Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

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

Exploitation des résultats de la méthode EBIOS® dans le cadre d'une démarche BS 7799

Version du 21 mars 2003

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01 71 75 84 15 - Fax 01 71 75 84 00

Qu'est-ce que le BS 7799 ?

Le *British Standard* 7799 (BS 7799) est composé de deux guides, l'ISO/IEC 17799:2000 et le BS 7799-2:2002.
L'ISO/IEC 17799:2000 est un catalogue regroupant 36 objectifs de contrôle, décomposés en 127 mesures de contrôle, et relatifs à 10 domaines (politique de sécurité, sécurité du personnel, contrôle des accès…). Les objectifs de contrôle présentent un but à atteindre et ce qu'il faut entreprendre pour y parvenir. Ils sont ensuite décomposés en mesures de contrôle qui expliquent avec plus ou moins de détails les points à mettre en œuvre pour implémenter ces mesures.
Le BS 7799-2:2002 présente un système de gestion de la sécurité de l'information (*Information Security Management System - ISMS*) en quatre étapes récurrentes (planifier, mettre en œuvre, vérifier, améliorer) se rapprochant des normes de qualité ISO 9001 et ISO 14001. L'étape de planification préconise d'employer l'ISO/IEC 17799:2000.

Quels sont les avantages de la méthode EBIOS dans le cadre d'une démarche BS 7799 ?

La réalisation préalable d'une étude EBIOS offre plusieurs avantages :

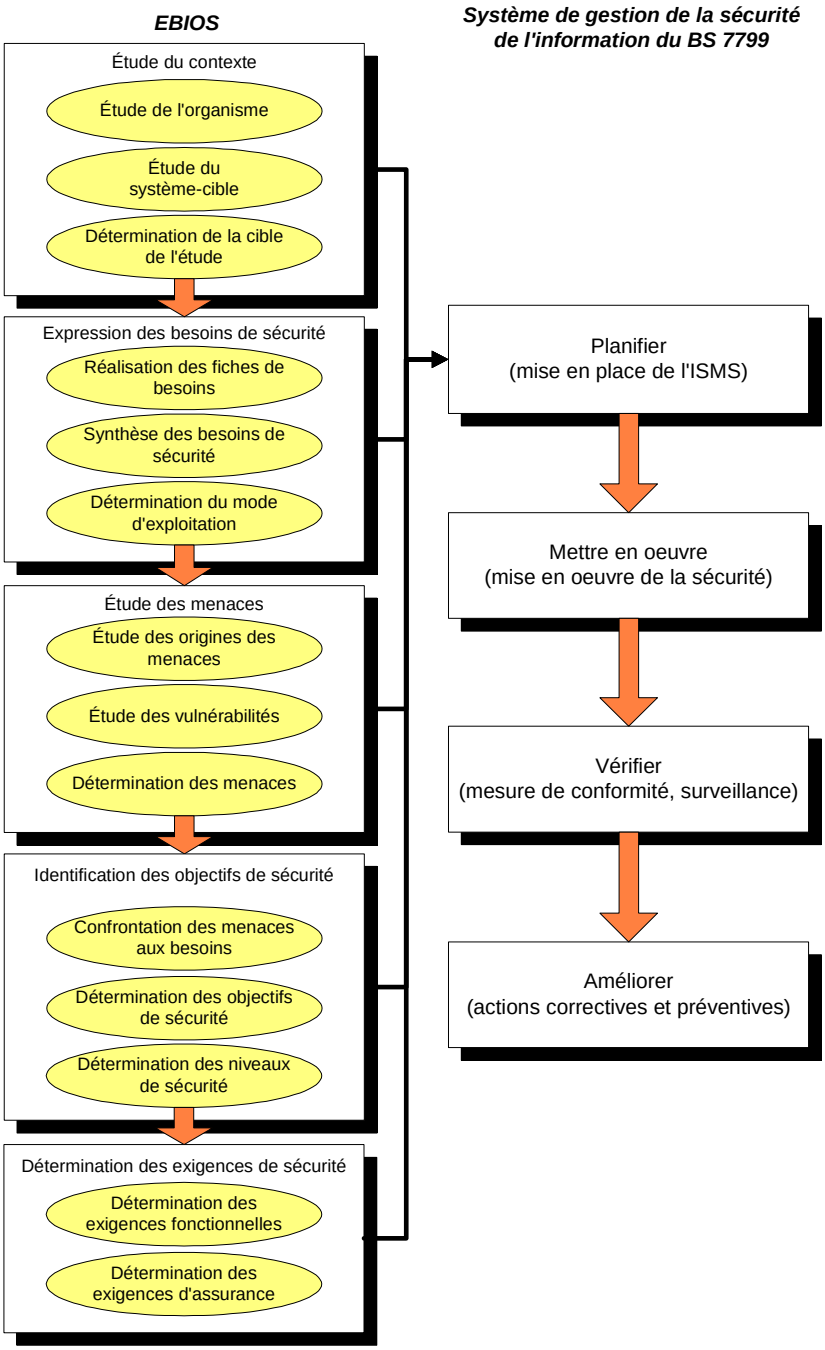
- la justification du choix des objectifs et mesures de contrôle du catalogue en fonction des besoins réels de l'organisme,
- le respect du cadre de la démarche proposée dans le BS 7799, qui préconise une appréciation des risques au préalable du choix des objectifs et mesures de contrôle,
- la fourniture de résultats réutilisables (contexte, besoins de sécurité, menaces, risques, objectifs de sécurité, exigences de sécurité) en vue des itérations ultérieures du système de gestion de la sécurité de l'information.

Comment mettre en œuvre une démarche BS 7799 en utilisant EBIOS ?

Une solution efficace pour mettre en œuvre une démarche BS 7799 consiste à :

- définir le domaine d’application du système de gestion de la sécurité de l’information (formaliser le périmètre),
- élaborer une politique de sécurité,
- réaliser une étude EBIOS globale afin d'effectuer l'analyse, l'évaluation et le traitement des risques, en choisissant les objectifs et mesures de contrôle permettant de couvrir les risques qui doivent être réduits,
- préparer une déclaration d'applicabilité,
- réaliser la suite du processus avec d'autres outils.

Pour cela, les données exploitables sont les suivantes :



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