# *Risk Manager - Méthode EBIOS*
## *EBIOS RM, préparation à la certification*

*Cours Pratique de 2 jours - 14h*
*Réf : EBU - Prix 2024 : 1 570€ HT*

La méthode EBIOS permet d'apprécier et de traiter les risques relatifs à la sécurité des SI en se fondant sur une expérience éprouvée en matière de conseil SI et d'assistance MOA. A l'issue de la formation, l'apprenant sera capable de manager les risques relatifs à la sécurité de l'information en se fondant sur les principes et usages de la méthode EBIOS.

### OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Comprendre les concepts et les principes d'EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité)

Cartographier les risques

Maîtriser les éléments de gestion des risques de base pour la sécurité de l'information en utilisant la méthode EBIOS

Analyser et communiquer les résultats d'une étude EBIOS

### MÉTHODES PÉDAGOGIQUES

Le support et l'animation sont en français.

### CERTIFICATION

Ce cours associé au cours EBX (EBIOS RM, examen de certification), la journée de passage d'examen, permet de préparer et passer la certification PECB certified EBIOS risk manager.

# LE PROGRAMME

dernière mise à jour : 07/2022

### 1) La méthode EBIOS risk manager

- Les fondamentaux de la gestion des risques.
- Zoom sur la cybersécurité (menaces prioritaires).
- Présentation d'EBIOS.
- Principales définitions d'EBIOS risk manager.

### 2) Cadrage et socle de sécurité

- Identification du périmètre métier et technique.
- Identification des événements redoutés et évaluation de leurs niveaux de gravité.
- Déterminer le socle de sécurité.

*Travaux pratiques : Identifier les événements redoutés.*

### 3) Sources de risques

- Identifier les sources de risques (SR) et leurs objectifs visés (OV).
- Évaluer la pertinence des couples.
- Évaluer les couples SR/OV et sélectionner ceux jugés prioritaires pour l'analyse.
- Évaluer la gravité des scénarios stratégiques.

*Travaux pratiques : Identifier les sources de risques (SR) et leurs objectifs visés (OV). Évaluer les couples SR/OV.*

### 4) Scénarios stratégiques

- Évaluer le niveau de menace associé aux parties prenantes.

### PARTICIPANTS

Consultants, responsables sécurité des SI, gestionnaires des risques, toute personne impliquée dans des activités d'appréciation des risques informatiques.

### PRÉREQUIS

Connaître le guide sécurité de l'ANSSI, avoir suivi le parcours introductif à la cybersécurité ou posséder des connaissances équivalentes sur la sécurité des systèmes d'information.

### COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

### MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

### MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

### MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

### ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

- Construction d'une cartographie de menace numérique de l'écosystème et les parties prenantes critiques.
- Élaboration des scénarios stratégiques.
- Définition des mesures de sécurité sur l'écosystème.

*Travaux pratiques : Évaluer le niveau de menace associé aux parties prenantes. Élaboration de scénarios stratégiques.*

### 5) Scénarios opérationnels

- Élaboration des scénarios opérationnels.
- Évaluation des vraisemblances.
- Threat modeling, ATT&CK.
- Common Attack Pattern Enumeration and Classification (CAPEC).

*Travaux pratiques : Élaboration des scénarios opérationnels. Évaluation des vraisemblances.*

### 6) Traitement du risque

- Réalisation d'une synthèse des scénarios de risque.
- Définition de la stratégie de traitement.
- Définir les mesures de sécurité dans un PACS.
- Évaluation et documentation des risques résiduels.
- Mise en place du cadre de suivi des risques.

*Travaux pratiques : Définir les mesures de sécurité dans un Plan d'Amélioration Continue de la Sécurité (PACS). Mise en place du cadre de suivi des risques.*

## LES DATES

| CLASSE À DISTANCE | PARIS |
| --- | --- |
| 2024 : 24 juin, 30 sept., 02 déc. | 2024 : 17 juin, 23 sept., 25 nov. |