



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

Mettre en place un
Système de Gestion de la Sécurité
des Systèmes d'Information (SGSSI)
à l'aide de la méthode EBIOS

MÉMENTO

Version du 10 novembre 2005

Introduction

La sécurité des systèmes d'information (SSI) doit être considérée globalement afin d'éviter d'omettre de prendre en compte des risques qui pourraient avoir un impact inacceptable sur les activités de l'organisme.

Cela signifie qu'il convient évidemment de considérer les questions techniques (logiciels, matériels, réseaux) et les questions non techniques (organisations, sites, personnels).

Il convient également d'intégrer la SSI tout au long du cycle de vie des systèmes d'information (étude d'opportunité, étude de faisabilité, conception générale, conception détaillée, réalisation et exploitation jusqu'à la fin de vie du système).

Par ailleurs, il convient, dans un principe de défense en profondeur, de considérer les événements et mesures à mettre en œuvre avant un sinistre (prévision et préparation, dissuasion), pendant (protection, détection, confinement, "lutte") et après (récupération, restauration, compensation).

Enfin, il convient d'impliquer tous les personnels (décideurs, maîtrise d'ouvrage, maîtrise d'œuvre, métiers, opérationnels, utilisateurs...) afin d'augmenter la culture de sécurité de l'organisme.

Cette vision globale est nécessaire à la mise en place d'un véritable Système de Gestion de la Sécurité des Systèmes d'Information (SGSSI) qui permettra de planifier, mettre en œuvre, vérifier et améliorer la SSI, et ce, de manière itérative.

Le processus continu de gestion des risques SSI est au cœur du SGSSI. Les risques doivent être appréciés (mis en évidence et hiérarchisés) pour être traités (refusés, optimisés, transférés ou pris). Le traitement des risques peut alors faire l'objet d'une homologation de sécurité. La communication relative aux risques représente l'échange ou le partage d'informations nécessaire concernant les risques.

La gestion des risques SSI permet de réaliser la planification, de servir de base à la mise en œuvre et à la vérification et de gérer l'amélioration continue du SGSSI.

Il conviendra d'adapter le SGSSI au niveau de maturité SSI de l'organisme, à son processus d'homologation et à son référentiel SSI. En effet, les actions et livrables SSI doivent correspondre d'une part aux pratiques dont l'organisme est capable et dont il a théoriquement besoin au regard des enjeux de sécurité, et d'autre part aux éléments composant les dossiers de sécurité des systèmes d'information de l'organisme.

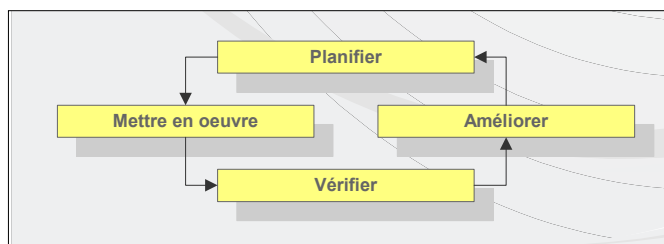
Ce mémento a pour objectif d'expliquer en quoi EBIOS est utile à la mise en place d'un SGSSI et comment utiliser spécifiquement la méthode dans ce cadre

Qu'est-ce qu'un SGSSI ?

La mise en œuvre de la démarche de l'ISO 27001

La norme internationale ISO 27001 spécifie un Système de Gestion de la Sécurité des Systèmes d'Information (SGSSI) / *Information Security Management System (ISMS)*.

Ce SGSSI est structuré en quatre étapes récurrentes (planifier, mettre en œuvre, vérifier, améliorer), afin de respecter le principe de la roue de Deming, issue du monde de la qualité. Ce concept permet d'établir un parallèle avec les normes relatives aux systèmes de management de la qualité (ISO 9001) et de l'environnement (ISO 14001).



