

Formation

Livret formateur

Version du 08/04/2020

**Sommaire**

[Objet du document 2](#_Toc37277366)

[Contributions et ressources utilisées 2](#_Toc37277367)

[1 Éléments à prévoir 3](#_Toc37277368)

[2 Séquencement 3](#_Toc37277369)

[Introduction (jour 1 matin) 3](#_Toc37277370)

[EBIOS *Risk Manager*, les bases (jour 1 matin) 4](#_Toc37277371)

[Atelier 1 (jour 1 matin) 5](#_Toc37277372)

[Atelier 2 (jour 1 après-midi) 6](#_Toc37277373)

[Atelier 3 (jour 1 après-midi) 7](#_Toc37277374)

[Atelier 4 (jour 1 après-midi) 8](#_Toc37277375)

[Atelier 5 (jour 1 après-midi) 8](#_Toc37277376)

[Synthèse (jour 1 après-midi) 9](#_Toc37277377)

[Étude de cas (jour 2) 9](#_Toc37277378)

[Conclusion (fin du jour 2) 10](#_Toc37277379)

# Objet du document

Ce document fait partie du kit de formation à la méthode EBIOS *Risk Manager*.

Le présent « Livret formateur » est destiné à être utilisé par le(s) formateur(s), avant la formation pour lui rappeler les éléments à prévoir, et au cours de la formation suivre son séquencement.

# Contributions et ressources utilisées

|  |  |  |
| --- | --- | --- |
| Type | Description | |
| Contenu | 2019-2020 – Création du document  Matthieu GRALL (SODIFRANCE) | Fichier:Logo Sodifrance bleu dégradé.png — Wikipédia |
| Julie DUCLOS et Maricela PELEGRIN-BOMEL (ANSSI) | Fichier:Anssi.png — Wikipédia |
| Logo | ANSSI | Fichier:Anssi.png — Wikipédia |

# Éléments à prévoir

Le(s) formateur(s) doit/doivent prévoir les éléments suivants :

* à installer :
  + ordinateur avec la présentation ;
  + vidéo projecteur et câble ;
  + *paper board* et feutres ;
* à imprimer :
  + guides EBIOS *Risk Manager* ;
  + fiches EBIOS *Risk Manager* ;
  + livrets stagiaires ;
  + feuille de présence ;
  + présentation ;
  + fiches d’évaluation vierges ;
* à fournir également :
  + feuilles blanches ;
  + stylos (en cas de besoin).

# Séquencement

Le tableau suivant présente le séquencement de la formation EBIOS *Risk Manager* pour une **session de deux jours**. Il précise les objectifs du/des formateur(s), les activités à mener, les messages clés et les éléments à utiliser pour chaque séquence :

