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

Expression des Besoins et Identification des Objectifs de Sécurité

EBIOS®

SECTION 1
INTRODUCTION

Version 2 – 5 février 2004

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

Ce document a été réalisé par le bureau conseil de la DCSSI
(SGDN / DCSSI / SDO / BCS)
en collaboration avec le Club EBIOS

Les commentaires et suggestions sont encouragés et peuvent être adressés 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

Historique des modifications

Version	Objet de la modification	Statut
02/1997 (1.1)	Publication du guide d'expression des besoins et d'identification des objectifs de sécurité (EBIOS).	Validé
23/01/2004	Révision globale : - Explications et mise en cohérence avec les normes internationales de sécurité et de gestion des risques - Mise en évidence du référentiel réglementaire par rapport à l'ensemble des contraintes à prendre en compte - Intégration des concepts d'hypothèse et de règles de sécurité (ISO/IEC 15408) - Transfert de la sélection des éléments essentiels dans l'Étude du système-cible - Amélioration de l'élaboration de l'échelle de besoins est améliorée : les valeurs représentant les limites acceptables pour l'organisme par rapport à des impacts personnalisés - Intégration de la détermination des besoins par élément dans l'activité suivante - Intégration de la détermination du mode d'exploitation dans les hypothèses - Adaptation des concepts à l'ISO/IEC 15408 : on étudie l'origine des menaces, c'est-à-dire les méthodes d'attaque et les éléments menaçants, ainsi que leur caractérisation, qui peut inclure un type (naturel, humain, environnemental) une cause (accidentelle, délibérée, en affinant en exposition, ressources disponibles, expertise, motivation), un potentiel d'attaque - Mise en évidence des méthodes d'attaque non retenues - Formalisation des menaces, au sens ISO/IEC 15408 (élément menaçant, attaque et bien sous la forme des entités), avant la confrontation aux besoins de sécurité - Modification de la confrontation des menaces aux besoins, qui permet d'identifier les risques - Mise en évidence des risques non retenus - Intégration de la détermination des objectifs de sécurité minimums dans les activités Formalisation des objectifs de sécurité et Détermination des exigences fonctionnelles - Modification de la détermination des objectifs de sécurité, qui prend en compte les hypothèses, règles de politique de sécurité, contraintes, référentiel réglementaire et risques - Ajout de la détermination des niveaux de sécurité, qui permet de déterminer le niveau des objectifs de sécurité (notamment en fonction des potentiels d'attaque) et de choisir un niveau d'assurance - Ajout de la détermination des exigences de sécurité fonctionnelles, qui permet de déterminer les exigences fonctionnelles couvrant les objectifs de sécurité et de présenter cette couverture - Ajout de la détermination des exigences de sécurité d'assurance, qui permet de déterminer les éventuelles exigences d'assurance Améliorations de forme, ajustements et corrections mineures (grammaire, orthographe, formulations, présentations, cohérence…)	Validé par le Club EBIOS
05/02/2004	Publication de la version 2 du guide EBIOS	Validé

Table des matières

Avant-propos

La recherche permanente d'une plus grande efficacité dans l'accomplissement de leur mission a conduit les différents services de l'État à mettre en œuvre des moyens de télécommunication, d'informatique et de bureautique. Le recours très large à ces technologies rend ces organismes dépendants de leurs systèmes d'information et donc vulnérables aux multiples menaces qui pèsent sur eux. Cet état de choses contribue considérablement à augmenter les risques qui résultent du traitement, du stockage et du transport des informations, au cœur de tout organisme.

Les nouvelles lignes directrices de l'Organisation de Coopération et de Développement Économiques [OCDE] font l'objet d'une recommandation de portée internationale. Elles ont pour objectif principal de promouvoir une "culture de la sécurité" en tant que moyen de protection des systèmes et réseaux d'information. Cela signifie qu'il est nécessaire de porter une très grande attention à la sécurité et d'adopter de nouveaux modes de pensée et de comportement lors du développement et de l'utilisation des systèmes d'information et des réseaux. Elles se présentent sous la forme de neuf principes qui se complètent et doivent être considérés comme un tout.

Dans le domaine de la société de l'information, le plan d'action [eEurope 2005] a pour objectif de développer les services publics en ligne et les accès à Internet haut débit. Cela se traduit notamment par des services publics en ligne modernes ("e-government", "e-learning", "e-health"), un environnement dynamique pour les affaires électroniques ("e-business"), une infrastructure d'information sécurisée, la disponibilité massive d'un accès large bande à des prix concurrentiels, une évaluation comparative ("benchmarking") et la diffusion de bonnes pratiques.

Le gouvernement français s'est engagé dans le domaine de l'administration électronique. Il s'agit de mettre les technologies de l'information au service de la modernisation des services publics, d'améliorer l'efficacité de l'action des administrations de l'État comme des collectivités locales et la qualité des relations entre celles-ci et leurs usagers. Cette dématérialisation "des services publics" ne peut s'effectuer sans une attention minimum portée sur la sécurité. C'est le rôle de la Direction centrale de la sécurité des systèmes d'information (DCSSI) du Secrétariat général de la défense nationale (SGDN) que de contribuer à la définition interministérielle et à l'expression de la politique gouvernementale en matière de sécurité des systèmes d'information.

L'action de l'État peut être mise en cause par les risques issus de l'utilisation des systèmes d'information. C'est pourquoi la protection de l'information et la sécurisation des systèmes d'information est une obligation nationale majeure.

