



EBIOS RISK MANAGER – Fiche méthode

Comment traiter les aspects non-intentionnels avec EBIOS RISK MANAGER ?

Date : 08/05/2026

Statut : Validé

Classification : PUBLIC – NON PROTÉGÉ

Nombre de pages : 17

Responsable des travaux : Ian GRISPAN

Validation : Groupe de travail

Approbation : Conseil d'administration

Licence :



Ce document a été réalisé par le Club EBIOS

Responsable(s) des travaux :

☐ Ian GRISPAN - Airbus PROTECT

Contributeur(s) :

☐ Damien AUVRAY

☐ Jean OLIVE – CGI Business Consulting

☐ Stéphane PAUL

☐ Zian DELAHAYE

Historique des modifications

Date	Objet de la modification	Auteur(s)	Statut
20/04/2026	Version initiale consolidée — périmètre élargi (risques non-intentionnels purs et facteurs non-intentionnels des scénarios intentionnels)	Collège des praticiens	Document de travail
06/05/2026	Consolidation après arbitrage du Collège : périmètre maintenu à 2 formes (Option A) ; intégration des retours D. Auvray (terminologie « facteur » / « élément »), J. Olive (précision §1.4 SI ciblé, variante écosystème §2.3), Z. Delahaye (validation) ; correction de coquilles ; reformulation §3.5	I. GRISPAN	Document de travail
08/05/2026	Version Finale	I.GRISPAN	Validé

Sommaire

1	INTRODUCTION.....	6
2	NOTIONS ET PÉRIMÈTRE.....	7
2.1	DÉFINITION DU RISQUE NON-INTENTIONNEL.....	7
2.2	TYPLOGIE DES SOURCES DE RISQUE NON-INTENTIONNELLES.....	7
2.3	DEUX APPROCHES DE TRAITEMENT.....	8
2.4	CAS LIMITE : ÉVÉNEMENT ACCIDENTEL PROVOQUÉ VOLONTAIREMENT.....	8
3	APPROCHE A : TRAITER UN RISQUE NON-INTENTIONNEL PUR.....	9
3.1	PRINCIPE.....	9
3.2	ÉTAPE 1 : RASSEMBLER LES ÉLÉMENTS D'ENTRÉE.....	9
3.3	ÉTAPE 2 : IDENTIFIER UN FAIT GÉNÉRATEUR.....	9
3.4	ÉTAPE 3 : RATTACHER LE FAIT GÉNÉRATEUR À UN ÉVÉNEMENT REDOUTÉ.....	10
3.5	ÉTAPE 4 : DÉCRIRE LE MODE OPÉRATOIRE.....	10
3.6	ÉTAPE 5 : ESTIMER LA VRAISEMBLANCE.....	10
3.7	ÉTAPE 6 : INTÉGRER EN ATELIER 5.....	11
4	APPROCHE B : INTÉGRER UN FACTEUR NON-INTENTIONNEL DANS UN SCÉNARIO INTENTIONNEL.....	12
4.1	PRINCIPE.....	12
4.2	PRISE EN COMPTE EN ATELIER 2.....	12
4.3	PRISE EN COMPTE EN ATELIER 3.....	12
4.4	PRISE EN COMPTE EN ATELIER 4.....	12
4.5	TRAITEMENT EN ATELIER 5.....	13
5	CHOISIR LA DÉMARCHE SELON LE CONTEXTE.....	14
6	TABLEAU DES FAITS GÉNÉRATEURS TYPES.....	15
6.1	FAITS GÉNÉRATEURS D'ORIGINE ACCIDENTELLE.....	15
6.2	FAITS GÉNÉRATEURS D'ORIGINE ENVIRONNEMENTALE.....	15
7	CONCLUSION.....	16
8	ANNEXES.....	17
8.1	ACRONYMES.....	17



CLUBEBIOS

8.2	GLOSSAIRE.....	17
8.3	BIBLIOGRAPHIE.....	17

1 Introduction

La méthode EBIOS Risk Manager appréhende les risques de cybersécurité selon deux approches complémentaires :

1. L'approche par conformité définit un socle de sécurité dimensionné pour les risques les plus communs, notamment les risques non-intentionnels les plus fréquents.
2. L'approche par scénarios identifie les risques avancés d'origine intentionnelle, en particulier les attaques ciblées ou sophistiquées.

