EBIOS RM : ateliers 3 à 5, scénarios et risque résiduel ANSSI

> EBIOS RM ateliers 3 à 5 : scénarios stratégiques, opérationnels, PdT et risque résiduel ANSSI. Exemple concret pour une collectivité territoriale en 2026.

La méthode EBIOS Risk Manager (EBIOS RM) publiée par l'ANSSI constitue le cadre de référence français pour l'analyse de risques cyber. Si les ateliers 1 et 2 posent les bases en identifiant les valeurs métier, les biens supports et les sources de risque, c'est dans les ateliers 3, 4 et 5 que la méthode prend toute sa puissance opérationnelle. L'atelier 3 construit les scénarios stratégiques en cartographiant les chemins d'attaque possibles depuis les sources de risque jusqu'aux événements redoutés. L'atelier 4 décline ces scénarios en séquences techniques précises, ancrées dans la réalité du système d'information. L'atelier 5, enfin, est le coeur décisionnel : il détermine quelles mesures de sécurité mettre en oeuvre, quels risques traiter en priorité, et quels risques résiduels sont acceptés par le management. Ce guide détaille la conduite pratique de ces trois ateliers, illustrés par un exemple complet pour une collectivité territoriale, et couvre l'articulation avec ISO 27001 et la qualification ANSSI. Que vous soyez RSSI, auditeur ou chef de projet sécurité, ce guide vous accompagne pas à pas dans la conduite opérationnelle des ateliers EBIOS RM les plus complexes.

À RETENIR

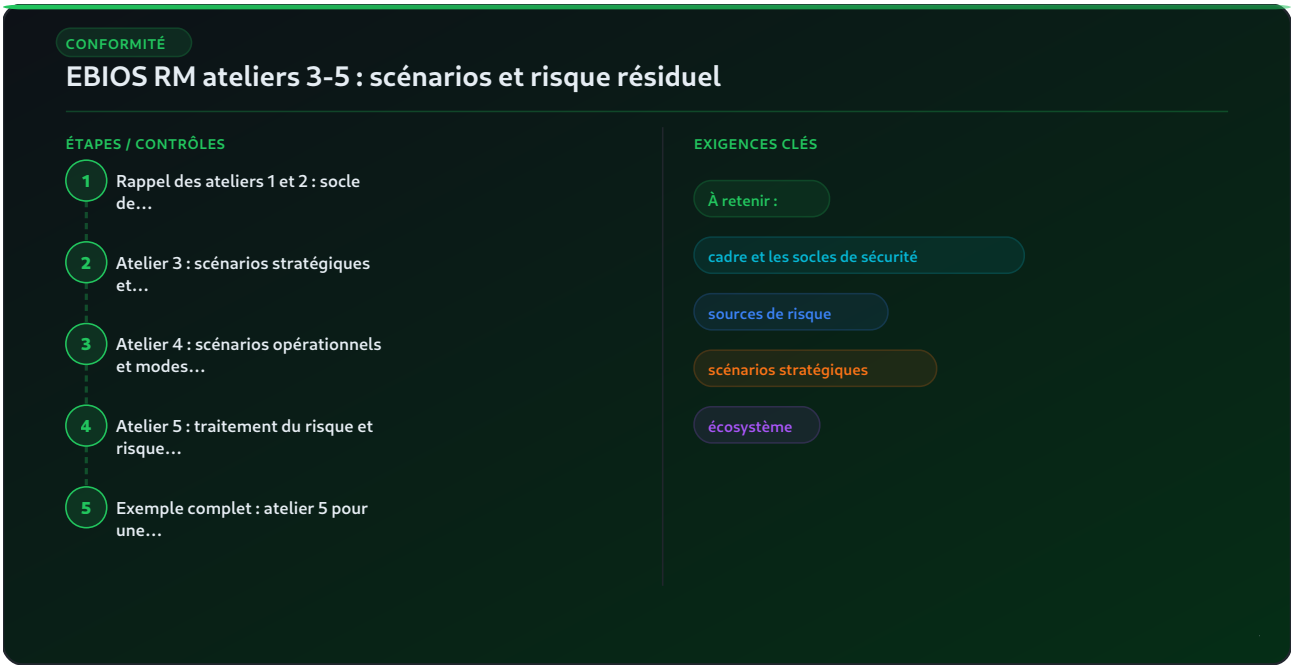
À retenir :

L'atelier 3 produit une matrice menaces/valeurs et des chemins d'attaque stratégiques permettant de prioriser les scénarios les plus vraisemblables et les plus graves.

