



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® pour rédiger un SSRS

Version du 21 novembre 2006

Ce document a été réalisé avec le Club EBIOS

Responsables des travaux :

- Cyril DEMONCEAUX (SGDN – Secrétariat général de la défense nationale)

Contributeurs :

- Bertrand FIVEL-DEMORET (ZENSI)
- Jean-Louis FLEISCH (FLH CONSEIL)
- Frédéric GARNIER (SGCUE – Secrétariat général du Conseil de l'Union européenne)
- Matthieu GRALL (SGDN – Secrétariat général de la défense nationale)
- Raphaël GUERAND (SGDN – Secrétariat général de la défense nationale)
- Alain HUITRIC (DGA – Délégation générale pour l'armement)
- Hugh JOURNEAU (SGDN – Secrétariat général de la défense nationale)
- Jean-Pierre LEBEE (DGA – Délégation générale pour l'armement)
- Serge LEBEL (SGDN – Secrétariat général de la défense nationale)
- Pierrick LE PORT (Ministère de la Défense)
- Franck ROUSSET (OTAN – Organisation du traité de l'Atlantique Nord)
- François-Xavier VINCENT (SGDN – Secrétariat général de la défense nationale)
- Franck YVELIN (SGDN – Secrétariat général de la défense nationale)

Les commentaires et suggestions sont encouragés et peuvent être adressés à l'adresse suivante
(voir formulaire de recueil de commentaires en fin de document) :

Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil
51 boulevard de La Tour-Maubourg
75700 PARIS 07 SP

ebios.dcssi@sgdn.pm.gouv.fr

Sommaire

1	Impératifs de sécurité pour les systèmes traitant des informations OTAN classifiées	4
2	Qu'est-ce qu'un SSRS ?	5
3	Quels sont les avantages de la méthode EBIOS pour la rédaction d'un SSRS ?	6
4	Comment rédiger un SSRS en utilisant EBIOS ?	7
4.1	Spécificités de l'étude EBIOS pour rédiger un SSRS	8
	Étape 1 – Étude du contexte	8
	Étape 2 – Expression des besoins de sécurité	10
	Étape 3 – Étude des menaces	11
	Étape 4 – Identification des objectifs de sécurité	12
	Étape 5 – Détermination des exigences de sécurité	13
4.2	Rédaction du SSRS à partir des résultats de l'étude EBIOS	14
	Section 1 – Introduction	14
	Section 2 – Définition du système	17
	Section 3 – Impératifs de sécurité	19
	Section 4 – Environnements de sécurité	21
	Section 5 – Mesures de sécurité	22
	Section 6 – Administration de la sécurité	23
	Formulaire de recueil de commentaires	25

1 Impératifs de sécurité pour les systèmes traitant des informations OTAN classifiées

La doctrine de sécurité de l'OTAN prévoit que les responsables d'un projet ou les autorités d'emploi¹ dès qu'elles sont désignées, établissent pour tous les systèmes et réseaux informatiques stockant, traitant ou transmettant des informations classifiées CONFIDENTIEL OTAN et au-dessus, un énoncé des impératifs de sécurité.

L'énoncé des impératifs de sécurité spécifie la manière d'obtenir, de gérer et de superviser la sécurité. Il représente un accord qui lie l'autorité d'emploi et l'autorité d'homologation de sécurité pour l'octroi d'une homologation à un système ou réseau informatique.

L'énoncé peut prendre une ou plusieurs formes, selon la nature et la complexité du système :

- ❑ un énoncé des impératifs de sécurité propres à un système (*System-specific Security Requirement Statement - SSRS*),
- ❑ un énoncé des impératifs de sécurité électroniques propres au système (*System-specific Electronic Security Requirement Statement - SEISRS*),
- ❑ un énoncé des impératifs de sécurité applicables à une interconnexion de systèmes (*System Interconnection Security Requirement Statement - SISRS*),
- ❑ un énoncé des impératifs de sécurité applicables à un ensemble d'interconnexion (*Community Security Requirement Statement - CSRS*).

Nous allons nous intéresser dans la suite du document au rôle du SSRS. Ce dernier décrit un système ou un réseau et les éléments de sécurité qu'il convient de mettre en œuvre pour celui-ci en termes de normes de sécurité, d'environnement, ainsi que de mesures techniques et administratives de sécurité.

¹ L'autorité d'emploi est responsable de la planification, de la conception et du déploiement des systèmes.

2 Qu'est-ce qu'un SSRS ?

Un SSRS est l'énoncé des impératifs de sécurité propres à un système particulier. Il s'agit d'un document dont l'utilisation et la forme sont définies par l'OTAN².

Les impératifs de sécurité permettent à la maîtrise d'ouvrage de décrire comment est assurée la sécurité du système, en présentant les menaces pesant sur le système, les normes minimales de sécurité et les énoncés de sécurité à respecter ainsi que la démarche de gestion de risques employée. La maîtrise d'œuvre y répond par un ensemble de mesures techniques et administratives.

Selon le niveau de maturité du système, le SSRS est plus ou moins détaillé. Au moment de la formulation des concepts et des normes ou standards de sécurité, le SSRS peut être assimilé, selon la réglementation française, à une Fiche d'Expression Rationnel d'Objectif de Sécurité (FEROS). Durant la phase de spécification du système, le SSRS est affiné, les normes sont développées en mesures de sécurité. À ce stade, selon son niveau de granularité, le SSRS contient des éléments que l'on retrouve dans une cible de sécurité système, un Plan De Sécurité (PDS) voire une Politique de Sécurité du Système d'Information (PSSI).

