Formation Audit Sécurité Informatique

Code : SE03 **Durée** : 2 jours **Classe** : Présentiel / à distance

Public

- RSSI et correspondants sécurité
- Risk managers et responsables conformité
- DSI et chefs de projet IT
- Auditeurs internes et externes
- Responsables techniques et administrateurs systèmes
- Toute personne impliquée dans la gouvernance ou le pilotage de la sécurité des SI

Prérequis

- Notions de base en informatique

Objectifs

- Comprendre les menaces informatiques actuelles
- Appliquer les règles de sécurité de base
- Protéger les réseaux et systèmes
- Réagir face aux incidents de sécurité

Programme détaillé

1- Introduction : Rappel sur les enjeux et les obligations en matière de

- Définitions
- Rappel sur les principes d'un système de management de la SSI (ISO 27001)
- Les exigences réglementaires et légales en matière de pilotage de la SSI

2- Les rôles et les responsabilités en matière pilotage et de suivi de la

- Rôles et responsabilités des acteurs impliqués dans la SSI (Direction générale, Directions métiers, DSI, RSSI, DPO, RPCA, Auditeur, contrôle interne, ...)
- Les instances de décisions
- La gouvernance à prévoir dans le cadre du pilotage et du suivi de la SSI

3- Audit de la sécurité des SI

- Les catégories d'audit (audit de configuration, tests intrusifs, audit de code, ...)
- La démarche à adopter par l'auditeur (préparation de la mission, réalisation de la mission, restitution de la mission, métriques, ...)
- L'audit dans le cadre de la sous-traitance
- La certification des auditeurs
- La prise en compte des résultats de l'audit par l'organisme (arbitrage, amélioration des dispositifs opérationnels, ...)
- Les indicateurs de suivi des audits

4- Tableaux de bord de la sécurité des SI

- Les démarches proposées (normes ISO 27004, ...)
- Les catégories d'indicateurs SSI de niveau stratégique et opérationnel

5- Contrôles de la sécurité des SI

- Les contrôles permanents de la SSI (détections d'intrusion, gestion des logs, journalisation, ...)
- Les contrôles périodiques de la SSI (enquêtes, gestion des traces, ...)
- Les revues de direction (démarche, objectifs, ...)

6- La prise en compte des audits, tableaux et contrôles de la SSI dans les

- Le cadre réglementaire tunisien en matière de sécurité des systèmes d'information
- Les obligations d'audit périodique imposées par l'ANCE (Agence Nationale de la Cybersécurité) pour les organismes publics et infrastructures critiques