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

Utilisation spécifique de la méthode EBIOS® pour élaborer une PSSI

Version du 22 septembre 2004

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 qu'une PSSI ?

La Politique de Sécurité des Systèmes d'Information (PSSI) est l'ensemble formalisé dans un document applicable, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection des systèmes d'information de l'organisme.

Elle traduit la reconnaissance officielle de l'importance accordée par la direction générale de l'organisme à la sécurité de ses systèmes d'information. D'une manière générale, elle contient une partie relative aux éléments stratégiques de l'organisme (périmètre, contexte, enjeux, orientations stratégiques en matière de SSI, référentiel réglementaire, échelle de sensibilité, besoins de sécurité, menaces) et une partie relative aux règles de sécurité applicables. Elle constitue donc une traduction concrète de la stratégie de sécurité de l'organisme.

Le guide PSSI édité par la DCSSI a pour objectif majeur l'accompagnement des responsables de sécurité dans l'élaboration d'une politique de sécurité d'un ou des systèmes d'information au sein de leur organisme.

Quels sont les avantages de la méthode EBIOS pour l'élaboration d'une PSSI ?

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

- l'élaboration de la PSSI est facilitée par une démarche structurée, qui permet en outre de déduire en les justifiant une partie des principes et des règles retenus dans la PSSI ;
- l'exploitation des résultats de l'étude EBIOS associée à d'autres éléments d'entrée, permet d'obtenir l'ensemble des éléments stratégiques, de choisir les principes et d'élaborer les règles de sécurité ;
- les différents acteurs du SI (décideurs, responsables SSI, maîtrise d'œuvre, maîtrise d'ouvrage, acteurs financiers, utilisateurs…) sont déjà sensibilisés à la SSI, notamment aux risques SSI et au fait que la sécurité organisationnelle constitue une part importante de la sécurité globale.

Comment élaborer une PSSI en utilisant EBIOS ?

Une solution efficace pour élaborer une PSSI consiste à :

- organiser le projet PSSI ;
- réaliser une étude EBIOS globale ;
- extraire les données nécessaires dans l'étude EBIOS (essentiellement dans l'étude du contexte, l'expression des besoins de sécurité et l'étude des menaces) ;
- réaliser les dernières tâches évoquées dans le guide PSSI :
    - choix des principes de sécurité et élaboration des règles de sécurité, facilités par l'exploitation des objectifs et exigences de sécurité issus de l'étude EBIOS,
    - élaboration des notes de synthèse,
    - finalisation et validation de la PSSI,
    - élaboration et validation du plan d'action.

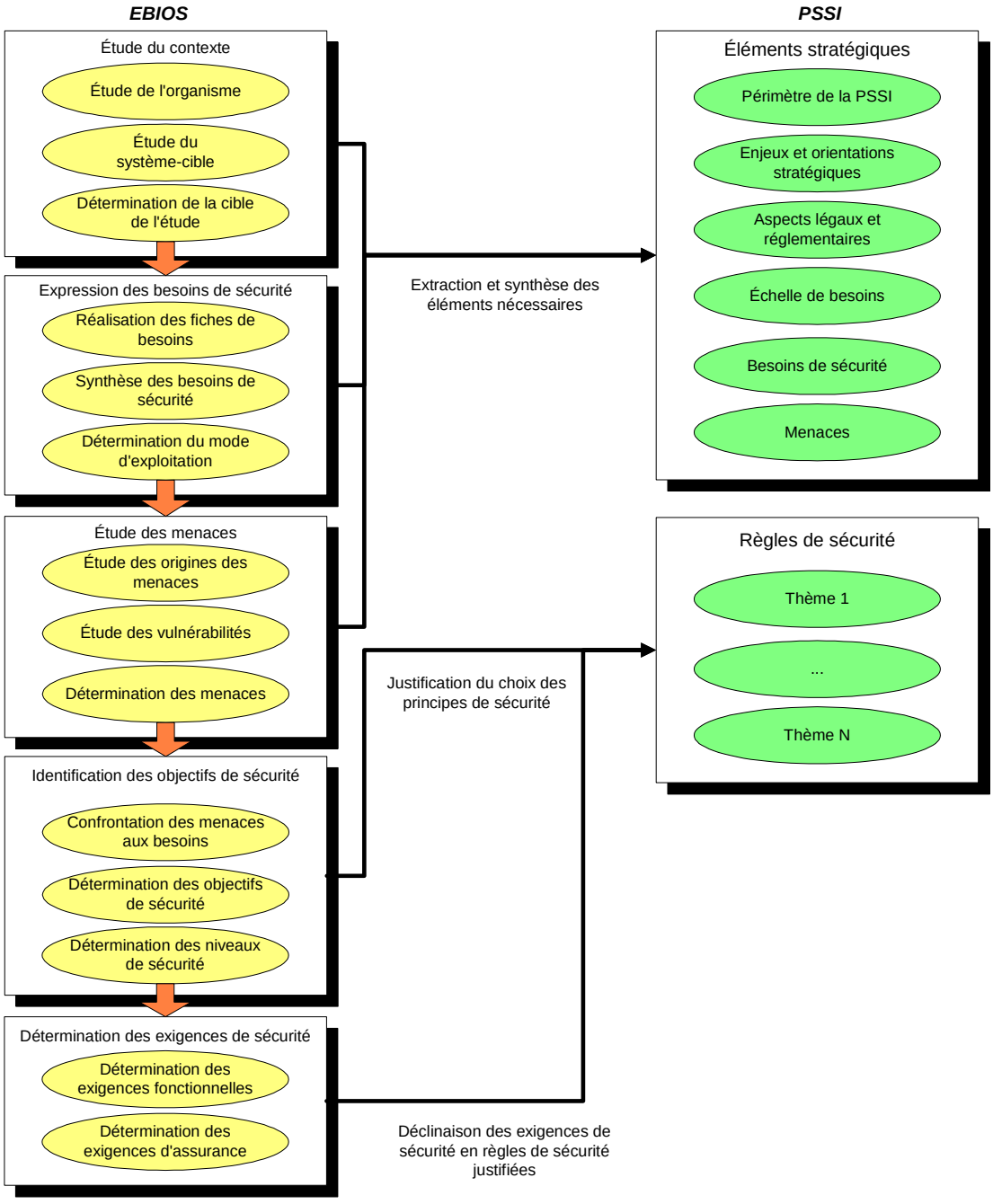
Pour cela, les activités de la méthode EBIOS sont utilisées de la manière suivante :

