



# **Cahier des charges de formation à la méthode d'analyse de risque *EBIOS Risk Manager***

EBIOS *Risk Manager* est une méthode développée par l'ANSSI en 2018 et soutenue par le Club EBIOS<sup>1</sup>. Elle permet de réaliser une appréciation et un management des risques numériques conformes à la norme ISO 27005 dont les valeurs reposent sur les aspects concret, efficient, convaincant et collaboratif.

EBIOS *Risk Manager* propose une méthode d'analyse de risque agile de l'ensemble des systèmes, dans leur environnement global, avec des résultats visibles étape par étape. Cette nouvelle version de la méthode permet de bâtir une vision partagée des risques entre les décideurs et les métiers pour pouvoir définir et mettre en œuvre la meilleure stratégie de management des risques.

La méthode a été conçue pour s'adapter facilement à tout type de contexte ou d'environnement. Elle peut s'appliquer aussi bien aux organismes publics que privés, quels que soient leur taille et leur secteur d'activité, que leur système d'information soit en cours d'élaboration ou déjà existant.

Ce cahier des charges est éligible à la labellisation SecNumedu-FC de l'ANSSI. Cette labellisation permet aux organismes délivrant cette formation d'être référencés sur le site de l'ANSSI et d'utiliser la marque et le logo associés à SecNumedu-FC. Pour plus de précisions, consulter <https://www.ssi.gouv.fr/entreprise/formations/secnumedu-fc-labellisation-de-formations-continues-en-cybersecurite/>.

Pour être considérée conforme au cahier des charges et obtenir le label SecNumedu-FC, une formation doit réunir les critères suivants :

- Le contenu, le déroulement, la durée et le nombre d'apprenants doivent être conformes aux attendus du présent cahier des charges
- Un descriptif de la formation doit être disponible sur le site web de l'organisme de formation et préciser les éléments suivants : descriptif de la formation (contenu, déroulement, volume horaire, nombre d'apprenants minimum et maximum), identité du ou des formateurs
- Le ou les formateurs animant la formation doi(ven)t être signataires de la *Charte du formateur Ebios Risk Manager* (<https://www.ssi.gouv.fr/entreprise/management-du-risque/la-methode-ebios-risk-manager/formation-ebios-risk-manager/> )

---

<sup>1</sup> Le Club EBIOS est une association de loi de 1901 regroupant des experts individuels et des organismes, issus des secteurs public ou privé. Il supporte et enrichit le référentiel français de gestion des risques depuis 2003.

## OBJECTIF

La formation vise à faire acquérir aux apprenants les connaissances et compétences nécessaires afin qu'ils puissent aider les organismes publics et/ou privés à mettre en place un management des risques de cybersécurité utilisant la méthodologie EBIOS *Risk Manager*

## DUREE

Deux ou trois jours de formation consécutifs comptabilisant un minimum de 14h et un maximum de 21h

## NOMBRE DE PARTICIPANTS

8 à 20 apprenants

## PRE -REQUIS

Connaissance générale en sécurité des systèmes d'information et en informatique

## PUBLIC VISE

- Risk managers
- Responsables de la sécurité des systèmes d'information
- Personnels en charge de l'homologation des systèmes d'information
- Consultants en sécurité des systèmes d'information
- Auditeurs sécurité des systèmes d'information
- Assureurs
- Directeurs des systèmes d'information
- Officiers de la sécurité des systèmes d'information

## SUPPORTS

- Support de cours apprenants
- Livret d'exercices et corrections
- Support de cours formateur (diaporama)
- Formulaire d'évaluation de la formation
- Guides méthodologiques pour les apprenants (téléchargeables sur le site de l'ANSSI)

## PEDAGOGIE

- Méthode Affirmative connue aussi comme méthode magistrale basée sur le *DIRE*. Cours magistral
- Méthode Interrogative : *DIRE ET FAIRE DIRE*. Echanges formateur apprenants
- Méthode Démonstrative : *FAIRE ET FAIRE-FAIRE*. Démonstrations et exercices de mise en œuvre
- Méthode Active : *FAIRE FAIRE*. Exercices et travaux pratiques à la fin de chaque atelier

## EVALUATION DE LA FORMATION

Formulaire d'évaluation de la formation pour identifier l'adéquation du contenu de la formation et les axes d'amélioration

# PROGRAMME DE LA FORMATION

## JOUR 1

### 1. Introduction

*Objectif : obtenir l'accord des apprenants sur le cadre de la formation.*

- ✓ Accueil des apprenants
- ✓ Recueil des attentes des apprenants
- ✓ Règles et programme

### 2. EBIOS Risk Manager, les bases

*Objectif : Illustrer les concepts de la gestion des risques et les grands principes de mise en œuvre de la méthode.*

- ✓ Le risque
- ✓ Le niveau de risque
- ✓ Principe du socle vs risques
- ✓ Principe d'itérations successives
- ✓ Principe d'efficacité vs exhaustivité

### 3. Atelier 1 – Cadrage et socle de sécurité

*Objectif : Faire comprendre comment réunir les éléments nécessaires pour adapter la gestion des risques au contexte particulier du sujet de l'étude.*

- ✓ Présentation du déroulement de l'atelier
- ✓ Valeurs métier et biens supports
- ✓ Événements redoutés (ER), impacts et gravité
- ✓ Socle de sécurité
- ✓ Mesures issues de l'atelier
- ✓ Exercice(s)

### 4. Atelier 2 – Sources de risque

*Objectif : Faire comprendre comment identifier et analyser l'origine des risques : les couples sources de risques (SR) / objectifs visés (OV)*

- ✓ Présentation du déroulement de l'atelier
- ✓ Couples sources de risques (SR) / objectifs visés (OV)
- ✓ Mesures issues de l'atelier
- ✓ Exercice(s)

### 5. Atelier 3 – Scénarios stratégiques

*Objectif : Expliquer comment élaborer les scénarios stratégiques.*

- ✓ Présentation du déroulement de l'atelier
- ✓ Parties prenantes : identification
- ✓ Parties prenantes : évaluation
- ✓ Scénarios stratégiques
- ✓ Mesures issues de l'atelier
- ✓ Exercice(s)

### 6. Atelier 4 – Scénarios pratiques

*Objectif : Expliquer comment élaborer les scénarios opérationnels.*

- ✓ Présentation du déroulement de l'atelier
- ✓ Scénarios opérationnels
- ✓ Mesures issues de l'atelier
- ✓ Exercice(s)

## JOUR 2

### 7. Atelier 5 – Traitement du risque

*Objectif : Expliquer comment choisir les traitements appropriés des risques, les planifier et suivre leur mise en œuvre.*

- ✓ Présentation du déroulement de l'atelier
- ✓ Mesures pour traiter les risques
- ✓ Suivi des risques

### 8. Étude de cas

*Objectif : S'assurer de la bonne appropriation de la logique globale.*

- ✓ Mise en pratique des concepts
- ✓ Déroulé des 5 ateliers dans le cadre d'un cas concret