L'atelier 4 décrit des séquences techniques précises (modes opératoires) qui ancrent les scénarios stratégiques dans la réalité technique du SI à protéger.

L'atelier 5 produit le Plan de Traitement du Risque (PdT) avec des mesures de sécurité priorisées et le niveau de risque résiduel accepté par la direction.

> L'outil EBIOS RM Tool de l'ANSSI (gratuit) facilite la conduite collaborative des cinq ateliers et génère automatiquement les livrables attendus.



Rappel des ateliers 1 et 2 : socle de l'analyse de risques

Avant d'aborder les ateliers 3 à 5, un rappel rapide des deux premiers ateliers est nécessaire pour comprendre les entrées disponibles. L'atelier 1 définit le **cadre et les socles de sécurité** : périmètre d'étude, valeurs métier (VM), biens supports (BS), événements redoutés (ER) avec leurs niveaux de gravité (1-4), et les socles de sécurité applicables (RGS, PGSSI-S, NIS 2). L'atelier 2 identifie les **sources de risque** (SR) : qui sont les attaquants potentiels (cybercriminels, États, initiaux malveillants, hacktivistes) et quelles sont leurs motivations et capacités ? Il établit les couples SR/Objectifs Visés (OV) pertinents, c'est-à-dire les associations "qui veut faire quoi à quelle VM".

Ces entrées alimentent directement l'atelier 3. Plus les ateliers 1 et 2 sont précis et exhaustifs, plus les scénarios stratégiques de l'atelier 3 seront réalistes et exploitables. La méthode complète est décrite dans le guide ANSSI disponible sur cyber.gouv.fr.

Atelier 3 : scénarios stratégiques et cartographie des menaces

L'atelier 3 est le pivot de la méthode EBIOS RM. Son objectif est de construire des **scénarios stratégiques** décrivant comment une source de risque peut atteindre ses objectifs visés en exploitant les biens supports identifiés. Chaque scénario stratégique possède un niveau de vraisemblance (1-4) basé sur les capacités de la SR et les vulnérabilités des biens supports.

> ⚡ **Retour terrain**
>
> Dans mes missions de conformité, j'observe que les entreprises sous-estiment systématiquement le délai de mise en œuvre des mesures techniques. Les mesures organisationnelles (politiques, procédures) s'écrivent en semaines ; les mesures techniques (segmentation réseau, chiffrement, MFA) se déploient en mois. Pour un plan de mise en conformité réaliste, je multiplie toujours les estimations initiales des équipes IT par 2,5 — et je n'ai jamais eu à réduire ce coefficient.

Chemins d'attaque et écosystème

Un élément distinctif d'EBIOS RM par rapport aux méthodes précédentes (MEHARI, EBIOS 2010) est la prise en compte de l'**écosystème** : partenaires, prestataires, clients, fournisseurs cloud. L'atelier 3 analyse les chemins d'attaque transitant par cet écosystème, ce qui est particulier un essentiel depuis les attaques supply chain (SolarWinds, Kaseya, 3CX).

Un chemin d'attaque se représente sous la forme d'un graphe orienté : SR → partie prenante de l'écosystème → bien support interne → valeur métier. Par exemple : groupe APT → prestataire de maintenance informatique → accès VPN des techniciens → système de gestion RH → fichier des salariés.

