Sécurité - Analyse de risque (méthode Ebios)

I. Introduction

La méthode EBIOS Risk Manager (EBIOS RM) est la méthode d'appréciation et de traitement du risque numérique publiée par l'Agence nationale de la sécurité et des systèmes d'information (ANSSI) avec le soutien du Club EBIOS.

Elle propose une boite à outils adaptable, dont l'utilisation varie selon l'objectif du projet et est compatible avec les référentiels normatifs en vigueur, en matière de gestion des risques comme en matière de sécurité numérique4. EBIOS Risk Manager permet d'apprécier les risques numériques et d'identifier les mesures de sécurité à mettre en œuvre pour les maitriser.

Elle permet aussi de valider le niveau de risque acceptable et de s'inscrire à plus long terme dans une démarche d'amélioration continue.

Enfin, cette méthode permet de faire émerger les ressources et arguments utiles à la communication et à la prise de décision au sein de l'organisation et vis-à-vis de ses partenaires.

La méthode EBIOS Risk Manager peut être utilisée à plusieurs fins :

- mettre en place ou renforcer un processus de management du risque numérique au sein d'une organisation ;
- apprécier et traiter les risques relatifs à un projet numérique, notamment dans l'objectif d'une homologation de sécurité ;
- définir le niveau de sécurité à atteindre pour un produit ou un service selon ses cas d'usage envisagés et les risques à contrer, dans la perspective d'une certification ou d'un agrément par exemple.

Elle s'applique aussi bien aux organisations publiques ou privées, quels que soient leur taille, leur secteur d'activité et que leurs systèmes d'information soient en cours d'élaboration ou déjà existants.

II. Principes de la méthode Ebios

La méthode EBIOS Risk Manager adopte une approche de management du risque numérique partant du plus haut niveau (grandes
missions de l'objet étudié) pour atteindre progressivement les fonctions métier et techniques, par l'étude des scénarios de risque
possibles. Elle vise à obtenir une synthèse entre « conformité » et « scénarios », en positionnant ces deux approches complémentaires
là où elles apportent la plus forte valeur ajoutée.

Cette démarche est symbolisée par la pyramide du management du risque numérique (cf. figure 1).
Avec EBIOS Risk Manager, l'ensemble des risques est appréhendé par la combinaison :

- d'une approche par conformité pour déterminer le socle de sécurité pour les risques les plus communs, y compris ceux liés à des événements accidentels et environnementaux ;
- et d'une approche par scénarios pour identifier les risques avancés, d'origine intentionnelle, et notamment les attaques
particulièrement ciblées ou sophistiquées.

Ces deux approches permettent d'éclairer les décideurs dans leurs choix de traitement du risque.

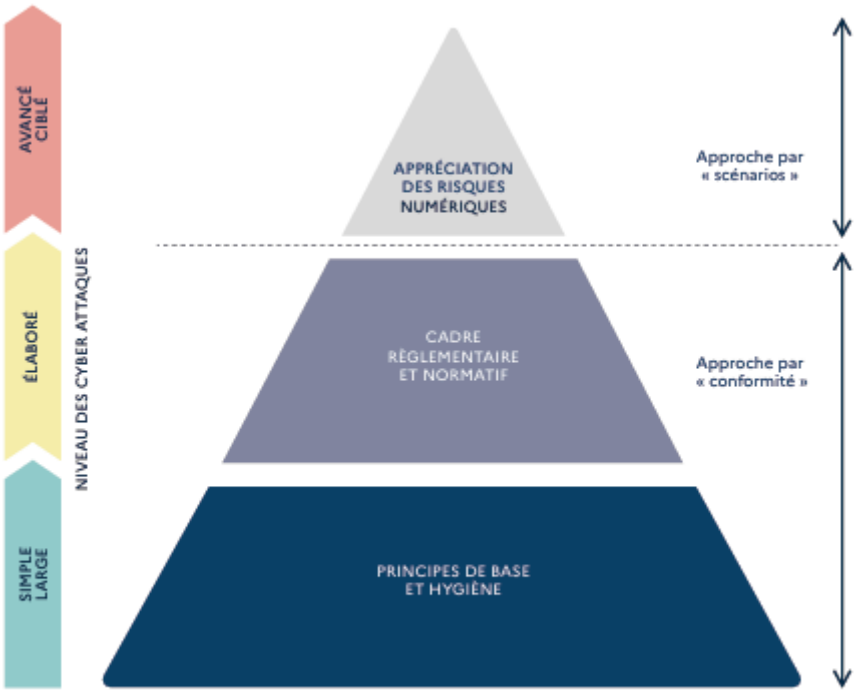

Figure 1 — Pyramide du management du risque numérique

III. Fonctionnement de la méthode Ebios

La méthode Ebios s'articule autour de 5 ateliers de manière itérative (cf. figure 2).

