AYI NEDJIMI Consultants

Cartographie des risques cyber avec EBIOS RM en 2026

Catégorie : Conformité Lecture : 9 min Publié le : 12/03/2026 Auteur : Ayi NEDJIMI

Découvrez la méthodologie EBIOS RM pour cartographier vos risques cyber. Guide pratique avec ateliers, exemples concrets et modèles adaptables.

Résumé exécutif

La cartographie des risques cyber constitue le socle fondamental de toute stratégie de cybersécurité mature et crédible auprès des parties prenantes internes et externes de l'organisation. La méthodologie EBIOS Risk Manager, développée et maintenue par l'ANSSI depuis 2018, propose un cadre structuré en cinq ateliers collaboratifs pour identifier exhaustivement, analyser méthodiquement et traiter efficacement les risques numériques pesant sur les activités critiques de votre organisation. Ce guide détaille chaque étape de la démarche de cartographie, depuis la définition du socle de sécurité et l'identification des sources de risque jusqu'à l'élaboration des scénarios stratégiques et opérationnels et la construction du plan de traitement, avec des exemples concrets issus de missions terrain, des modèles directement réutilisables et des retours d'expérience permettant d'éviter les écueils classiques rencontrés lors du déploiement de la méthodologie dans des organisations de toutes tailles et secteurs d'activité.

La gestion des risques cyber ne se résume plus à dresser une liste de vulnérabilités techniques ou à cocher des cases dans un tableur Excel vieillissant. Dans un contexte où les menaces évoluent à une vitesse sans précédent, où les **attaques par supply chain** se multiplient et où la réglementation européenne impose des exigences toujours plus strictes avec NIS 2 et DORA, les organisations doivent adopter une approche méthodique et reproductible pour cartographier leurs risques numériques de manière exhaustive et documentée. La méthodologie *EBIOS Risk Manager*, publiée par l'ANSSI en 2018 et régulièrement enrichie depuis, offre précisément ce cadre structuré qui permet de passer d'une vision purement technique de la sécurité à une analyse stratégique intégrant les scénarios d'attaque réalistes, les parties prenantes de l'écosystème et les objectifs métiers de l'organisation. Que vous soyez RSSI cherchant à rationaliser votre approche du risque, DPO devant alimenter vos analyses d'impact sur la protection des données, ou consultant GRC accompagnant vos clients dans leur mise en conformité réglementaire, la maîtrise complète d'EBIOS RM est devenue un prérequis incontournable en 2026 pour toute démarche de gouvernance des risques cyber sérieuse et crédible auprès des parties prenantes internes comme externes.

Pourquoi choisir EBIOS RM pour cartographier vos risques cyber ?

Parmi les méthodologies d'analyse de risques disponibles sur le marché, EBIOS RM se distingue par plusieurs caractéristiques fondamentales qui en font un choix particulièrement pertinent pour les organisations françaises et européennes soumises au cadre réglementaire continental. Contrairement à des approches purement quantitatives comme **FAIR** (Factor Analysis of Information Risk), EBIOS RM adopte une démarche qualitative et scénarisée qui facilite considérablement la communication avec les décideurs non techniques du COMEX et du conseil d'administration.

La méthode est conçue pour s'intégrer nativement dans un cadre de conformité NIS 2 et s'aligne naturellement avec les exigences de la norme ISO 27005 pour la gestion des risques liés à la sécurité de l'information. EBIOS RM se structure autour de cinq ateliers progressifs qui permettent de couvrir l'ensemble du spectre analytique, depuis la compréhension approfondie du contexte métier jusqu'à la définition précise des mesures de traitement et de leur suivi dans le temps.

Cette structuration en ateliers collaboratifs facilite la conduite de sessions impliquant les parties prenantes métiers, techniques et managériales, créant ainsi un langage commun autour du risque cyber. La méthodologie intègre également une dimension écosystémique unique qui permet de cartographier les risques liés aux tiers, un aspect devenu critique après les attaques de type SolarWinds et Kaseya qui ont démontré la vulnérabilité des chaînes d'approvisionnement numériques.

Avez-vous déjà tenté de présenter une matrice de risques de 200 lignes à votre COMEX sans obtenir des regards vitreux et une demande immédiate de synthèse en une seule page ?

Mon avis : Après avoir déployé EBIOS RM dans une douzaine d'organisations de tailles et secteurs variés, je constate que la méthode brille par sa capacité à structurer le dialogue entre les équipes techniques et la direction générale. Son principal défi reste la charge de travail nécessaire pour animer correctement les cinq ateliers, surtout dans les structures où la culture du risque est encore embryonnaire. Prévoyez systématiquement un sponsor fort au niveau direction et un facilitateur expérimenté pour les premières itérations.

Comment se déroulent les cinq ateliers EBIOS RM ?