Activités EBIOS	Mise en œuvre dans le but d'élaborer une PSSI
ÉTAPE 1 Étude du contexte	En résumé : l'étude du contexte est approfondie et figurera dans la note de stratégie de sécurité de la PSSI
1.1 – Étude de l'organisme	L'activité doit être détaillée et complète. Elle s'adaptera à l'objet de la PSSI et à la nature de l'organisme. Elle doit servir à identifier clairement les différents processus et fonctions présentes et les contraintes générales afin d'assurer la meilleure définition du système-cible. Il est essentiel de ne pas omettre les références réglementaires et légales ainsi que les normes que l'organisation doit respecter.
1.2 – Étude du système-cible	L'activité doit être détaillée et complète. Les enjeux doivent être définis et évalués afin de pouvoir éventuellement classer le(s) système-cible(s) (les uns) par rapport aux autres et indiquer la place qu'occupe le système-cible en terme de continuité d'entreprise. Ne seront retenus que les éléments véritablement essentiels. Il importe que la description du système-cible soit claire, concise et aussi standardisée que possible. La définition des hypothèses, règles de sécurité et références réglementaires ainsi que les contraintes est indispensable pour disposer d'un contexte complet et adéquat. Il est important de considérer les interfaces avec les autres systèmes d'information. S'il s'agit d'une PSSI globale d'organisme, les éléments essentiels considérés pourront être les domaines d'activités et les processus majeurs de l'entreprise.
1.3 – Détermination de la cible de l'étude de sécurité	Cette activité contribue à la détermination des objectifs et exigences de sécurité, qui serviront à la rédaction des règles de sécurité. Les principales entités (ou types d'entités) sont décrites et croisées avec les éléments essentiels.