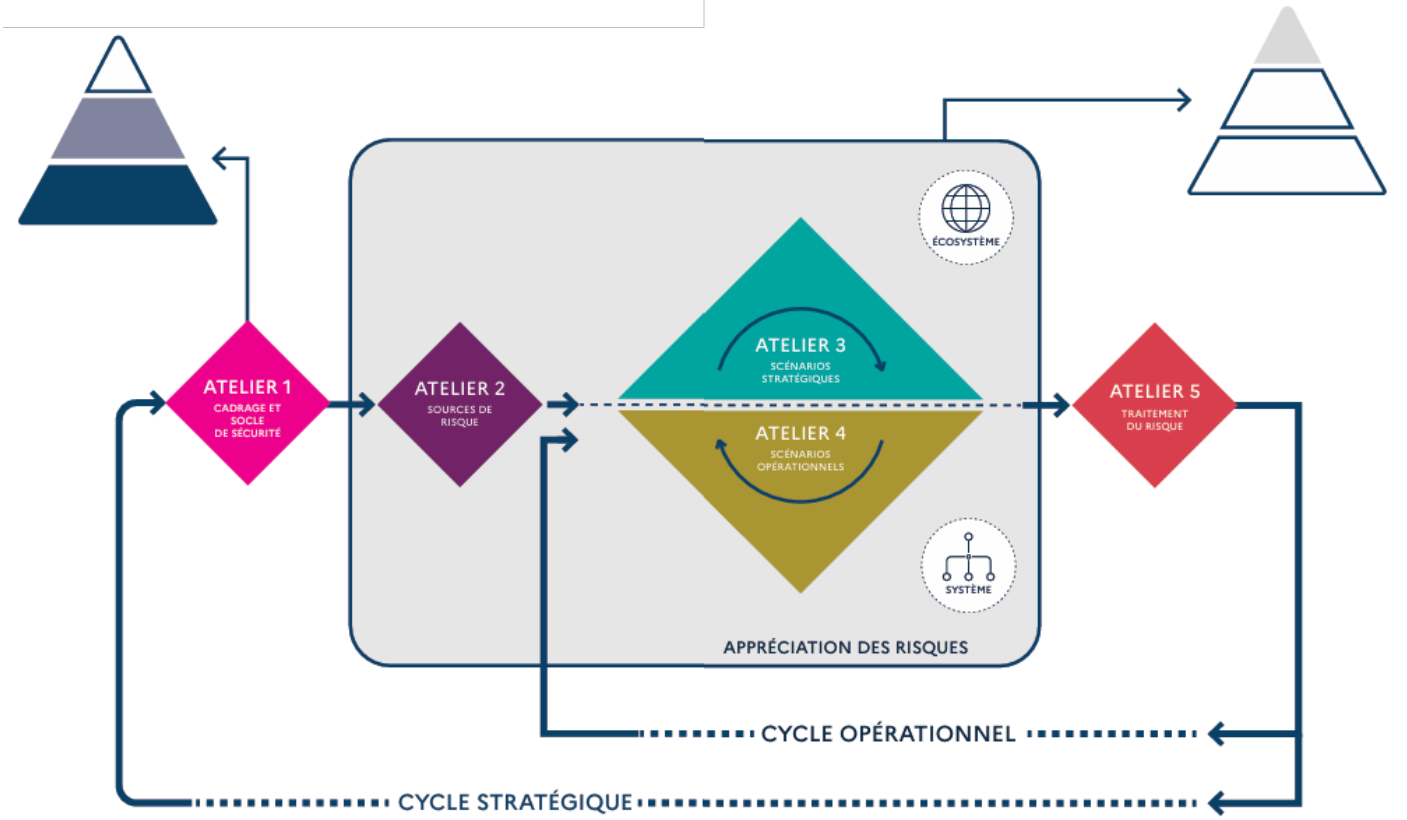

Figure 2 — Une démarche itérative en 5 ateliers

3.1 Atelier 1 - Cadrage et socle de sécurité

Le premier atelier vise à identifier l’objet de l’étude, les participants aux ateliers et le cadre temporel.