Le guide EBIOS RM mentionne à plusieurs reprises la catégorie des risques non délibérés ou non ciblés. Lorsque de tels risques sont identifiés lors de l'analyse du socle ou des événements redoutés, le guide prévoit qu'ils soient intégrés à la matrice des risques afin que des mesures adéquates figurent au plan de traitement. Dans la pratique, ces risques prennent deux formes distinctes qui appellent deux traitements différents.

Cette fiche traite les deux formes.

D'une part, les risques non-intentionnels au sens propre, dans lesquels un fait générateur d'origine accidentelle ou environnementale provoque directement un événement redouté, sans intervention volontaire d'un attaquant.



D'autre part, les facteurs non-intentionnels qui facilitent un scénario d'attaque intentionnel en ouvrant une brèche, en dégradant une mesure de sécurité ou en offrant un moyen d'accès à une source de risque malveillante.

Ces deux situations partagent la même cause racine, l'absence d'intention de nuire chez l'acteur humain ou l'origine non humaine du fait générateur, mais elles se traduisent différemment dans la méthode.

La fiche propose, pour chaque situation, une démarche opérationnelle aussi proche que possible de la pratique standard d'EBIOS RM. Elle s'adresse aux praticiens ayant déjà une maîtrise de la méthode et qui souhaitent enrichir leurs études d'une prise en compte explicite du non-intentionnel.

2 Notions et périmètre

2.1 Définition du risque non-intentionnel

La méthode EBIOS Risk Manager décrit classiquement un risque de cybersécurité sous la forme d'un scénario allant d'une source de risque à l'objectif qu'elle vise. Cette formulation, orientée vers les risques délibérés, suppose une intention de nuire.

Pour les risques non-intentionnels, la présente fiche retient la définition suivante :

« Un risque non-intentionnel est la possibilité qu'un événement redouté survienne d'un fait générateur, sans intention de nuire. »

Deux notions complémentaires sont mobilisées tout au long de la fiche :

- **Fait générateur** : cause humaine accidentelle, technique ou environnementale à l'origine d'un événement redouté ou d'une action exploitée ensuite par un attaquant.
- **Vulnérabilité associée** : défaut ou faiblesse du système qui rend possible le passage du fait générateur à l'événement redouté, ou qui augmente la vraisemblance d'une action élémentaire dans un scénario intentionnel.

2.2 Typologie des sources de risque non-intentionnelles

Les sources non-intentionnelles se regroupent en deux catégories :

Sources accidentelles (humaines). Parties prenantes humaines (collaborateurs, prestataires, visiteurs) pouvant, par erreur, omission, inattention ou défaut de compétence, provoquer un fait générateur sans intention de nuire. Exemples : mauvaise manipulation, envoi d'un fichier vers un mauvais destinataire, effacement accidentel, oubli d'une étape d'une procédure, divulgation involontaire d'identifiants.

Sources environnementales. Événements ou phénomènes extérieurs à l'activité humaine du périmètre, de nature physique ou naturelle, ainsi que les défaillances matérielles et bogues logiciels. Exemples : crise sanitaire, incendie, inondation, coupure d'électricité, défaillance matérielle, bogue logiciel, phénomène climatique.

Par convention, les défaillances matérielles et les bogues logiciels sont rattachés à la catégorie environnementale : bien qu'internes au système, ils ne résultent pas d'une action humaine volontaire et partagent avec les phénomènes environnementaux l'absence d'acteur intentionnel.

2.3 Deux approches de traitement

La fiche distingue deux approches de traitement, selon la place que prend le facteur non-intentionnel dans le scénario.

Approche A : Risque non-intentionnel pur. Un fait générateur non-intentionnel provoque directement un événement redouté, sans intervention d'une source de risque malveillante. Traitement détaillé au chapitre 3 (démarche empirique en six étapes).

Approche B : Facteur non-intentionnel dans un scénario intentionnel. Un événement non-intentionnel (erreur humaine, négligence, panne) crée un élément qu'une source de risque malveillante exploite dans son chemin d'attaque. Traitement détaillé au chapitre 4 (intégration aux ateliers 2 à 4).

