**Nicolas Mayer** – nicolas.mayer@tudor.lu
Ingénieur R&D – Centre de Recherche Public Henri Tudor – Luxembourg ; Doctorant à l'Institut d'Informatique de l'Université de Namur
**Jean-Philippe Humbert** – jean-philippe.humbert@tudor.lu
Ingénieur R&D – Centre de Recherche Public Henri Tudor – Luxembourg ; Doctorant au Centre de Recherche sur les Médiations (CREM) – Université Paul Verlaine de Metz

# La méthode EBIOS : présentation et perspective d'utilisation pour la certification ISO 27001

*EBIOS est actuellement la méthode de gestion des risques de sécurité des systèmes d'information (SSI) développée et maintenue par la DCSSI (Direction centrale de la sécurité des systèmes d'information - France). Cette méthode a la particularité d'être disponible gratuitement, pour tout organisme souhaitant mener une étude des risques SSI et mettre en place une politique adéquate de sécurité de l'information. L'article présente de manière générale la méthode et ses spécificités, puis montre ses perspectives dans le domaine en plein développement que constitue la certification ISO 27001.*

## 1. Introduction

Le développement économique de tout organisme repose aujourd'hui sur l'utilisation quasi-systématique d'outils informatiques et bureautiques, généralement interconnectés à différents réseaux de télécommunication et principalement à Internet. Cependant, les programmes ou protocoles sur lesquels reposent ces technologies n'ont pas été développés avec des exigences fortes de sécurité. De fait, les différents organismes, via leur système d'information (SI) et de communication, apparaissent, la plupart du temps, vulnérables aux multiples menaces pesant sur eux. Afin de protéger leurs ressources et faire face à ces différents dangers, la SSI cherche à déterminer les besoins de sécurité (généralement en termes de confidentialité, d'intégrité et de disponibilité, mais parfois également de traçabilité, non-répudiation…), et en conséquence, les mesures de sécurité à mettre en œuvre, qu'elles soient techniques (logiciels, matériels, réseaux, télécoms, supports…) ou non techniques (organisations, lieux, personnels…).
Pour faciliter cette démarche, la gestion des risques SSI permet de satisfaire les besoins de sécurité exprimés, mais ce processus demeure difficile à appréhender pour des non-spécialistes. Lors d'un précédent article paru dans MISC 24 [3], la gestion des risques SSI a été présentée dans son ensemble. L'article avait pour but de détailler les concepts sous-jacents, ainsi que le processus (générique) employé lors d'une démarche de gestion des risques. Pour rappel, la gestion des risques SSI a trois finalités principales :

1. Améliorer la sécurisation des SI
2. Justifier le budget alloué à la sécurisation du SI
3. Prouver la crédibilité du SI en termes de sécurité à l'aide des analyses effectuées

Au niveau de la sécurisation du SI, une méthode de gestion des risques SSI est donc un outil d'analyse, identifiant les risques de sécurité pesant sur l'organisme, puis y remédiant en proposant des solutions à ces risques. Il sera bien entendu du ressort de l'entreprise de veiller à la bonne mise en place de ces solutions, afin que la sécurité soit effective. Il faut toutefois noter que les méthodes de gestion des risques SSI permettent généralement un suivi de ces étapes d'implémentation à l'aide, par exemple, de tableaux de bord, puis assurent une démarche d'amélioration continue de la sécurité, point sur lequel nous reviendrons au sein de la section 4.
Afin de conduire efficacement une démarche de ce type, il est vivement conseillé de faire confiance à des méthodes éprouvées. Un challenge ? Certainement, car plus de 200 méthodes de gestion/analyse des risques se déclinent actuellement à travers le monde

(OCTAVE [10], MEHARI [11], CRAMM [12]…). Au cœur de ces méthodes, certaines sont actuellement très populaires, faisant référence dans leur domaine [3]. L'objectif de cet article est de présenter l'une d'elles : la méthode EBIOS [1], qui constitue aujourd'hui une réponse efficace à cette problématique de gestion des risques.