Le premier atelier, **Cadrage et socle de sécurité**, pose les fondations de l'analyse en identifiant les missions critiques de l'organisation, les valeurs métier à protéger prioritairement, le périmètre exact de l'étude et les référentiels de sécurité applicables. On y définit le socle de sécurité, ensemble des mesures considérées comme acquises ou en cours de déploiement, qui sert de point de départ pour l'analyse des risques résiduels. Cet atelier consomme typiquement deux à trois journées de travail collaboratif.

Le deuxième atelier, **Sources de risque**, identifie les acteurs menaçants susceptibles de cibler l'organisation. On distingue les sources de risque telles que les groupes APT étatiques, les cybercriminels motivés par l'appât du gain, les hacktivistes idéologiques, les concurrents

pratiquant l'espionnage économique et les initiés malveillants ou négligents, puis on les associe à leurs objectifs visés spécifiques. Pour chaque couple source-objectif, on évalue la pertinence par rapport au contexte propre de l'organisation. Cette étape nécessite une connaissance fine du paysage des menaces, alimentée par des plateformes de threat intelligence.

Le troisième atelier, **Scénarios stratégiques**, cartographie l'écosystème complet de l'organisation et identifie les chemins d'attaque passant par les parties prenantes tierces. On modélise les risques liés à la supply chain, aux prestataires informatiques, aux partenaires commerciaux et aux sous-traitants. Le quatrième atelier, **Scénarios opérationnels**, détaille les modes opératoires techniques que pourraient employer les attaquants, depuis le vecteur d'intrusion initial (phishing ciblé, exploitation de vulnérabilité, compromission de la chaîne logicielle) jusqu'à l'impact sur les valeurs métier identifiées en atelier un.

Le cinquième atelier, **Traitement du risque**, synthétise l'ensemble des scénarios évalués, positionne les niveaux de risque sur une matrice de décision et définit la stratégie de traitement pour chaque risque identifié : réduction par des mesures techniques ou organisationnelles, transfert via une assurance cyber ou un contrat, évitement par l'abandon de l'activité risquée, ou acceptation documentée avec validation de la direction.

Quelles sont les étapes clés de préparation de la cartographie ?

La réalisation d'une cartographie des risques cyber avec EBIOS RM exige une préparation rigoureuse en amont des ateliers. Il faut constituer l'équipe projet pluridisciplinaire, collecter la documentation existante comprenant la PSSI, le schéma d'architecture technique, le registre des traitements RGPD, les rapports d'audit précédents et les incidents passés, et définir un planning réaliste des sessions de travail. La préparation consomme typiquement trente pour cent de l'effort total du projet mais conditionne la qualité des résultats obtenus.

Pendant la phase d'analyse proprement dite, chaque atelier produit des livrables spécifiques qui alimentent les ateliers suivants dans une logique d'entonnoir progressif. Il est absolument essentiel de maintenir la traçabilité bidirectionnelle entre tous les éléments pour garantir la cohérence globale de l'analyse et faciliter les mises à jour ultérieures. Les outils dédiés comme **MONARC** ou des solutions commerciales facilitent grandement cette gestion, mais un ensemble de tableurs bien structurés peut suffire pour une première itération. La phase de restitution traduit les résultats techniques en langage compréhensible par la direction, en lien avec la protection des données RGPD.

Atelier EBIOS RM	Objectif principal	Livrables produits	Durée indicative
1 - Cadrage et socle	Définir périmètre et socle de sécurité	Fiche de cadrage, socle de sécurité	2-3 jours
2 - Sources de risque	Identifier les menaces pertinentes	Liste des couples SR/OV retenus	1-2 jours
3 - Scénarios stratégiques	Cartographier l'écosystème et chemins	Graphes d'attaque stratégiques	2-3 jours
4 - Scénarios opérationnels	Détailler les modes opératoires	Scénarios techniques séquencés	2-3 jours
5 - Traitement du risque	Définir la stratégie de traitement	PACS et risques résiduels acceptés	1-2 jours

Lors de l'attaque SolarWinds découverte en décembre 2020, les organisations ayant réalisé une cartographie EBIOS RM intégrant l'écosystème fournisseurs dans leur atelier 3 avaient correctement identifié le risque de compromission de la supply chain logicielle comme un scénario stratégique prioritaire. Celles qui s'étaient limitées à une analyse périmétrique classique n'avaient tout simplement pas anticipé ce vecteur d'attaque indirect passant par un éditeur de confiance, ce qui a retardé leur détection et leur capacité de réponse de plusieurs semaines critiques.

Comment intégrer EBIOS RM dans votre SMSI ISO 27001 ?

L'intégration d'EBIOS RM dans un système de management de la sécurité de l'information existant repose sur l'alignement des processus d'analyse de risques avec les exigences de la clause 6.1 de l'ISO 27001. La méthodologie de l'ANSSI remplace ou complète avantageusement le processus d'appréciation des risques exigé par la norme internationale. Les résultats de l'atelier cinq, notamment le plan de traitement des risques et les mesures de sécurité retenues, alimentent directement la déclaration d'applicabilité et le plan de traitement des risques requis par le SMSI.