| Séquencement | Objectif du/des formateur(s) | Activités de formation |
| --- | --- | --- |
| Introduction (jour 1 matin) | Faire connaître le cadre de la formation et obtenir l’adhésion des apprenants | |
| * 1. Accueil | Intégrer les apprenants à la formation | * Accueillir les apprenants   + [diapositive 1] * Demander de créer un chevalet et d'inscrire son prénom * Faire signer la feuille de présence |
| * 1. Attentes | Adapter la formation aux attentes spécifiques des apprenants, et leur faire comprendre ce qui sera traité et ce qui ne sera pas traité | * Faire un tour de table en demandant leurs fonctions et leurs attentes spécifiques * Noter les attentes   + [*paperboard*] |
| * 1. Objectif de *la formati*on | Rappeler l’objectif de la formation | * Énoncer l’objectif pédagogique   + [diapositive 2]   + *Principal message : l’objectif est d’être capable d’utiliser la méthode EBIOS Risk Manager et ses outils pour réaliser ou piloter une étude des risques.* * Vérifier l’adhésion des apprenants |
| * 1. Règles et programme | Énumérer la manière dont la formation va se dérouler et faire adhérer les apprenants | * Énoncer les règles (horaires, contraintes spécifiques, *etc*.)   + [diapositive 3] * Présenter le programme et le matériel fourni : présentation, livret stagiaire, guide *EBIOS Risk Manager* et fiches, corrections de l’étude de cas fournie le 2e jour   + *Principal message : une journée pas-à-pas sur les étapes clés de la méthode (cela signifie ici qu’on ne va pas voir dans le détail l’ensemble des étapes mais uniquement les points les plus importants), et une journée sur une étude de cas complète.* * Vérifier l’adhésion |
| EBIOS *Risk Manager*, les bases (jour 1 matin) | Faire découvrir et comprendre les concepts de la gestion des risques et les grands principes de mise en œuvre de la méthode EBIOS *Risk Manager*   * + [diapositive 4] | |
| 1. Le risque | Faire distinguer les éléments constitutifs d'un risque | * Présenter les composants des risques à l'aide d'un exemple   + [diapositives 5 à 8] * Faire un exercice collégial : faire s’interroger les apprenants successivement sur la source de risque, le bien support, la valeur métier, l'événement redouté, les impacts et l'objectif visé   + [diapositive 9] * Corriger l'exercice   + [diapositive 10]   + *Principal message : le risque est un scénario composé de plusieurs objets. Il qui décrit comment une « source de risques » peut causer un « événement redouté » sur une « valeur métier », qui aurait des « impacts » sur l’organisme, pour atteindre son « objectif visé ».* |
| 1. Le niveau de risque | Faire comprendre comment estimer un risque en cybersécurité | * Présenter les notions de gravité, vraisemblance et niveau de risque   + [diapositives 11 à 13]   + *Principal message : le niveau d’un risque est constitué de sa gravité et de sa vraisemblance.* * Faire un exercice collégial : pour chaque élément présenté, indiquer s’il est utile à l’estimation de la gravité ou de la vraisemblance des risques   + [diapositive 14] * Corriger l'exercice   + [diapositive 15] |
| 1. Démarche et principe de mise à jour | Faire comprendre qu’il y a 5 ateliers et faire reconnaitre le besoin de mettre à jour l’étude | * Présenter le cheminement général de l’étude et la notion d’itérations   + [support diapositive 16]   + *Principal message : il y a 5 ateliers dans l’étude. L’étude doit être tenue à jour* * Faire un exercice collégial : pour chaque cas présenté, indiquez s’il peut engendrer une mise à jour   + [diapositive 17] * Corriger l'exercice   + [diapositive 18] |
| 1. Principe du socle vs. risques | Faire prendre conscience de la nécessité d’appliquer les mesures de base avant d’étudier les risques | * Présenter la notion de socle vs. scénarios de risques intentionnels   + [diapositive 19 et 20]   + *Principal message : d'abord l'hygiène et la règlementation, ensuite l’étude des risques* * Faire un exercice collégial : Pour chaque menace listée, indiquez si elle concerne le socle ou l’étude des risques   + [diapositive 21] * Corriger l'exercice   + [diapositive 22] |
