

Les principes clés des normes ISO 27001 et ISO 27002

La norme ISO 27001 permet une approche processus pour la mise en œuvre, le fonctionnement, la surveillance et l'amélioration du système de management de la sécurité de l'information d'une entreprise. Avec son annexe A, l'ISO 27002, elle détaille les mesures de sécurité qui peuvent être prises. L'application de ces normes permettent aux organisations de satisfaire les parties prenantes aux attentes de bonne gouvernance des données et de responsabilité.

Compétences visées

- Appliquer les normes ISO 27001 et ISO 27002 à son SMSI
- Auditer son SMSI pour vérifier la conformité à la norme ISO 27001

Objectifs pédagogiques

- Identifier les principes fondamentaux de la norme ISO 27001 et de son annexe la norme ISO 27002
- Réaliser l'appréciation des risques au sein d'une organisation
- Mettre en place des mesures de sécurité en corrélation à l'analyse des risques

Public

RSSI, directeurs, chefs de projet, ingénieurs en sécurité des systèmes d'information, toute personne souhaitant connaître les fondamentaux des normes ISO 27001 et ISO 27002.

Prérequis

Une connaissance de systèmes d'information et des notions de base en sécurité SI sont recommandées.

Programme

Introduction

- Définir une norme ISO
- Identifier les normes ISO 2700x
- Rappeler le champ de la sécurité d'un SI
- Définir la gestion de la qualité d'un SM grâce à la roue de Deming (PDCA)

Étudier la norme ISO 27001

- Identifier les exigences de la norme : articles 4 à 10
- Définir les phases du modèle PDCA sur les exigences de la norme ISO 27001

Mettre en œuvre des mesures de sécurité

- Identifier les objectifs de sécurité de l'organisation
- Réaliser une appréciation des risques
- Étudier la norme ISO 27002

- S'appuyer sur la norme ISO 27002 pour identifier les mesures de sécurité à prendre
- Documenter les mesures de sécurité
- Définir la déclaration d'applicabilité (DdA)

Auditer les mesures de sécurité

- Concevoir des audits internes pour vérifier la mise en œuvre des mesures de sécurité
- Analyser et améliorer les processus

Atelier

- Cas pratique sur l'application de la norme ISO 27001 à des exemples de SI

Durée

2 jours - 14 heures

Prix inter

1350 €HT

Prochaines dates

20 au 21 septembre 2018

5 au 6 novembre 2018

6 au 7 décembre 2018

Méthodes pédagogiques

12 participants maximum. Alternance d'apports théoriques et pratiques. Support de cours et documents d'application remis en fin de formation.

Validations des acquis

Quizz final et évaluation de la formation.

Formateur

Formateur expert dans le management de la sécurité des systèmes d'information

Après cette formation, vous pouvez suivre les formations RSSI, La Sécurité des SI et le Droit, ISO 27001 Lead Auditor, ISO 27001 Lead Implementer, EBIOS Risk Manager et ISO 27005 Risk Manager.