Pour maintenir la cartographie des risques vivante et pertinente dans la durée, il convient d'établir un cycle de révision annuel ou déclenché par des événements significatifs tels qu'un changement majeur d'architecture, un incident de sécurité important, l'entrée en vigueur d'une nouvelle réglementation, ou une opération de fusion-acquisition. Chaque révision ne nécessite pas de reprendre l'intégralité des cinq ateliers ; une mise à jour ciblée des éléments impactés suffit généralement à maintenir la pertinence de l'analyse. Les résultats actualisés doivent alimenter le SOC pour orienter la surveillance opérationnelle et adapter les règles de détection aux scénarios de risque identifiés.

Quels outils utiliser pour conduire EBIOS RM en pratique ?

Plusieurs outils facilitent la mise en œuvre opérationnelle d'EBIOS RM au quotidien. **MONARC**, développé par le CASES Luxembourg sous licence open source, implémente nativement la méthodologie complète et permet de gérer les bibliothèques de menaces, de vulnérabilités et de mesures de sécurité tout en automatisant les calculs de risques et la génération de rapports. Des solutions commerciales françaises comme *EGERIE* ou ALL4TEC Agile Risk Manager offrent des fonctionnalités supplémentaires de gestion collaborative, de tableaux de bord dynamiques et d'intégration avec d'autres outils GRC de l'écosystème.

Pour les organisations qui débutent leur démarche, un ensemble de tableurs structurés associé à un outil de diagramme comme Draw.io peut suffire pour les premières itérations à condition de maintenir rigoureusement la cohérence entre les ateliers et d'assurer la traçabilité des éléments. La documentation officielle de l'ANSSI sur EBIOS RM fournit des modèles de fiches directement exploitables. L'essentiel est de choisir un outillage adapté à la taille de l'organisation et à la maturité de ses processus de gestion des risques, en lien avec la gestion des vulnérabilités.

Comment présenter les résultats de la cartographie au COMEX ?

La restitution des résultats au comité exécutif est un exercice de communication stratégique qui conditionne l'efficacité de toute la démarche de cartographie des risques. Les dirigeants n'ont ni le temps ni l'appétence technique pour parcourir des dizaines de scénarios détaillés. Il faut leur présenter une synthèse visuelle et percutante articulée autour de trois éléments essentiels : la **cartographie des risques majeurs** positionnés sur une matrice probabilité-impact avec un code couleur intuitif, les *scénarios de risque critiques* exprimés exclusivement en termes d'impact métier quantifié (perte financière estimée, durée d'interruption d'activité, atteinte à la réputation, sanctions réglementaires), et le plan de traitement priorisé avec son budget associé et son calendrier de mise en œuvre.

L'utilisation de **heat maps** et de graphiques radar permet de visualiser rapidement le niveau d'exposition global par domaine de risque (infrastructure, applications, supply chain, données, humain). Chaque risque majeur doit être accompagné d'un indicateur de tendance montrant l'évolution depuis la dernière évaluation. Les informations consolidées alimentent le tableau de bord cyber présenté régulièrement au management, en cohérence avec le log management SOC.

Sources et références : CNIL · ANSSI

Faut-il combiner EBIOS RM avec d'autres référentiels de risques ?

La combinaison d'EBIOS RM avec d'autres cadres de référence enrichit considérablement la profondeur et la couverture de l'analyse des risques cyber. L'utilisation conjointe avec le NIST Cybersecurity Framework permet de structurer les mesures de traitement selon les cinq fonctions universellement reconnues (Identify, Protect, Detect, Respond, Recover). L'intégration avec **ISO 27005** assure la conformité formelle aux exigences du SMSI ISO 27001, tandis que le

rapprochement avec *MITRE ATT&CK* apporte une granularité technique incomparable aux scénarios opérationnels de l'atelier quatre en mappant les techniques d'attaque sur des tactiques observées dans la réalité.

Pour les organisations soumises à des réglementations sectorielles spécifiques, EBIOS RM peut également s'articuler avec les cadres dédiés : DORA pour le secteur financier avec ses exigences de tests de résilience opérationnelle, HDS pour les hébergeurs de données de santé, LPM pour les opérateurs d'importance vitale, ou encore les référentiels spécifiques des autorités de supervision bancaire et assurantielle. Cette approche multi-référentiel évite la duplication coûteuse des efforts d'analyse tout en couvrant exhaustivement l'ensemble des obligations réglementaires applicables à votre organisation.

À retenir : EBIOS RM est bien plus qu'une simple méthodologie d'analyse de risques techniques. C'est un outil de dialogue stratégique qui permet d'aligner la cybersécurité sur les enjeux métiers réels de l'organisation. La clé du succès réside dans l'implication active des parties prenantes métiers dès l'atelier un et dans la capacité à maintenir la cartographie vivante au fil du temps. Prévoyez un investissement initial de 15 à 25 jours-homme pour une première itération complète sur un périmètre ciblé.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr