



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 de la méthode EBIOS[®] pour rédiger
une cible de sécurité de système d'information

Version du 25 janvier 2005

Qu'est-ce qu'une cible de sécurité SI ?

Une cible de sécurité d'un système d'information (SI) constitue la réponse de la maîtrise d'œuvre aux objectifs de sécurité identifiés par la maîtrise d'ouvrage. Elle permet à la maîtrise d'ouvrage et aux utilisateurs du SI de se rendre compte de l'adéquation du SI à leurs besoins.

La cible de sécurité d'un SI constitue l'un des éléments du dossier de sécurité qui servira à l'homologation du SI. Elle apporte en particulier une traçabilité entre les objectifs de sécurité identifiés par la maîtrise d'ouvrage et les exigences de sécurité définies par la maîtrise d'œuvre. Elle est directement utilisée en tant que spécifications à mettre en œuvre et sert de base à la rédaction des règles de sécurité de la politique de sécurité du(des) système(s) d'information (PSSI). Il s'agit d'un élément clé pour le maintien du niveau de sécurité visé tout au long du cycle de vie du SI. Elle est obligatoire dans le cadre des SI traitant des informations classifiées de défense¹.

Elle contient au minimum (dans le cas où l'étude menant aux objectifs de sécurité n'aurait pas été affinée, sinon il convient de se rapprocher du plan énoncé par l'ISO 15408) :

- la référence aux objectifs de sécurité couverts, sous la forme d'une fiche d'expression rationnelle des objectifs de sécurité² (FEROS) ou de tout autre cahier des charges,
- l'ensemble des exigences de sécurité fonctionnelles et d'assurance issues de divers référentiels ou créées de toute pièce,
- la démonstration de couverture des objectifs de sécurité par les exigences de sécurité fonctionnelles.

Quels sont les avantages de la méthode EBIOS pour la rédaction d'une cible de sécurité SI ?

Une cible de sécurité SI doit être complète et cohérente. EBIOS permet de fournir tous les éléments nécessaires à la rédaction d'une cible de sécurité SI, tout en garantissant leur cohérence. Elle offre de surcroît plusieurs avantages :

- la pertinence des exigences de sécurité couvrant les objectifs de sécurité,
- la justification des exigences à l'aide de l'appréciation des risques SSI,
- l'exhaustivité de l'étude grâce à sa démarche structurée,
- l'implication des parties prenantes (Direction, maîtrise d'ouvrage, maîtrise d'œuvre, utilisateurs...);
- le maintien du niveau de sécurité tout au long du cycle de vie du SI, en offrant la possibilité de mesurer les impacts sur l'organisation, les objectifs...

¹ *Instruction générale interministérielle sur la protection du secret de la défense nationale – N°1300 / SGDN / PSE / SSD (2003).*

² *Fiche d'Expression Rationnelle des Objectifs de Sécurité des systèmes d'information (FEROS) – SGDN / SCSSI (1991).*

Comment rédiger une cible de sécurité SI en utilisant EBIOS ?