## 2. EBIOS : la réponse de la DCSSI à la problématique de gestion des risques SSI

Historiquement, le gouvernement français, qui s'est engagé dans le domaine de l'administration électronique, a souhaité répondre concrètement au problème de développement des SI peu sécurisés. En effet, la 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), de contribuer à la définition interministérielle et à l'expression de la politique gouvernementale en matière de SSI. La DCSSI publie des guides méthodologiques, disponibles gratuitement [4] et destinés à contribuer à l'amélioration de la sécurisation des SI des organismes publics ou privés. Ils s'appuient sur des documents éprouvés au sein de l'administration, ainsi que sur l'expérience et le savoir-faire de nombreux industriels.
Parmi ces guides, la DCSSI a développé un outil essentiel en termes de gestion des risques : une méthodologie complète, gratuite, outillée et mise à jour par consensus avec des experts représentatifs des besoins du marché. Il s'agit de la méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité), créée en 1995 et mise à jour en 2004, qui se décompose en cinq sections (Introduction, Démarche, Techniques, Outillage pour l'appréciation des risques et Outillage pour le traitement des risques), accompagnées de documents de références sur les meilleures pratiques d'utilisation, et d'un logiciel support. L'objectif général de la méthode est la formalisation d'objectifs et d'exigences de sécurité adaptés aux besoins du système étudié et de son contexte. La méthode est disponible en 4 langues [4,5] et des formations à la méthode sont régulièrement dispensées (CFSSI [6], ENST [7], FIDENS [8]…). La méthode est actuellement utilisée par de nombreux organismes, aussi bien publics (Ministères, OTAN, Caisse Nationale d'Assurance Maladie…) que privés (Michelin, Aéroports de Paris…).

## 3. La démarche EBIOS

La démarche EBIOS se décompose en 5 étapes présentant les activités à réaliser dans le cadre d'une étude des risques SSI. Il faut noter que l'ensemble des activités proposées peuvent être adaptées, afin de répondre au mieux aux besoins d'une organisation donnée vis-à-vis de son contexte et de ses caractéristiques (type d'organisation, taille de la structure, culture…). Les 5 étapes sont résumées ci-dessous et représentées sur la figure 1. Une étude de cas, proposant l'application de la méthode à une entreprise, est disponible [1] et permet d'avoir un exemple concret de la démarche.

**Nicolas Mayer** – nicolas.mayer@tudor.lu
Ingénieur R&D – Centre de Recherche Public Henri Tudor – Luxembourg ; Doctorant à l'Institut d'Informatique de l'Université de Namur
**Jean-Philippe Humbert** – jean-philippe.humbert@tudor.lu
Ingénieur R&D – Centre de Recherche Public Henri Tudor – Luxembourg ; Doctorant au Centre de Recherche sur les Médiations (CREM) – Université Paul Verlaine de Metz

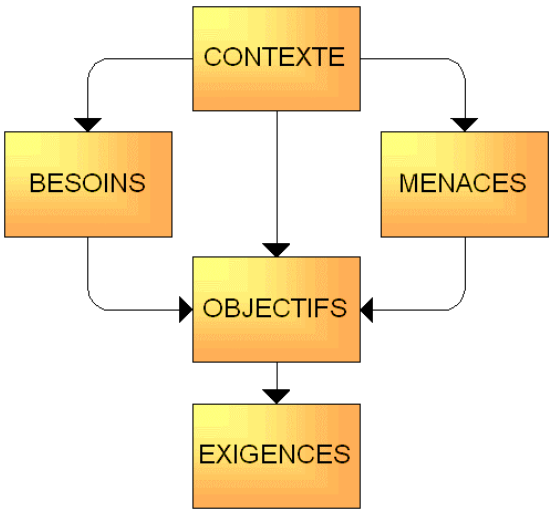


**Figure 1: La démarche EBIOS**

### Étape 1 : Étude du contexte

Lors de cette première étape, l'organisme est présenté (métier, mission, structure...), ses caractéristiques et ses contraintes (politiques, stratégiques, légales…) sont détaillées et son SI décrit fonctionnellement. Le "système cible", correspondant au sous-ensemble du SI global qui va être étudié, est délimité et ses enjeux sont mis en évidence.
Au sein du système cible sont identifiés les *assets*[1] au niveau *business*, ou "éléments essentiels", généralement partagés entre les fonctions (ex : gestion d'un produit d'assurance, comptabilité…) et les informations (ex : données clients, procédure…) sensibles.
À partir des éléments essentiels, il est facile de déduire les ressources du SI sur lesquelles ils reposent, appelées ici : "entités". 7 types d'entités sont identifiés : les matériels (ex : serveur, desktop…), les logiciels (ex : système d'exploitation, suite bureautique…), les réseaux (ex : réseau WIFI, réseau Ethernet…), les personnels (ex : personnel de maintenance du SI...), les sites (ex : centre informatique…), les organisations (ex : procédures…) et les systèmes (ex : agrégats d'entités appartenant aux autres types décrits ci-avant).
Cette première étape est à considérer avec la plus grande attention et constitue régulièrement la partie demandant le plus de temps. En effet, elle implique de nombreux acteurs (décideurs, maîtrise d'ouvrage, responsables métiers…) qui doivent s'accorder précisément sur la délimitation d'un périmètre et sur son fonctionnement. Nous obtenons donc comme résultats principaux à cette étape une description complète du contexte ainsi qu'une identification précise des éléments essentiels à protéger, faisant partie du métier de l'organisation et reliés aux entités les supportant au sein du SI.