Matrice menaces/valeurs métier

La matrice menaces/valeurs est le livrable central de l'atelier 3. Elle croise les événements redoutés (ER) avec les scénarios stratégiques (SS) pour visualiser les risques bruts avant traitement. Pour chaque cellule de la matrice, on note la gravité (issue de l'atelier 1) et la vraisemblance (calculée en atelier 3), ce qui permet de positionner chaque risque dans une carte de chaleur.

```
 MATRICE RISQUES BRUTS - Atelier 3
=========================================================
                    | ER1: Fuite RH | ER2: Chiffr SI | ER3: Surf Portail
--------------------|---------------|----------------|-----------------
SS1: APT+prestataire| G=4 / V=2     | G=4 / V=2      | G=3 / V=1
SS2: Cybercriminel  | G=3 / V=3     | G=4 / V=4      | G=2 / V=3
SS3: Initie malin   | G=4 / V=2     | G=3 / V=1      | G=2 / V=2
=========================================================
(G=Gravite 1-4, V=Vraisemblance 1-4)
```

Niveau de risque et priorisation

EBIOS RM ne prédefinit pas de formule de calcul rigide : le niveau de risque résulte d'un jugement expert sur la combinaison gravité/vraisemblance. La pratique courante utilise une matrice 4x4 avec des seuils de traitement : risques en zone rouge (G=4+V=3 ou G=3+V=4) à traiter immédiatement, zone orange à planifier, zone verte acceptable.

Atelier 4 : scénarios opérationnels et modes opératoires

L'atelier 4 traduit les scénarios stratégiques en **scénarios opérationnels** détaillant les techniques d'attaque concrètes. C'est l'atelier qui nécessite la plus grande expertise technique : les participants doivent connaître les modes opératoires des attaquants (chaînes d'exploitation, outils, TTPs MITRE ATT&CK) et les dépendances techniques du SI.

Séquences techniques et dépendances SI

Chaque scénario opérationnel décrit une séquence d'actions techniques de la source de risque. EBIOS RM recommande de s'appuyer sur le framework MITRE ATT&CK pour décrire les tactiques (TA) et techniques (T) utilisées. Cette correspondance EBIOS RM / MITRE facilite le lien avec les capacités de détection du SOC.

```
 SCENARIO OPERATIONNEL SO1 - Ransomware via prestataire
=======================================================
SS de reference: SS2 (Cybercriminel+Ransomware)
ER vise: ER2 (Chiffrement du SI)

Sequence technique:
1. [TA0001-Initial Access] Spear-phishing ciblant technicien prestataire
   Technique: T1566.001 (Spearphishing Attachment)
2. [TA0002-Execution] Macro Office -> PowerShell dropper
   Technique: T1059.001 (PowerShell)
3. [TA0003-Persistence] Cle Run registre
   Technique: T1547.001
4. [TA0005-Defense Evasion] Desactivation Windows Defender
   Technique: T1562.001
5. [TA0008-Lateral Movement] Pass-the-Hash via NTLM
   Technique: T1550.002
6. [TA0040-Impact] Chiffrement LockBit 3.0
   Technique: T1486

Biens supports impactes: BS3 (VPN prestataire), BS7 (AD), BS12 (Serveurs fichiers)
Vraisemblance: 4/4 (TTPs connus, lacunes SSI avere)
```

Dépendances et propagation

L'atelier 4 doit explicitement modéliser les dépendances entre biens supports qui permettent la propagation d'une attaque. Ces dépendances sont souvent sous-estimées : un système de gestion des bons de commande peut sembler peu critique, mais s'il partage un segment réseau avec l'Active Directory, il devient un pivot potentiel pour un mouvement latéral vers le coeur du SI.

L'articulation avec notre guide de cartographie des risques cyber EBIOS RM est ici fondamentale : une cartographie précise des flux et des dépendances SI est le prérequis indispensable à un atelier 4 de qualité.

Atelier 5 : traitement du risque et risque résiduel

L'atelier 5 est le coeur décisionnel d'EBIOS RM. Il détermine pour chaque scénario opérationnel les **mesures de sécurité** à mettre en oeuvre, construit le **Plan de Traitement du Risque** (PdT) et formalise les **risques résiduels** acceptés par la direction. Cet atelier est conduit avec la direction générale et les métiers car il implique des décisions d'investissement et d'acceptation de risque à fort enjeu organisationnel.

Options de traitement du risque

Pour chaque scénario, quatre options de traitement sont possibles : **réduction** (mise en oeuvre de mesures de sécurité pour diminuer la vraisemblance ou la gravité), **transfert** (assurance cyber, externalisation), **évitement** (abandon de l'activité à risque), **acceptation** (le risque résiduel est jugé tolérable). L'option la plus fréquente est la réduction par des mesures techniques et organisationnelles.

