

EBIOS-RM : mise en pratique de la méthode et des outils

(formation conforme au cahier des charges ANSSI, labellisation SecNumÉdu-FC en cours)

Organisation

Durée : 16 heures à distance sur 2 semaines

Dates : 11-22 octobre 2021 et 15-26 mars 2022
+sessions à la demande (présentiel possible)

Formation à distance

- outils collaboratifs Office365/teams
- 8h de travail (asynchrone) /sem en autonomie et en groupe avec tuteurs (dont 2 à 3 classes virtuelles synchrones d'échanges avec les experts)
- **2 semaines**

Évaluation de la formation

- Évaluation qualitative de la participation et des productions donnant droit à la délivrance d'une attestation de participation
- Évaluation de la qualité (certification Qualiopi en cours)

Renseignements et inscription

Benoît GAUDICHEAU
benoit.gaudicheau@univ-ubs.fr
tél. +33 (0)2 97 01 72 70

Tarifs

1600€ individuel
et nous consulter pour les groupes

Objectifs

L'objectif est de pouvoir **mettre en œuvre la méthode** et/ou être moteur au sein de son organisation afin que la **prise de conscience, la prise en compte et l'acceptation des risques SI** soit la plus partagée possible et optimise le service rendu.

Personnes concernées

RSSI, risk-manageurs, personnels en charge de l'homologation des SI, consultants SSI, auditeurs SSI, assureurs, DSI, officiers de la SSI, chef d'entreprise/projet SSI...

Prérequis

Sensibilisation à la SSI

<https://secnumacademie.gouv.fr/> devra avoir été suivi avant la formation (partie à distance dans tous les cas)

Compétences à l'issue de la formation

Mettre en place un management des risques de cybersécurité utilisant la méthode EBIOS Risk Manager

- en étant efficace plutôt qu'exhaustif
- en prenant en compte l'écosystème
- en organisant selon les objectifs ateliers et participants
- associant conformité et scénarios de risque
- alternant entre point de vue de l'organisation et de l'attaquant
- en utilisant les outils et méthode recommandés par l'ANSSI

Programme

- Accueil, **recueil des attentes/contextes**, modalités
- Rappels sur le contexte de la gestion du risque SI (ISO 27k,...)
- **1^{er} cas pratique étudié tous ensemble** : cadrage et socle de sécurité, sources de risques, scénarios stratégiques, scénarios opérationnels, mesures correctives
- **Seconde étude de cas pratique en groupe**, utilisation d'un logiciel d'aide à l'analyse

Méthodes pédagogiques actives

- Formation **à distance** : utilisation d'outils de travail en groupe synchrone et asynchrone (visio, chat de groupe, partage d'écrans,...)

Responsable et intervenants

- Julien BREYAULT, enseignant en cyberdéfense à l'ENSIBS **formé à EBIOS-RM par le CFSSI de l'ANSSI**
julien.breyault@univ-ubs.fr
- Logan FERNANDEZ, CISO, certifié ISO27001 Lead auditor & ISO27005 Lead Risk manager.

Public**Organisation de la formation**

<ul style="list-style-type: none">• Dirigeants,• Responsables des Systèmes d'Information (RSI/DSI),• Responsables de la Sécurité des Systèmes d'Information (RSSI),• Responsables métiers avec forte dépendance cyber	<p>Notions de base en SSI nécessaires pour l'analyse de risque (2h, dont 1h en visio)</p> <ol style="list-style-type: none">1. Les enjeux de la sécurité des S.I.2. Les besoins de sécurité3. Notions de vulnérabilité, menace, attaque4. Panorama de quelques menaces5. Le droit des T.I.C. et l'organisation de la sécurité en Europe6. ... en France7. ... dans le monde
	<p>EBIOS Risk Manager : les bases (30min, visio)</p>
	<p>Première étude de cas simplifiée et commentée (4h30) <i>Réalisation des 5 ateliers en groupe à partir d'une cartographie des processus métier et d'une cartographie SI + rapport d'audit de sécurité SI</i> <u>Accompagnement global</u></p> <ul style="list-style-type: none">• Les bases d'EBIOS-RM : objectifs et organisation• Atelier 1 : cadrage et socle de sécurité• Atelier 2 : sources de risque• Atelier 3 : scénarios stratégiques• Atelier 4 : scénarios opérationnels• Atelier 5 : traitement du risque
	<p>Seconde étude de cas plus complexe/réaliste (8h, dont 1h de visio par groupe) <i>Réalisation des 5 ateliers en groupe à partir d'une cartographie des processus métier et d'une cartographie SI + rapport d'audit de sécurité SI</i> <u>Accompagnement personnalisé</u></p> <ul style="list-style-type: none">• Atelier 1 : cadrage et socle de sécurité• Atelier 2 : sources de risque• Atelier 3 : scénarios stratégiques• Atelier 4 : scénarios opérationnels• Atelier 5 : traitement du risque <p>Témoignage et échanges avec un CISO certifié ISO27001 (1h, visio)</p>