| 1. Principe d’efficacité vs. exhaustivité | Faire accepter de privilégier l’efficacité à l’exhaustivité | * Présenter la notion de filtres successifs, de choix effectués à chaque atelier (efficacité vs. exhaustivité)   + [diapositive 23]   + *Principal message : (en plus du socle de sécurité) étudier les risques les plus importants permet d'arriver rapidement à des résultats concrets et contribue à traiter les autres risques* |
| Atelier 1 (jour 1 matin) | Faire comprendre comment réunir les éléments nécessaires pour comprendre le contexte particulier du sujet de l'étude et pouvoir adapter la gestion des risques en conséquence   * + [diapositive 24] | |
| * 1. Les tâches de l'atelier 1 | Présenter l’objectif de l’atelier, les participants et les éléments utiles à sa conduite | * Présenter les principales questions, actions à mener, éléments en sortie, et références utilisables (guide, fiches, *etc*.)   + [diapositive 25]   + *Principal message : pour mener cet atelier, il faut que la direction et les métiers soient impliqués avec le RSSI et le DSI. Les éléments existants (mesures de sécurité en place, analyses de risques précédentes,…) doivent être repris : on ne part pas d’une feuille blanche* |
| * 1. Valeurs métier et biens supports | Expliquer comment déterminer les éléments nécessaires à la description du périmètre | * Présenter les questions à se poser pour définir le périmètre   + [diapositive 26]   + *Principal message : définir et s’accorder sur le périmètre est une étape indispensable de l’étude des risques (si le périmètre n’est pas clairement défini, l’étude partira dans tous les sens)* * Faire un exercice en petits groupes : au vu du cas présenté, déterminez les valeurs métier et biens supports   + [diapositive 27] * Corriger l'exercice   + [diapositive 28] * Expliquer qu’il faut limiter le nombre de valeurs métier et de biens supports   + [diapositive 29] |
| * 1. Événements redoutés (ER), impacts et gravité | Expliquer comment déterminer les événements redoutés | * Présenter les événements redoutés, types et exemples d’impacts et exemple d’échelle de gravité   + [diapositives 30 à 33]   + *Principal message : un événement redouté associe une valeur métier et un critère de sécurité. Il peut engendrer différents impacts. C’est au métier d’identifier les impacts potentiels et d’estimer le niveau de gravité* * Faire un exercice en petits groupes : au vu du cas étudié, des types d’impacts et de l’échelle présentés, déterminez les principaux événements redoutés (que craint-on le plus ?), imaginez les principaux impacts (quelles seraient les conséquences potentielles ? Vous pouvez vous aider des bases de connaissances d’impacts) et estimez leur gravité   + [diapositive 34] * Corriger l’exercice   + [diapositive 35] |
| * 1. Socle de sécurité | Expliquer comment identifier le socle de sécurité | * Présenter le concept de socle et son usage   + [diapositive 36]   + *Principal message : dans le cadre d’EBIOS Risk Manager, on considère comme faisant partie du socle* ***uniquement*** *les référentiels formulant des exigences (actions directement applicables) en matière de sécurité* * Faire un exercice collégial : au vu du cas étudié, pour chaque élément fourni (PSSI, RGPD, *etc*.), indiquer s’il fait partie du socle ou non   + [diapositive 37] * Corriger l’exercice   + [diapositive 38] * Expliquer les tactiques possibles si le socle n’est pas (bien) appliqué   + [diapositive 39]   + *Principal message :* ce n’est pas mécanique, à chacun de décider |
| * 1. Mesures issues de l'atelier | Préciser que le plan d'action peut être alimenté par cet atelier | * Expliquer qu’on peut d’ores-et-déjà alimenter le plan d’action en présentant les éléments de l’atelier 1 qui sont susceptibles de générer des mesures au plan d’action   + [diapositive 40] * Faire un exercice collégial : au vu du cas étudié, quelles mesures pourrait-on préconiser à l’issue de cet atelier ?   + [commencer une liste de mesures sur un *paper board* à partir des réponses jugées comme valables (la liste servira de fil rouge)] |
| Atelier 2 (jour 1 après-midi) | Faire comprendre comment identifier et analyser l'origine des risques : les couples SR/OV   * + [diapositive 42] | |
| 1. Les tâches de l'atelier 2 | Présenter l’objectif de l’atelier, les participants et les éléments utiles à sa conduite | * Présenter les principales questions, actions à mener, éléments en sortie, et références utilisables (guide, fiches, *etc*.)   + [diapositive 43]   + *Principal message : à partir de cet atelier on prend le point de vue de l’attaquant pour challenger le socle de sécurité : on commence donc par identifier quels sont les attaquants qui peuvent nous cibler et leurs objectifs. On ne cherche pas l’exhaustivité des couples SR/OV, on sélectionne certains pour une première itération et les autres seront traités à l’itération suivante* |
| 1. Couples sources de risques (SR) / objectifs visés (OV) | Expliquer comment déterminer et estimer les couples SR/OV | * Expliquer comment identifier les couples SR/OV   + [diapositive 44]   + *Principal message : dans le cadre de mon étude, qui peut m’attaquer ? pour quelles raisons/finalités ?* * Expliquer comment estimer la pertinence des couples SR/OV (pour ne retenir que les plus pertinents)   + [diapositive 45] * Faire un exercice en petits groupes : au vu du cas présenté, identifiez les principaux couples sources de risques / objectifs visés, et estimer leur pertinence   + [diapositive 46]   + *Principal message : pour ne retenir que les plus pertinents, on peut estimer leur pertinence, par exemple selon leurs ressources et motivation* * Corriger l’exercice   + [diapositive 47] * Expliquer le lien entre les couples SR/OV et les ER   + [diapositive 48] |
| 1. Mesures issues de l'atelier | Préciser que le plan d'action peut être alimenté par cet atelier | * Expliquer qu’on peut d’ores-et-déjà alimenter le plan d’action en présentant les éléments de l’atelier 2 qui sont susceptibles de générer des mesures au plan d’action   + [diapositive 49] * Faire un exercice collégial : au vu du cas étudié, quelles mesures pourrait-on préconiser à l’issue de cet atelier ?   + [poursuivre la liste de mesures sur le *paper board* à partir des réponses jugées comme valables] |
| Atelier 3 (jour 1 après-midi) | Expliquer comment élaborer les scénarios stratégiques   * + [diapositive 51] | |
| * 1. Les tâches de l'atelier 3 | Présenter l’objectif de l’atelier, les participants et les éléments utiles à sa conduite | * Présenter les principales questions, actions à mener, éléments en sortie, et références utilisables (guide, fiches, *etc*.)   + [diapositives 52 et 53]   + *Principal message : prendre en compte son écosystème, regarder au-delà de son SI (environnement, exposition, parties prenantes).* |
| * 1. Parties prenantes : identification | Expliquer comment identifier les parties prenantes | * Présenter le concept d’écosystème et de parties prenantes, expliquer comment les identifier   + [diapositive 54]   + *Principal message : le RSSI ne peut pas réaliser cette activité seul, il faut qu’il sollicite les différentes personnes de l’entreprise pour qu’il obtienne une vision d’ensemble de l’écosystème* |
| * 1. Parties prenantes : évaluation | Expliquer comment étudier les parties prenantes et sélectionner les plus critiques | * Expliquer qu’il convient de s’interroger sur différents critères pour évaluer la dangerosité des parties prenantes et déterminer celles qui sont critiques * Présenter les exemples d’échelle, d’estimations et de représentations visuelles   + [diapositives 55 à 59]   + *Principal message : on ne cherche pas une évaluation absolue mais une position relative des parties prenantes les unes par rapport aux autres afin de sélectionner les plus critiques pour la suite de l’étude. On cherche un consensus entre les participants de l’atelier. Les critères (dépendance, pénétration, maturité cyber et confiance) et échelles proposés poussent à se poser des questions.*   + [discussion collégiale] |