Mesures de sécurité et priorisation

Les mesures de sécurité identifiées en atelier 5 sont classées selon leur efficacité sur chaque scénario (réduction de vraisemblance, réduction de gravité ou les deux) et leur coût de mise en oeuvre. On utilise typiquement une matrice impact/effort pour prioriser le PdT. Les mesures à fort impact et faible effort (quick wins) sont planóes en premier.

```
 PLAN DE TRAITEMENT DU RISQUE - Atelier 5 (extrait)
=====================================================
Mesure | Scenario | Impact | Cout | Priorite | Pilote | Echeance
-------|----------|--------|------|----------|--------|--------
MFA sur VPN prestataires | SO1 | -V:3->1 | Moyen | P1 | DSI | T+3m
Segmentation reseau OT/IT | SO1,SO3 | -V:4->2 | Eleve | P2 | DSI | T+9m
Sauvegardes offline 3-2-1 | SO1,SO2 | -G:4->2 | Moyen | P1 | DSI | T+2m
Forma. phishing prestataires| SO1 | -V:3->2 | Faible | P1 | RH | T+1m
EDR sur postes nomades | SO1,SO2 | -V:3->2 | Moyen | P2 | DSI | T+6m
=====================================================
```

Calcul du risque résiduel

Après application des mesures de sécurité planifiées, le risque résiduel est recalculé pour chaque scénario. Ce risque résiduel est présenté à la direction pour acceptation formelle. La **fiche de risque résiduel** constitue un livrable clé de l'homologation ANSSI et de la certification ISO 27001. Elle documente : le scénario résiduel, le niveau de risque résiduel (G x V), les mesures de traitement appliquées, et la décision d'acceptation signée par l'autorité compétente.

Exemple complet : atelier 5 pour une collectivité territoriale

Illustrons la conduite d'un atelier 5 pour une commune de 50 000 habitants. Le périmètre couvre le SI administratif, l'état civil, la gestion RH et le portail citoyen. Les ateliers 1-4 ont identifié 6 scénarios opérationnels prioritaires, dont SO1 (ransomware via prestataire) et SO4 (défacement du portail citoyen par hacktivistes).

Déroulement de l'atelier 5 de la collectivité

L'atelier 5 réunit le DSI, la DGA (Directrice Générale Adjointe), le DPO, et la responsable RH. La facilitation est assurée par le prestataire RSSI externalisé. La séance de travail dure 3 heures, précédée d'une préparation de 2 jours par le facilitateur.

Pour SO1 (ransomware, G=4, V=4, risque CRITIQUE), les mesures décidées sont : MFA sur tous les accès VPN (T+3 mois, budget 8 000€), sauvegardes offline testées mensuellement (T+2 mois, budget 5 000€), PCA/PRA formalisé pour les services essentiels (état civil, paie) (T+6 mois, budget 15 000€), et formation phishing annuelle de tout le personnel (T+1 mois, budget 3 000€). Risque résiduel après traitement : G=4 / V=2 → risque IMPORTANT mais accepté sous conditions (suivi trimestriel obligatoire).

Ce type d'approche s'inscrit parfaitement dans la démarche d'homologation ANSSI et facilite la mise en conformité NIS 2 pour les collectivités concernées.

Articulation EBIOS RM avec ISO 27001 et la qualification ANSSI

EBIOS RM et ISO 27001 sont complémentaires et non concurrents. L'ISO 27001:2022 exige une analyse de risques formelle (clause 6.1.2) sans prescrire de méthode spécifique. EBIOS RM répond à cette exigence de manière exemplaire, et ses livrables (tableau de risques, PdT, fiches risques résiduels) correspondent directement aux exigences documentaires de l'annexe A de l'ISO 27001:2022.

Mapping EBIOS RM / ISO 27001:2022

L'atelier 1 EBIOS RM (contexte, valeurs métier) correspond aux clauses 4 (contexte), 5.4 (responsabilités) et 8.1 (planification) de l'ISO 27001. L'atelier 5 (traitement, PdT) correspond directement à la clause 8.3 (traitement des risques) et aux contrôles de l'annexe A. Pour la qualification ANSSI (PASSI, SecNumCloud), les livrables EBIOS RM constituent les pièces justificatives attendues par les auditeurs lors de l'instruction du dossier.

