Analyse des risques SI

Durée : 2 jours Référence : ANRSQ

Cette formation vous permettrait de savoir identifier et d'analyser les menaces qui pèsent sur votre système d'information, ainsi que leurs impacts potentiels sur votre SI. Vous travaillerez sur une étude de cas concrète, qui vous permettra de maîtriser les principales étapes d'une analyse de risques.

Contenu

- La notion de risque en sécurité de l'information
- L'identification des ressources
- L'analyse de risque
- Les méthodes utiles
- Les normes
- Etablissement du plan de traitement des risques

Participants

Responsable du service informatique. RSSI. Chef de projet en sécurité.

Pré-requis

Connaissances dans le domaine de la sécurité des SI.

Etude de cas

Une étude de cas servira de moyen, afin de voir l'intégralité de la méthode pratique d'analyse des risques.

Programme

La notion de risque en sécurité de l'information

- Les probabilités et la vraisemblance.
- Les impacts sur le SI et sur les métiers.

- La quantification du niveau de gravité.
- Les types de risques.
- La gestion par les risques. Principes. Avantages.
- Travaux pratiques
    - Questionnaire sur les risques SI et leur gestion.

L'identification des ressources

- Faire l'inventaire des biens : les informations et leurs supports (primaires, secondaires).
- L'organisation en place, le périmètre à couvrir.
- La classification DICT.
- Les intérêts et la méthode.
- Etude de cas
    - Réalisation d'un inventaire et d'une classification des informations et de leurs supports.

L'analyse de risque

- Identification des menaces et des vulnérabilités.
- Evaluation des risques encourus.
- Priorisation : la matrice des risques, la notion de scénario.
- Travaux pratiques
    - Identifier les risques et les prioriser grâce à l'utilisation de la matrice.

Les méthodes utiles

- Les méthodes françaises : EBIOS, MEHARI.
- Les méthodes internationales : OCTAVE.
- Les apports, les avantages et les inconvénients de chaque méthode.
- Le choix approprié d'une méthode et la personnalisation.
- Travaux pratiques
    - Réflexion de groupe sur les critères de choix et les avantages/inconvénients des différentes méthodes.

Les normes

- Les différentes normes utiles pour les analyses de risques.
- La démarche d'analyse de risques dans le cadre 27001.
- L'approche PDCA (Plan - Do - Check - Act).
- Les apports de l'ISO 27002, de BS25999 et de l'ISO 31000.
- Travaux pratiques
- Exemples d'application d'une norme.

Elaboration du plan de traitement des risques

- La palette des actions : prévention, protection, report de risque, externalisation, assurances.
- Construire un plan de traitement des risques à partir de la matrice des risques et des autres sources (audits, incidents).
- Que contient le plan : les objectifs et les mesures, les indicateurs d'avancement et de qualité.
- Les risques résiduels.
- La gestion et les usages du plan de traitement des risques.
- Etude de cas
    - Réalisation d'un plan de traitement des risques.