Activités EBIOS	Mise en œuvre dans le but d'élaborer une PSSI
ÉTAPE 2 Expression des besoins de sécurité	En résumé : l'échelle de besoins est détaillée et figurera dans la note de stratégie de sécurité de la PSSI
2.1 – Réalisation des fiches de besoins	L'activité doit être détaillée, complète et enrichie d'exemples issus de l'organisme. Ses résultats seront intégrés dans la note de stratégie de sécurité de la PSSI. Les critères de sécurité, l'échelle de besoins et les impacts choisis devraient être les mêmes pour l'ensemble des PSSI de l'organisation.
2.2 – Synthèse des besoins de sécurité	Une synthèse de cette activité pourra enrichir la note de stratégie de sécurité de la PSSI. Elle précisera les besoins de sécurité généraux en dessous desquels il est inacceptable de descendre. Il peut s'avérer utile de compléter totalement les fiches d'expression des besoins de sécurité (et non de remplir uniquement les valeurs finales) afin de bien mettre en évidence le lien entre les éléments essentiels et les impacts, ainsi que l'importance relative des impacts.
ÉTAPE 3 Étude des menaces	En résumé : l'origine des menaces est détaillée et figurera dans la note de stratégie de sécurité de la PSSI, l'étude des vulnérabilités contribuera davantage à la suite de la PSSI
3.1 – Étude des origines des menaces	L'activité doit être détaillée et complète. La caractérisation des méthodes d'attaque et des éléments menaçants doit être particulièrement claire et précise. Le potentiel d'attaque de chaque élément menaçant doit être indiqué, explicité et justifié. La liste justifiée des méthodes d'attaque non retenues doit être réalisée.
3.2 – Étude des vulnérabilités	Cette activité contribue à la détermination des objectifs et exigences de sécurité, qui serviront à la rédaction des règles de sécurité. Elle peut ne pas être réalisée dans le cas d'une PSSI globale. Toutes les vulnérabilités pertinentes doivent être relevées, qu'elles soient avérées ou non. L'échelle éventuellement utilisée pour les niveaux de vulnérabilité devrait être la même pour l'ensemble des PSSI de l'organisation.
3.3 – Formalisation des menaces	Cette activité contribue à la détermination des objectifs et exigences de sécurité, qui serviront à la rédaction des règles de sécurité. Elle doit être claire (à des fins de communication) et précise. Il est préférable de formuler des menaces unitaires et spécifiques (une vulnérabilité par menace). La hiérarchisation des menaces peut être utile dans le but de déterminer des priorités de traitement.

Activités EBIOS	Mise en œuvre dans le but d'élaborer une PSSI
ÉTAPE 4 Identification des objectifs de sécurité	En résumé : les objectifs de sécurité sont factorisés et figureront dans la note de stratégie de sécurité, ils constituent une aide au choix et à la justification des principes et règles retenus
4.1 – Confrontation des menaces aux besoins	Cette activité contribue à la détermination des objectifs et exigences de sécurité, qui serviront à la rédaction des règles de sécurité. Les risques doivent être identifiés et formulés de manière uniforme. Ils doivent également être hiérarchisés afin de déterminer des priorités de traitement et les éventuels risques résiduels doivent être mis en évidence.
4.2 – Formalisation des objectifs de sécurité	Dans la mesure du possible, les objectifs de sécurité doivent être factorisés pour enrichir les axes stratégiques de la note de stratégie de sécurité de la PSSI. La rédaction des objectifs de sécurité doit être claire, précise et uniforme afin de les justifier par leur contenu. Les éventuels risques résiduels doivent être mis en évidence.
4.3 – Détermination des niveaux de sécurité	Cette activité contribue à la détermination des exigences de sécurité, qui serviront à la rédaction des règles de sécurité. Elle peut ne pas être réalisée dans le cas d'une PSSI globale. Les niveaux de sécurité doivent être explicites et dûment justifiés.
ÉTAPE 5 Détermination des exigences de sécurité	En résumé : les exigences de sécurité fonctionnelles et d'assurance pourront directement constituer des règles de sécurité de la PSSI, elles seront éventuellement complétées par d'autres règles, élaborées en réponse à des besoins non couverts par l'étude EBIOS.
5.1 – Détermination des exigences de sécurité fonctionnelles	Idéalement, les exigences de sécurité fonctionnelles doivent être spécifiques (un acteur, un domaine à la fois), mesurables (définition du moyen de contrôle), atteignables (éventuellement en plusieurs étapes, en donnant les ressources nécessaires), réalistes (en fonction des acteurs, de leurs capacités) et liés au temps (il y a une date buttoir, un délai, une période définie). Une fois triées, elles pourront constituer directement une partie des règles de sécurité de la PSSI. Les éventuels risques résiduels doivent être mis en évidence. Les exigences de sécurité devraient être classées selon les domaines couverts par la PSSI.
5.2 – Détermination des exigences de sécurité d'assurance	Dans la mesure du possible, les exigences de sécurité d'assurance doivent être spécifiques (un acteur, un domaine à la fois), mesurables (définition du moyen de contrôle), atteignables (éventuellement en plusieurs étapes, en donnant les ressources nécessaires), réalistes (en fonction des acteurs, de leurs capacités) et liés au temps (il y a une date buttoir, un délai, une période définie). Une fois triées, elles pourront constituer directement une partie des règles de sécurité de la PSSI.

En résumé, les données exploitables sont les suivantes :



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