Qualification ANSSI et dossier d'homologation

Dans le cadre d'une homologation ANSSI (OIV, OSE, systèmes qualifiés), le dossier de sécurité doit inclure l'analyse de risques EBIOS RM avec au minimum les ateliers 1, 2 et 5 complets. Les ateliers 3 et 4 sont fortement recommandés pour les systèmes à enjeux élevés. La communauté

des praticiens EBIOS RM se retrouve sur club-ebios.org pour échanger bonnes pratiques et retours d'expérience.

Livrables attendus des ateliers 3 à 5

La conduite rigoureuse des ateliers 3 à 5 produit un ensemble de livrables formalisés qui constituent le coeur du dossier d'analyse de risques. Ces livrables doivent être maintenus à jour lors de chaque révision annuelle de l'analyse (exigée par ISO 27001 clause 8.2 et préconisée par l'ANSSI).

Tableau des risques (atelier 3 et 4)

Le tableau des risques synthétise tous les scénarios identifiés avec leur gravité, vraisemblance, niveau de risque brut, biens supports impactés et événements redoutés associés. Il est la référence centrale pour l'atelier 5. Format recommandé : tableur partagé avec versionnage, ou directement dans l'EBIOS RM Tool ANSSI.

Plan de Traitement du Risque (atelier 5)

Le PdT liste toutes les mesures de sécurité décidées avec leur coût, leur pilote, leur échéance, l'impact attendu sur le risque et le statut de mise en oeuvre. Il est renseigné et suivi trimestriellement par le RSSI. Son format doit permettre son intégration dans le Plan Directeur de Sécurité (PDS) global de l'organisation.

Fiches de risques résiduels

Chaque risque non réduit à un niveau acceptable fait l'objet d'une fiche de risque résiduel signée par l'autorité d'homologation ou la direction générale. Cette fiche documente : la définition du risque résiduel, les justifications de son acceptation, les conditions de surveillance, et la date de

révision. Elle engage formellement la direction sur sa responsabilité en cas de réalisation du risque.

Outils : EBIOS RM Tool ANSSI et méthode collaborative

L'ANSSI met à disposition gratuitement l'**EBIOS RM Tool**, une application web open-source qui guide la conduite des cinq ateliers et génère automatiquement les livrables. L'outil permet l'export des tableaux de risques en PDF et XLSX, la gestion des versions de l'étude, et le travail collaboratif en équipe.

```
 # Installation EBIOS RM Tool (Docker)
git clone https://github.com/nickvdyck/weasyprint
# Voir https://github.com/nickvdyck/ebios-rm pour l'outil officiel

# Alternative : utilisation directe en ligne
# https://ebios-rm.cyber.gouv.fr (outil ANSSI en ligne)
```

Pour les organisations souhaitant s'appuyer sur un accompagnement expert pour conduire une analyse EBIOS RM, consulter notre offre de cartographie des risques cyber et notre article sur la phase opérationnelle NIS 2 en 2026.

FAQ — Questions fréquentes sur les ateliers 3 à 5 EBIOS RM

Combien d'ateliers sont nécessaires pour une homologation ANSSI minimale ?

Pour une homologation ANSSI dans le cadre réglementaire (OIV, OSE), la méthode EBIOS RM exige un minimum de trois ateliers obligatoires : l'atelier 1 (cadre et socles), l'atelier 2 (sources de risque) et l'atelier 5 (traitement). Les ateliers 3 et 4 sont fortement recommandés pour les systèmes à enjeux critiques ou lorsque des scénarios complexes multi-étapes sont plausibles. En pratique, une homologation solide qui résistera à l'examen des auditeurs ANSSI comporte

presque toujours les cinq ateliers. L'absence des ateliers 3 et 4 peut conduire à des mesures de traitement sous-optimales, d'où une homologation provisoire plutôt que définitive.

Quelle est la différence entre scénario stratégique et scénario opérationnel ?