| * 1. Scénarios stratégiques | Expliquer comment créer des scénarios stratégiques | * Présenter les concepts de scénario stratégique et de chemin d’attaque et le lien avec la gravité   + [diapositive 60]   + *Principal message : les scénarios stratégiques sont des scénarios de haut niveau, compréhensibles par tous, prenant en compte l’écosystème.* * Faire un exercice collégial : au vu du cas étudié, identifiez et représentez les chemins d’attaques possibles pour un couple SR/OV   + [diapositive 61] * Corriger l’exercice   + [diapositive 62] |
| * 1. Mesures issues de l'atelier | Préciser que le plan d'action peut être alimenté par cet atelier | * Expliquer qu’on peut d’ores-et-déjà alimenter le plan d’action en présentant les éléments de l’atelier 3 qui sont susceptibles de générer des mesures au plan d’action   + [diapositive 63] * Faire un exercice en petits groupes : au vu du cas étudié, quelles mesures pourrait-on préconiser à l’issue de cet atelier ?   + [poursuivre la liste de mesures sur le *paper board* à partir des réponses jugées comme valables] |
| Atelier 4 (jour 1 après-midi) | Expliquer comment élaborer les scénarios opérationnels   * + [diapositive 65] | |
| 1. Les tâches de l'atelier 4 | Présenter l’objectif de l’atelier, les participants et les éléments utiles à sa conduite | * Présenter les principales questions, actions à mener, éléments en sortie, et références utilisables (guide, fiches, *etc*.)   + [diapositives 66 et 67]   + *Principal message : dans cet atelier, on rassemble les compétences « techniques » (RSSI, DSI, architectes, etc.)* |
| 1. Scénarios opérationnels | Expliquer comment créer des scénarios opérationnels | * Présenter les concepts liés aux scénarios opérationnels (séquence d’attaque type, graphe d’attaque)   + [diapositive 68]   + *Principal message : pour construire les scénarios opérationnels on se base sur une séquence d’attaques modulaires* * Faire un exercice en petits groupes : au vu du cas présenté, imaginez un ou plusieurs scénarios opérationnels permettant de mettre en œuvre l’un des chemins d’attaques d’un scénario stratégique   + [diapositive 69] * Corriger l’exercice   + [diapositive 70] * Présenter la manière d’estimer la vraisemblance   + [diapositives 71 et 72]   + *Principal message : pour estimer la vraisemblance, on peut dans un premier temps estimer la vraisemblance globale du graphe d’attaque puis affiner avec le contenu de chaque action élémentaire au regard des mesures de sécurité en place* |
| 1. Mesures issues de l'atelier | Préciser que le plan d'action peut être alimenté par cet atelier | * Expliquer qu’on peut d’ores-et-déjà alimenter le plan d’action en présentant les éléments de l’atelier 3 qui sont susceptibles de générer des mesures au plan d’action   + [diapositive 73] * Faire un exercice en petits groupes : au vu du cas étudié, quelles mesures pourrait-on préconiser à l’issue de cet atelier ?   + [poursuivre la liste de mesures sur le *paper board* à partir des réponses jugées comme valables] |
| Atelier 5 (jour 1 après-midi) | Expliquer comment choisir les traitements appropriés des risques, les planifier et suivre leur mise en œuvre   * + [diapositive 75] | |
| * 1. Les tâches de l'atelier 5 | Présenter l’objectif de l’atelier, les participants et les éléments utiles à sa conduite | * Présenter les principales questions, actions à mener, éléments en sortie, et références utilisables (guide, fiches, *etc*.)   + [diapositives 76 et 77]   + *Principal message : l’objectif est ici de réaliser une synthèse des risques et de les traiter* |
| * 1. Mesures pour traiter les risques | Expliquer comment déterminer des mesures de sécurité applicables à l’objet de l’étude, argumenter les choix de traitement | * Présenter une manière de représenter les risques   + [diapositive 78]   *Principal message : présenter les résultats de l’étude de manière visuelle aide à les évaluer et à décider de la stratégie de traitement*   * Indiquer qu’il existe plusieurs options de traitement   + [diapositive 79] * Montrer comment présenter un plan d’action   + [diapositive 80] * Faire un exercice collégial : priorisez les mesures identifiées dans les ateliers précédents et justifiez   + [diapositive 81]   + [utiliser la liste de mesures notées sur le *paper board*] |