Concernant les systèmes traitant des informations classifiées de défense, l'[IGI 1300] prévoit notamment que les systèmes d'information doivent "être sécurisés conformément à une politique de sécurité définie en fonction du niveau de protection requis, en particulier du niveau de classification des informations traitées et sur la base d'une analyse des risques".

Ce document fait partie d'une série de guides méthodologiques publiés par la DCSSI. Ces guides sont destinés à contribuer à l'amélioration de la sécurisation des systèmes d'information des organismes publics ou privés. Ils peuvent être obtenus par simple demande à la DCSSI.

Ces guides s'appuient sur des documents qui ont déjà largement été discutés au sein de l'administration, ainsi que sur l'expérience et le savoir-faire de nombreux industriels. Les auteurs considèrent que les concepts et les idées exposés à travers ces documents et ces méthodes ont été pesés avec soin et que la structure retenue optimise la cohérence, la compréhension et la facilité d'utilisation.

Note : les références [entre crochets] sont présentées dans la bibliographie en fin de document. On trouvera également un glossaire des termes et acronymes utilisés.

1 Introduction

1.1 La démarche de sécurité

1.1.1 La sécurité des systèmes d'information

La sécurité des systèmes d'information (SSI) traite en premier lieu et essentiellement des informations et des "traitements" qui leur sont appliqués. Les besoins, exigences et objectifs techniques ou organisationnels en découlent naturellement. Trois critères fondamentaux sont à prendre en ligne de compte : la confidentialité, l'intégrité et la disponibilité, tant des informations que des systèmes et des environnements dans lesquels ils se trouvent. On pourra, dans certains cas, s'inquiéter des besoins de non-répudiation, d'autorisation, d'authentification sous le couvert de moyens d'audit qu'il faudra clairement définir.
La SSI est directement associée à une appréciation et un traitement des risques. Ces risques sont qualifiés d'opérationnels car ils agissent directement sur les activités des administrations et des entreprises. En effet, l'organisme utilisant des moyens des technologies de l'information et de communication (TIC) et en particulier de l'Internet, pour réaliser ses activités et transactions commerciales, est directement concernée par la SSI.

1.1.2 Les objets et domaines de sécurité

Puisque la SSI considère l'information, le traitement, le système et son environnement, les objets de la démarche de sécurité seront :

- les informations,
- les processus, fonctions ou applications,
- la technologie (matériel et systèmes d'exploitation),
- l'environnement physique (bâtiments, locaux…),
- les intervenants humains.

Tous ces objets, dont certains sont particulièrement actifs, comme les processus et les hommes, doivent êtes clairement définis. Chacun est plus particulièrement concerné par un domaine de sécurité spécifique, et chacun intervient peu ou prou dans chaque domaine.
Une politique de sécurité qui ne prendrait pas en compte tous ces objets et domaines serait instable et incomplète. Elle produirait une solution dangereuse reposant sur un faux sentiment de sécurité plus dommageable encore que de ne rien faire.

1.1.3 Les démarches normalisées

Depuis une dizaine d'années, de nombreux efforts sont entrepris pour fixer des règles, ou du moins des directives générales, pour la gestion de la sécurité des technologies de l'information. Ces travaux se sont traduits par des normes nationales et internationales (telles que les normes [ISO 13335], [ISO 17799]…). Bien que ces normes soient en évolution et pas encore totalement stabilisées, il est possible de s'en inspirer fortement.

En France, la rédaction d'une [FEROS] est obligatoire dans le cas de systèmes traitant des informations classifiées de défense, et recommandée sinon. Elle fait partie du dossier de sécurité utile à l'agrément en vue d'une homologation d'un système.

Par ailleurs, les normes internationales subordonnent la politique de sécurité d'un système d'information spécifique à la politique de sécurité globale des systèmes d'information, qui elle-même est dépendante de la sécurité de l'information, de la politique des technologies de l'information et des communications, de la politique du personnel et de la politique financière et budgétaire. Le tout n'a de sens que si les actions sont définies en accord avec la stratégie et la politique générale de l'entreprise ou de l'organisation.

L'élaboration des Critères Communs [ISO 15408], a permis de développer la réflexion sur la sécurité des systèmes d'information aussi bien chez les utilisateurs que chez les constructeurs. Les Critères Communs permettent d'évaluer l'assurance offerte, tant au niveau de la conformité de la réalisation des fonctions dédiées à la sécurité que du point de vue de leur efficacité pour contrer les menaces identifiées. Ils ont été élaborés en relation avec les industriels européens de l'informatique, par la DCSSI et les services homologues allemands, américains, britanniques, canadiens et néerlandais.

Certaines institutions internationales poussent à la normalisation des approches par la publication de principes et d'objectifs précis. Citons l'OCDE et ses principes et la Commission européenne qui produit régulièrement des directives auxquelles les États membres doivent se conformer. À titre d'exemple, la démarche de sécurité devrait intervenir dès la première idée d'un nouveau système d'information. Ainsi, la conception du système d'information (SI) intègre les éléments de sécurité nécessaires en même temps que les éléments fonctionnels et opérationnels dès le début de l'étude du projet. Elle assure une efficacité maximum, des coûts minimum et un retour sur investissement très positif. Par ailleurs, la démarche de sécurité devrait englober la totalité du SI et de son environnement ou de son contexte opérationnel. Elle devrait être présente à tous les niveaux de l'organisme et du SI.