Par ailleurs, le SSRS sert de base à la rédaction des Procédures d'Exploitation de Sécurité (PES) appelées SecOPs (*Security Operating Procedures*).

L'AC/35-D/1015 précise qu'une évaluation de risques³ doit toujours faire partie des considérations entrant dans un SSRS, en même temps que l'énoncé de sécurité. La suite du document explique comment rédiger un SSRS à l'aide de la méthode de gestion de risques⁴ EBIOS.

Remarque : d'autres organisations internationales, telles que l'Union européenne, utilisent également des SSRS. Même si les principes généraux sont communs à ceux de l'OTAN, l'utilisation et la forme précises de ces SSRS leur sont généralement propres. Ainsi, il conviendra d'adapter le contenu de ce guide aux autres types de SSRS.

² AC/35-D/1015-REV2 – *Guidelines for the development of security requirement statements* – OTAN (29 avril 2004).

³ Définition de l'évaluation du risque au sens du Guide ISO 73 : processus de comparaison du risque estimé avec des critères de risque donnés pour déterminer l'importance d'un risque.

⁴ Définition de la gestion du risque au sens du Guide ISO 73 : activités coordonnées visant à diriger et piloter un organisme vis-à-vis du risque. La gestion du risque inclut typiquement l'appréciation du risque, le traitement du risque, l'acceptation du risque et la communication relative au risque.

3 Quels sont les avantages de la méthode EBIOS pour la rédaction d'un SSRS ?

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

- ❑ l'assurance de conformité aux processus d'analyse de risques définis par la directive AC/35-D/1017-REV2,
- ❑ une garantie d'exhaustivité et de cohérence ; le recueil des informations à faire figurer dans le SSRS étant réalisé conformément à une vraie démarche méthodologique,
- ❑ une vision globale de la sécurité qui prend en considération non seulement les aspects techniques mais aussi les caractéristiques organisationnelles et fonctionnelles de l'organisme,
- ❑ la mise en évidence des véritables risques qui pèsent sur le système grâce à une dichotomie entre l'expression de besoins de sécurité et l'analyse de la menace,
- ❑ la cartographie des risques qui facilite la prise de décision par l'autorité d'homologation du système,
- ❑ un dialogue clarifié entre la maîtrise d'ouvrage et la maîtrise d'œuvre dans le respect des rôles de chacun,
- ❑ une démarche raisonnée et traçable qui permet d'identifier les mesures techniques et organisationnelles du SSRS en prenant en compte les composantes du risque et les éléments du contexte, le tout en conformité avec la réglementation OTAN,
- ❑ la définition d'un niveau d'assurance des impératifs de sécurité adapté au potentiel d'attaque de l'élément menaçant,
- ❑ la mise en évidence et l'appréciation des risques résiduels tout au long de la démarche de manière méthodique,
- ❑ la disponibilité des guides méthodologiques EBIOS en français, anglais, allemand et espagnol qui assure une diffusion internationale,
- ❑ la conformité du vocabulaire et des concepts EBIOS aux normes de gestion de risques internationalement reconnues.

4 Comment rédiger un SSRS en utilisant EBIOS ?

Une analyse de risques doit être réalisée dès la conception du projet. Cette analyse de risques évolue en fonction de la maturité du projet (définition des besoins, développement et acceptation du système). Elle fournit en permanence tous les éléments nécessaires à l'instruction du SSRS au cours de son évolution (par exemple spécification de l'architecture, réévaluation de la menace...). C'est dans ce cadre que le SSRS connaît différents stades de rédaction.

Dans une première phase, la maîtrise d'ouvrage exprime, à travers une analyse des services attendus du système, des besoins de sécurité minimaux admissibles pour l'organisme et le référentiel de sécurité à respecter (normes de sécurité OTAN). Le SSRS qui en résulte n'est à ce stade qu'une simple trame.

Tout au long du développement du projet, l'analyse de risques se précise. Le SSRS qui en est issu devient à terme un énoncé des mesures de sécurité nécessaires et suffisantes au système.

Lorsque la nature des services, l'architecture et le contexte d'emploi du système rentrent dans le cadre réglementaire de l'OTAN, l'analyse de risques reste de haut niveau. Il suffit alors de décliner en mesures les politiques et directives AC/35 et AC/322 de l'OTAN. Les niveaux de granularité de ces directives sont généralement suffisantes. Dans ce cas, le SSRS est lui-même un document de haut niveau puisqu'il s'appuie sur les référentiels de sécurité de l'OTAN.

En revanche, lorsque la nature des services, l'architecture ou le contexte d'emploi du système sortent de ce cadre réglementaire habituel, l'analyse de risques doit, au contraire, être détaillée. La qualité de cette analyse de risques doit alors être garantie par une démarche méthodologie éprouvée, reconnue et structurée telle qu'EBIOS afin d'identifier correctement les risques propres au système et de définir des mesures justes et pertinentes.

Les pages suivantes décrivent comment rédiger un SSRS à l'aide de la méthode EBIOS.

4.1 Spécificités de l'étude EBIOS pour rédiger un SSRS

Les chapitres suivants expliquent la manière d'aborder chaque activité de la méthode EBIOS pour obtenir les éléments nécessaires à l'élaboration d'un SSRS.

Étape 1 – Étude du contexte

Résumé : l'étude du contexte doit être approfondie.

Activité 1.1 – Étude de l'organisme

La description de l'organisme doit être concise et explicite afin de situer le contexte d'utilisation du système-cible.

