

Programme de formation Certification ISO 27002 Foundation

● Objectifs

Cette formation vous permettra d'appréhender les aspects fondamentaux de la mise en oeuvre des mesures de sécurité de l'information, conformément à la norme ISO/IEC 27002. Après une introduction générale sur la sécurité de l'information et ses concepts, vous étudierez les corrélations entre les différentes normes et cadres réglementaires. Les approches, méthodes, techniques et l'ensemble des bonnes pratiques en matière de sécurité de l'information seront ensuite passées en revue. Des exercices théoriques et pratiques vous permettront d'appréhender sereinement les exigences prévues par la norme ISO 27002 et d'y répondre grâce à la mise en oeuvre de mesures adéquates. A l'issue de notre formation, les participants passeront la certification ISO/IEC 27002 Foundation. L'examen s'effectuera durant la dernière journée de formation, sous la supervision d'un formateur accrédité. Les frais d'examen et de certification sont inclus dans le prix de la formation.

● Pré requis

Des connaissances générales sur la sécurité des systèmes d'information sont un atout.

● Durée

2 jours

● Public

Auditeurs, Chefs-de-projet, Consultants, Responsable-securite, Risk-managers

● Plan de formation

Introduction à la formation ISO 27002 Foundation

Retour sur la sécurité de l'information
Notions fondamentales : donnée, information, confidentialité, intégrité, disponibilité...
Le SMSI, Système de Management de la Sécurité de l'Information
La gestion des risques
Fiabilité de l'information, les critères à connaître (confidentialité, intégrité, disponibilité)
Présentation de la famille de normes ISO 2700x : origines et objectifs
Les termes et concepts essentiels
Processus et bénéfices de l'obtention d'une certification

La norme ISO/IEC 27002:2013

Présentation des thèmes principaux
Structure et objectifs de la norme
Relations avec l'ISO 27001 et les autres normes ISO 2700x

Risques, menaces et vulnérabilités

Menaces et risques : quelles différences, quelles relations ?
Typologie des menaces et préjudices
Effets sur la sécurité de l'information
Hacking et phishing
Mesures : préventives, répressives et correctives
Analyser, évaluer et traiter les risques
Stratégies de gestion des risques

Organisation

Politique de sécurité : principes, règles, rôles...
L'approche organisationnelle : mettre en place un SMSI
Classification des informations
Processus d'escalade des incidents
Gérer les incidents : connaître leur cycle de vie, impacts potentiels

Mesures de sécurité

Comprendre l'importance des mesures de sécurité

Structurer, établir et exécuter les différentes mesures

Mesures physiques : contrôle d'accès, biométrie, risques encourus...

Mesures techniques : authentification numérique, cryptographie, pare-feu, logiciels malveillants...

Mesures organisationnelles : séparation des tâches, sécurité des RH, élaboration d'un PCA (Plan de Continuité d'Activité), PRA (Plan de Reprise d'Activité)...

L'aspect législatif et réglementaire

Lois et réglementations, exemples

Respecter la réglementation : les mesures de conformité (audit, code de pratique)

Législation relative à la protection des données personnelles

Législation relative à la criminalité informatique

Etude de cas

Passage de l'examen de certification ISO 27002 Foundation

Révisions, examen blanc et correction commentée

Trucs et astuces pour le passage d'examen

Modalités d'évaluation