Référentiel de formation à la méthode d'analyse de risque EBIOS *Risk Manager*

TABLE DES MATIÈRES

INTRODUCTION

EBIOS *Risk Manager* (EBIOS RM) est une méthode d'analyse de risques développée par l'ANSSI et soutenue par le Club EBIOS[1]. Elle permet de réaliser une appréciation et un management des risques numériques conformes à la norme ISO 27005:2022. Elle permet de bâtir une vision partagée des risques entre les décideurs, les référents métiers et les opérationnels afin de 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.

OBJET DU DOCUMENT

Ce document a pour objectif d'offrir un modèle de formation à l'analyse de risques EBIOS Risk Manager aux organismes de formation.

Il détaille les enseignements minimaux à intégrer dans un programme afin d'obtenir une formation de qualité permettant aux apprenants, à l'issue de la formation, d'être en capacité de mettre en place une analyse de risques EBIOS RM au sein de leur entreprise.

Label SecNumedu-FC

Les formations conformes aux exigences de ce référentiel peuvent obtenir la labellisation SecNumedu-FC. Les formations labellisées sont référencées sur le site de l'ANSSI et peuvent utiliser le logo associé à SecNumedu-FC.

Le processus d'acquisition du label et ses modalités sont présentés sur le site web de l'ANSSI à l'adresse suivante : https://cyber.gouv.fr/labellisation-secnumedu-fc-comment-proceder.

[1] 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.

L'analyse de risques EBIOS RM

Objectifs de la formation

Le contenu de la formation permet aux apprenants d'acquérir les connaissances et compétences nécessaires à la mise en place d'un management des risques de cybersécurité utilisant la méthodologie EBIOS RM au sein de leur structure.

Public visé

Personnes en charge de la réalisation d'une analyse de risques en cybersécurité :

- Managers de risques (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 en sécurité des systèmes d'information
- Assureurs en sécurité des systèmes d'information
- Directeurs des systèmes d'information
- Officiers de la sécurité des systèmes d'information

Programme

1. Introduction
2. EBIOS Risk Manager, les bases
3. Atelier 1 – Cadrage et socle de sécurité
4. Atelier 2 – Sources de risque
5. Atelier 3 – Scénarios stratégiques
6. Atelier 4 – Scénarios pratiques
7. Atelier 5 – Traitement du risque
8. Étude de cas

Prérequis

Connaissances générales en informatique et en sécurité des systèmes d'informations

Durée de la formation

2 à 3 jours
(soit entre 14H et 21H)

Nombre de participants

20 participants maximum

Mode d'apprentissage

Présentiel, distanciel ou hybride

Méthodes pédagogiques

- Cours théoriques
- Travaux pratiques
- Exercices de mise en situation

Pédagogie d'enseignement

- méthode affirmative connue aussi comme méthode magistrale (« dire »)
- méthode interrogative favorable aux échanges entre formateur et apprenants (« faire exprimer »)
- méthode démonstrative où se succèdent démonstrations et exercices de mise en œuvre (« faire » et « faire faire »)

PROGRAMME DÉTAILLÉ[2]

JOUR 1

Introduction

Objectif : Adapter la formation aux attentes des apprenants

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

1. 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

2. Atelier 1 – Cadrage et socle de sécurité

Objectif : Réunir les éléments nécessaires permettant d'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 appréciation de leur gravité
- Socle de sécurité
- Mesures issues de l'atelier
- Exercice(s)

3. Atelier 2 –Sources de risque

Objectif : Être en capacité d'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)

4. Atelier 3 – Scénarios stratégiques

Objectif : Être en capacité d'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)

5. Atelier 4 – Scénarios pratiques

Objectif : Savoir élaborer les scénarios opérationnels

- Présentation du déroulement de l'atelier
- Scénarios opérationnels et appréciation de leur vraisemblance
- Identification et priorisation des mesures issues de l'atelier
- Exercice(s)

JOUR 2

6. Atelier 5 – Traitement du risque

Objectif : Être en capacité de choisir les traitements appropriés aux risques retenus, les planifier et suivre leur mise en œuvre

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

7. Étude de cas

Objectif : Mettre en œuvre les concepts d'EBIOS RM par une étude de cas

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

[2] Le support dédié au formateur détaille le contenu de chaque atelier en offrant des modèles de documents et des exemples : Support de Formation (1).pdf

L'obtention du label SecNum*edu*-FC EBIOS RM est conditionnée par le respect des exigences listées infra.

