

# Gouvernance de la sécurité des systèmes d'information avec les normes ISO 2700x-2016

## Certification ISO/IEC 27002 - Information Security Foundation

La norme ISO 27001 révisée en 2016 décrit les exigences pour la mise en place d'un Système de Management de la Sécurité de l'Information (SMSI). Le SMSI recense les mesures de sécurité, dans un périmètre défini, afin de garantir la protection des actifs informationnels. L'objectif est de protéger les informations de toute perte, vol ou altération, et les systèmes informatiques de toute intrusion.

L'ISO/CEI 27001 énumère un ensemble de points de contrôles à respecter pour s'assurer de la pertinence du SMSI, pour permettre de l'exploiter et de le faire évoluer. Plus précisément, l'annexe A de la norme est composée des 114 mesures de sécurité de la norme ISO/CEI 27002.

La version 2016 ne fait plus explicitement allusion au PDCA (ou roue de Deming) pour l'évaluation et l'amélioration des processus. Elle utilise les cycles de vie des processus et les concepts hérités des modèles de maturité comme le Capability Maturity Model.

L'objectif de la formation est d'apprendre à implémenter un système de management des SI conforme à la norme ISO 27001: 2016 et aux guides associés (ISO 27002:2016, ISO 27003, ISO 27004 et ISO 27005:2016).

La formation explique les normes et comment s'en servir concrètement, avec des exemples pour que chacun puisse les reproduire chez lui, en sachant organiser son projet et le dimensionner. Les exercices sont conçus à partir des retours d'expérience de praticiens. Ils permettront, par des études de cas, d'apprendre à mettre en œuvre et à prendre les bonnes décisions.

La formation prépare également à la **certification internationale «Information Security Foundation based on ISO/IEC 27002»**. Cette certification fournit la preuve que la matière du cours a été acquise et assimilée.

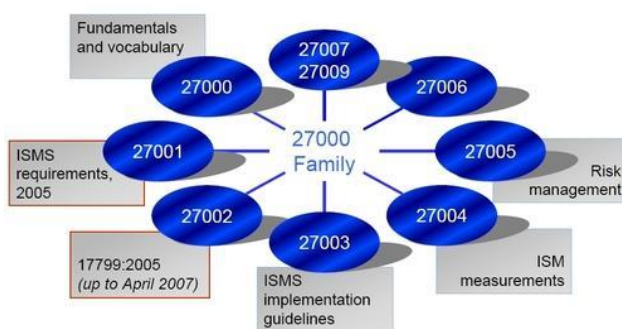
L'examen de certification est facultatif. Il permet d'évaluer les connaissances et la compréhension de l'ensemble du programme « Information Security Foundation based on ISO/IEC 27002 ». Sa durée est de 60 minutes et comprend 40 questions à choix multiple. Il se déroule en fin d'après-midi du dernier jour de cours dans nos locaux ou un jeudi à convenir. Sa préparation se fait sur la base d'examens à blanc à effectuer en dehors des heures de cours et discutés et corrigés dans le cadre du cours. Cette formule permet de réduire la durée du présentiel et ainsi de réduire le coût de la formation.

### Pour qui :

- gestionnaire responsable de la mise en œuvre de la sécurité à tous les niveaux, du management à l'opérationnel
- responsable de la sécurité des systèmes d'information et leurs équipes
- responsable de services opérationnels
- directeur des systèmes d'information et leurs équipes

### Objectifs :

- connaître les exigences de la norme ISO 27001:2016
- connaître les caractéristiques d'un SMSI - Système de Management de la Sécurité de l'Information
- savoir utiliser la norme ISO 27001 et ses guides associés (ISO 27002:2016, ISO 27003, ISO 27004 et ISO 27005:2016)
- savoir implémenter un SMSI - Système de Management de la Sécurité de l'Information



*Suite au verso*

## Gouvernance de la sécurité des systèmes d'information avec les normes ISO 2700x:2016

- se préparer à l'examen de certification « Information Security Foundation based on ISO/IEC 27002:2016 »

### Prérequis :

- expérience dans le domaine de la sécurité informatique, ou position de cadre dans une entreprise

### Programme:

- Première partie
  - Principes généraux de sécurité de l'information, mythes et réalité
  - Les besoins des exigences commerciales, réglementation
  - Présentation de la famille des normes ISO 27000
  - Processus de certification et d'accréditation
  - Introduction aux systèmes de gestion
  - Gestion et discipline documentaire
  - L'approche processus
  - Capability Maturity Model
- Deuxième partie
  - ISO 27001 et son SMSI - Système de Management de la Sécurité de l'Information
  - Survol de la norme ISO 27001
  - Vue générale du SMSI
  - Exigences de la norme
  - Les étapes d'implémentation d'un SMSI
- Troisième partie
  - Concepts fondamentaux de la gestion des risques
  - ISO 27005 et gestion des risques
  - Autres méthodes d'évaluation des risques
  - Approche et technique pour l'audit de sécurité
- Quatrième partie (ISO 27002)
  - Champ d'application
  - Références normatives
  - Termes et définitions
  - Structure de cette norme internationale
  - Stratégies de sécurité des informations
  - Organisation de la sécurité informatique
  - Sécurité des ressources humaines
  - Gestion d'actifs
  - Contrôle d'accès
  - Cryptographie
  - Sécurité physique et environnementale
  - Sécurité des opérations
  - Sécurité des communications
  - Maintenance, de développement et d'acquisition de système
  - Relations avec les fournisseurs
  - Gestion de l'information security incidente
  - Aspects de sécurité des informations de gestion de continuité des affaires et conformité
- Préparation à l'examen de certification ISO/IEC 27002

### Durée, prix :

Formation	Jours	Prix	Prix/j
Gouvernance de la sécurité des SI avec les normes ISO 2700x:2016	3	2'250.-*	750.-*
Examen de certification ISO/IEC 27002 - Information Security Foundation	60 min.	240.-	n/a

selon conditions générales. Le prix comprend toute la documentation distribuée. Les cours se déroulent de 09:00 à 12:00 et de 13:30 à 17:00

\* Remise de 5 % aux membres ADI, GRI, aux diplômé(e)s ISEIG CP, titulaires du BFI, DFI ou certifié(e)s MCSA, MCSE, MCSD formé(e)s à l'ISEIG

\*\*L'examen de certification se déroule à la fin du dernier jour de cours ou un jeudi au choix du candidat. Le prix de l'examen est fixé par l'organisme de certification.

