

# Gestion des risques avec ISO/IEC 27005 & EBIOS

## INFORMATIONS GÉNÉRALES

**Type de formation :** Formation continue

**Éligible au CPF :** Non

**Domaine :** Cybersécurité - sécurité informatique

**Action collective :** Non

**Filière :** Pilotage de la sécurité organisationnelle

**Rubrique :** Certifications ISO

**Code de formation :** MG216

## PRÉSENTATION

### Objectifs & compétences

Le programme de cette formation est axé essentiellement sur la norme ISO 27005 pour aborder les bases de la gestion des risques. Ultérieurement les méthodes EBIOS 2010 et EBIOS Risk Manager sont étudiées en détails pour une mise en pratique à la suite de la formation.

### Public visé

consultant en sécurité de l'information, risk manager.

### Pré-requis

connaissances générales en sécurité des systèmes d'information.

### € Tarifs

**Prix public :** 4049 €

### Tarif & financement :

Nous vous accompagnons pour trouver la meilleure solution de financement parmi les suivantes :

**Le plan de développement des compétences de votre entreprise :** rapprochez-vous de votre service RH.

**Le dispositif FNE-Formation.**

**L'OPCO** (opérateurs de compétences) de votre entreprise.

**France Travail:** sous réserve de l'acceptation de votre dossier par votre conseiller Pôle Emploi.

**CPF -MonCompteFormation**

Contactez nous pour plus d'information : contact@aston-institut.com

## PROGRAMME

### Section 1 fondamentaux de la gestion des risques

Le système d'information et la gestion des risques

Fondamentaux de la gestion des risques (probabilité, impact, calcul, vision des risques)

La gouvernance, risque, ISO 2700

### Section 2 la phase de contexte par ISO 27005

Présentation de l'ISO 27005 (comités, normes)

Terminologie ISO 27005

PDCA

Contexte interne/externe

Objectifs, valeurs, missions, stratégie

Établir un SWOT

Comprendre l'environnement interne

Identification des exigences

Identifier les objectifs

Critères de bases, d'acceptation, d'évaluation, d'impact et de probabilité de la gestion des risques

### Section 3 Phase d'identification des risques

- Description de la phase d'appréciation des risques avec l'identification, l'estimation et l'évaluation

- Collecter des informations

- Types d'actifs

### Section 4 Phase d'estimation et d'évaluation des risques

- Approche qualitative vs quantitative
- Les différentes méthodes de calcul des risques
- Calcul du risque

### Section 5 Phase de traitement et d'acceptation des risques

- Établir un plan de traitement des risques

### Section 6 La méthode EBIOS 2010 et la phase contexte

## 📍 Lieux & Horaires

**Durée :** 35 heures

**Délai d'accès :** Jusqu'à 8 jours avant le début de la formation, sous condition d'un dossier d'inscription complet

## 📅 Prochaines sessions

Consultez-nous pour les prochaines sessions.

- Historique d'EBIOS (Expression des besoins et identification des objectifs de sécurité)
- Alignement d'EBIOS 2010 et l'ISO 27005
- Définir le cadre de la gestion des risques
- Préparer les métriques
- Identifier les biens
- Éléments dimensionnants d'une étude
- Exemples et application

**Section 7** Les évènements redoutés

- Apprécier les évènements redoutés

**Section 8** Les scénarios de menaces

- Mécanique de sélection des menaces
- Les différents scénarios de menaces

**Section 9** Étude des risques

- Apprécier les risques
- Choix de traitement du risque

**Section 10** Mesures de sécurité

- Formaliser les mesures de sécurité à mettre en oeuvre
- Mettre en oeuvre les mesures de sécurité

**Section 11** introduction à la méthode EBIOS Risk Manager

- Les fondamentaux de la gestion des risques
- Présentation d'EBIOS
- Zoom sur la Cybersécurité (menaces prioritaires)
- Principales définitions EBIOS RM
- Exercice 1 : Compréhension de la terminologie

**Section 12** Atelier 1 "Cadrage et socle de sécurité"

- Présentation de l'atelier
- Définition du cadre de l'étude et du projet
- Identification du périmètre métier et technique
- Identification des évènements redoutés et évaluation de leur niveau de gravité
- Déterminer le socle de sécurité

**Section 13** Atelier 2 "Sources de risques"

- Présentation de l'atelier
- 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

**Section 14** Atelier 3 "Scénarios stratégiques"

- Présentation de l'atelier
- Évaluer le niveau de menace associé aux parties prenantes
- Construction d'une cartographie de menace numérique de l'écosystème et les parties prenantes critiques

**Section 15** Atelier 3 "Scénarios stratégiques"

- Présentation de l'atelier
- Évaluer le niveau de menace associé aux parties prenantes
- Construction d'une cartographie de menace numérique de l'écosystème et les parties prenantes critiques

**Section 16** Atelier 5 "Traitement du risque"

- Présentation de l'atelier
- Réalisation d'une synthèse des scénarios de risques
- Définition de la stratégie de traitement
- Définir les mesures de sécurité dans un plan d'amélioration continue de la sécurité (PACS)
- Évaluation et documentation des risques résiduels
- Mise en place du cadre de suivi des risques

**MODALITÉS****Modalités**

**Modalités :** en présentiel, distanciel ou mixte . Toutes les formations sont en présentiel par défaut mais les salles sont équipées pour faire de l'hybride. – Horaires de 9H à

12H30 et de 14H à 17H30 soit 7H – Intra et Inter entreprise.

**Pédagogie :** essentiellement participative et ludique, centrée sur l'expérience, l'immersion et la mise en pratique. Alternance d'apports théoriques et d'outils pratiques.

**Ressources techniques et pédagogiques :** Support de formation au format PDF ou PPT Ordinateur, vidéoprojecteur, Tableau blanc, Visioconférence : Cisco Webex / Teams / Zoom.

**Pendant la formation :** mises en situation, autodiagnostic, travail individuel ou en sous-groupe sur des cas réels.

### **Méthode**

**Fin de formation :** entretien individuel.

**Satisfaction des participants :** questionnaire de satisfaction réalisé en fin de formation.

**Assiduité :** certificat de réalisation.

**Validations des acquis :** grille d'évaluation des acquis établie par le formateur en fin de formation.