



PREMIER MINISTRE  
Secrétariat général de la défense nationale  
Direction centrale de la sécurité des systèmes d'information  
Sous-direction des opérations  
Bureau conseil

# **MEILLEURES PRATIQUES POUR LA GESTION DES RISQUES SSI**

---

Utilisation spécifique de la méthode EBIOS®  
pour rédiger une FEROS

**Version du 18 avril 2005**

## Qu'est-ce qu'une FEROS ?

La Fiche d'Expression Rationnelle des Objectifs de Sécurité (FEROS)<sup>1</sup> est un document à caractère obligatoire dans le cas de systèmes traitant des informations classifiées de défense<sup>2</sup> et recommandé sinon<sup>3</sup>.

Ce document consiste à formaliser tous les éléments nécessaires à l'acceptation de la mise en œuvre d'un système par une autorité. Il présente donc non seulement tous les objectifs de sécurité du système étudié et les risques résiduels, mais aussi la démarche et l'argumentation qui a permis de les identifier.

## Quels sont les avantages de la méthode EBIOS pour la rédaction d'une FEROS ?

La méthode EBIOS est connue comme "l'outil idéal pour rédiger des FEROS". Elle a été conçue dans ce but et permet donc de rédiger une FEROS quasiment intégralement. Elle offre de surcroît plusieurs avantages :

- la pertinence des objectifs de sécurité, qui couvrent les risques pesant réellement sur l'organisme,
- la justification des objectifs de sécurité à l'aide de l'appréciation des risques SSI,
- l'exhaustivité de l'étude grâce à sa démarche structurée,
- l'implication des parties prenantes, et notamment de l'autorité qui devra valider la FEROS.

## Comment rédiger une FEROS en utilisant EBIOS ?

Une solution efficace pour rédiger une FEROS consiste à :

- réaliser une étude EBIOS sur le périmètre concerné par la FEROS,
- extraire les données nécessaires dans l'étude (une grande partie de l'étude),
- réorganiser les objectifs de sécurité (à classer par exemple par domaine technique ou non technique),
- rédiger l'introduction (définition des responsabilités, agrément ou caution, évaluation, homologation, relation entre les documents, interconnexion de systèmes).

Remarque : la FEROS est avant tout un document destiné à être approuvé par une autorité, son contenu peut varier selon ce que cette autorité souhaite y voir figurer pour engager sa responsabilité.

---

<sup>1</sup> Fiche d'Expression Rationnelle des Objectifs de Sécurité des systèmes d'information (FEROS) - SGDN/SCSSI (1991).

<sup>2</sup> La sécurité des systèmes d'information qui font l'objet d'une classification de défense pour eux-mêmes ou pour les informations traitées - SGDN et DISSI (1993).