Elle permet de rappeler les éléments caractéristiques qui définissent l'identité de l'organisme. Il s'agit de définir la structure de l'organisme, sa vocation principale, son métier, les missions, les valeurs propres et les axes stratégiques.

Elle doit servir à identifier clairement les contraintes, les références réglementaires et légales ainsi que les normes que l'organisation doit respecter.

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.

Une description claire de l'organisme permet d'assurer une meilleure définition du système-cible.

Activité 1.2 – Étude du système-cible

La présentation du système-cible doit être concise et précise afin de délimiter clairement le périmètre de l'étude.

Les enjeux doivent être définis et évalués afin d'indiquer le rôle et la place qu'occupe le système-cible vis-à-vis des missions de l'organisme.

Sur la base de la description fonctionnelle de l'organisme, il convient d'identifier les éléments véritablement essentiels pour l'organisme : fonctions critiques et informations sensibles ou classifiées stockées, traitées et transmises sur le système.

La définition des hypothèses, des règles de sécurité, des références réglementaires ainsi que des contraintes est indispensable pour disposer d'un contexte complet et adéquat.

Les hypothèses sont imposées par l'organisme pour des raisons politiques internes ou externes. Elles permettent notamment de recenser les pratiques et mécanismes de sécurité existant dans l'organisme et peuvent être classées selon les domaines de sécurité de l'AC/35-D-1015-REV02.

Si la certification d'un produit de sécurité est prévue dans le processus d'homologation, il convient de définir en hypothèse le périmètre du SEISRS énonçant les fonctions de sécurité visées. Cette démarche permet de réduire ensuite les vulnérabilités sur le système en s'appuyant sur les hypothèses.

À terme, les hypothèses doivent être vérifiées. En effet, elles peuvent constituer des risques résiduels si elles ne sont pas avérées.

Les contraintes à prendre en compte sur le système sont de différents types : technique, financier, calendaire, organisationnel...

Le mode d'exploitation de sécurité du système doit être défini (exclusif, dominant, multi-niveaux).

Les références réglementaires permettent de prendre en compte les lois, les règlements susceptibles, de limiter le choix des solutions matérielles ou des procédures. Il convient de référencer les politiques et directives du comité de sécurité de l'OTAN (AC/35) et du Bureau des C3 de l'OTAN (AC/322) auquel le système est soumis :

- la politique de sécurité de l'OTAN C-M(2002)49,
- la directive principale sur l'INFOSEC AC/35-D2004 – AC/322-D/0052,

- ❑ la directive sur la gestion de l'INFOSEC AC/35-D2005,
- ❑ les directives sur les aspects techniques et la mise en œuvre de l'INFOSEC AC/322, notamment :
 - AC/322-D/0048 sur les ordinateurs et les réseaux locaux,
 - AC/322-D/0030-REV4 les interconnexions de systèmes d'information de communication...

Par ailleurs, il convient de référencer les règles de sécurité auquel le système est confronté comme la stratégie d'homologation du système. Notamment, dans le cadre d'un ensemble d'interconnexions, il convient de prendre en considération les impératifs de sécurité définis dans la CSRS et les SISRS de chaque interconnexion.

Activité 1.3 – Détermination de la cible de l'étude de sécurité

Cette activité permet de décrire l'architecture technique et non technique du système à travers un ensemble d'entités de différents types (matériel, logiciel, réseau, personnels, sites, organisations, systèmes).

Le niveau de granularité des entités varie selon le niveau de maturité du système. Cette activité doit être aussi détaillée que les spécifications le permettent.

Il convient, dans le cadre d'un SSRS d'organiser les entités en 3 catégories :

- ❑ GSE (*Global Security Environment*) : environnement de sécurité global dans lequel est situé le système et n'étant pas sous le contrôle direct de l'autorité d'exploitation du système.
- ❑ LSE (*Local Security Environment*) : environnement de sécurité relevant de l'autorité d'exploitation du système.
- ❑ ESE (*Electronic Security Environment*) : définit le système lui-même en terme de sécurité.

Les principales entités du système sont décrites et croisées avec les éléments essentiels pour définir leurs dépendances.

Pour chaque entité, il est important de spécifier son type ; les vulnérabilités de la base de connaissances EBIOS étant classées par type d'entités

Étape 2 – Expression des besoins de sécurité

Résumé : l'expression des besoins de sécurité est détaillée et réalisée en cohérence avec les éventuels énoncés de sécurité auquel le système est soumis.

Activité 2.1 – Réalisation des fiches de besoins

Les critères de sécurité doivent être clairement identifiés et définis sans ambiguïté et en cohérence avec un éventuel énoncé de sécurité tel qu'un CSRS.

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.

Les impacts peuvent utilement refléter les enjeux du système-cible. Ils doivent être cohérents avec une éventuelle politique de sécurité.

Voici un exemple d'échelles de besoins de sécurité :

- pour la disponibilité :
 - Aucun besoin de disponibilité
 - Long terme (dans le mois)
 - Moyen terme (dans la journée)
 - Court terme (dans l'heure)
 - Très court terme (dans la minute)
- pour l'intégrité :
 - Perte d'intégrité admise
 - Perte d'intégrité admise dans la mesure où elle est détectée
 - Parfaitement intègre
- pour la confidentialité :
 - NATO UNCLASSIFIED
 - NATO RESTRICTED
 - NATO CONFIDENTIAL
 - NATO SECRET
 - TOP COSMIC SECRET

Activité 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...

Étape 3 – Étude des menaces

Résumé : le niveau de détail de l'étude des menaces dépend de l'état d'avancement des spécifications.

