisationnel réel ou inspiré de cas concrets.
- Définition du périmètre du SMSI et identification des actifs critiques.
- Construction du registre de risques et proposition de plan de traitement.

Élaboration des principaux livrables

- Politique de sécurité de l'information.
- Modèle de registre de risques et plan de traitement.
- Exemple de Déclaration d'Applicabilité (SoA).
- Bases d'un plan d'audit interne et d'un programme d'amélioration.

Préparation à la certification Lead Implementer

- Structure type de l'examen Lead Implementer.
- Conseils pour la gestion du temps et la stratégie de réponse.

PROGRAMME DE LA FORMATION – DÉTAILLÉ

- Quiz de révision et questions d'entraînement.

Questions / réponses et plan d'action post-formation

- Échanges sur vos projets SMSI et vos contraintes spécifiques.
- Recommandations pour lancer ou renforcer un projet ISO/IEC 27001,