Ces deux approches ne s'excluent pas : une étude EBIOS RM peut les combiner selon son contexte. Le chapitre 5 donne des repères pour choisir la démarche appropriée selon l'objet de l'étude.

2.4 Cas limite : événement accidentel provoqué volontairement



Un **événement de forme accidentelle ou environnementale** peut être provoqué volontairement par une source de risque intentionnelle ciblant le SI étudié : incendie allumé par malveillance pour forcer une évacuation, coupure électrique orchestrée pour interrompre un service.

Dans ces situations, le risque relève de l'intentionnel et doit être traité par scénario classique, non par la présente fiche.

La forme accidentelle du fait générateur ne présume pas de la nature non-intentionnelle du risque ; c'est l'absence d'intention qui caractérise le non-intentionnel.

3 Approche A : Traiter un risque non-intentionnel pur

3.1 Principe

La démarche est délibérément empirique.

Elle vise à intégrer les risques non-intentionnels dans la matrice des risques sans recourir à l'ensemble du formalisme des ateliers 2, 3 et 4 de la méthode EBIOS RM.

Le risque non-intentionnel est construit à partir d'un écart au socle de sécurité ou d'un événement redouté identifié, caractérisé par un fait générateur simple.

La démarche se déploie en six étapes courtes qui peuvent être menées rapidement, y compris en complément d'un atelier déjà tenu.

3.2 Étape 1 : Rassembler les éléments d'entrée

Les éléments d'entrée sont la liste des événements redoutés établis en atelier 1 avec leur gravité associée, la liste des écarts au socle de sécurité identifiés, et, le cas échéant, les analyses de risques environnementaux déjà disponibles (étude d'inondation, analyse incendie).

Un écart au socle ou un événement redouté qui fait émerger un risque non-intentionnel potentiel devient candidat à la suite de la démarche.

3.3 Étape 2 : Identifier un fait générateur

Pour chaque élément candidat retenu à l'étape précédente (écart au socle, événement redouté ou analyse de risque environnemental), une formulation du fait générateur non-intentionnel le plus plausible doit être exprimée, en précisant la source de risque non-intentionnelle dont il relève (accidentelle ou environnementale, cf. typologie §2.2) ainsi que la vulnérabilité associée.

Exemple : Destruction accidentelle de données de production par un administrateur système → vulnérabilité : absence de contrôle de validation avant exécution de commandes critiques (ex. `rm -rf` lancé sur le mauvais environnement).

L'administrateur n'a aucune intention de nuire. L'action dommageable est purement accidentelle. Il n'y a pas d'acteur tiers malveillant en arrière-plan.

Les faits générateurs peuvent survenir directement sur le SI étudié ou dans son écosystème (hébergeur, fournisseur critique, service tiers) et se propager jusqu'à lui. Dans tous les cas, le rattachement à l'événement redouté reste direct et doit être traité ici et en dehors de l'atelier 3.

3.4 Étape 3 : Rattacher le fait générateur à un événement redouté

Pour chaque fait générateur identifié, on se pose la question : cet événement peut-il provoquer un événement redouté issu de l'atelier 1 ? Si oui, le rattachement est établi ; sinon, le risque n'est pas pertinent pour l'étude.

Exemple : Destruction accidentelle de données de production par un administrateur système → Perte irrémédiable de données métier critiques (événement redouté).

La gravité du risque non-intentionnel est celle de l'événement redouté, telle qu'évaluée en atelier 1. Elle n'a pas à être réestimée.

3.5 Étape 4 : Décrire le mode opératoire

Sans reconstruire un scénario opérationnel complet, il est recommandé de décrire en quelques mots comment le fait générateur peut aboutir à l'événement redouté. Ce mode opératoire synthétique permet de rendre le risque lisible et contrôlable en atelier 5.

Exemple : Destruction accidentelle de données de production par un administrateur → absence de contrôle de validation avant exécution de commandes critiques → suppression non détectée et non bloquée → écrasement des données de production sans possibilité de rollback immédiat → indisponibilité du service métier concerné

3.6 Étape 5 : Estimer la vraisemblance

La vraisemblance est estimée selon un mode « express », sans reconstruction d'un enchaînement d'actions élémentaires.