Étapes	Objectifs
Planifier	<ul style="list-style-type: none"> Définir le cadre du SGSSI Formaliser les bases de la SSI Apprécier les risques SSI Spécifier le traitement des risques SSI retenus
Mettre en œuvre	Implémenter et maintenir les mesures (traiter les risques SSI)
Vérifier	<ul style="list-style-type: none"> Vérifier que les mesures mises en place pour traiter les risques SSI fonctionnent conformément à ce qui a été prévu lors de l'étape de planification Identifier les améliorations possibles du SGSSI
Améliorer	Mettre en œuvre les améliorations identifiées pour le SGSSI

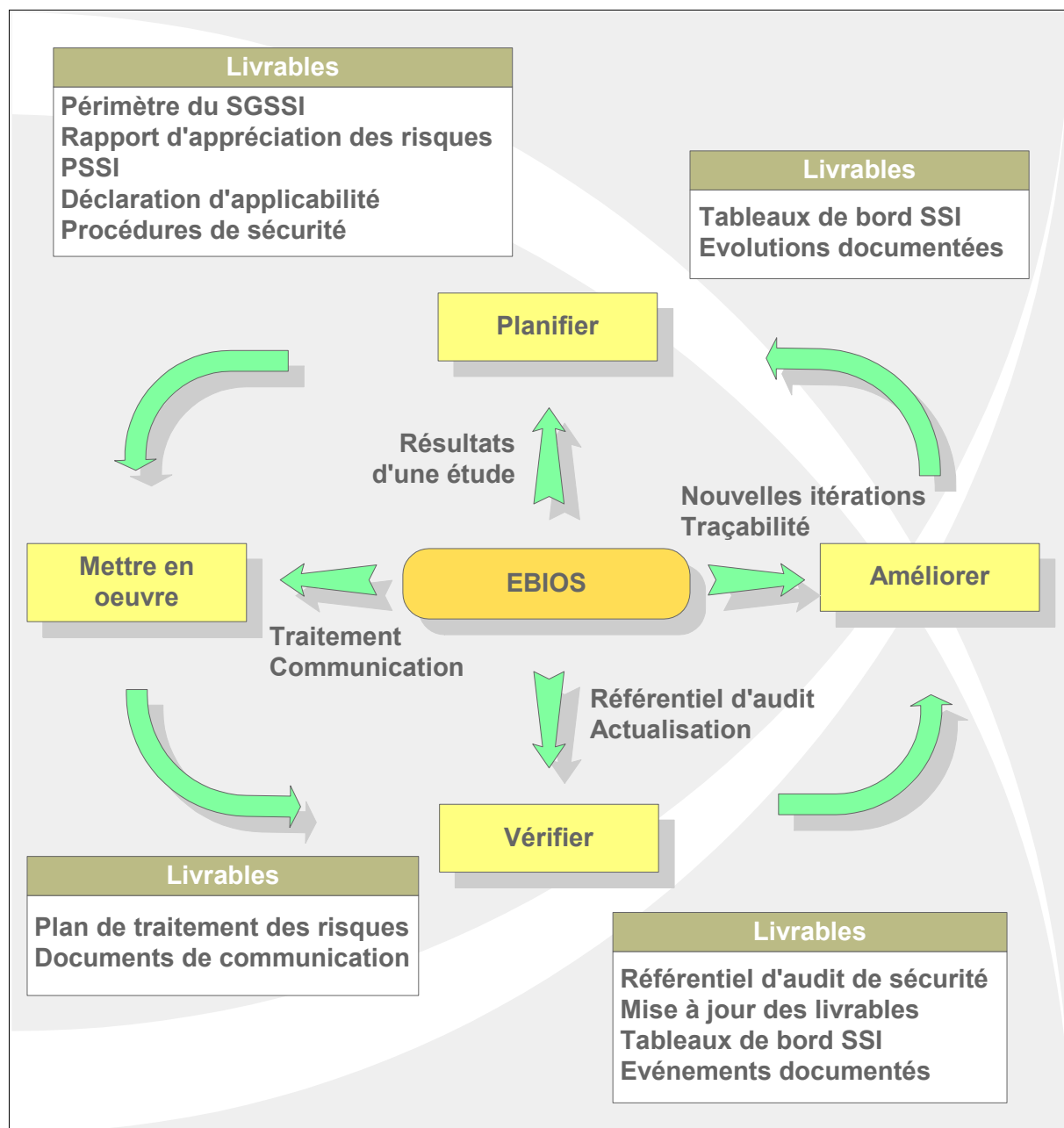
L'exploitation des meilleures pratiques de l'ISO 17799

Pour opérer ce SGSSI, l'ISO 27001 préconise d'employer son annexe A ou l'ISO 17799 pour identifier les mesures de sécurité à mettre en œuvre au cours de l'étape de planification.