Activité 3.1 – Étude des origines des menaces

Cette activité permet de lister les méthodes d'attaque pertinentes pour le système. Elle permet à la maîtrise d'ouvrage de spécifier les pans de sécurité qu'elle souhaite étudier.

La caractérisation des éléments menaçants doit être particulièrement claire et précise :

- ❑ le type d'élément menaçant (naturel, humain, environnemental),
- ❑ la cause (délibérée, accidentelle),
- ❑ le potentiel d'attaque (niveau d'expertise, de ressource et de motivation de l'élément menaçant).

La section 4 du guide de la méthode EBIOS présente une liste de méthodes d'attaque et des exemples d'éléments menaçants.

La directive AC/35-D/1020-REV03 définit un ensemble de scénarios de menaces et présente différents types d'éléments menaçants.

L'identification d'un potentiel d'attaque pour chaque élément menaçant est nécessaire dans le cadre d'un SSRS. Une échelle de niveaux de potentiel d'attaque doit alors être définie.

Les méthodes d'attaque non retenues doivent être justifiées et constituent des risques résiduels.

La liste des méthodes d'attaque peut se présenter sous la forme d'un tableau comme à la section 3 du guide de la méthode EBIOS.

Activité 3.2 – Étude des vulnérabilités

Cette activité ne peut être réalisée que si l'état d'avancement des spécifications le permet.

La section 4 du guide de la méthode EBIOS liste un ensemble de vulnérabilités classées par méthode d'attaque et type d'entité.

La directive AC/35-D/1020-REV03 définit un ensemble de vulnérabilités qui pèsent sur les systèmes d'information et de communication (SIC).

Selon le niveau de maturité et de criticité du système, les vulnérabilités sont de haut niveau ou détaillées. Il s'agit de s'assurer que les vulnérabilités spécifiées dans la directive existent et d'identifier celles spécifiques au système.

Il peut être défini une échelle de niveaux de vulnérabilité à partir de l'exemple proposé à la section 3 du guide de la méthode EBIOS.

Activité 3.3 – Formalisation des menaces

Selon le niveau de maturité et de criticité du système, le niveau de granularité des menaces varie.

La formulation des menaces est réalisée avec ou sans les vulnérabilités, selon l'état d'avancement des spécifications et les spécificités du système.

Les menaces peuvent se présenter sous une forme minimaliste comme une liste de méthodes d'attaque sélectionnées ou plus complète, en présentant, pour chaque méthode d'attaque sélectionnées, les éléments menaçant et les vulnérabilités par entité du système concerné.

Cette activité doit être claire (à des fins de communication) et précise.

Il est conseillé de présenter les menaces sous la forme d'un tableau.

Étape 4 – Identification des objectifs de sécurité

Résumé : l'identification des impératifs de sécurité prend en compte les risques et les éléments du contexte.

Activité 4.1 – Confrontation des menaces aux besoins

Les risques doivent être identifiés et formulés de manière uniforme.

À partir de la liste des menaces, on définit l'atteinte sur les éléments essentiels et sur l'organisme en se basant sur la matrice éléments essentiels / entités, les besoins de sécurité et atteintes en DIC des méthodes d'attaque (cf. section 3 de la méthode EBIOS - Confrontation des menaces aux besoins).

Si aucune vulnérabilité n'a été définie, il convient au groupe de travail d'apprécier les éléments essentiels atteints par les risques et les impacts sur l'organisme.

Activité 4.2 – Formalisation des objectifs de sécurité

Les objectifs de sécurité peuvent être assimilés aux impératifs de sécurité du SSRS rédigés par la maîtrise d'ouvrage.

Les objectifs traduisent la volonté de couverture des risques et des éléments du contexte (hypothèses, références réglementaires, règles de sécurité, contraintes...).

Pour chacun des risques et des éléments du contexte, on spécifie le mode de traitement : accepter, réduire, transférer ou éviter. Les objectifs de sécurité forment ainsi le plan de traitement des risques et des éléments du contexte.

Le plan de traitement peut être présenté sous la forme d'un tableau.

Activité 4.3 – Détermination des niveaux de sécurité

Il convient de définir le niveau d'assurance requis par les objectifs de sécurité sur la base d'une échelle à définir. Un exemple d'échelle de niveau d'assurance est défini à la section 3 du guide EBIOS.

Généralement, le niveau d'assurance des objectifs de sécurité relatifs à des risques correspond au potentiel d'attaque de l'élément menaçant.

Étape 5 – Détermination des exigences de sécurité

Résumé : les mesures de sécurité sont déterminées en fonction des impératifs de sécurité.

Activité 5.1 – Détermination des exigences de sécurité fonctionnelles

Les exigences de sécurité fonctionnelles constituent les mesures de sécurité techniques (Section V – Mesures de sécurité) et organisationnelles (Section VI - Administration de la sécurité) du SSRS.

Chaque impératif de sécurité du SSRS peut être couvert par une ou plusieurs mesures de sécurité en fonction du niveau d'assurance requis.

Les mesures sont définies par la maîtrise d'œuvre et peuvent être issues de divers référentiels (normes nationales ou internationales) ou créées de toute pièce.

Elles doivent être rédigées en adéquation avec les impératifs de sécurité qui prennent en compte au-delà des risques :

- ❑ les hypothèses (mesures de sécurité existantes, fonctions de sécurité des SEISRS...),
- ❑ les références réglementaires (politiques, directives AC/35 et AC/322 de l'OTAN),
- ❑ les règles de sécurité concernées (stratégie d'homologation, CSRS, SISRS...),
- ❑ les contraintes sur l'organisme et le système,
- ❑ les enjeux.

