

## Formation ISO 27001

|   |  |
|---|--|
| <b>Durée :</b>                                | 5 jours  |
| <b>Public :</b>                               | Chefs de projets, Architectes  |
| <b>Pré-requis :</b>                           | Posséder une formation initiale au minimum de second cycle ou justifier d'une expérience professionnelle d'au moins 5 ans dans le domaine de la sécurité informatique ou des normes ISO  |
| <b>Objectifs :</b>                            | - Présenter l'ensemble des normes ISO 27001 traitant de la sécurité du système d'information et de son management - Grâce à l'alternance systématique de phases pratiques et théoriques, il permet d'acquérir la maîtrise de l'implémentation des normes 27000 pour les adapter à votre contexte dans un périmètre allant d'un projet informatique sensible à l'ensemble de la Sécurité du Système d'information |
| <b>Sanction :</b>                             | Attestation de fin de stage mentionnant le résultat des acquis   |
| <b>Taux de retour à l'emploi:</b>             | Aucune donnée disponible   |
| <b>Référence:</b>                             | ARC100323-F  |
| <b>Note de satisfaction des participants:</b> | 4,64 / 5   |

### Présentation des normes ISO 2700X

Historique des normes ISO  
Les normes actuelles (ISO 27001, 27002, 27003, 27004 et 27005)  
Rappels.Terminologie ISO 27000  
Définitions : menace, vulnérabilité, protection  
La classification CAID (Confidentialité, Auditabilité, Intégrité, Disponibilité)  
Description de la notion d'ISMS (Système de Management de la sécurité de l'information)  
Présentation du modèle PDCA (Plan, Do, Check, Act)  
Analyse de la sinistralité. Tendances. Enjeux  
La gestion du risque (prévention, protection, report de risque, externalisation)  
L'apport de l'ISO pour les cadres réglementaires  
Liens avec COBIT, ITIL et CMMI dans le cadre de la gouvernance SI

### Le référentiel d'audit ISO 27001

A/ Description des points de contrôles et des éléments Techniques de l'Annexe A de ISO 27001  
B/Présentation des lignes directrices de l'audit définies dans l'ISO 19011  
Processus continu et complet. Etapes, priorités  
Les catégories d'audits, organisationnel, technique...  
L'audit interne, externe, tierce partie, comment 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 (type PDCA) pour l'audit  
Les qualités des auditeurs, leur évaluation  
L'audit organisationnel : démarche, méthodes  
Apports comparés, les implications humaines

## **Contenus du référentiel documentaire SMSI conformément à l'ISO 27001**

Indicateurs et surveillance du SMSI : les contrôles et l'audit interne  
Exposé des principes de l'ISO 27003  
Guide d'implémentation d'un SMSI et de l'ISO 27004  
Indicateurs de mesures  
Mesures physiques: authentification, biométrie, politique de nettoyage des bureaux  
Mesures techniques : authentification numérique et gestion des accès, Firewall, PKI, VPN, Backup  
Mesures organisationnelles : Elaboration et gestion du plan de continuité des activités (PCA), PRA, gestion du changement  
Points clés d'un audit de certification

## **Présentation du projet d'implémentation**

De la définition, à l'organisation et à la mise en oeuvre  
Naissance du SMSI  
Analyse et gestion des risques  
Présentation de la démarche ISO 27005  
Mise en oeuvre opérationnelle  
Politiques et processus supports au système de Management de la Sécurité de l'Information  
Politiques et usages SMSI  
Comités  
Gestion des incidents  
Gestion documentaire  
Les bonnes pratiques juridiques  
Application d'une loi, d'une règle de droit, d'une décision de justice  
La propriété intellectuelle des logiciels, la responsabilité civile délictuelle et contractuelle  
Responsabilité : pénale, des dirigeants, délégation de pouvoir, sanctions, loi LCEN  
Entre conformité ISO et conformité juridique

## **Préparation à l'examen**

Préparation à l'examen "Lead Implementer"