Elle traduit la probabilité que l'enchaînement décrit à l'étape 4 survienne sur la période considérée, compte tenu des mesures du socle effectivement en place et des éventuels indicateurs statistiques disponibles (historique d'incidents, études environnementales).

Si vous n'avez pas d'échelle propre, vous pouvez utiliser l'échelle ci-dessous :

Niveau	Libellé	Description indicative
1	Rare	Peut se produire dans des circonstances exceptionnelles, moins d'une fois tous les 10 ans.
2	Peu probable	Peut se produire mais n'est pas attendu (fréquence typique : 5 à 10 ans).
3	Probable	Pourrait se produire occasionnellement (fréquence typique : 1 à 5 ans).
4	Quasi certain	Se produit fréquemment ou en continu.

Pour les risques accidentels, l'estimation tient compte de la récurrence constatée (incidents précédents), de la familiarité des acteurs avec les tâches concernées, de la surcharge des acteurs à origine du fait générateur, du niveau de formation, de la disponibilité des procédures, et des mécanismes de détection et de correction (contrôle à quatre yeux, supervision).

Pour les risques environnementaux, l'estimation s'appuie sur les analyses existantes et sur les dispositifs de prévention et de détection déjà déployés.

3.7 Étape 6 : Intégrer en atelier 5

Une fois la gravité (héritée de l'atelier 1) et la vraisemblance (estimée à l'étape 5) établies, le risque non-intentionnel est inséré dans la matrice des risques. Il est ensuite traité en atelier 5 selon la même logique que les risques intentionnels : acceptation, réduction, évitement, transfert.

Les mesures de traitement sont définies au cas par cas, mais peuvent être communes à celles des risques intentionnels.

Pour les sources accidentelles, elles peuvent viser le renforcement de la sélection et de la qualification des ressources humaines, le renforcement des équipes, la formation, la mise à disposition de procédures et de guides, le déploiement de contrôles manuels ou automatisés.

Pour les sources environnementales, elles peuvent viser l'évitement (relocalisation), les dispositifs de gestion de crise, les plans de continuité et de reprise d'activité.

4 Approche B : Intégrer un facteur non-intentionnel dans un scénario intentionnel

4.1 Principe

Dans cette approche, le facteur non-intentionnel n'est pas l'origine du risque mais un élément qui en augmente la vraisemblance ou qui ouvre une voie d'attaque préalablement bloquée.

Le scénario de risque reste intentionnel : il a une source de risque malveillante, un objectif visé, un chemin d'attaque. Le facteur non-intentionnel s'y intègre au même titre qu'une vulnérabilité exploitée par l'attaquant.



La démarche reste fidèle aux ateliers 2 à 4 de la méthode EBIOS RM. Elle n'introduit pas de nouveau concept structurant : les facteurs non-intentionnels sont traités comme des actions élémentaires du scénario opérationnel, avec leurs conséquences sur la vraisemblance.

4.2 Prise en compte en atelier 2

L'atelier 2 identifie les couples source de risque / objectif visé pertinents. Pour un scénario susceptible d'être facilité par un facteur non-intentionnel, aucune adaptation n'est nécessaire à ce stade : la source reste malveillante, l'objectif reste un bénéfice recherché.

La question du facteur non-intentionnel sera posée plus loin dans l'analyse, lorsque le chemin d'attaque sera précisé.

4.3 Prise en compte en atelier 3

Les scénarios stratégiques construits en atelier 3 peuvent mobiliser des parties prenantes dont une action non-intentionnelle serait exploitée par la source de risque. Cela n'appelle pas de modification méthodologique : la partie prenante est identifiée selon la pratique habituelle.

4.4 Prise en compte en atelier 4

C'est à l'atelier 4 que le facteur non-intentionnel se matérialise explicitement dans la démarche. Le scénario opérationnel décrit une suite d'actions élémentaires menées par l'attaquant. Lorsqu'une de ces actions s'appuie sur un facteur non-intentionnel, celui-ci est explicité dans le mode opératoire et pris en compte dans la vraisemblance.

Deux pratiques complémentaires sont recommandées :

1. **Documenter le facteur non-intentionnel dans le scénario opérationnel.**
Plutôt que de le masquer dans la formulation d'une action élémentaire, le nommer explicitement.

Exemple : au lieu d'écrire « L'attaquant obtient des identifiants valides », écrire « L'attaquant obtient des identifiants valides laissés sur un post-it par un collaborateur ».