Au cours de cet atelier, vous recensez les missions, valeurs métier5 et biens supports relatifs à l’objet étudié.

Vous identifiez les événements redoutés associés aux valeurs métier et estimez la gravité de leurs impacts.

Vous évaluez également la conformité au socle de sécurité.

> **NOTE** : l'atelier 1 permet de suivre une approche par « conformité », correspondant aux deux premiers étages de la pyramide
> du management du risque numérique et d'aborder l'étude du point de vue de la « défense ».

3.2 Atelier 2 - Sources de risque

Dans le deuxième atelier, vous identifiez et caractérisez les sources de risque (SR) et leurs objectifs de haut niveau, appelés objectifs visés (OV).

Les couples SR/OV jugés les plus pertinents sont retenus au terme de cet atelier.

Les résultats sont formalisés dans une cartographie des sources de risque.

3.3 Atelier 3 - scénarios stratégiques

Dans l'atelier 3, vous allez acquérir une vision claire de l'écosystème et établir une cartographie du niveau de dangerosité induit par la relation avec les parties prenantes majeures de l'objet étudié.

Ceci va vous permettre de bâtir des scénarios de haut niveau, appelés scénarios stratégiques.

Ils représentent les chemins d'attaque qu'une source de risque est susceptible d'emprunter pour atteindre son objectif.

Ces scénarios se conçoivent à l'échelle de l'écosystème et des valeurs métier de l'objet étudié.

Leur gravité est ensuite estimée.

À l'issue de cet atelier, vous pouvez déjà définir des mesures de sécurité sur l'écosystème.

3.4 Atelier 4 - Scénarios Opérationnels

Le but de l’atelier 4 est de construire des scénarios techniques reprenant les modes opératoires susceptibles d’être utilisés par les sources de risque pour réaliser les scénarios stratégiques.

Cet atelier adopte une démarche similaire à celle de l’atelier précédent mais se concentre sur les biens supports critiques.

Vous estimez ensuite le niveau de vraisemblance des scénarios opérationnels obtenus.

> **Info** : Les ateliers 3 et 4 s’alimentent naturellement au cours d’itérations successives.

> **Info** : Les ateliers 2, 3 et 4 permettent d’apprécier les risques, ce qui constitue le dernier étage de la pyramide du management
> du risque numérique. Ils sollicitent le socle de sécurité selon des axes d’attaque différents, pertinents au regard des menaces
> considérées et en nombre limité pour en faciliter l’analyse.

3.5 Atelier 5 - Traitement du risque

Le dernier atelier consiste à synthétiser l’ensemble des risques étudiés et à définir une stratégie de traitement du risque. Cette dernière
est ensuite déclinée en mesures de sécurité inscrites dans un plan de traitement du risque. Lors de cet atelier, vous établissez la synthèse des risques résiduels et définissez le cadre de suivi des risques.

