Auditer et contrôler la sécurité du SI

14 heures
SR239

Objectifs pédagogiques

- Être capable de construire les indicateurs et les tableaux de bord nécessaires à l'audit et au suivi de la sécurité du SI.
- Connaître les enjeux et les obligations en matière de pilotage de la sécurité
- Disposer d'une méthodologie d'audit de la sécurité
- Comprendre comment réaliser des tableaux de bord parlants et efficaces
- Pouvoir maîtriser les techniques de contrôle de la sécurité des SI

Public(s)

RSSI ou correspondants sécurité, risk manager, DPD, DSI, chefs de projet, auditeurs, responsables techniques

Pré-requis

Connaissances de base en sécurité informatique

Modalités pédagogiques

- Un panorama complet des outils et techniques d'audit et du contrôle de la sécurité.
- Le séminaire alterne entre présentation de fondamentaux théoriques et études de cas.
- Les retours d'expériences et conseils d'un consultant expert en sécurité qui étayera son approche de nombreux exemples concrets.

Moyens et supports pédagogiques

Support(s) de formation par apprenant

Modalités d'évaluation et de suivi

Évaluation en cours et fin de formation
Cette formation ne fait pas l'objet d'un contrôle des acquis via une certification

Formateur

Programme

Introduction : rappel sur les enjeux et les obligations en matière de pilotage de la SSI

- 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

Les rôles et les responsabilités en matière de pilotage et de suivi de la SSI

- 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

Audit de la sécurité des SI

- Les catégories d'audit (audit de configuration, tests intrusifs, audit de code, ...)
- Les recommandations de l'ANSSI (Guide PASSI)
- 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

Tableaux de bord de la sécurité des SI

- Les démarches proposées (normes ISO 27004, démarche proposée par l'ANSSI, démarche proposée par le CIGREF, ...)
- Les catégories d'indicateurs SSI de niveau stratégique et opérationnel
- La construction et l'alimentation des tableaux de bord SSI
- Le traitement des écarts (identification des non-conformités, définition des mesures correctives,...)

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, ...)

La prise en compte des audits, tableaux et contrôles de la SSI dans les démarches projets

- La démarche GISSIP proposée par l'ANSSI
- Les nouvelles règles Européennes imposées par le règlement Européen (Privacy By Design)

Étude de cas

- Mise en oeuvre de tableaux de bord SSI