Cybersécurité : cadre GRC et certifications

Durée: 1 jour
Public cible: Professionnel TI

À qui s'adresse cette formation ?

- RSSI
- Responsables de conformité
- Gestionnaires TI
- Auditeurs
- Dirigeants impliqués en gouvernance de la cybersécurité

Objectifs de la formation

- Comprendre le rôle de la GRC en cybersécurité
- Explorer les cadres de référence majeurs (ISO 27001, SOC 2, NIST, Loi 25)
- Apprendre à concevoir et mettre en place un programme GRC
- Se préparer à un audit ou à une certification

Description sommaire

Cette formation donne une compréhension claire de la gouvernance, la gestion des risques et la conformité (GRC) appliquées à la cybersécurité. Elle explore les normes internationales, les programmes de certification et le rôle de la GRC dans la résilience organisationnelle.

Contenu du plan de cours

Module 1 : Introduction à la GRC en cybersécurité

- Définition et concepts fondamentaux
- La GRC comme boussole stratégique
- Parties prenantes et responsabilités

Module 2 : Normes et cadres de référence

- ISO/IEC 27001 et base d'un SMSI

- Critères de confiance SOC 2
- NIST Cybersecurity Framework et AI Risk Framework
- Loi 25 et survol du RGPD

Module 3 : Construire un programme GRC

- Méthodologies d'évaluation des risques
- Développement de politiques et choix de contrôles
- Suivi, audit et amélioration continue

Module 4 : Certifications et préparation aux audits

- Processus de certification ISO et SOC 2
- Préparation de la documentation et des preuves
- Étude de cas : mise en place d'un GRC dans une PME

Approche et méthode pédagogique

- Présentation progressive des concepts de gouvernance, gestion des risques et conformité en cybersécurité
- Explication des principaux cadres de référence et normes (ISO 27001, SOC 2, NIST, Loi 25) à partir d’exemples concrets
- Mise en contexte des enjeux de résilience organisationnelle, d’audit et de certification
- Études de cas pour illustrer la mise en place d’un programme GRC, notamment dans une PME
- Échanges et accompagnement du formateur pour faciliter l’application des notions à la réalité des participants

Prérequis

- Connaissances générales en cybersécurité
- Aucun prérequis en GRC ou en conformité n’est requis

Recommandations

-

Intérêt pour la gouvernance, la gestion des risques et la conformité

- Être impliqué dans des enjeux de sécurité, d’audit, de conformité ou de gestion TI
- Avoir une compréhension générale du fonctionnement d’une organisation et de ses obligations réglementaires
- Expérience en sécurité, audit, conformité ou gestion des risques (atout)