1.2 La réponse de la DCSSI

La méthode EBIOS a été élaborée dans la continuité et dans l'esprit de ces démarches. Elle s'utilise généralement au niveau de la phase d'élaboration d'un schéma directeur opérationnel d'un système d'information. Son objectif principal est de permettre à tout organisme, dont les administrations de l'État, de déterminer les actions de sécurité qu'il convient d'entreprendre.

Elle peut être mise en œuvre par l'expert sécurité de l'organisme et peut s'appliquer à tous les niveaux de la structure d'un système d'information à concevoir ou existant (sous-systèmes, applications).

Dans sa première version, la méthode EBIOS permettait en particulier, la rédaction des objectif de sécurité [FEROS].
En 2000, après avoir pris en compte la nécessaire convergence vers la rédaction de profils de protection et sur la base de la version 2.0 des Critères Communs [ISO 15408], la DCSSI a engagé l'adaptation de la méthode EBIOS à ces critères.

Les résultats d'une étude EBIOS fournissent les informations nécessaires à la rédaction d'un cahier des charges SSI du système étudié (FEROS, profil de protection ou autre) et contribuent également à l'élaboration de l'architecture fonctionnelle sécurisée. Dans l'optique d'une évaluation Critères Communs, les résultats de l'étude fournissent des informations nécessaires à l'établissement des spécifications de la cible d'évaluation (ils contribuent à l'élaboration de la cible de sécurité).

Dans son essence et sa philosophie générale, la démarche EBIOS est également applicable à tous les niveaux du SI – de la politique de sécurité du système d'information (PSSI) globale à l'application particulière – sans changer ni sa formulation, ni ses techniques. Seules quelques adaptations de vocabulaire pourraient s'avérer utiles pour traduire les concepts de la méthode dans le contexte particulier. Par exemple, le terme "fonction" qui apparaît fréquemment dans la méthode comme objet de l'étude, pourra se traduire par "métier, processus, système….
Afin de faciliter cette traduction et d'informer le public sur la grande variété des utilisations de la démarche et de la méthode EBIOS, une série de guides de "Meilleures Pratiques" a été développée.

1.3 Les guides de la méthode

La méthode EBIOS[1] est composée de cinq sections complémentaires.

- Section 1 – Introduction
  Cette section présente le contexte, l'intérêt et le positionnement de la démarche EBIOS. Elle contient aussi une bibliographie, un glossaire et des acronymes.
- Section 2 – Démarche
  Cette section expose le déroulement des activités de la méthode.
- Section 3 – Techniques
  Cette section propose des moyens de réaliser les activités de la méthode. Il conviendra d'adapter ces techniques aux besoins et pratiques de l'organisme.
- Section 4 – Outillage pour l'appréciation des risques SSI
  Cette section constitue la première partie des bases de connaissances de la méthode EBIOS (types d'entités, méthodes d'attaques, vulnérabilités).
- Section 5 – Outillage pour le traitement des risques SSI
  Cette section constitue la seconde partie des bases de connaissances de la méthode EBIOS (objectifs de sécurité, exigences de sécurité, tableaux de détermination des objectifs et exigences de sécurité fonctionnelles).

Le présent document constitue la première section de la méthode.

[1] EBIOS est une marque déposée du Secrétariat général de la défense nationale en France.

2 Présentation de la méthode EBIOS

2.1 Qu'est-ce que la méthode EBIOS ?

EBIOS signifie Expression des Besoins et Identification des Objectifs de Sécurité.

Il s'agit non seulement d'une **méthode d'appréciation des risques SSI**, mais aussi d'un véritable **outil d'assistance à la maîtrise d'ouvrage** (définition d'un périmètre d'étude, expression de besoins, responsabilisation des acteurs…). Associée aux Critères Communs et aux avancées dans le domaine de la gestion de la sécurité de l'information (par exemple la norme [ISO 17799]), EBIOS devient aussi une **méthode de traitement des risques SSI**.

EBIOS répond à la commande d'une autorité (chef de projet, maîtrise d'ouvrage, autorité d'homologation du système, direction de l'organisme…). Elle permet de rationaliser des objectifs et des exigences de sécurité en fonction de risques identifiés et éventuellement retenus.

Elle constitue une main courante dans la perception de l'organisme sur le plan de la sécurité pris au sens le plus large du terme. Cette vision et cette approche globale de la problématique de la sécurité permettent d'une part de prendre en compte l'existant sécurité, et d'autre part de déterminer un référentiel cohérent sur lequel s'appuieront les développements futurs.

2.2 Au préalable d'une étude EBIOS

Idéalement, l'étude EBIOS s'appuie sur différents documents relatifs à l'organisme, à son système d'information et au système à étudier :

- le schéma directeur de l'organisme ;
- la politique de sécurité des systèmes d'information (PSSI) ;
- les spécifications générales du système (à concevoir ou réalisé).

On constate cependant que ces documents ne sont pas toujours formalisés. Le travail commencera donc par le recueil des éléments qui devraient constituer ces pièces stratégiques.

Par ailleurs, la finesse de l'étude sera proportionnelle à celle des spécifications générales du système. Un système dont on ignore la finalité ne pourra pas faire l'objet d'une étude de sécurité, comme il ne peut non plus faire l'objet d'une étude fonctionnelle.

