# ISO 27001 / ISO 2700-Les fondamentaux

## INFORMATIONS GÉNÉRALES

**Type de formation :** Formation continue

**Domaine :** Management du SI

**Filière :** Management SI

**Rubrique :** ITIL® produites par un Authorised Training Center

**Éligible au CPF :** Non

**Action collective :** Non

## PRÉSENTATION

### Objectifs & compétences

Être capable de présenter la norme ISO 27001:2013, les processus de sécurité qui lui sont associés et la démarche de certification
Savoir présenter la norme ISO 27002:2013 et les mesures de sécurité
Comprendre les contextes d'implémentation des mesures de sécurité et leur intégration dans l'organisation générale de la sécurité
Savoir sélectionner et approfondir des mesures de sécurité en prenant en compte l'appréciation des risques, les pièges à éviter et l'audit de ces mesures
Disposer d'une vue globale des référentiels existants, des guides d'implémentation ou des bonnes pratiques des mesures de sécurité

### Public visé

Toute personne qui souhaite prendre connaissance des normes ISO 27001 et 27002, améliorer sa maîtrise des mesures de sécurité de l'information et enrichir sa connaissance des référentiels existants pour faciliter leur mise en oeuvre
Opérationnels (techniques ou métiers) et auditeurs souhaitant améliorer leur compréhension des mesures propres à la SSI
RSSI souhaitant avoir un panorama des mesures, organiser leur plan d'action, ou dynamiser les échanges avec les opérationnels

### Pré-requis

Culture dans le domaine de la sécurité de l'information

## PROGRAMME

**1 - Normes et cadres réglementaires**
Qu'est-ce que l'ISO ?
La famille de normes ISO/IEC 27000
Normes et règlementations relatives à la sécurité de l'information
Avantages d'ISO/IEC 27001:2022
Raisons d'adopter ISO/IEC 27001:2022
Déterminez les trois avantages les plus significatifs qu'un organisme peut obtenir en adoptant un système de management de la sécurité de l'information (SMSI) basé sur ISO/IEC 27001:2022

**2 - Système de management de la sécurité de l'information (SMSI)**
Définition de système de management
Normes relatives aux systèmes de management
Systèmes de management intégrés
Définition d'un SMSI
Approche processus
Vue d'ensemble - articles 4 à 10
Vue d'ensemble - Annexe A

**3 - Concepts et principes fondamentaux de la sécurité de l'information**
Information et actif
Sécurité de l'information
Confidentialité, intégrité et disponibilité
Vulnérabilité, menace et impact
Risque de sécurité de l'information

**Code de formation :** MG206

### € Tarifs

**Prix public :** 2090 €

**Tarif & financement :**
Nous vous accompagnons pour trouver la meilleure solution de financement parmi les suivantes :
**Le plan de développement des compétences de votre entreprise :** rapprochez-vous de votre service RH.
**Le dispositif FNE-Formation**.
**L'OPCO** (opérateurs de compétences) de votre entreprise.
**France Travail:** sous réserve de l'acceptation de votre dossier par votre conseiller Pôle Emploi.
**CPF** -MonCompteFormation
Contactez nous pour plus d'information : contact@aston-institut.com

### Lieux & Horaires

**Campus :** Ensemble des sites

**Durée :** 14 heures

**Délai d'accès :** Jusqu'a 8 jours avant le début de la formation, sous condition d'un dossier d'insciption complet

**Distanciel possible :** Oui

### Prochaines sessions

Cliquez sur la date choisie pour vous inscrire :

- 06 / 05 / 2025
  : Ensemble des sites
  : Distanciel possible
  : 14 heures
  : 2 jours
- 26 / 06 / 2025
  : Ensemble des sites
  : Distanciel possible
  : 14 heures
  : 2 jours
- 23 / 10 / 2025
  : Ensemble des sites
  : Distanciel possible
  : 14 heures
  : 2 jours
- 20 / 11 / 2025
  : Ensemble des sites
  : Distanciel possible
  : 14 heures

Intelligence artificielle (IA)
Informatique en nuage (Cloud computing)
**4 - Compréhension de l'organisation et de son contexte**
Mission, objectifs, valeurs et stratégies de l'organisme
Objectifs SMSI
Définition préliminaire du périmètre
Environnement interne et externe
Parties intéressées
Exigences métier
**5 - Leadership**
Rôle de la direction dans le projet du SMSI
Politique de sécurité de l'information
Structure organisationnelle pour la sécurité de l'information
Rôles et responsabilités des parties intéressées
Principaux comités
**6 - Planification**
Processus de gestion des risques
Méthodologie d'appréciation des risques
Etablissement du contexte
Identification des risques
Estimation des risques
Evaluation des risques
Traitement des risques
Risque résiduel
**7 - Support**
Gestion des ressources
Compétence et développement des personnes
Formation, sensibilisation et communication
Informations documentées sur SMSI
**8 - Fonctionnement**
Planification opérationnelle
Gestion des changements
Continuité d'activité et reprise d'activité après sinistre
**9 - Evaluation de le performance**
Surveillance, mesure, analyse et évaluation de la performance
Type d'audits
audit interne
Documenter les non-conformités
Revue de direction
**10 - Amélioration**
Actions correctives
Plans d'action
Amélioration continue
**11 - Mesure de sécurité de l'information**
Classification des mesures de sécurité par type
Classification des mesures de sécurité par fonction
Introduction des mesures de l'Annexe A
**12 - Passage des examens de certification "PECB Certified ISO/IEC 27001 Foundation" et "PECB Certified ISO/CEI 27002 Foundation" (en ligne après la formation)**
Révision des concepts en vue du passage des certifications
Un voucher permettant le passage du test de certification est adressé à l'issue de la session
Chaque participant doit créer son profil sur l'espace PECB puis, une fois le profil validé, choisir un créneau pour passer l'examen et télécharger l'application PECB Exams
Le jour de l'examen ils doivent se connecter 30 minutes avant le début de la session
Retrouvez les instructions pour le passage de l'examen en ligne
L'examen de certification ISO 27001 est en français. L'examen se déroule sur 1 heure
Il est nécessaire de signer le code de déontologie du PECB afin d'obtenir les certifications
En cas d'échec les candidats bénéficient d'une seconde chance pour passer l'examen dans les 12 mois suivant la première tentative
L'examen "PECB Certified ISO/IEC 27001 Foundation" couvre les domaines de compétences suivants : Domaine 1 : Principes et concepts fondamentaux du Système de management de la sécurité de l'information - Domaine 2 : Système de management de la sécurité de l'information

: 2 jours

## MODALITÉS

### Modalités

**Modalités :** en présentiel, distanciel ou mixte . Toutes les formations sont en présentiel par défaut mais les salles sont équipées pour faire de l'hybride. – Horaires de 9H à 12H30 et de 14H à 17H30 soit 7H – Intra et Inter entreprise.
**Pédagogie :** essentiellement participative et ludique, centrée sur l'expérience,

l'immersion et la mise en pratique. Alternance d'apports théoriques et d'outils pratiques.
**Ressources techniques et pédagogiques :** Support de formation au format PDF ou PPT Ordinateur, vidéoprojecteur, Tableau blanc, Visioconférence : Cisco Webex / Teams / Zoom.
**Pendant la formation :** mises en situation, autodiagnostics, travail individuel ou en sous-groupe sur des cas réels.

## Méthode

**Fin de formation :** entretien individuel.
**Satisfaction des participants :** questionnaire de satisfaction réalisé en fin de formation.
**Assiduité :** certificat de réalisation.
**Validations des acquis** : grille d'evalution des acquis établie par le formateur en fin de formation.