1. Exigences d'ordre général

- Le déroulement de la formation est structuré selon les grands chapitres du programme de formation type
- La durée de la formation est comprise entre 2 et 3 jours consécutifs, comptabilisant un minimum de 14h et un maximum de 21h
- Le nombre d'apprenants est au maximum de 20 personnes
- Un descriptif de la formation est disponible sur le site web de l'organisme de formation et précise les éléments suivants :
  - le contenu de la formation
  - le mode d'apprentissage (présentiel, hybride ou distanciel dont les modalités sont développés infra)
  - le volume horaire
  - le nombre d'apprenants minimum et maximum
  - l'identité du ou des formateurs
- Tout formateur animant la formation est signataire de la *Charte du formateur* EBIOS *Risk Manager* (https://cyber.gouv.fr/formation-ebios-risk-manager)
- La formation comprend différents supports :
  - un support de cours au profit des apprenants
  - un livret d'exercices et ses corrections
  - un support de cours formateur (diaporama)
  - un formulaire d'évaluation de la formation (pour identifier l'adéquation du contenu de la formation et les axes d'amélioration)
  - les guides méthodologiques au profit des apprenants (téléchargeables sur le site de l'ANSSI) : La méthode EBIOS Risk Manager - Le guide | ANSSI

Pour accompagner le développement de la méthode EBIOS Risk Manager, un kit de formation est mis à disposition des formateurs : https://cyber.gouv.fr/formation-ebios-risk-manager

- La pédagogie d'enseignement employée comprend différentes méthodes :
  - méthode affirmative
  - méthode interrogative
  - méthode démonstrative

2. EXIGENCES SELON LE MODE D'APPRENTISSAGE SUIVI

2.1. Formation en présentiel

Tous les apprenants sont réunis physiquement dans la même pièce pour les cours magistraux.

La formation est dispensée par un ou deux formateurs.

2.2. Formation en mode hybride

Le mode hybride est une formation en présentiel avec la possibilité d'avoir jusqu'à 25% d'apprenants à distance (avec un maximum de 5 stagiaires à distance par session).

Il est préconisé d'avoir deux formateurs.

Afin d'assurer une formation de qualité pour l'ensemble des apprenants, les conditions suivantes doivent être réunies :

- Le stagiaire à distance dispose :
  - d'une qualité de connexion audio et vidéo suffisante ;
  - d'une caméra et d'un micro allumés en permanence durant toute la formation ;
  - d'un ordinateur (PC, Mac) pour assister à la formation (l'utilisation d'un téléphone portable ou d'une tablette n'est pas autorisée) ;

L'organisme de formation exige au préalable ces prérequis. Si l'apprenant n'est pas en mesure de disposer d'une caméra et d'un micro, il ne peut être éligible à la formation à distance.

- L'organisme de formation / formateur dispose :
  - d'un outil de visioconférence / formation à distance, permettant la gestion de groupe et la création de salle virtuelle. Le formateur est formé à l'utilisation de cet outil ;
  - d'une salle virtuelle et d'une visioconférence configurées et préparées en amont de la formation ;
  - d'une bonne qualité audio : le formateur est audible par tous, quel que soit l'endroit où il se trouve, y compris lorsqu'il se déplace dans la salle. (L'utilisation d'un micro-cravate est suggérée) ;

- Les stagiaires à distance sont pleinement intégrés au groupe présent en salle afin de faciliter les interactions.
  - La salle de formation dispose d'un second écran permettant de projeter les caméras des stagiaires à distance. De la même manière, une caméra permet aux apprenants à distance de voir la salle, ainsi tous les stagiaires se voient et peuvent créer des interactions.
  - Une seconde caméra filme le formateur et l'endroit où il se trouve. De cette manière, les stagiaires à distance peuvent voir l'ensemble de la gestuelle et des supports pédagogiques utilisés (tableau blanc…) par le formateur. La vue du formateur est projetée sur l'écran des stagiaires à distance.
  - Lors de la création des groupes pour les exercices et l'étude de cas, les stagiaires à distance sont regroupés au sein du même groupe (pas de groupe mixte présentiel-distanciel). À cette occasion les micros des stagiaires et de la salle sont coupés.

2.3. Formation à distance

Le mode distanciel est une formation permettant à tous les stagiaires d'être à distance (pas de salle physique).

La formation est obligatoirement dispensée par deux formateurs.

Afin d'assurer une formation de qualité pour l'ensemble des apprenants, l'ensemble des conditions d'apprentissage à distance du mode « hybride » doivent être respectées en excluant les exigences liées à la configuration de la salle.

L'organisme de formation précisera, lors de sa demande de labellisation, le mode d'apprentissage suivi (présentiel, hybride ou distanciel). En mode « hybride » ou « distanciel », l'organisme de formation devra fournir le nom de la solution de visioconférence utilisée.