

## Méthode EBIOS

**Durée : 3 jours**   **Référence : EBIOS**

Cette formation présente la méthode EBIOS qui permet d'analyser et de traiter les risques relatifs à la sécurité des SI en se basant sur les expériences dans le conseil SI. Cette formation vous apportera toutes les connaissances utiles à sa mise en œuvre en situation réelle.

---

### Contenu

- Introduction
  - Etude du contexte
  - Etude des événements redoutés
  - Etude des scénarios de menaces
  - Etude des risques
  - Etude des mesures de sécurité
  - Conclusion
- 

### Participants

RSSI, Chef de projet en sécurité.

---

### Pré-requis

Connaissances de la gestion de la sécurité des SI et de la norme 27005.

---

### Programme

#### Introduction

- Objectifs d'EBIOS 2010. Evolution EBIOS v2.
- Compatibilités normatives 27001 et 27005.
- Présentation de la démarche méthodologique.
- Historique, rôle de l'ANSSI et du club EBIOS.
- Domaine d'application de la démarche : cible secteur public ou privé, tailles et secteurs d'activité visés.
- Application de la méthode sur systèmes de sécurité existants ou en cours de d'élaboration.
- Diffusion de la méthode EBIOS.

## Etude du contexte

- Caractéristiques du contexte : identification du domaine d'application.
- Biens essentiels (actifs primaires) : biens supports.
- Les menaces principales.
- Les enjeux de sécurité du périmètre.
- Travaux pratiques
  - Echanges interactifs sur la gestion des risques. définir quel est le sujet de l'étude.

## Etude des événements redoutés

- Appréciation des événements de sécurité redoutés.
- Identification, analyse et évaluation de chaque événement.
- Travaux pratiques
  - Identification, avec échanges interactifs, de l'ensemble des événements craints. Identification des plus graves.

## Etude des scénarios de menaces

- Appréciation des scénarios de menaces. Identification.
- Analyse et évaluation de chaque scénario de menace.
- Travaux pratiques
  - Définir les scénarios possibles. Définir ceux qui sont les plus vraisemblables.

## Etude des risques

- Analyse et évaluation des risques.
- Identification des objectifs de sécurité.
- Traitement des risques : choix des options.
- Travaux pratiques
  - Cartographie des risques. Traiter les différents risques.

## Etude des mesures de sécurité

- Identifier les mesures de sécurité à appliquer.

- Evaluation du risque résiduel (après application des mesures).
- Appréciation des risques résiduels.
- Rédaction de la déclaration d'applicabilité.
- Mise en œuvre des mesures de sécurité et élaboration d'un plan d'action.
- Suivi de l'efficacité des mesures.
- Acceptation (homologation) des risques résiduels.
- Travaux pratiques
  - Identification des mesures à appliquer. Définir l'acceptabilité des risques résiduels.

## **Conclusion**

- Synthèse sur la méthode EBIOS.
- Personnalisation de son analyse de risques.
- Revue de l'analyse : vers une démarche PDCA.
- Intégration de la démarche dans un SMSI.