2.3 Quel est le résultat de EBIOS ?

EBIOS sert à formaliser un raisonnement, afin de générer le référentiel documentaire de sécurité approuvable par une autorité.

La méthode permet d'identifier des objectifs et exigences de sécurité à la suite d'une appréciation de risques, elle permet donc de contribuer à la réalisation :

- d'un schéma directeur SSI ;
- d'une politique de sécurité ;
- d'un plan d'action SSI ;
- d'une fiche d'expression rationnelle des objectifs de sécurité [FEROS], réglementaire dans le cas de systèmes classifiés de défense [IGI 900], recommandée dans tous les autres cas, par exemple informations sensibles [REC 901] ;
- de spécifications adaptées et justifiées pour la maîtrise d'œuvre (cahier des charges) ;
- d'un profil de protection (PP) ou d'une cible de sécurité (au sens de l'[ISO 15408])…

EBIOS est aussi bien plus que cela :

- un raisonnement simple, souple et cohérent ;
- un outil de négociation et d'arbitrage dans le processus SSI ;
- un moyen d'unifier vocabulaire, concepts et interprétation du système ;
- une approche visant à sensibiliser, responsabiliser et impliquer tous les acteurs ;
- un outil compatible avec les outils SSI existants ([PSSI], [TDBSSI], [MASSIA], [MAQSSIA], [ISO 15408], [ISO 17799]…).

2.4 Ce que ne permet pas la méthode EBIOS

L'étude EBIOS n'est pas un catalogue de solutions ou de règles de sécurité prêtes à l'emploi. Il ne s'agit en aucun cas d'une "boite noire" avec une entrée et une sortie. Dans ce contexte, elle ne permet pas de fournir de solutions immédiates et génériques aux problèmes de sécurité. En effet, les exigences de sécurité seront déterminées afin de spécifier des mesures de sécurité, mais leur mise en œuvre sera réalisée à la suite de l'étude.

2.5 Ce que permet la méthode EBIOS

2.5.1 Assister la maîtrise d'ouvrage

La méthode EBIOS contribue à l'élaboration des tâches que la maîtrise d'ouvrage doit réaliser :

- détermination de l'objet de l'étude en gardant une vision globale du système étudié dans son contexte ;
- expression des besoins (biens à protéger) ;
- identification des menaces ;
- détermination des actions de sécurité qu'il convient d'entreprendre ;
- détermination des éléments de spécification utiles pour la rédaction de [FEROS] ou [PP] ;
- définition d'un plan de projet et des responsabilités.

2.5.2 Offrir à la maîtrise d'œuvre un outil de choix et d'appréciation

La méthode EBIOS permet à la maîtrise d'œuvre de :

- adhérer aux objectifs exprimés par la maîtrise d'ouvrage ;
- répondre sur la faisabilité, les coûts et les délais induits ;
- choisir des solutions ;
- réaliser des cibles de sécurité.

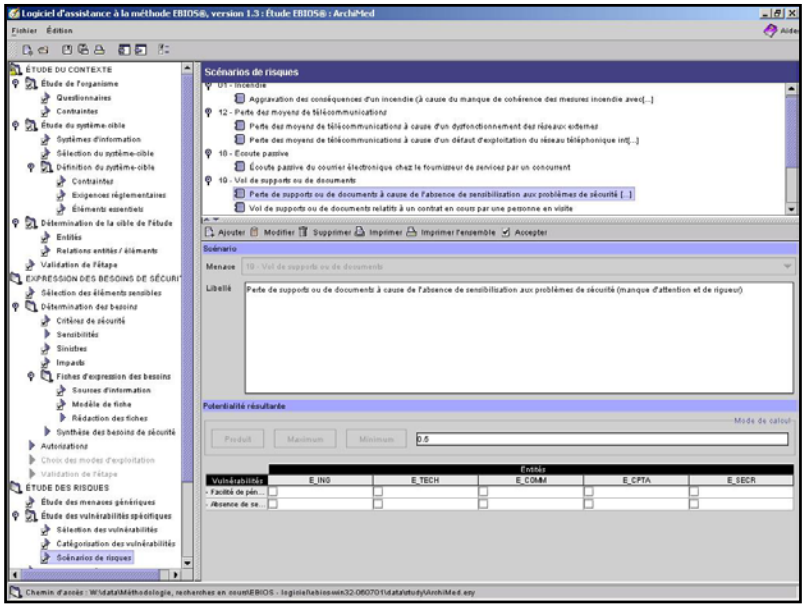
2.5.3 Offrir un outil de mesure d'impact et de négociation entre la maîtrise d'ouvrage et la direction (du projet, de l'organisme…)

La méthode EBIOS aide la direction à :

- mesurer l'impact sur l'environnement ;
- contrôler l'adéquation des SI ;
- centraliser les études et la SSI ;
- prendre des décisions stratégiques dans le domaine de la sécurité et des opérations.

3 Les outils de la méthode EBIOS

3.1 Le logiciel libre



Le logiciel EBIOS facilite grandement la réalisation des études EBIOS. Il permet en effet de consigner l'ensemble des résultats d'une étude et de produire les documents de synthèse nécessaires. D'une prise en main intuitive, il permet aussi de personnaliser ses bases de connaissances.

Il s'agit d'un logiciel libre, disponible gratuitement, avec ses sources, sur simple demande en envoyant ses coordonnées à ebios.dcssi@sgdn.pm.gouv.fr.