La norme internationale ISO 17799 est un guide de bonnes pratiques regroupant 39 objectifs de sécurité, décomposés en 133 mesures de sécurité, et relatifs à 11 domaines (politique de sécurité, sécurité du personnel, contrôle des accès...). Les objectifs de sécurité présentent un but à atteindre et les mesures de sécurité présentent les activités permettant d'y parvenir, expliquant les actions à mettre en œuvre pour implémenter ces mesures.

EBIOS est au cœur de la mise en œuvre du SGSSI

EBIOS intervient principalement dans la première étape du SGSSI (planifier), mais également dans les trois étapes suivantes (mettre en œuvre, vérifier, améliorer), comment le présente le schéma suivant :



Les tableaux des pages suivantes présentent les apports de la méthode EBIOS pour chaque action du SGSSI.

Étape 1 – Planifier

EBIOS est indispensable à cette étape dont elle supporte efficacement l'ensemble des actions :

Actions du SGSSI	Apports de la méthode EBIOS
a) Définir le périmètre	L'étape 1 (Étude du contexte) décrit clairement l'organisme (structure, enjeux, contraintes), les entités (matériels, logiciels, réseaux, organisations, locaux, personnels), les éléments essentiels (informations, fonctions)...
b) Définir la politique de sécurité du(des) système(s) d'information (PSSI)	<p>Une étude EBIOS permet d'élaborer une PSSI</p> <p>Élaborer une PSSI sans étude des risques produit un résultat moins pertinent, donc une base de mise en œuvre du SGSSI susceptible de générer des dérives et de nuire à son efficacité</p> <p><i>La méthode PSSI diffusée par la DCSSI constitue un complément utile</i></p>
c) Définir l'approche d'appréciation des risques SSI	<p><i>Il convient tout d'abord de faire valider l'utilisation de la méthode EBIOS</i></p> <p>EBIOS permet de définir non seulement une échelle de besoins de sécurité et une liste d'impacts inacceptables pour l'organisme, mais aussi une échelle d'opportunité de la menace qui permettront de qualifier et hiérarchiser les risques</p>
d) Identifier les risques SSI	<p>Les étapes 1 (Étude du contexte), 2 (Expression des besoins de sécurité) et 3 (Étude des menaces) de la démarche EBIOS correspondent à cette action</p> <ol style="list-style-type: none"> 1. Étude du contexte : les biens sont identifiés en distinguant les entités (logiciels, matériels, réseaux, organisations, locaux et personnels) des éléments essentiels (patrimoine informationnel) 2. Expression des besoins de sécurité : les besoins de sécurité des éléments essentiels sont exprimés en termes de disponibilité, intégrité, confidentialité... en lien avec les impacts sur l'organisme 3. Étude des menaces : les méthodes d'attaque (événements), les éléments menaçants (origines) et les vulnérabilités sont caractérisés