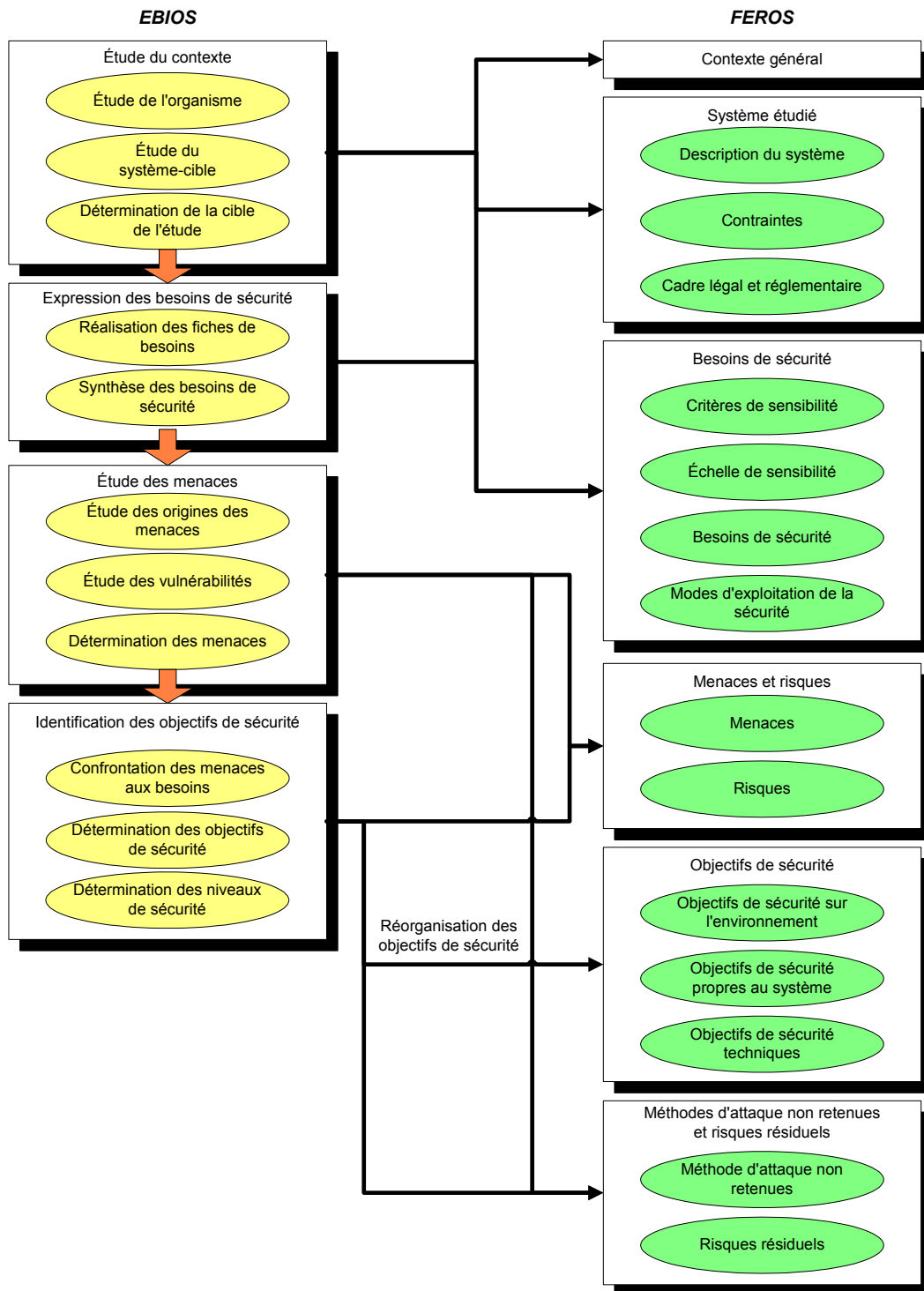
<sup>3</sup> Recommandation pour la protection des systèmes d'information traitant des informations sensibles non classifiées de défense - SGDN et DISSI (1994).

Pour cela, les activités de la méthode EBIOS sont utilisées de la manière suivante :

Activités EBIOS	Mise en œuvre dans le but de rédiger une FEROS
<p align="center"><b>ÉTAPE 1</b></p> <p align="center">Étude du contexte</p>	<p align="center">En résumé : l'étude du contexte est approfondie et pourra être complétée tout au long des travaux</p>
<p>1.1 – Étude de l'organisme</p>	<p>La description de l'organisme doit être concise et explicite afin de situer le contexte d'utilisation du système-cible.</p> <p>Les contraintes pesant sur l'organisme et les références réglementaires applicables à l'organisme doivent être listées afin d'adapter la gestion des risques à l'organisme.</p> <p>Concernant la description fonctionnelle du système d'information global de l'organisme, il peut s'agir d'une brève description des processus de l'organisme.</p>
<p>1.2 – Étude du système-cible</p>	<p>La présentation du système-cible doit être concise et précise afin de délimiter clairement le périmètre de l'étude.</p> <p>Les éléments essentiels doivent être listés et décrits précisément.</p> <p>La description fonctionnelle du système-cible doit être détaillée, claire et aussi standardisée que possible. Il est important de considérer les interfaces avec les autres systèmes d'information.</p> <p>Les enjeux doivent être listés afin d'être utiles à l'expression des besoins de sécurité.</p> <p>Le mode d'exploitation de sécurité doit être identifié parmi les hypothèses.</p> <p>Les règles de sécurité existantes (notamment une éventuelle politique de sécurité), qu'elles soient formalisées ou non, les contraintes et les références réglementaires spécifiques au système-cible doivent être listées afin d'adapter la gestion des risques au système-cible.</p>
<p>1.3 – Détermination de la cible de l'étude de sécurité</p>	<p>Cette activité doit être aussi détaillée que les spécifications le permettent. Il se peut qu'il ne soit possible de recenser que les grands types d'entités pour une première FEROS.</p>
<p align="center"><b>ÉTAPE 2</b></p> <p align="center">Expression des besoins de sécurité</p>	<p align="center">En résumé : l'expression des besoins de sécurité est détaillée et réalisée en cohérence avec l'éventuelle politique de sécurité</p>
<p>2.1 – Réalisation des fiches de besoins</p>	<p>Les critères de sécurité doivent être clairement identifiés et définis sans ambiguïté et en cohérence avec l'éventuelle politique de sécurité.</p> <p>L'échelle de besoins doit être simple, claire, bornée et non ambiguë. Elle doit être comprise et acceptée par ceux qui l'utiliseront. Elle doit aussi être cohérente avec l'éventuelle politique de sécurité.</p> <p>Les impacts peuvent utilement refléter les enjeux du système-cible. Ils doivent être cohérents avec l'éventuelle politique de sécurité.</p>