Il a été développé en Java et XML, et peut être amélioré par la communauté des utilisateurs dans la mesure où un retour est effectué au Secrétariat général de la défense nationale.

3.2 Les meilleures pratiques

La méthode EBIOS constitue une véritable boîte à outils modulaire. En effet, le déroulement des activités de la méthode et leur finesse peuvent varier selon le livrable attendu. À cet égard, un ensemble de meilleures pratiques a été rédigé pour expliquer comment exploiter les résultats de la méthode EBIOS en fonction de la finalité désirée.

- Élaboration d'un schéma directeur de la sécurité des systèmes d'information
- Élaboration d'une politique de sécurité des systèmes d'information [PSSI]
- Rédaction d'une FEROS (fiche d'expression rationnelle des objectifs de sécurité)
- Rédaction d'un SSRS (*System-specific Requirement Statement* – OTAN)
- Rédaction d'un profil de protection (conformément à l'ISO/IEC 15408)
- Rédaction d'une cible de sécurité (conformément à l'ISO/IEC 15408)
- Mise en œuvre d'un cadre de gestion de la sécurité de l'information
- Rédaction d'une politique de certification
- Étude d'un système à concevoir
- Étude d'un système existant…

Ces documents sont disponibles sur l'Internet (http://www.ssi.gouv.fr/).

3.3 La formation

Le CFSSI (centre de formation de la DCSSI) organise des stages de formation à la méthode EBIOS pour le secteur public français.

La DCSSI propose également une formation de formateurs afin de transférer les connaissances et d'éviter les éventuelles dérives dans la diffusion et l'emploi de la méthode.

Les renseignements relatifs aux formations sont disponibles sur Internet à l'adresse http://www.ssi.gouv.fr/formation.

3.4 Le club EBIOS

Le club des grands utilisateurs de la méthode EBIOS a été créé en 2003 afin de réunir une communauté d'experts, de partager des expériences et d'améliorer la méthode et ses outils.

Glossaire

La traduction en anglais des termes du glossaire figure entre parenthèses pour chaque terme. Le texte en italique correspond aux exemples. Le texte souligné dans les définitions correspond aux concepts définis dans le présent document.

Acceptation du risque
(risk acceptance)

Décision d'accepter un risque traité selon les critères de risque.

Analyse du risque
(risk analysis)

Utilisation systématique de données pour l'identification des origines des attaques et l'estimation du risque.

Appréciation du risque
(risk assessment)

Ensemble du processus d'analyse du risque et d'évaluation du risque. [ISO Guide 73]

Attaque
(attack)

Exploitation d'une ou plusieurs vulnérabilités à l'aide d'une méthode d'attaque avec une opportunité donnée.

Exemples :

- *forte opportunité d'utilisation de logiciels contrefaits ou copiés du fait de l'absence totale de sensibilisation ou d'information sur la législation des droits d'auteur ;*
- *altération du logiciel par un virus du fait de la facilité d'introduire des logiciels à effets malicieux sur le réseau bureautique de l'organisme ;*
- *…*

Besoin de sécurité
(sensitivity)

Définition précise et non ambiguë des niveaux correspondant aux critères de sécurité (disponibilité, confidentialité, intégrité…) qu'il convient d'assurer à un élément essentiel.

Bien
(asset)

Toute ressource qui a de la valeur pour l'organisme et qui est nécessaire à la réalisation de ses objectifs. On distingue notamment les éléments essentiels et les entités qu'il convient de protéger.

Exemples :

- *liste de noms ;*
- *requête de certification ;*
- *gestion de la facturation ;*
- *algorithme de chiffrement ;*
- *micro-ordinateur portable ;*
- *Ethernet ;*
- *système d'exploitation ;*
- *…*

Communication relative au risque
(risk communication)

Échange ou partage d'informations concernant le risque entre le décideur et d'autres parties prenantes. [ISO Guide 73]

Confidentialité
(confidentiality)

Propriété des éléments essentiels de n'être accessibles qu'aux utilisateurs autorisés.

Critère de sécurité — Caractéristique d'un élément essentiel permettant d'apprécier ses différents besoins de sécurité.

Critères de risque (risk criteria) — Termes de référence permettant d'apprécier l'importance des risques.

Disponibilité (availability) — Propriété d'accessibilité au moment voulu des éléments essentiels par les utilisateurs autorisés.

Élément essentiel (essential element) — Information ou fonction ayant au moins un besoin de sécurité non nul.

Exemples :

- *une liste de noms ;*
- *une requête de certification ;*
- *gérer la facturation ;*
- *un algorithme de chiffrement ;*
- *…*

Élément menaçant (threat agent) — Action humaine, élément naturel ou environnemental qui a des conséquences potentielles négatives sur le système. Elle peut être caractérisée par son type (naturel, humain, ou environnemental) et par sa cause (accidentelle ou délibérée). Dans le cas d'une cause accidentelle, elle est aussi caractérisée par une exposition et des ressources disponibles. Dans le cas d'une cause délibérée, elle est aussi caractérisée par une expertise, des ressources disponibles et une motivation.

Exemples :

- *ancien membre du personnel ayant peu de compétences techniques et de temps mais susceptible d'avoir une forte motivation ;*
- *pirate avec de fortes compétences techniques, bien équipé et une forte motivation liée à l'argent qu'il peut gagner ;*
- *climat très fortement pluvieux pendant trois mois par an ;*
- *virus ;*
- *utilisateurs ;*
- *développeurs ;*
- *…*

Entité (entity) — Il s'agit d'un bien qui peut être de type organisation, site, personnel, matériel, réseau, logiciel, système.