| * 1. Suivi des risques | Expliquer comment définir des outils de suivi | * Présenter la notion de risque résiduel et différentes manières de suivre ces risques dans le temps   + [diapositives 82 et 83]   + *Principal message : les risques résiduels doivent être acceptés formellement par la direction. Le suivi des risques doit être réalisé au travers du suivi du plan d’action et des incidents grâce à un tableau de bord* |
| Synthèse (jour 1 après-midi) | Rappeler les éléments constitutifs de la méthode et y mettre de l'ordre   * + [diapositive 84] | |
| * 1. Rappel de la démarche complète et du vocabulaire | Rappeler les éléments constitutifs de la méthode et y mettre de l'ordre | * Faire un exercice collégial : identifiez ou imaginez les composants du risque depuis le contenu de l’article   + [diapositive 85] * Corriger l’exercice   + [diapositive 86] |
| Étude de cas (jour 2) | S’assurer de la bonne appropriation de la logique globale   * + [diapositive 87] | |
| 1. Ancrage des concepts | S’assurer de la bonne compréhension des concepts | * Faire un exercice collégial : identifiez ou imaginez les composants du risque depuis le contenu de l’article   + [diapositive 88] * Corriger l’exercice   + [diapositive 89] |
| 1. Étude de cas | Faire appliquer les connaissances du début de la formation et s’assurer que les apprenants sont capables de gérer rapidement un cas spécifique en créant un consensus au sein d’un groupe | * Présenter le cas d’étude   + [diapositive 90] * Créer des petits groupes, si possible en mélangeant les profils (notamment techniques et non techniques) * Débuter l’étude de cas en petits groupes : au vu des éléments présentés, identifiez les principales valeurs métier, leurs supports et leurs responsables   + [diapositive 91] * Corriger l’exercice   + [diapositive 92] * Poursuivre l’étude de cas en petits groupes : décrivez les principaux événements redoutés et leurs impacts en vous aidant des exemples présentés, et estimez-les en termes de gravité en utilisant l’échelle présentée   + [diapositives 93 à 96] * Corriger l’exercice   + [diapositive 97] * Poursuivre l’étude de cas en petits groupes : identifiez et estimez les couples SR/OV en utilisant la matrice présentée   + [diapositives 98 et 99] * Corriger l’exercice   + [diapositive 100] * Poursuivre l’étude de cas en petits groupes : établissez le lien entre les ER et les couples SR/OV   + [diapositive 101] * Corriger l’exercice   + [diapositive 102] * Présenter la technique proposée pour estimer la dangerosité des parties prenantes   + [diapositives 103 et 104] * Poursuivre l’étude de cas en petits groupes : estimez la dangerosité (niveau de menace) des parties prenantes, en utilisant la technique proposée   + [diapositives 105 et 106] * Corriger l’exercice   + [diapositives 107 et 108] * Poursuivre l’étude de cas en petits groupes : élaborez des scénarios stratégiques   + [diapositive 109] * Corriger l’exercice   + [diapositive 110] * Poursuivre l’étude de cas en petits groupes : élaborez des scénarios opérationnels   + [diapositive 111] * Corriger l’exercice   + [diapositive 112] * Présenter l’échelle de vraisemblance proposée * Poursuivre l’étude de cas collégialement : positionnez vos risques dans la cartographie des risques   + [diapositive 114]   + [*paper board*] * Poursuivre l’étude de cas collégialement : déterminez les mesures de sécurité les plus utiles pour traiter les risques et faites-en un plan d’action   + [diapositive 115]   + [*paper board*] |
| Conclusion (fin du jour 2) | Terminer la formation   * + [diapositive 116] | |
| 1. Conclusion |  | * Rappeler le contenu de la formation * Conclure   + *Principal message : c’est la pratique de la méthode dans son propre contexte qui permettra d’intégrer complètement les éléments étudiés pendant la formation* * Faire remplir les évaluations   + [fiches d’évaluation] * Remercier les participants |