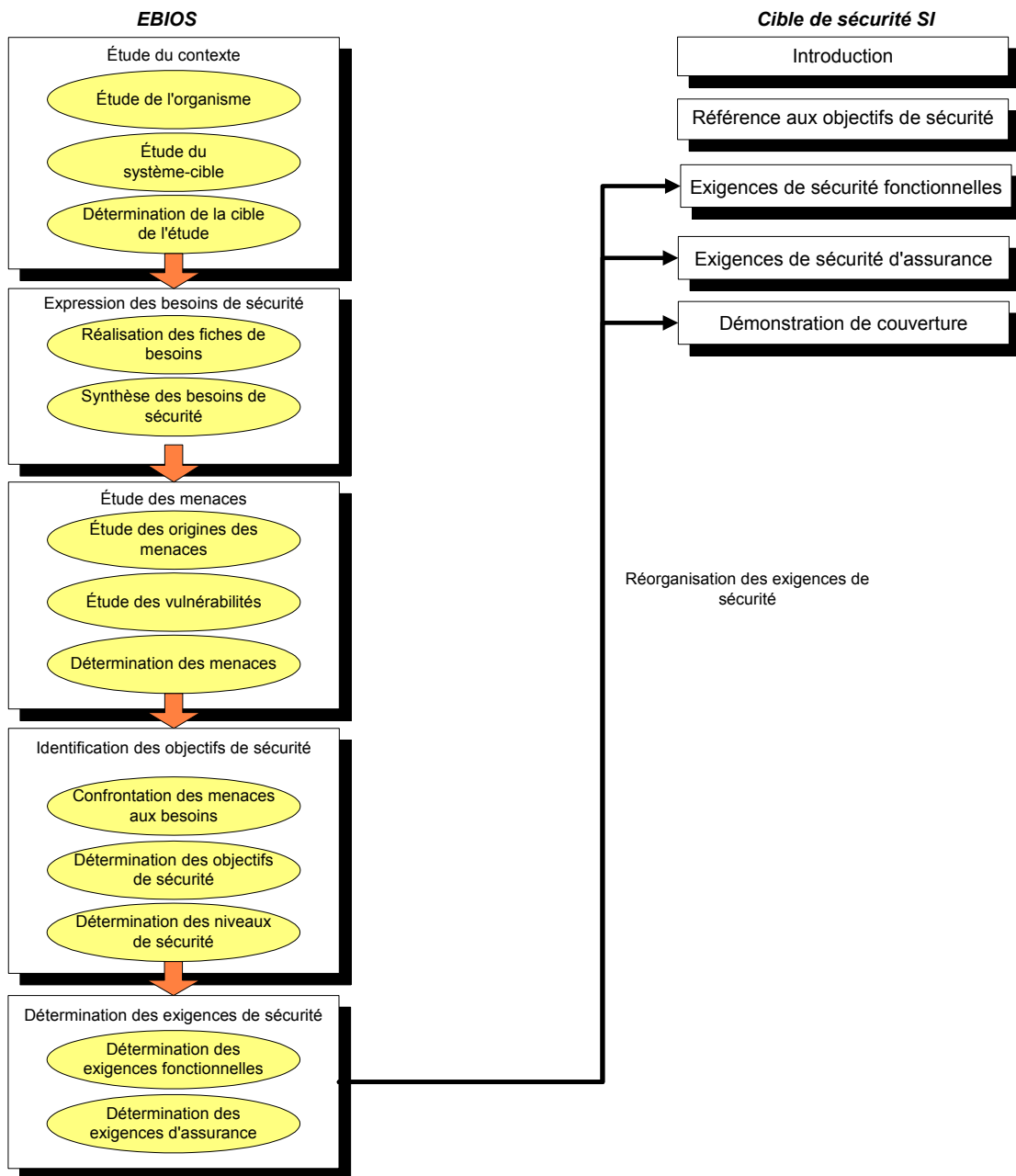
Une solution efficace pour rédiger une cible de sécurité SI consiste à :

- obtenir l'étude EBIOS portant sur le périmètre de la cible de sécurité SI et ayant permis d'identifier les objectifs de sécurité, qui peut éventuellement être affinée,
- réaliser la suite de l'étude EBIOS en déterminant les exigences de sécurité fonctionnelles couvrant les objectifs de sécurité validés et les éventuelles exigences de sécurité d'assurance requises,
- extraire les données nécessaires dans l'étude (exigences de sécurité et couverture, et ce qui a éventuellement été affiné en début d'étude),
- éventuellement réorganiser les exigences de sécurité (à classer selon leur portée),
- rédiger une introduction (identification de la cible de sécurité SI, cadre d'homologation et vue d'ensemble),
- rédiger une partie précisant la référence aux objectifs de sécurité identifiés.

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 cible de sécurité SI
ÉTAPE 1 à 4	En résumé : aucun travail supplémentaire car l'étude ne change pas jusqu'à l'identification des objectifs de sécurité, à moins que des points ne soient affinés (entités, vulnérabilités, menaces, risques, objectifs de sécurité)
ÉTAPE 5 Détermination des exigences de sécurité	En résumé : les exigences de sécurité fonctionnelles sont déterminées.
5.1 – Détermination des exigences de sécurité fonctionnelles	<p>Les exigences de sécurité fonctionnelles doivent être déterminées pour couvrir les objectifs de sécurité identifiés au niveau requis. Elles peuvent être issues de divers référentiels ou créées de toute pièce. Elles doivent être détaillées et directement applicables.</p> <p>La démonstration de couverture doit être détaillée.</p> <p>Les exigences de sécurité fonctionnelles peuvent être classées par domaine.</p>
5.2 – Détermination des exigences de sécurité d'assurance	<p>Les exigences de sécurité d'assurance doivent être déterminées si un niveau d'assurance est requis. Dans le cas contraire, elles peuvent néanmoins compléter la couverture des objectifs de sécurité.</p> <p>Elles peuvent être issues de l'ISO 15408 ou d'autres référentiels (normes nationales ou internationales, recueils de meilleures pratiques...), ou bien créées de toute pièce.</p> <p>L'argumentaire relatif aux exigences de sécurité d'assurance doit être détaillé.</p>

En résumé, les données exploitables sont les suivantes :



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