Actions du SGSSI	Apports de la méthode EBIOS
e) Analyser et évaluer les risques SSI	<p>EBIOS permet de mettre en évidence les besoins de sécurité touchés et les impacts sur l'organisme en confrontant les éléments précédemment identifiés</p> <p>Dans l'étape 2 (Expression des besoins de sécurité), la manière dont les besoins de sécurité sont exprimés permet d'identifier un ensemble de risques avec un impact inacceptable pour l'organisme</p> <p>L'étape 3 (Étude des menaces) prend en compte les mesures de sécurité existantes</p> <p>Les risques sont hiérarchisés dans l'étape 4 (Identification des objectifs de sécurité) selon leur niveau d'opportunité et l'atteinte maximale des besoins de sécurité</p>
f) Identifier et évaluer les options pour traiter les risques SSI	<p>Les étapes 4 (Identification des objectifs de sécurité) et 5 (Détermination des exigences de sécurité) correspondent au traitement des risques SSI (refus, optimisation, transfert ou prise de risque)</p>
g) Sélectionner les objectifs et mesures de sécurité pour traiter les risques SSI	<p>Le traitement des risques SSI à l'aide de la méthode EBIOS permet de sélectionner les objectifs et mesures de sécurité issus de l'annexe A de l'ISO 27001 ou de l'ISO 17799 en prenant en compte les références réglementaires et en justifiant les choix effectués</p>
h) Obtenir la validation des risques résiduels	<p>L'étude EBIOS inclut la démonstration de couverture des risques par des objectifs de sécurité (objectifs de sécurité) et de ces objectifs de sécurité par des exigences de sécurité (mesures de sécurité), mettant ainsi en évidence les éventuels risques résiduels</p>
i) Obtenir l'autorisation de mettre en œuvre et d'exploiter le SGSSI	<p>L'étude EBIOS fournit tous les éléments nécessaires à la prise de décision (sous forme de FEROS, de cible de sécurité, de PSSI...), notamment la description précise du périmètre, les enjeux, les contraintes et références réglementaires à prendre en compte, l'appréciation et le traitement des risques menés de façon argumentée</p> <p><i>Cette action constitue une "homologation" sur la base d'un dossier de sécurité (expression des objectifs de sécurité de la maîtrise d'ouvrage, réponse de la maîtrise d'œuvre sous la forme d'une cible de sécurité...)</i></p>
j) Préparer une déclaration d'applicabilité	<p>L'étude EBIOS fournit les informations et argumentaires nécessaires à l'élaboration d'une déclaration d'applicabilité</p> <p>La justification des objectifs et mesures de sécurité écartés est obtenue par les démonstrations de couverture des risques et des objectifs de sécurité</p>

Étape 2 – Mettre en œuvre

Lors de cette étape, EBIOS contribue à l'élaboration du plan de traitement des risques et à la communication relative aux risques :

Actions du SGSSI	Apports de la méthode EBIOS
a) Formuler un plan de traitement des risques SSI	L'étude EBIOS fournit non seulement une hiérarchie des risques SSI, mais aussi des spécifications pour les traiter
b) Mettre en œuvre le plan de traitement des risques SSI	L'emploi d'une démarche structurée telle que celle de la méthode EBIOS permet d'élaborer un plan de traitement des risques cohérent et applicable
c) Mettre en œuvre les mesures de sécurité	<i>La méthode d'élaboration et de mise en œuvre de tableaux de bord SSI (TDBSSI), diffusée par la DCSSI, permet de suivre la mise en œuvre des mesures de sécurité</i>
d) Définir comment mesurer l'efficacité des mesures de sécurité	<i>La méthode d'élaboration et de mise en œuvre de tableaux de bord SSI (TDBSSI), diffusée par la DCSSI, est particulièrement indiquée à cet effet</i>
e) Mettre en œuvre les programmes de sensibilisation et de formation	La traçabilité requise par EBIOS contribue à l'élaboration d'une communication adaptée relative aux risques SSI pertinents Mener une étude EBIOS impliquant de nombreux acteurs (décideurs, maîtrise d'ouvrage, maîtrise d'œuvre, propriétaires de données...) contribue à mettre en place et améliorer la culture de sécurité dans l'organisme
f) Gérer les opérations	<i>Pas d'apport spécifique d'EBIOS au cours de cette action</i>
g) Gérer les ressources	<i>Pas d'apport spécifique d'EBIOS au cours de cette action</i>
h) Mettre en œuvre les procédures et autres mesures pour détecter et réagir face aux incidents de sécurité	<i>Pas d'apport spécifique d'EBIOS au cours de cette action</i>

Étape 3 – Vérifier

EBIOS fournit le référentiel d'audit et est réactualisée pour mettre à jour le niveau des risques :