La traçabilité du facteur non-intentionnel est ainsi conservée pour l'atelier 5.

2. **Moduler la vraisemblance de l'action élémentaire concernée.** La vraisemblance de l'action élémentaire qui bénéficie du facteur non-intentionnel est évaluée en tenant compte de la fréquence attendue de ce facteur (historique d'incidents, niveau de maturité cyber des acteurs concernés, faiblesse des mesures compensatoires existantes).

Exemple : un scénario d'exfiltration de données R&D est facilité par le fait que le système ne garantit pas qu'un collaborateur ne partage pas ses identifiants d'accès distant par messagerie personnelle.

Le scénario opérationnel comporte alors une action élémentaire « Acquisition d'identifiants valides via un canal non sécurisé » dont la vraisemblance est évaluée en tenant compte de l'historique d'incidents et de la présence (ou l'absence) d'une authentification multi-facteurs qui rendrait les identifiants insuffisants à eux seuls.

4.5 Traitement en atelier 5

Le traitement du scénario intentionnel se fait en atelier 5 selon la pratique standard.

La présence d'un facteur non-intentionnel comme élément facilitant ouvre cependant un jeu de mesures complémentaires spécifiques :

- sensibilisation ciblée des parties prenantes concernées ;
- contrôles techniques qui réduisent l'impact d'un comportement non-intentionnel (authentification multi-facteurs, supervision des partages, détection de fuites de données) ;
- amélioration des procédures ambiguës ou contraignantes qui favorisent les contournements involontaires.

5 Choisir la démarche selon le contexte

Le choix de l'une, l'autre, ou des deux démarches dépend de la nature de l'objet de l'étude et des risques qui le caractérisent.

Les trois cas suivants couvrent les situations typiques rencontrées dans les études EBIOS RM.

Cas 1 : Objet principalement exposé à des risques non-intentionnels. Typiquement un datacenter, une infrastructure hébergée en propre, un environnement à forte dimension sûreté de fonctionnement. L'approche A est centrale. L'approche B peut rester implicite si aucun scénario d'attaque intentionnel significatif n'est retenu dans l'étude.

Cas 2 : Objet principalement exposé à des risques intentionnels. Typiquement un service web exposé sur Internet, une plateforme SaaS, une application grand public. L'approche B est centrale. L'approche A peut être traitée succinctement pour couvrir les rares risques non-intentionnels purs identifiés (défaillance d'hébergeur, bogue de mise à jour).

Cas 3 : Objet exposé aux deux types de risques. Typiquement un système d'information d'entreprise hébergé en propre, un écosystème mixte (infrastructures et services hébergés). Les deux approches sont mobilisées conjointement. C'est le cas le plus courant.

Ce découpage est un repère, pas une prescription. Dans tous les cas, la décision finale revient au pilote de l'étude, en fonction des objectifs qui ont été assignés à l'analyse de risque et des livrables attendus.

6 Tableau des faits générateurs types

Le tableau ci-dessous propose un aide-mémoire pour l'identification d'un fait générateur (Approche A) ou d'un facteur non-intentionnel (Approche B). Il n'est ni exhaustif ni prescriptif : les faits générateurs retenus dépendent du contexte de l'objet de l'étude.

6.1 Faits générateurs d'origine accidentelle

Fait générateur type	Exemple
Erreur de manipulation	Suppression accidentelle d'une base de données en production.
Envoi erroné	Transmission d'un document sensible à un mauvais destinataire.
Non-respect d'une procédure	Maintenance effectuée sans respect du processus de sauvegarde préalable.
Mauvaise configuration	Ouverture non-intentionnelle d'un service en accès public.
Oubli	Absence de désactivation d'un compte lors d'un départ.
Perte ou égarement	Perte d'un équipement mobile contenant des données sensibles.
Divulgaration involontaire	Partage d'identifiants par messagerie, publication de données sur un service public non contrôlé.
Contournement par commodité	Désactivation temporaire d'une mesure de sécurité pour réaliser une tâche plus rapidement, sans réactivation.