Activités EBIOS	Mise en œuvre dans le but de rédiger une FEROS
2.2 – Synthèse des besoins de sécurité	Cette activité doit permettre de déterminer les besoins de sécurité en dessous desquels il est inacceptable de descendre en termes de disponibilité, intégrité, confidentialité...
<p style="text-align: center;"><b>ÉTAPE 3</b></p> <p style="text-align: center;">Étude des menaces</p>	<p>En résumé : le niveau de détail de l'étude des menaces dépend de l'état d'avancement des spécifications</p>
3.1 – Étude des origines des menaces	<p>L'origine des menaces est étudiée en cohérence avec l'éventuelle politique de sécurité. La caractérisation des méthodes d'attaque et des éléments menaçants doit être particulièrement claire et précise. Le potentiel d'attaque de chaque élément menaçant peut être indiqué.</p> <p>La liste justifiée des méthodes d'attaque non retenues doit être réalisée.</p>
3.2 – Étude des vulnérabilités	Cette activité ne peut être réalisée que si l'état d'avancement des spécifications le permet, auquel cas elle doit être détaillée et complète.
3.3 – Formalisation des menaces	<p>La formulation des menaces est réalisée avec ou sans les vulnérabilités, selon l'état d'avancement des spécifications.</p> <p>Cette activité doit être claire (à des fins de communication) et précise. Il est préférable de formuler des menaces unitaires et spécifiques (une vulnérabilité par menace).</p>
<p style="text-align: center;"><b>ÉTAPE 4</b></p> <p style="text-align: center;">Identification des objectifs de sécurité</p>	<p>En résumé : l'identification des objectifs de sécurité doit prendre en compte l'ensemble des risques et des éléments de l'étude du contexte</p>
4.1 – Confrontation des menaces aux besoins	<p>Les risques doivent être identifiés et formulés de manière uniforme.</p> <p>Théoriquement, il ne doit pas apparaître de risques résiduels.</p>
4.2 – Formalisation des objectifs de sécurité	<p>La rédaction des objectifs de sécurité doit être claire, précise et uniforme afin de les justifier par leur contenu. Ils peuvent être classés en "objectifs de sécurité sur l'environnement", "objectifs de sécurité propres au système" et "objectifs de sécurité techniques".</p> <p>La prise en compte des contraintes, références réglementaires, hypothèses et règles de sécurité doit être démontrée.</p> <p>Les éventuels risques résiduels doivent être mis en évidence.</p>
4.3 – Détermination des niveaux de sécurité	Les niveaux de sécurité peuvent être indiqués si les potentiels d'attaque ont été déterminés.
<p style="text-align: center;"><b>ÉTAPE 5</b></p> <p style="text-align: center;">Détermination des exigences de sécurité</p>	<p>En résumé : cette étape n'est pas nécessaire à la rédaction d'une FEROS.</p>

En résumé, les données exploitables sont les suivantes :



Note : si l'étude EBIOS est livrée avec la FEROS, cette dernière peut ne constituer qu'une courte synthèse de l'étude mettant essentiellement en évidence les objectifs de sécurité et les risques résiduels.

(pour tout complément d'information : [ebios.dcssi@sgdn.pm.gouv.fr](mailto:ebios.dcssi@sgdn.pm.gouv.fr))