Exemples :

- *société d'infogérance ;*
- *locaux de l'organisme ;*
- *administrateur système ;*
- *micro-ordinateur portable ;*
- *Ethernet ;*
- *système d'exploitation ;*
- *portail de téléprocédure ;*
- *…*

Estimation du risque (risk estimation) — Processus utilisé pour affecter des valeurs à l'opportunité et aux pertes qu'un risque peut engendrer.

Évaluation du risque
(risk evaluation)

Processus de comparaison du risque estimé avec des critères de risque donnés pour déterminer l'importance d'un risque. [ISO Guide 73]

Exigence d'assurance de sécurité
(security assurance requirement)

Spécification d'assurance des fonctions de sécurité à mettre en œuvre pour participer à la couverture d'un ou plusieurs objectifs de sécurité, et portant généralement sur l'environnement de développement du système.

Exemples :

- *le développeur doit fournir des spécifications fonctionnelles ;*
- *les spécifications fonctionnelles doivent décrire le but et le mode d'emploi de toutes les interfaces externes des fonctions de sécurité, en fournissant, lorsque cela est approprié, les détails complets sur tous les effets, les exceptions et les messages d'erreur ;*
- *les éléments de preuve doivent justifier que les mesures de sécurité fournissent le niveau de protection nécessaire pour maintenir la confidentialité et l'intégrité du système ;*
- *…*

Exigence de sécurité
(security requirement)

Spécification fonctionnelle ou d'assurance sur le système d'information ou sur l'environnement de celui-ci, portant sur les mécanismes de sécurité à mettre en œuvre et couvrant un ou plusieurs objectifs de sécurité.

Exigence fonctionnelle de sécurité
(security functional requirement)

Spécification fonctionnelle des fonctions de sécurité à mettre en œuvre afin de participer à la couverture d'un ou plusieurs objectifs de sécurité portant sur le système-cible.

Exemples :

- *le système doit générer les clés cryptographiques conformément à un algorithme de génération de clés cryptographiques spécifié et à des tailles de clés cryptographiques spécifiées qui satisfont aux normes spécifiées ;*
- *le système doit détecter de façon non ambiguë une intrusion physique qui pourrait le compromettre ;*
- *un dispositif paratonnerre doit être mis en place dans les locaux de l'organisme ;*
- *…*

Expertise
(expertise)

Niveau attendu de compétence technique d'un élément menaçant dont la cause est délibérée. Ce niveau peut être caractérisé par des compétences techniques faibles, moyennes ou fortes.

Exemples [Guide 650] :

- *compétences techniques faibles ;*
- *compétences techniques moyennes ;*
- *compétences techniques fortes.*

Exposition
(exposure)

Niveau d'exposition naturelle d'un système-cible face à un élément menaçant dont la cause est accidentelle. Ce niveau peut être caractérisé par une exposition faible, modérée ou forte.

Exemples :

- *exposition faible ;*
- *exposition modérée ;*
- *exposition forte.*

Fonction
(function)

Traitement ou ensemble de traitements contribuant au fonctionnement d'une activité d'un organisme, qui crée, modifie, détruit ou transporte des informations.

Exemples :

- *créer des plans techniques ;*
- *établir les devis ;*
- *gérer la facturation ;*
- *un algorithme de chiffrement ;*
- *générer un certificat ;*
- *…*

Gestion du risque
(risk management)

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. [ISO Guide 73]

Hypothèse
(assumption)

Postulat, posé sur l'environnement opérationnel du système, permettant de procurer les fonctionnalités de sécurité attendues.

Exemples :

- *le système sera placé dans une pièce conçue pour minimiser les émanations électromagnétiques ;*
- *l'administrateur sera placé dans une zone d'accès réservé ;*
- *les utilisateurs n'écriront pas leurs mots de passe ;*
- *le réseau ne sera pas connecté à un réseau dont la confiance n'aura pas été établie ;*
- *chacun au sein de la société connaît ses responsabilités en cas de diffusion illicite d'informations métiers ou de manipulation illégale de données nominatives ;*
- *…*

Identification des origines des attaques
(source identification)

Processus permettant de trouver, recenser et caractériser les origines des attaques (éléments menaçants et méthodes d'attaque).

Impact
(impact)

Conséquence sur l'organisme de la réalisation d'une menace.

Exemples :

- *perte d'image de marque vis-à-vis de la clientèle ;*
- *perte financière à hauteur de 10% du chiffre d'affaires ;*
- *infraction aux lois et aux règlements donnant lieu à des poursuites judiciaires à l'encontre du Directeur ;*
- *…*

Information
(information)

Renseignement ou élément de connaissance susceptible d'être représenté sous une forme adaptée à une communication, un enregistrement ou un traitement. [IGI 900] [REC 901]

Exemples :

- *un message ;*
- *une liste de noms ;*
- *une requête de certification ;*
- *liste de révocation ;*
- *…*

Intégrité
(integrity)

Propriété d'exactitude et de complétude des éléments essentiels.

Menace
(threat)

Attaque possible d'un élément menaçant sur des biens.