Les mesures de sécurité doivent être classées par domaine de sécurité :

- ❑ mesures techniques : contrôle d'accès, identification et authentification, compatibilité, audit de sécurité, intégrité et disponibilité, échange/communication de données, impératifs juridiques,
- ❑ mesures de sécurité organisationnelles : gestion de sécurité, gestion des risques de sécurité, procédures d'exploitation de sécurité, contrôle de configuration, formation et sensibilisation à la sécurité, traitement et compte rendu des incidents intéressant la sécurité, homologation/ré-homologation de sécurité, retrait du service.

Il convient de définir pour chaque mesure de sécurité technique l'environnement de sécurité concerné (GSE, LSE, ESE).

Le fait de classer les mesures techniques et organisationnelles par domaine de sécurité et environnement de sécurité permet de positionner directement les mesures dans le SSRS.

La démonstration de couverture des risques par les mesures et les hypothèses doit être détaillée.

La couverture partielle d'un impératif de sécurité constitue un risque résiduel qu'il convient de mettre en évidence. Le défaut de couverture d'un impératif peut résulter d'une couverture partielle d'un risque ou du non-respect des éléments du contexte (références réglementaires, règles de sécurité, contraintes, enjeux).

Activité 5.2 – Détermination des exigences de sécurité d'assurance

Cette activité n'est pas mise en œuvre pour la rédaction d'un SSRS.

4.2 Rédaction du SSRS à partir des résultats de l'étude EBIOS

Les chapitres suivants présentent comment exploiter le résultat d'une étude EBIOS par chapitre du SSRS⁵.

Pour chacun des chapitres du SSRS présentés ci-dessous :

- ❑ l'objectif est rappelé,
- ❑ les activités de la méthode EBIOS nécessaires à sa rédaction sont listées,
- ❑ leurs modalités sont ensuite proposées.

Section 1 – Introduction

Références documentaires

Objectif : lister les références documentaires pertinentes pour le système

Activités EBIOS concernées :

Étude du contexte – Lister les règles de sécurité

Étude du contexte – Lister les références réglementaires spécifiques au système-cible

Modalités :

Extraire les énoncés de sécurité que le système doit respecter (stratégie d'homologation, CSRS, SISRS...) listés au niveau des règles de sécurité de l'étude EBIOS.

Extraire les politiques et directives AC/35 et AC/322 OTAN pertinentes pour le système, listées au niveau des références réglementaires de l'étude EBIOS.

Sous-section 1.1 – Données de base

Objectif : présenter brièvement le système et son rôle

Activités EBIOS concernées :

Étude du contexte – Faire une description fonctionnelle du SI global

Modalités :

Extraire de cette activité les informations relatives à l'architecture fonctionnelle du système.

Sous-section 1.2 – Objet du document

Objectif : présenter brièvement le rôle du SSRS et sa structure

EBIOS n'intervient pas dans ce chapitre.

Une trame est proposée en exemple à l'appendice 2 de l'annexe 1 de l'AC/35-D/1015-REV2.

Sous-section 1.3 – Portée

Objectif : identifier la cible du système étudié

Activités EBIOS concernées :

Étude du contexte – Présenter le système-cible

Modalités :

Extraire de la présentation du système-cible les informations relatives au périmètre de la cible étudié.

⁵ La structure du SSRS est définie dans annexe 1 de l'appendice 2 de l'AC/35 D/1015 REV2.

Sous-section 1.4 – Emplacement du système et de ses composantes

Objectif : identifier l'emplacement du système et de ses composantes

Activités EBIOS concernées :

Étude du contexte – Présentation du système

Étude du contexte – Lister et décrire les entités du système

Modalités :

Extraire les entités de types sites, matériel et réseau de l'étude du contexte

Sous-section 1.5 – Principales dates cibles

Objectif : présenter les principales dates liées au cycle de vie du système

Activités EBIOS concernées :

Étude du contexte – Contraintes sur le système

Modalités :

Extraire de l'étude du contexte les contraintes de temps relatives au projet.

Sous-section 1.6 – Responsabilités en matière de sécurité

Objectif : décrire les principales responsabilités en matière de sécurité

EBIOS n'intervient pas directement dans ce chapitre.

Activités EBIOS concernées :

Étude du contexte – Lister et décrire les entités du système

Détermination des exigences de sécurité – Détermination des exigences de sécurité fonctionnelles

Modalités :

Les utilisateurs sont identifiés au niveau des entités.

Les différentes autorités en matière de sécurité doivent être mentionnées dans les exigences de sécurité fonctionnelles de l'étude EBIOS. Elles sont référencées à la section 5 du SSRS.

Sous-section 1.7 – Politique de classification et de marquage

Objectif : définir une politique de classification et de marquage des informations du système

La méthode EBIOS n'intervient pas directement dans ce chapitre.

Une trame est proposée en exemple à l'appendice 2 de l'annexe 1 du l'AC/35-D/1015-REV2.

Activités EBIOS concernées :

Expression des besoins de sécurité

Détermination des exigences de sécurité – Détermination des exigences de sécurité fonctionnelles

Modalités :

Le niveau de classification des informations est spécifié à l'étape 2 *Expressions des besoins de sécurité* de la méthode EBIOS.

Les règles de gestion des informations classifiées au sein du système doivent être mentionnées dans les exigences de sécurité fonctionnelles de l'étude EBIOS. Elles sont référencées à la section 5 du SSRS.

Sous-section 1.8 – Processus d’homologation de sécurité

Objectif : définir une stratégie d’homologation

Les résultats de l’étude EBIOS ne sont pas exploités dans ce chapitre.

