

Mis à jour le 22/08/2025

S'inscrire

Formation Risk Manager - Méthode EBIOS

2 jours (14 heures)

PRÉSENTATION

Maîtrisez la gestion des risques informatiques grâce à notre formation « Risk Manager - Méthode EBIOS ». Un parcours structuré et progressif, alliant théorie et ateliers immersifs, pour comprendre les concepts fondamentaux de la gestion des risques et la méthodologie EBIOS RM.

Durant cette formation, vous apprendrez à maîtriser l'ensemble des étapes de la méthode EBIOS afin d'identifier, analyser et traiter les risques relatifs à la sécurité de l'information. Nous aborderons les notions clés de la gestion des risques (actifs, menaces, vulnérabilités, impacts, acceptabilité du risque), la modélisation des menaces et la construction de scénarios d'attaque réalistes, tout en les reliant aux référentiels et bonnes pratiques de l'ANSSI et aux normes ISO (27001 / 27005).

Vous développerez une expertise opérationnelle vous permettant de conduire une étude complète de bout en bout : du cadrage et de l'identification des actifs essentiels, jusqu'à la hiérarchisation des risques, l'arbitrage (réduction, transfert, acceptation, évitement) et l'élaboration d'un plan de traitement adapté. Vous serez également formés à analyser et restituer vos résultats auprès de différents publics (direction, RSSI, métiers), afin de favoriser la prise de décision et la mise en œuvre efficace des mesures de sécurité.

Enfin, vous serez entraînés à travers des cas pratiques fil rouge et mises en situation, qui vous permettront de mettre immédiatement en application chaque étape de la méthode EBIOS et de vous préparer à une restitution en conditions réelles. Cette formation, résolument tournée vers l'action, vous donnera les outils indispensables pour renforcer la résilience, améliorer la gouvernance et piloter la cybersécurité au sein de votre organisation.

OBJECTIFS

- Comprendre les concepts et les principes relatifs à la gestion des risques de la méthode EBIOS
- Maîtriser les étapes de la méthode EBIOS pour la réalisation complète d'une étude
- Gérer les risques de sécurité de l'information en utilisant la méthode EBIOS

- Analyser et communiquer les résultats d'une étude EBIOS

PUBLIC VISÉ

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

Pré-requis

- 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.

Programme de Notre Formation Risk Manager - Méthode EBIOS

[Jour 1 - Matin]

Structure de la méthode EBIOS (EBIOS Risk Manager)

- Les 5 ateliers EBIOS RM : 1) Cadrage, 2) Sources de risque, 3) Scénarios stratégiques, 4) Scénarios opérationnels, 5) Traitement des risques
- Entrées / Sorties / Livrables par atelier (cartographie des actifs, événements redoutés, scénarios, mesures, justificatifs)
- Rôles & responsabilités : sponsor, animateur, métiers, RSSI, IT, juridique
- Jalons & planning type d'une étude, critères d'arrêt, gestion des dépendances
- Articulation avec ISO 27005 (appréciation du risque) et contribution au SMSI ISO 27001
- Atelier pratique : Mapping « ateliers / livrables » sur un mini-cas.

[Jour 1 - Après-midi]

Cadrage de la méthode EBIOS

- Définir le périmètre, les objectifs et le contexte de l'analyse
- Identifier les parties prenantes et leurs attentes
- Atelier pratique : Cadrage d'une étude (cas réel/simulé).

Étude du contexte et des événements redoutés

- Identifier les actifs essentiels et les besoins de sécurité
- Définir les événements redoutés et leurs impacts potentiels
- Atelier pratique : Analyse du contexte d'une organisation fictive.

[Jour 2 - Matin]

Scénarios de menace

- Identification des sources de risque et des scénarios de menace
- Typologie des menaces et modes opératoires, modélisation d'attaques
- Atelier pratique : Construction de scénarios sur le cas d'étude.

Revue des mesures existantes

- Identifier et évaluer les mesures déjà en place
- Cartographier les forces & faiblesses de l'organisation
- Atelier pratique : Analyse critique d'un plan de sécurité.

[Jour 2 - Après-midi]

Traitement des risques & Communication des résultats

- Calcul et hiérarchisation des risques, critères d'acceptation
- Élaboration d'un plan de traitement (mesures techniques, organisationnelles, contractuelles)
- Structurer la restitution : rapport, supports COMEX/métiers
- Présenter les résultats aux parties prenantes (direction, métiers, RSSI)
- Atelier pratique : Élaborer un plan de traitement & restituer une étude EBIOS simulée.

Sociétés concernées

Cette formation s'adresse à la fois aux particuliers ainsi qu'aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d'auto-évaluation nous permettant d'apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d'anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l'acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.