Exemples :

- *un ancien membre du personnel, ayant peu de compétences techniques mais susceptible d'avoir une forte motivation, altère volontairement les logiciels du système par un virus, profitant de la facilité d'introduire des logiciels à effets malicieux sur le réseau bureautique de l'organisme ; ceci pouvant notamment affecter la fonction d'établissement de devis et la génération de certificats de signature ;*
- *un pirate avec une bonne expertise, un matériel standard et payé pour le faire, vole des fichiers confidentiels en accédant à distance au réseau de la société ;*
- *un développeur, membre du personnel, avec une très bonne expertise des codes sources mais peu de connaissances SSI, modifie volontairement le code source ;*
- *un visiteur vole un matériel contenant des informations confidentielles ;*
- *…*

Mesure de sécurité
(security measure)

Moyen destiné à améliorer la sécurité, spécifié par une exigence de sécurité et à mettre en œuvre pour la satisfaire. Il peut s'agir de mesures de prévision ou de préparation, de dissuasion, de protection, de détection, de confinement, de "lutte", de récupération, de restauration, de compensation…

Méthode d'attaque
(attack method)

Moyen type (action ou événement) pour un élément menaçant de réaliser une attaque.

Exemples :

- *vol de supports ou de documents ;*
- *piégeage du logiciel ;*
- *atteinte à la disponibilité du personnel ;*
- *écoute passive ;*
- *crue ;*
- *…*

Motivation
(motivation)

Motif d'un élément menaçant. Elle peut avoir un caractère stratégique, idéologique, terroriste, cupide, ludique ou vengeur et diffère selon qu'il s'agit d'un acte accidentel (curiosité, ennui…) ou délibéré (espionnage, appât du gain, volonté de nuire, idéologie, jeu, fraude, vol, piratage, défi intellectuel, vengeance, chantage, extorsion de fonds…).

Exemples [Guide 650] :

- *caractère stratégique ;*
- *caractère idéologique ;*
- *caractère terroriste ;*
- *caractère cupide ;*
- *caractère ludique ;*
- *caractère vengeur ;*

[…]

- *dans le cas d'un acte délibéré :*
  - *espionnage,*
  - *appât du gain,*
  - *volonté de nuire,*
  - *idéologie,*
  - *jeu,*
  - *fraude,*
  - *vol,*
  - *piratage,*

- *défi intellectuel,*
- *vengeance,*
- *chantage,*
- *extorsion de fonds,*
- *…*

- *dans le cas d'un acte accidentel :*
  - *curiosité,*
  - *ennui,*
  - *…*

Objectif de sécurité (security objective)

Expression de l'intention de contrer des menaces ou des risques identifiés (selon le contexte) et/ou de satisfaire à des politiques de sécurité organisationnelles et à des hypothèses ; un objectif peut porter sur le système-cible, sur son environnement de développement ou sur son environnement opérationnel.

Exemples :

- *objectifs "ouverts" (grande marge de manœuvre pour couvrir l'objectif de sécurité) :*
  - *les configurations des postes du réseau interne doivent être évolutives ;*
  - *les locaux doivent être protégés contre la foudre ;*
  - *…*
- *objectifs "fermés" (faible marge de manœuvre pour couvrir l'objectif de sécurité) :*
  - *le système doit identifier et authentifier de façon unique les utilisateurs, et ce, avant toute interaction entre le système et l'utilisateur ;*
  - *deux antivirus différents et compatibles doivent être mis en place et leurs bases de signatures mises à jour toutes les deux semaines ;*
  - *…*

Opportunité (opportunity)

Mesure de la possibilité de survenance d'une attaque.

Exemples :

- *improbable ;*
- *fortement probable ;*
- *totalement infaisable ;*
- *15 % de chances de se réaliser ;*
- *…*

Politique de sécurité de système d'information (information systems security policy)

Ensemble, formalisé dans un document applicable, des éléments stratégiques, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection du (des) système(s) d'information de l'organisme. [PSSI]

Principe de sécurité (security principle)

Les principes de sécurité sont l'expression des orientations de sécurité nécessaires et des caractéristiques importantes de la sécurité pour l'élaboration d'une politique et en particulier des règles de sécurité la constituant. [PSSI]

Prise de risque (risk retention)

Acceptation de la charge de la perte d'un risque particulier.

Réduction du risque (risk reduction)

Processus visant à minimiser les conséquences négatives et les opportunités d'une menace.

Règle de sécurité
(organisational security policy)

Règle, procédure, code de conduite ou ligne directrice de sécurité qu'une organisation impose pour son fonctionnement. [ISO 15408]

Exemples :

- *tous les produits utilisés par l'État doivent être conformes aux normes nationales pour la génération de mots de passe et la cryptologie ;*
- *tous les produits utilisés dans le domaine bancaire doivent être certifiés au niveau EAL4 augmenté du composant ADV_IMP.2 ;*
- *le contrôle d'accès se fait par identifiant / mot de passe ;*
- *chaque ingénieur est responsable du fichier qu'il traite ;*
- *une alarme anti-intrusion est active durant les heures de fermeture (19h-7h) ;*
- *…*

Ressources disponibles
(available resources)

Moyens attendus d'un élément menaçant. Le niveau des ressources disponibles constitue son potentiel d'attaque et peut être caractérisé par des ressources faibles, modérées ou élevées.

Exemples :

- *ressources faibles ;*
- *ressources modérées ;*
- *ressources élevées.*

Risque
(risk)

Combinaison d'une menace et des pertes qu'elle peut engendrer, c'est-à-dire : de l'opportunité de l'exploitation d'une ou plusieurs vulnérabilités d'une ou plusieurs entités par un élément menaçant employant une méthode d'attaque ; et de l'impact sur les éléments essentiels et sur l'organisme.