Une trame est proposée en exemple à l’appendice 2 de l’annexe 1 du l’AC/35-D/1015-REV2.

Ce chapitre doit être rédigé en conformité avec la stratégie d’homologation du système.

Sous-section 1.9 – Processus de révision du document

Objectif : définir une stratégie de révision du document

Les résultats de l’étude EBIOS ne sont pas exploités dans ce chapitre.

À chaque changement du contexte du système, il convient de mettre à jour l’étude EBIOS, d’identifier les nouveaux risques et de s’assurer que les mesures sont toujours pertinentes. Une fois l’étude EBIOS mise à jour, il convient de répercuter les évolutions éventuelles dans le SSRS.

Section 2 – Définition du système

Rôle du système

Objectif : présenter le rôle du système

Activités EBIOS concernées :

Étude du contexte – Présentation du système

Étude du contexte – Lister les enjeux

Modalités :

Extraire de l'étude EBIOS la présentation du système et son rôle stratégique au niveau des enjeux.

a. Informations

Objectif : lister les informations traitées par le système et spécifier leurs niveaux de classification

Activités EBIOS concernées :

Étude du contexte – Lister les éléments essentiels

Expression des besoins de sécurité - Synthèse des besoins de sécurité

Modalités :

Extraire de la synthèse des besoins de sécurité les informations critiques stockées, traitées et transmises sur le système et préciser leur niveau de classification.

Extraire éventuellement de la liste des éléments essentiels la description de ces informations critiques.

b. Utilisateurs

Objectif : lister les catégories d'utilisateurs

Activités EBIOS concernées :

Étude du contexte – Lister et décrire les entités du système

Étude du contexte – Lister les contraintes pesant sur l'organisme

Étude du contexte – Faire une description fonctionnelle du SI global

Étude du contexte – Lister les contraintes sur le système

Étude du contexte – Lister les hypothèses sur le système

Modalités :

Extraire les différentes catégories d'utilisateurs définies au niveau des entités.

Les informations complémentaires à extraire sont définies au niveau des hypothèses (niveau d'habilitation, privilèges...) et des contraintes (contraintes de types personnel, organisationnel, environnemental...).

Extraire éventuellement de la description fonctionnelle du système les acteurs externes.

c. Architecture du système

Objectif : description générale de l'architecture du système

Activités EBIOS concernées :

Étude du contexte – Lister et décrire les entités du système

Modalités :

Rédiger une synthèse de l'architecture à partir de la liste des entités.

d. Mode d'exploitation de sécurité

Objectif : déterminer la manière dont est globalement géré l'accès aux informations

Activités EBIOS concernées :

Étude du contexte – Mode d'exploitation de sécurité

Modalités :

Extraire le mode d'exploitation de sécurité du système.

Section 3 – Impératifs de sécurité

Sous-section 3.1 – Normes minimales de sécurité

Objectif : définir les normes minimales de sécurité

Activités EBIOS concernées :

Étude du contexte – Règles de sécurité

Étude du contexte – Références réglementaires

Modalités :

Extraire des règles de sécurité les énoncés de sécurité à prendre en compte pour le système et les contre-mesures existantes.

Extraire des références réglementaires de l'étude EBIOS les politiques de sécurité et directives pertinentes pour le système.

Sous-section 3.2 – Gestion des risques de sécurité

Objectif : définir la stratégie d'évaluation des risques.

Les résultats de l'étude EBIOS ne sont pas exploités dans ce chapitre.

La méthode EBIOS permet de réaliser l'ensemble des étapes relatives à la gestion des risques de sécurité définies dans l'AC/35-D/1015-REV2.

Sous-section 3.3 – Criticité des informations et des services et ressources systèmes supports

Objectif : définir la criticité des informations et services du système et les ressource associées

Activités EBIOS concernées :

Étude du contexte - Croiser les éléments essentiels et les entités

Expressions des besoins de sécurité - Déterminer l'échelle de besoins

Expressions des besoins de sécurité - Déterminer les impacts pertinents

Expressions des besoins de sécurité - Synthèse des besoins de sécurité

Modalités :

Présenter l'échelle des besoins de sécurité et les impacts craints par l'organisme.

Lister les informations et fonctions essentielles et préciser leurs besoins en disponibilité, intégrité et confidentialité en fonction des impacts.

Si une justification des besoins de sécurité a été réalisée au niveau de l'étude EBIOS, il convient de la rapporter.

La matrice entité / éléments essentiels permet de définir les dépendances entre les informations et services critiques du système et les différentes composantes de l'architecture.

Sous-section 3.4 – Introduction aux menaces d'attaque, vulnérabilités et risques

Objectif : présenter les concepts de *menace*, *vulnérabilité* et *risque*

Les résultats de l'étude EBIOS ne sont pas exploités dans ce chapitre.

Le glossaire de la section 1 du guide EBIOS définit le vocabulaire se rapportant à la gestion des risques SSI.

Sous-section 3.5 – Menaces, vulnérabilités et risques spécifiques au système

Objectif : identifier les risques spécifiques au système

Activités EBIOS concernées :

Étude des menaces - Formalisation des menaces

Identification des objectifs de sécurité – Formuler explicitement les risques

Identification des objectifs de sécurité – Hiérarchiser les risques selon l'impact sur les éléments essentiels et l'opportunité des menaces

Modalités :

Extraire la liste des menaces et des risques.

Extraire le tableau de hiérarchisation des risques.

