ANSSI

Agence nationale de la sécurité des systèmes d'information

# Vous n'osez plus parler de SSI à vos décideurs ?
# Il vous manque peut-être un outil pour les convaincre…

## Les bons messages aux décideurs

- Présentation hiérarchique des risques
  *arbitrage en connaissance de cause*
- Décision face aux enjeux métiers
- Investissement justifié et optimisé
- Fiabilité des processus métiers
- Effort approprié et résultats concrets

## La gestion efficace de vos risques SSI

- Implication des métiers
- Cartographie rapide des risques
- Production d'un référentiel cohérent
- Adaptation aux contraintes métiers
- Itération simple quand le SI évolue
- Compatibilité avec ISO 2700x

# EBIOS

## La méthode de gestion des risques

## Une méthode internationale éprouvée

- 15 ans d'expérience
- Traduite en plusieurs langues
- Un réseau d'utilisateur international
- Échange d'expériences au Club EBIOS
- Utilisée par les secteurs privé et public
- Développée et entretenue par l'ANSSI

## Pratique

Conseils , exemples et cas concrets

## Adaptable

Études optimisées selon les besoins

## Outillée

Guides, bases de connaissances, logiciel...

## Gratuite

Diffusée sur le site de l'ANSSI

ANSSI Agence nationale de la sécurité des systèmes d'information

# Foire aux questions

## « La norme ISO 27005 ne remplace-t-elle pas la méthode EBIOS ? »

ISO 27005 est un cadre pour toutes les méthodes de gestion des risques SSI : elle énonce des lignes directrices.
« *La présente Norme internationale ne fournit aucune méthodologie spécifique à la gestion de risque en sécurité de l'information. […] Plusieurs méthodologies existantes peuvent être utilisées en cohérence avec le cadre décrit dans la présente Norme internationale pour appliquer les exigences du SMSI* » [ISO 27005]
Une méthode telle qu'EBIOS est donc nécessaire pour les mettre en application de manière opérationnelle.

## « Je n'ai pas beaucoup de temps pour faire une étude de risque. J'ai besoin de réactivité et d'efficacité. Existe-t-il une EBIOS "Light" ? »

Une EBIOS est forcément "Light". Sinon, cela signifie qu'elle est mal employée ! En effet, la durée d'une étude EBIOS est optimisée, car elle permet d'obtenir les éléments nécessaires et suffisants selon le résultat attendu.
Par ailleurs, il est préférable de commencer par mener une étude sans rentrer dans les détails, puis, si besoin de raffiner l'étude là où cela est jugé nécessaire. Cela permet d'ajuster la charge aux ressources dont on dispose, tout en garantissant une vraie pertinence des résultats. Ainsi, une étude EBIOS peut parfaitement produire un résultat concret en quelques heures.

## « Je souhaite que mon service soit certifié ISO 27001, EBIOS va-t-elle m'aider ? »

L'ISO 27001 définit les exigences à satisfaire pour qu'un système de management de la sécurité de l'information (SMSI) soit certifié ; et le cœur d'un SMSI est la gestion des risques.
La méthode EBIOS constitue un outil pertinent pour satisfaire les exigences de la norme dans ce domaine. En effet, elle permet d'adapter la sécurité au contexte particulier de l'organisme, d'apprécier les risques, de déterminer les mesures de sécurité nécessaires et suffisantes pour les traiter, et de produire une déclaration d'applicabilité qui exploite l'ISO 27002 (catalogue de mesures de sécurité).

## « En ce moment, je dois à la fois mettre en place un SMSI, améliorer la sécurité physique de ma "salle serveurs" et fournir des clauses contractuelles pour externaliser une partie de mon système d'information (SI). En quoi EBIOS peut-elle m'aider ? »

EBIOS est la méthode idéale pour chacune de ces préoccupations. C'est en effet une véritable boîte à outils qui s'adapte à l'objet de l'étude et aux livrables attendus.
Pour mettre en place un SMSI, on réalisera une étude globale et de haut niveau, en exploitant les mesures de sécurité de l'ISO 27002.
Concernant la "salle serveurs", on réalisera une étude détaillée sur ce périmètre, en ne considérant que les menaces et les biens supports (locaux, matériels et personnes) liés aux aspects physiques.
Enfin, pour définir des clauses contractuelles d'externalisation, on étudiera la partie du SI à externaliser pour définir uniquement des objectifs de sécurité, qui pourront constituer des clauses contractuelles.

## « J'ai déjà utilisé EBIOS dans sa version précédente (v2). Aujourd'hui, mon SI ayant évolué, je dois mettre à jour mes études et souhaite utiliser la nouvelle version de la méthode. Comment dois-je m'y prendre ? »

Les études faites avec EBIOSv2 n'ont évidemment pas à être refaites. Il est toujours possible de les tenir à jour.
Pour transposer une étude existante dans la nouvelle version, il convient de changer la terminologie (ex : "sources de menaces" plutôt que "élément menaçant") et d'adapter certaines activités de la boîte à outils :

- module 1 : regrouper les paramètres, métriques et sources, identifier les mesures existantes ;
- module 2 : relier les sources aux événements redoutés, estimer la gravité ;
- module 3 : employer les nouvelles typologies, estimer la vraisemblance ;
- module 4 : relier les mesures existantes, choisir d'éviter, réduire, prendre, ou transférer les risques ;
- module 5 : compléter la détermination des mesures (défense en profondeur et optimisation).

Enfin, les nouvelles activités d'EBIOS peuvent améliorer la démarche (cadrage de l'étude, plan d'action…).