Exemples :

- *un ancien membre du personnel, ayant peu de compétences techniques mais susceptible d'avoir une forte motivation, altère volontairement les logiciels du système par un virus, profitant de la facilité d'introduire des logiciels à effets malicieux sur le réseau bureautique de l'organisme ; ceci pouvant notamment affecter la disponibilité et l'intégrité de la fonction d'établissement de devis et de la génération de certificats de signature, ce qui pourrait engendrer une incapacité à fournir un service, une impossibilité de remplir des obligations contractuelles et de graves conséquences en termes d'image de marque ;*
- *un pirate avec une bonne expertise, un matériel standard et payé pour le faire, vole des fichiers confidentiels en accédant à distance au réseau de la société, entraînant de ce fait l'échec d'une transaction avec un partenaire et une perte d'image de marque ;*
- *…*

Risque résiduel
(residual risk)

Risque subsistant après le traitement du risque. [ISO Guide 73]

Sécurité des systèmes d'information (SSI)
(information security)

Protection des systèmes d'information, et en particulier des éléments essentiels, contre toute atteinte des critères de sécurité non autorisée, qu'elle soit accidentelle ou délibérée.

Système d'information (SI)
(information system)

Ensemble d'entités organisé pour accomplir des fonctions de traitement d'information.

Traitement du risque
(risk treatment)

Processus de sélection et de mise en œuvre des mesures visant à modifier le risque, ce qui signifie une réduction du risque, un transfert du risque ou une prise de risque.

Transfert du risque
(risk transfer)

Partage avec une autre partie de la charge de la perte d'un risque particulier.

Exemples :

- *souscription d'une assurance ;*
- *…*

Utilisateur
(user)

Personne ou chose qui utilise les services d'une organisation.

Vulnérabilité
(vulnerability)

Caractéristique d'une entité qui peut constituer une faiblesse ou une faille au regard de la sécurité des systèmes d'information.

Exemples :

- *absence d'organisation sécurité incendie pour une entité de type Organisation ;*
- *peu de sensibilisation aux problèmes de sécurité pour une entité de type Personnel ;*
- *facilité de pénétrer sur le site pour une entité de type Site ;*
- *possibilité de créer ou modifier des commandes systèmes pour une entité de type Réseau ;*
- *…*

Acronymes

BCS	Bureau Conseil en Sécurité des systèmes d'information
CC	(*Common Criteria*) – Critères Communs, l'intitulé utilisé historiquement pour la norme à la place de l'intitulé officiel de l'ISO : "Critères d'évaluation de la sécurité des technologies de l'information"
CFSSI	Centre de Formation en Sécurité des Systèmes d'Information
DCSSI	Direction Centrale de la Sécurité des Systèmes d'Information
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité
FEROS	Fiche d'Expression Rationnelle des Objectifs de Sécurité des SI
PP	(*Protection Profile*) – Profil de protection
PSSI	Politique de Sécurité des Systèmes d'Information
SDO	Sous-Direction des Opérations
SDSSI	Schéma Directeur de la Sécurité des Systèmes d'Information
SGDN	Secrétariat Général de la Défense Nationale
SI	Système d'Information
SSI	Sécurité des Systèmes d'Information
TIC	Technologies de l'Information et de Communication

Références bibliographiques

[eEurope 2005] *Plan d'action eEurope 2005 : une société de l'information pour tous, COM(2002)263 final* – Commission européenne (2002).

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

Disponible sur le site http://www.ssi.gouv.fr

[Guide 650] *La menace et les attaques informatiques* – N°650 / DISSI / SCSSI (1994).

Disponible sur le site http://www.ssi.gouv.fr

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

[IGI 900] *La sécurité des systèmes d'information qui font l'objet d'une classification de défense pour eux-mêmes ou pour les informations traitées* – SGDN et DISSI (1993).

[ISO 13335] *Information technology – Security techniques – Guidelines for the management of IT security (GMITS)* – International Organization for Standardization (ISO) (2001).

[ISO 15408] *Critères Communs pour l'évaluation de la sécurité des Technologies de l'Information*, – International Organization for Standardization (ISO) – version 2.0 (1998).

[ISO 17799] *Information technology – Code of practice for information security management* – International Organization for Standardization (ISO) (2000).

[ISO Guide 73] *Management du risque – Vocabulaire – Principes directeurs pour l'utilisation dans les normes* – International Organization for Standardization (ISO) (2002).

[MASSIA] *Méthode d'Audit de la Sécurité des Systèmes d'Information de l'Armement* – CELAR/CASSI/GESSI – version 1.0 (1994).

[OCDE] *Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité* – Organisation de coopération et de développement économiques (OCDE) (2002).

[PSSI] *Guide d'élaboration de politique de sécurité de système d'information* – DCSSI (2004).

Disponible sur le site http://www.ssi.gouv.fr

[REC 901] *Recommandation pour la protection des systèmes d'information traitant des informations sensibles non classifiées de défense* – SGDN et DISSI (1994).

TDBSSI *Guide d'élaboration de tableaux de bord de sécurité de système d'information pour les administrations* – DCSSI (2004).

Disponible sur le site http://www.ssi.gouv.fr

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
conseil.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