Le niveau de granularité des menaces et des risques varie selon le niveau de maturité et de criticité du système. Les risques peuvent être de haut niveau et présentées sous la forme d'un tableau comme le préconise l'AC35-D1015-REV2 ou beaucoup plus détaillés sous forme littérale.

La méthode de rédaction des menaces et des risques selon le niveau de granularité du système est définie dans le tableau précédent.

Section 4 – Environnements de sécurité

a. GSE

Objectif : décrire l'environnement général de sécurité dans lequel le système est situé

Activités EBIOS concernées :

Étude du contexte – Lister et décrire les entités du système

Étude du contexte – Lister les hypothèses

Modalités :

Extraire des entités les composantes constituant l'environnement de sécurité physique du système. Les types d'entités concernés sont : zone, site, organisationnel, personnel...

Extraire les éléments de sécurité déjà existant au niveau du GSE éventuellement définis au niveau des hypothèses.

b. LSE

Objectif : décrire l'environnement de sécurité local dans lequel le système est situé

Activités EBIOS concernées :

Étude du contexte – Lister et décrire les entités du système

Étude du contexte – Lister les hypothèses

Modalités :

Extraire des entités les composantes constituant l'environnement local du système. Les types d'entités concernés sont : local, service essentiel, réseau, organisationnel, personnel, ...

Extraire les éléments de sécurité déjà existant au niveau du LSE éventuellement définis au niveau des hypothèses.

c. ESE

Objectif : décrire l'environnement de sécurité électronique

Activités EBIOS concernées :

Étude du contexte – Lister et décrire les entités du système

Étude du contexte – Lister les hypothèses

Modalités :

Extraire des entités les composantes constituant l'environnement local du système. Les types d'entités concernés sont : matériel, réseau, logiciel, système...

Extraire les éléments de sécurité déjà existant au niveau de l'ESE éventuellement définis au niveau des hypothèses.

Section 5 – Mesures de sécurité

Sous-section 5.1 – Introduction

Objectif : décrire la démarche utilisée dans les chapitres suivants pour définir les mesures de sécurité par domaine de sécurité en considérant les risques et les hypothèses.

Les résultats de l'étude EBIOS ne sont pas exploités dans ce chapitre. La méthode EBIOS permet d'identifier des mesures de sécurité en fonction des risques et des hypothèses sur le système. Les mesures de sécurité sont ensuite affinées et constituent les procédures d'exploitation de sécurité au niveau des SecOPs. L'annexe 1 de l'appendice 2 de l'AC/35-D/1015-REV2 propose en exemple une trame pour rédiger ce chapitre.

Sous-sections 5.2 à 5.8

Objectif : définir les mesures de sécurité techniques par domaine de sécurité

Activités EBIOS concernées :

Identification des objectifs de sécurité – Formuler des objectifs de sécurité

Détermination des exigences de sécurité - Détermination des exigences de sécurité fonctionnelles

Modalités :

Pour chaque domaine de sécurité (contrôle d'accès, identification et authentification, compatibilité, audit de sécurité, intégrité et disponibilité, échange/communication de données, impératifs juridiques), on réalise les actions suivantes :

- ❑ rappeler éventuellement les impératifs de sécurité concernés par le contrôle d'accès à partir des règles de sécurité et des références réglementaires,
- ❑ identifier les principaux risques relatifs au domaine de sécurité concerné à partir de la liste des risques de l'étude EBIOS. Pour chacun des risques à réduire :
 - à partir des exigences de sécurité fonctionnelles de l'étude EBIOS classées par domaine de sécurité, extraire les mesures de sécurité du domaine de sécurité concerné, classées par environnement de sécurité (ESE, GSE, LSE),
 - extraire de la liste les hypothèses relatives à la catégorie concernée.

Sous-section 5.9 – Risques résiduels

Objectif : identifier les risques résiduels du système

Activités EBIOS concernées :

Étude des menaces - Étude des origines des menaces

Détermination des exigences de sécurité - Détermination des exigences de sécurité fonctionnelles

Modalités :

Extraire de l'étude EBIOS les risques résiduels :

- ❑ les méthodes d'attaque non sélectionnées issues de l'activité *Étude de l'origine des menaces* et extraire la justification,
- ❑ la couverture partielle des impératifs de sécurité par les mesures (couverture partielle des risques, non respect des règles de sécurité et contraintes).

Extraire du rapport d'audit technique et organisationnel les risques identifiés (les hypothèses non vérifiées, les mesures non appliquées ou partiellement appliquées).

Extraire de l'étude EBIOS la matrice risques / exigences de sécurité.

Extraire de l'étude EBIOS la matrice éléments du contexte (hypothèses, références réglementaire, règles de sécurité, contraintes sur l'organisme et le système...) / exigences de sécurité.

Section 6 – Administration de la sécurité

Sous-sections 6.1 à 6.8

Objectif : définir les mesures de sécurité organisationnelles par domaine de sécurité