Le scénario stratégique (atelier 3) décrit le "quoi" et le "qui" à un niveau abstrait : une source de risque cherche à atteindre un objectif visé en exploitant un chemin d'attaque passant par l'écosystème et les biens supports. Il n'entre pas dans les détails techniques. Le scénario opérationnel (atelier 4) décline le "comment" avec précision : quelles techniques ATT&CK sont utilisées, dans quel ordre, quels biens supports sont traversés. Un scénario stratégique peut générer plusieurs scénarios opérationnels correspondant à différents modes opératoires pour atteindre le même objectif.

Comment éviter le piège de l'analyse de risques "vitrine" dans l'atelier 5 ?

L'écueil principal de l'atelier 5 est de produire un PdT irréaliste (trop de mesures, budgets insuffisants, échéances intenables) ou de systématiquement accepter les risques élevés faute de budget. Pour éviter ces pièges, l'atelier 5 doit impérativement être conduit avec la direction générale disposant d'un mandat décisionnel réel. Les mesures du PdT doivent être SMART (Spécifiques, Mesurables, Atteignables, Réalistes, Temporelles) et faire l'objet d'un portage budgétaire dédié. Un suivi trimestriel de l'avancement du PdT, rapporté en Comité de direction, est la garantie que l'analyse de risques ne reste pas un exercice théorique.

Pour aller plus loin : Mise en œuvre pratique

La conformité réglementaire nécessite une approche structurée et documentée. Ces ressources complémentaires permettent d'approfondir les points techniques et juridiques abordés dans cet article.

Outils d'auto-évaluation

ANSSI — Outil d'évaluation cybersécurité — Le Diagnostic de Cybersécurité de l'ANSSI permet d'évaluer le niveau de maturité de votre organisation sur 5 domaines clés. Gratuit et disponible sur diagnostic.ssi.gouv.fr.

ENISA — Outil d'auto-évaluation NIS2 — Questionnaire structuré pour identifier les exigences applicables à votre secteur et votre taille d'organisation.

Logiciels GRC — Des solutions comme Vanta, Drata ou TrustCloud automatisent la collecte de preuves de conformité et accélèrent les processus d'audit.

Documentation à produire en priorité

Politique de Sécurité du Système d'Information (PSSI) — document fondateur

Registre des activités de traitement (RGPD, article 30)

Analyse d'impact relative à la protection des données (AIPD/DPIA)

Plan de continuité d'activité (PCA) et plan de reprise d'activité (PRA)

Procédure de gestion des incidents de sécurité (notification ANSSI/CNIL)

Accompagnement et conseil

La mise en conformité implique souvent une assistance externe pour les organisations ne disposant pas d'expertise interne. Les RSSI externalisés ou les consultants spécialisés en conformité peuvent accélérer significativement le processus, notamment pour la préparation aux audits de certification ISO 27001 ou pour la mise en conformité NIS 2 avec un délai contraint.

Synthèse et feuille de route conformité

La conformité réglementaire est un processus continu, non un projet ponctuel. Les organisations qui abordent ISO 27001, NIS 2, RGPD ou HDS comme des certifications à obtenir une fois pour

toutes échouent systématiquement lors des audits de renouvellement. La clé du succès est l'intégration des exigences réglementaires dans les processus opérationnels quotidiens, non leur traitement comme des obligations externes.

En pratique, les organisations matures en matière de conformité fonctionnent avec un SMSI vivant : des revues de direction trimestrielles, un audit interne annuel, des exercices de gestion de crise bi-annuels, et une veille réglementaire hebdomadaire. Le coût de la conformité maintenue en continu est significativement inférieur au coût d'une remise à niveau précipitée avant un audit ou une notification de violation. Les amendes CNIL, les pénalités NIS 2, et les pertes de contrats liées à une non-conformité documentée représentent des risques financiers et réputationnels mesurables que la gouvernance de direction doit intégrer dans l'analyse des risques métier. La valeur de la méthode EBIOS RM réside dans son approche itérative : les ateliers 3 à 5 ne sont pas un exercice ponctuel mais un processus vivant qui doit être révisé à chaque changement significatif du contexte ou des valeurs métier, garantissant que les scénarios de risque restent alignés avec la réalité opérationnelle de l'organisation.