6.2 Faits générateurs d'origine environnementale

Fait générateur type	Description
Incendie externe	Incendie provenant de l'extérieur du site, pouvant se propager ou provoquer une évacuation.
Incendie interne	Incendie lié à une défaillance électrique ou à un matériel défectueux.
Inondation	Montée des eaux ou rupture de canalisation.
Phénomène climatique	Tempête, forte pluie, vague de chaleur.
Phénomène sismique	Séisme affectant bâtiments et infrastructures.
Perte d'électricité	Coupure du réseau électrique.
Défaillance du refroidissement	Surchauffe des équipements critiques.
Perte réseau	Indisponibilité des services de télécommunication.
Crise sanitaire	Indisponibilité du personnel et contraintes organisationnelles.
Défaillance matérielle	Panne d'un équipement critique.
Bogue logiciel	Défaut de code provoquant un dysfonctionnement.

7 Conclusion

Le traitement du non-intentionnel dans une étude EBIOS RM s'ancre dans deux approches complémentaires.

L'approche A, purement non-intentionnelle, intègre des risques dont l'origine est accidentelle ou environnementale ; elle mobilise une démarche empirique en six étapes, ancrée sur la gravité de l'atelier 1 et le traitement en atelier 5.

L'approche B, mixte, intègre des facteurs non-intentionnels dans des scénarios intentionnels ; elle s'appuie sur les ateliers 2 à 4 sans modification structurelle de la méthode, en rendant explicite le facteur non-intentionnel dans le scénario opérationnel et en l'intégrant à l'évaluation de la vraisemblance.

Le socle de sécurité, même parfaitement appliqué, ne couvre ni l'intégralité des situations accidentelles plausibles, ni les écarts opérationnels qui existent de fait sur le terrain (exigences non applicables, dérogations, angles morts du référentiel).

Les risques non-intentionnels ont souvent des conséquences directes significatives et peuvent, dans certains cas, aggraver des scénarios intentionnels auxquels ils se combinent. Les traiter explicitement dans l'étude EBIOS RM renforce la qualité globale de l'analyse et la pertinence du plan de traitement.

La démarche proposée dans cette fiche se veut cumulable avec les pratiques existantes et modulable selon le contexte de l'étude, sans alourdir significativement le processus. Elle pourra être complétée par des travaux ultérieurs du Collège des praticiens, notamment sur l'analyse des risques multifactoriels et sur les classifications alternatives des sources de risque.

8 Annexes

8.1 Acronymes

ANSSI	Agence nationale de la sécurité des systèmes d'information
EBIOS RM	Expression des Besoins et Identification des Objectifs de Sécurité — Risk Manager
ER	Événement redouté
SR	Source de risque
OV	Objectif visé
SI	Système d'information
R&D	Recherche et Développement
SaaS	Software as a Service

8.2 Glossaire

Risque non-intentionnel	Possibilité qu'un événement redouté survienne d'un fait générateur, sans intention de nuire.
Fait générateur	Cause humaine accidentelle, technique ou environnementale à l'origine d'un événement redouté ou d'une action exploitée ensuite par un attaquant.
Source de risque accidentelle	Partie prenante humaine susceptible, par erreur, omission, inattention ou défaut de compétence, de provoquer un fait générateur sans intention de nuire.
Source de risque environnementale	Événement ou phénomène extérieur à l'activité humaine du périmètre (physique, naturel) ou défaillance matérielle/logicielle susceptible de provoquer un événement redouté.
Facteur non-intentionnel	Événement non-intentionnel qui, dans un scénario d'attaque intentionnel, crée ou aggrave un élément exploité par une source de risque malveillante.
Approche A	Traitement des risques non-intentionnels purs, sans intervention d'une source de risque malveillante.
Approche B	Prise en compte des facteurs non-intentionnels comme éléments facilitants au sein de scénarios intentionnels.
Mode opératoire (non-intentionnel)	Description synthétique de l'enchaînement par lequel un fait générateur aboutit à un événement redouté, sans reconstruction d'un scénario opérationnel complet.

8.3 Bibliographie

Les références suivantes apparaissent entre crochets dans le présent document.

- [ANSSI-EBIOS-RM-V1.5] ANSSI, La méthode EBIOS Risk Manager — Le guide, version 1.5, 2024.
- [ANSSI-EBIOS-RM-FICHES] ANSSI, EBIOS Risk Manager — Fiches méthodes, 2018-2024.