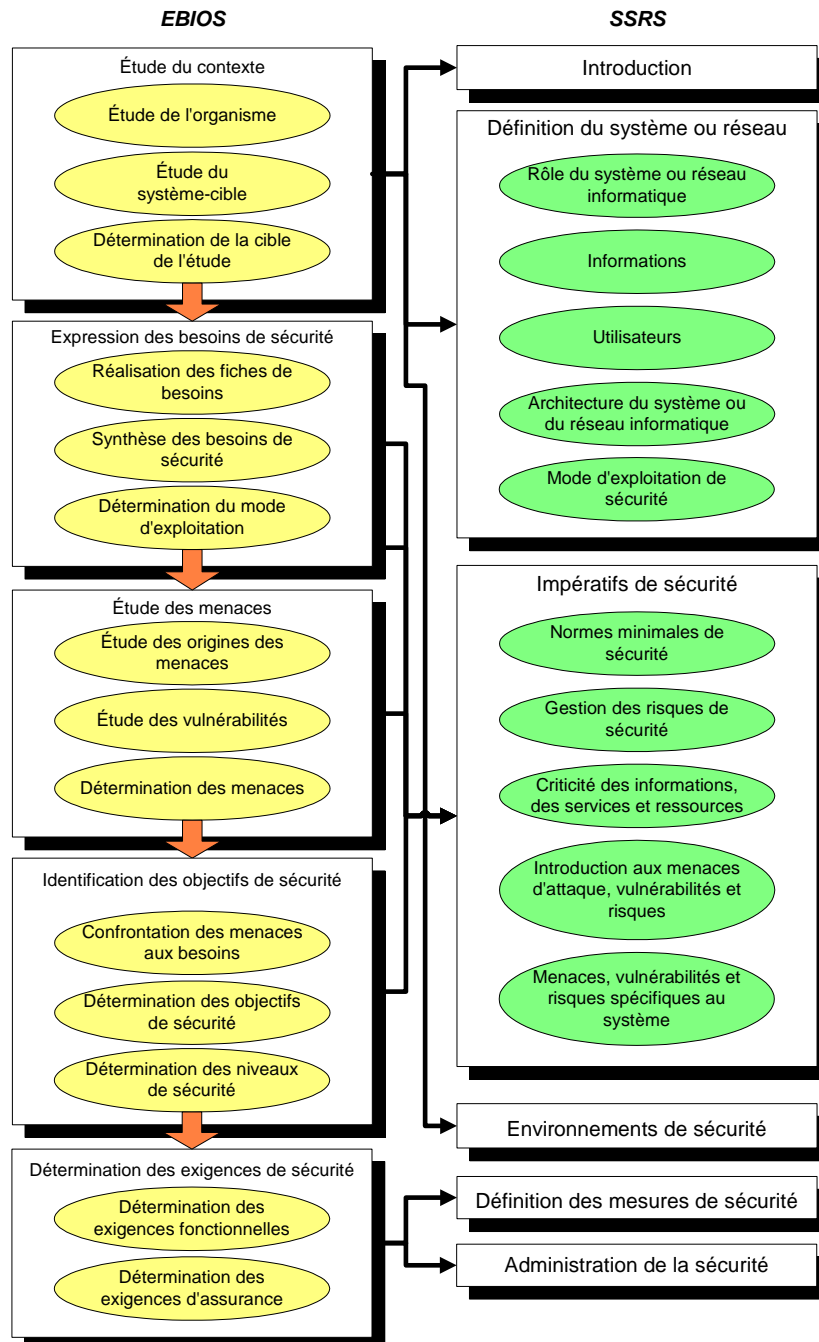
Activités EBIOS concernées :

Détermination des exigences de sécurité – Détermination des exigences de sécurité fonctionnelles

Modalités :

À partir de la liste des exigences de sécurité fonctionnelles classées par domaine de sécurité (gestion de sécurité, gestion des risques de sécurité, procédures d'exploitation de sécurité, contrôle de configuration, formation et sensibilisation à la sécurité, traitement et compte rendu des incidents intéressant la sécurité, homologation/ré-homologation de sécurité, retrait du service) de l'étude EBIOS, extraire les mesures de sécurité organisationnelles du domaine de sécurité concerné.

Le processus de rédaction d'un SSRS à partir d'une étude EBIOS peut se présenter macroscopiquement comme ceci :



Formulaire de recueil de commentaires

Ce formulaire peut être envoyé à l'adresse suivante :

Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil
51 boulevard de La Tour-Maubourg
75700 PARIS 07 SP
ebios.dcssi@sgdn.pm.gouv.fr

Identification de la contribution

Nom et organisme (facultatif) :

Adresse électronique :

Date :

Remarques générales sur le document

Le document répond-il à vos besoins ? Oui Non

Si oui :

Pensez-vous qu'il puisse être amélioré dans son fond ? Oui Non

Si oui :

Qu'auriez-vous souhaité y trouver d'autre ?

Quelles parties du document vous paraissent-elles inutiles ou mal adaptées ?

Pensez-vous qu'il puisse être amélioré dans sa forme ? Oui Non

Si oui :

Dans quel domaine peut-on l'améliorer ?

- lisibilité, compréhension
- présentation
- autre

Précisez vos souhaits quant à la forme :

Si non :

Précisez le domaine pour lequel il ne vous convient pas et définissez ce qui vous aurait convenu :

Quels autres sujets souhaiteriez-vous voir traiter ?

Remarques particulières sur le document

Des commentaires détaillés peuvent être formulés à l'aide du tableau suivant.

"N°" indique un numéro d'ordre.

"Type" est composé de deux lettres :

La première lettre précise la catégorie de remarque :

- O Faute d'orthographe ou de grammaire
- E Manque d'explications ou de clarification d'un point existant
- I Texte incomplet ou manquant
- R Erreur

La seconde lettre précise son caractère :

- m mineur
- M Majeur

"Référence" indique la localisation précise dans le texte (numéro de paragraphe, ligne...).

"Énoncé de la remarque" permet de formaliser le commentaire.

"Solution proposée" permet de soumettre le moyen de résoudre le problème énoncé.

N°	Type	Référence	Énoncé de la remarque	Solution proposée
1				
2				
3				
4				
5				

Merci de votre contribution