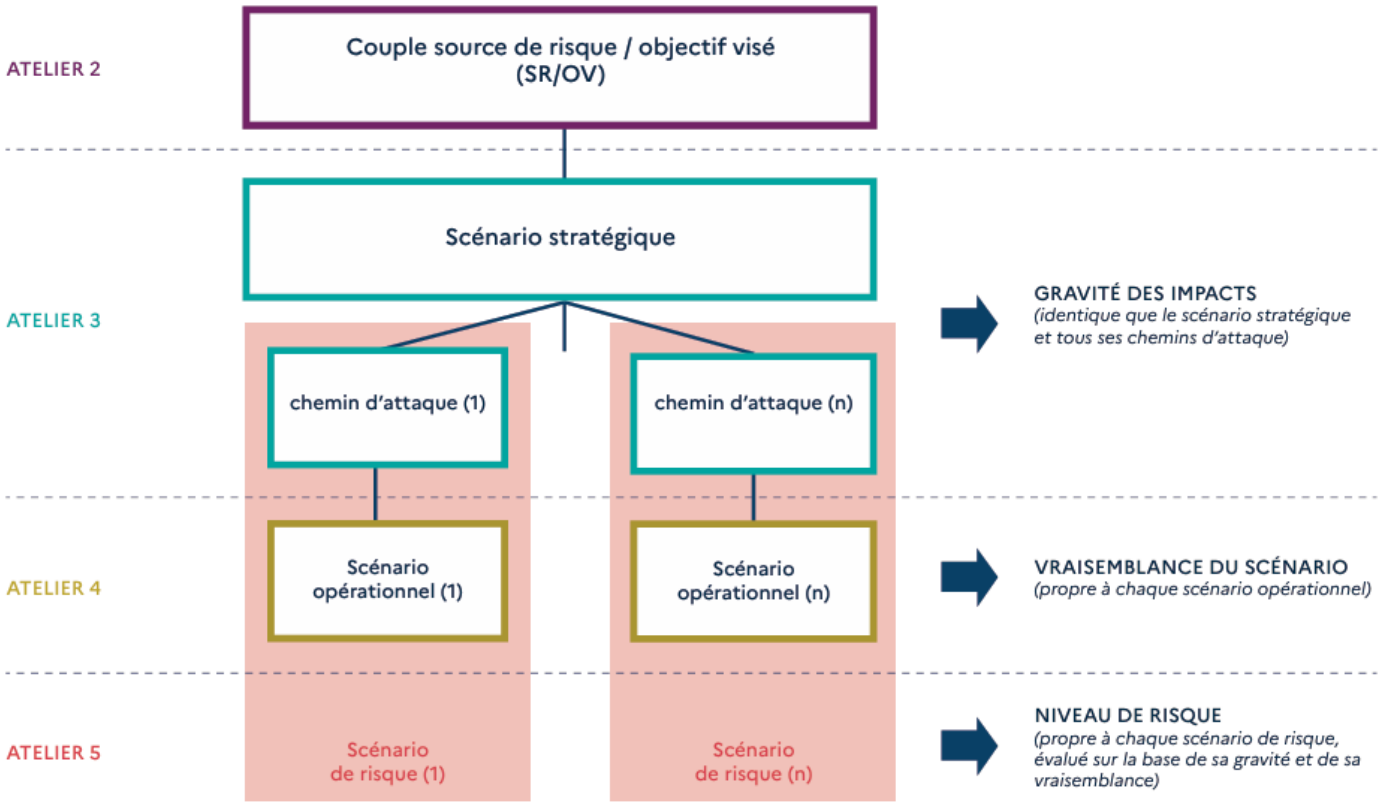

Figure 3 —Lien entre les différents ateliers

> **Note** : en général, chaque chemin d'attaque d'un scénario stratégique donne lieu à un scénario opérationnel. Un scénario de risque correspond à l'association d'un chemin d'attaque et de son scénario opérationnel.

IV. Conclusion

EBIOS Risk Manager est une méthode adaptable. Elle constitue une véritable boîte à outils, dont le niveau de détail et le séquencement
des activités à réaliser pour chaque atelier, seront adaptés en fonction des objectifs.

La manière dont s'applique la méthode diffère selon le sujet étudié, les livrables attendus, le degré de connaissance du périmètre de l'étude ou encore le secteur auquel on l'applique.

La grille ci-après propose des cas d'usage selon l'objectif visé.

OBJECTIF DE L'ÉTUDE	ATELIERS PRINCIPAUX À CONDUIRE OU EXPLOITER				
	1	2	3	4	5
Identifier le socle de sécurité adapté à l'objet de l'étude	X				
Être en conformité avec les référentiels de sécurité numérique	X				X
Évaluer le niveau de menace de l'écosystème vis-à-vis de l'objet de l'étude			X (note 1)		
Identifier et analyser les scénarios de haut niveau, intégrant l'écosystème		X	X		
Réaliser une étude préliminaire de risque pour identifier les axes prioritaires d'amélioration de la sécurité	X (note 2)	X	X (note 3)		X (note 4)
Conduire une étude de risque complète et fine, par exemple sur un produit de sécurité ou en vue de l'homologation d'un système	X	X	X	X	X
Orienter un audit de sécurité et notamment un test d'intrusion			X	X	
Orienter les dispositifs de détection et de réaction, par exemple au niveau d'un centre opérationnel de la sécurité (SOC)			X	X	

Revision #2
Created 2026-07-17 20:41:29 UTC by Olivier
Updated 2026-07-17 20:42:05 UTC by Olivier