

Best

## ISO 27001 / ISO 27002 - Les fondamentaux

Les bonnes pratiques pour la gestion de la sécurité de l'information - Certification incluse

★★★★★ 4,6/5 (14 avis)

👤 Présentiel ou en classe à distance



2 jours (14 h)

Réf.: MG206

Formation officielle

# PECB

La norme ISO 27001 est devenue la référence internationale en termes de système de management de la sécurité de l'information (SMSI). Les projets de mise en conformité se multipliant et une connaissance des éléments fondamentaux pour la mise en oeuvre et la gestion d'un SMSI devient nécessaire. La norme ISO 27001 décrit une approche pragmatique de la gestion de la sécurité de l'information avec le choix de mesures de sécurité découlant d'une appréciation des risques. Elle s'appuie sur le guide ISO 27002 pour fournir des recommandations sur le choix et l'implémentation des mesures de sécurité.

Cette formation prépare à la certification PECB ISO/IEC 27001 Foundation et inclus le voucher pour passer l'examen.

### A qui s'adresse cette formation ?



#### Pour qui

- 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



#### Prérequis

- Culture dans le domaine de la sécurité de l'information
- **Disposez-vous des connaissances nécessaires pour suivre cette formation ? Testez-vous !**

### Programme

#### 1 - Normes et cadres réglementaires

- Qu'est-ce que l'ISO ?
- La famille de normes ISO/IEC 27000
- Normes et réglementations 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
- 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 de l'examens de certification "PECB Certified ISO/IEC 27001 Foundation"

- 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



### Les objectifs de la formation

- 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



### Evaluation

- Pendant la formation, le formateur évalue la progression pédagogique des participants via des QCM, des mises en situation et des travaux pratiques. Les participants passent un test de positionnement avant et après la formation pour valider leurs compétences acquises. Il est fortement recommandé d'être en possession de la norme pour le passage de l'examen.



### Les points forts de la formation

- Des exercices pratiques individuels et collectifs basés sur une étude de cas viennent enrichir ce cours magistral basé sur les normes.
- Les animateurs de ce module sont des formateurs certifiés ISO 27001 et ISO 27002.
- Le passage des examens de certification est compris dans le prix de la formation.
- 85% des participants à cette formation se sont déclarés satisfaits ou très satisfaits au cours des 12 derniers mois.