Actions du SGSSI	Apports de la méthode EBIOS
a) Exécuter les procédures de vérification et autres mesures	<i>Pas d'apport spécifique d'EBIOS au cours de cette action</i>
b) Vérifier régulièrement la performance du SGSSI	<i>Pas d'apport spécifique d'EBIOS au cours de cette action</i>
c) Mesurer l'efficacité des mesures de sécurité	<i>La méthode d'élaboration et de mise en œuvre de tableaux de bord SSI (TDBSSI), diffusée par la DCSSI, fournit un support dans la mesure de l'efficacité des mesures de sécurité</i>
d) Vérifier régulièrement l'appréciation des risques, ainsi que le niveau du risque résiduel et du risque acceptable	<p>La mise à jour d'une étude EBIOS permet de réaliser cette action en prenant en compte tous les changements dans le périmètre du SGSSI</p> <p>Cela permet également de disposer d'une méthode itérative autorisant la traçabilité de tous les éléments considérés dans l'étude</p>
e) Mener des audits internes réguliers du SGSSI	<p>L'étape 5 (Détermination des exigences de sécurité) fournit des spécifications détaillées permettant de mener les audits internes</p> <p>L'emploi d'une méthode itérative facilite l'exploitation des résultats des audits et le suivi des éléments considérés dans l'audit (traçabilité)</p>
f) Vérifier régulièrement le management du SGSSI	<i>Pas d'apport spécifique d'EBIOS au cours de cette action</i>
g) Mettre à jour les plans de sécurité pour prendre en compte les résultats des actions précédentes	La mise à jour d'une étude EBIOS, notamment de l'étude des vulnérabilités et de la détermination des exigences de sécurité, permet de prendre en compte les améliorations identifiées
h) Enregistrer les actions et événements pouvant impacter la performance du SGSSI	Le formalisme de la méthode EBIOS facilite l'enregistrement des biens, des risques et des mesures de sécurité sélectionnées, susceptibles d'impacter la performance du SGSSI

Étape 4 – Améliorer

L'exploitation des résultats actualisés de l'étude EBIOS contribue à l'amélioration du SGSSI :

Actions du SGSSI	Apports de la méthode EBIOS
a) Mettre en œuvre les améliorations identifiées pour le SGSSI	La réitération de la méthode permet de sélectionner des mesures de sécurité pertinentes au vu des résultats des audits et des études des risques initiales et courantes
b) Prendre les mesures correctives et préventives appropriées	L'étude EBIOS fournit non seulement une hiérarchie des risques SSI, mais aussi des spécifications pour les traiter <i>La méthode d'élaboration et de mise en œuvre de tableaux de bord SSI (TDBSSI), diffusée par la DCSSI, contribue à cette action en assurant la cohérence entre les indicateurs et l'amélioration des exigences de sécurité</i>
c) Communiquer les résultats et actions, consulter les parties prenantes	La traçabilité requise par EBIOS contribue à l'élaboration d'une communication adaptée relative aux risques SSI pertinents <i>La méthode d'élaboration et de mise en œuvre de tableaux de bord SSI (TDBSSI), diffusée par la DCSSI, contribue à cette action</i>
d) S'assurer que les révisions réalisent leurs objectifs prévus	<i>La méthode d'élaboration et de mise en œuvre de tableaux de bord SSI (TDBSSI), diffusée par la DCSSI, contribue à cette action</i>

Utilisation spécifique d'EBIOS

Dans le cadre de la mise en œuvre d'un SGSSI, les activités de la méthode EBIOS sont utilisées de la manière suivante :

Activités EBIOS	Spécificités dans le cadre de la mise en œuvre d'un ISMS
ÉTAPE 1 Étude du contexte	Le niveau de détail de l'étude du contexte doit être cohérent avec le périmètre et la finalité de l'étude
1.1 – Étude de l'organisme	Le niveau de détail de cette activité doit être cohérent avec le périmètre et la finalité de l'étude
1.2 – Étude du système-cible	Si le périmètre est large (ex. organisme entier), les éléments essentiels étudiés peuvent être uniquement des processus (et non de fonctions et informations), selon le niveau de détail requis
1.3 – Détermination de la cible de l'étude de sécurité	Si le périmètre est large, il est difficile de recenser les entités de manière détaillée ; il convient de ne recenser que les types d'entités
ÉTAPE 2 Expression des besoins de sécurité	L'expression des besoins de sécurité doit faciliter l'évaluation des risques SSI, l'identification de mesures pertinentes, leur mise en œuvre et la vérification de leur efficacité
2.1 – Réalisation des fiches de besoins	L'activité doit être réalisée en impliquant de nombreux acteurs (utilisateurs, maîtrises d'ouvrage, décideurs...) pour les sensibiliser aux valeurs relatives des éléments essentiels, améliorer leur compréhension de l'étude, les faire adhérer aux résultats auxquels ils contribuent et les responsabiliser au travers des choix qu'ils font
2.2 – Synthèse des besoins de sécurité	Les besoins de sécurité doivent systématiquement représenter les valeurs limites acceptables dans l'échelle de besoins Pour chaque besoin de sécurité exprimé, il convient d'affiner les impacts concrets pesant sur l'organisme
ÉTAPE 3 Étude des menaces	L'étude des menaces est complète mais peu détaillée
3.1 – Étude des origines des menaces	Les méthodes d'attaques retenues doivent être listées et caractérisées par les critères de sécurité qu'elles peuvent affecter ; celles qui sont écartées doivent être listées avec des justifications Les éléments menaçants doivent être décrits, soit de manière générique, soit par méthode d'attaque
3.2 – Étude des vulnérabilités	Les vulnérabilités doivent être identifiées de manière générique et caractérisées par un niveau
3.3 – Formalisation des menaces	Un tableau listant les méthodes d'attaques et les vulnérabilités susceptibles de les exploiter (sans les grouper afin de faciliter le traitement des risques) suffit à présenter les menaces

Activités EBIOS	Mise en œuvre dans le cadre du BS 7799
<p>ÉTAPE 4 Identification des objectifs de sécurité</p>	<p>L'identification des objectifs de sécurité référence clairement les risques et permet de sélectionner les objectifs de sécurité de l'annexe A de l'ISO 27001 ou de l'ISO 17799</p>
<p>4.1 – Confrontation des menaces aux besoins</p>	<p>Les risques doivent être déterminés, formalisés et hiérarchisés selon le niveau maximal de besoins de sécurité concernés et l'opportunité. Les impacts sur l'organisme doivent être mis en évidence.</p>
<p>4.2 – Formalisation des objectifs de sécurité</p>	<p>Les objectifs de sécurité doivent être choisis parmi les objectifs de sécurité de l'annexe A de l'ISO 27001 ou l'ISO 17799 et classés selon le même plan de la norme. La couverture des risques SSI et des éléments du contexte doit être démontrée et les risques résiduels doivent être mis en évidence.</p>
<p>4.3 – Détermination des niveaux de sécurité</p>	<p>Cette activité n'est possible qu'après estimation du potentiel d'attaque des éléments menaçants, un niveau de résistance pouvant alors être déterminé pour chaque objectif de sécurité. Il n'est pas nécessaire de déterminer un niveau d'assurance sécurité.</p>
<p>ÉTAPE 5 Détermination des exigences de sécurité</p>	<p>La détermination des exigences de sécurité exploite les mesures de sécurité de l'annexe A de l'ISO 27001 ou de l'ISO 17799</p>
<p>5.1 – Détermination des exigences de sécurité fonctionnelles</p>	<p>Les exigences de sécurité doivent être choisies parmi les mesures de sécurité de l'annexe A de l'ISO 27001 ou de l'ISO 17799 correspondant aux objectifs de sécurité retenus et classés selon le plan de la norme. Il convient ensuite de les affiner et de les personnaliser afin qu'elles soient spécifiques (un acteur, un domaine à la fois), mesurables (définition du moyen de contrôle), atteignables (éventuellement en plusieurs étapes, selon les ressources disponibles), réalistes (en fonction des acteurs, de leurs capacités) et délimitées dans le temps (fixer une date butoir, un délai, une période définie). La couverture des objectifs de sécurité doit être démontrée et les risques résiduels doivent être mis en évidence.</p>
<p>5.2 – Détermination des exigences de sécurité d'assurance</p>	<p>La notion de niveau d'assurance sécurité n'est pas pertinente dans le contexte d'un SGSSI. Cette activité EBIOS n'est donc pas requise dans le cadre d'une démarche SGSSI.</p>

Ces activités doivent être réalisées une première fois lors de la première étape du SGSSI (planifier), revues lors de la troisième étape (vérifier) et à chaque itération du cycle complet (planifier, mettre en œuvre, vérifier, améliorer).

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