### Étape 2 : Expression des besoins de sécurité

En guise de préliminaire à cette étape sont choisis les critères de sécurité à prendre en compte (généralement disponibilité, intégrité et confidentialité). Pour chaque critère est

[1] Asset est un anglicisme couramment utilisé dans le domaine qui définit un bien, actif, ressource ayant de la valeur pour l'organisme et nécessaire à son bon fonctionnement.

défini une échelle présentant les différents niveaux de besoins associés à l'aide de valeurs (par exemple, de 0 à 4).
Les impacts majeurs que souhaite éviter l'organisme (ex : perte d'image de marque, atteinte à la sécurité du personnel…) sont mis en évidence afin d'aider à envisager différents points de vue dans l'expression des besoins de sécurité. Pour chaque élément essentiel, en fonction de chaque critère de sécurité et de chaque impact majeur, il est alors possible de définir la valeur limite acceptable dans l'échelle précédemment déterminée. Une fois la valeur choisie, l'impact réel du non-respect de ce besoin peut être estimé et les choix effectués doivent être justifiés, notamment lorsqu'un consensus entre plusieurs personnes doit être obtenu. La méthode permet ainsi aux maîtrises d'ouvrage, aux utilisateurs et aux responsables métiers ou équivalents d'exprimer leurs propres besoins de sécurité pour les éléments essentiels les concernant et les conséquences possibles de l'atteinte de ces besoins.

**Étape 3 : Étude des menaces**

Au vu des entités composant le système cible et à l'aide des bases de connaissances de la méthode EBIOS, sont mises en évidence les menaces pertinentes pesant sur le SI.
La méthode permet tout d'abord de se focaliser sur des types d'incidents ou de sinistres, appelés "méthodes d'attaque", et de préciser les critères de sécurité qu'ils peuvent affecter. Pour chacune d'elles, les "éléments menaçants" à leur origine pourront être décrits et caractérisés suivant leur type (généralement naturel ou humain), leur cause (accidentelle ou délibérée), et un niveau reflétant leur potentiel (motivation, ressources, expertise…).
En s'appuyant sur les bases de connaissances, ainsi que sur l'expertise disponible, les vulnérabilités exploitables du système cible (techniques, organisationnelles, humaines…) peuvent alors être recensées et évaluées. Les menaces sont ainsi formulées et rédigées de manière claires et explicites, et leur possibilité de réalisation, appelée "opportunité", peut être estimée à l'aide d'une échelle pouvant aller, par exemple, de 0 (totalement improbable) à 4 (certain). Cette étape permet d'obtenir une liste exhaustive et ordonnée de l'ensemble des menaces pouvant se réaliser.

**Étape 4 : Identification des objectifs de sécurité**

Afin de faire émerger les risques réels pesant sur le système étudié, l'ensemble des besoins de sécurité exprimés à l'étape 2 est confronté à l'ensemble des menaces identifiées à l'étape 3. Chaque risque est donc défini précisément, en intégrant son(ses) impact(s) mis en évidence à l'étape 2. Le classement des risques (obtenu grâce à la sévérité des impacts et l'opportunité des menaces), permettra de déterminer les priorités des mesures de sécurité à mettre en place. Pourront également être ignorés de la suite de l'étude certains risques (qui seront donc résiduels), caractérisés par une opportunité ou un impact suffisamment faible, en justifiant clairement ce choix. Ces risques seront considérés comme acceptés.
La méthode permet ensuite de déterminer des objectifs de sécurité, qui présentent la volonté de couvrir les risques, sans préjuger des solutions pour y parvenir. Une liste très complète d'objectifs de sécurité génériques est proposée au sein des bases de connaissances. Le but est de pouvoir couvrir l'ensemble des risques, tout en respectant les caractéristiques du contexte identifiées lors de l'étape 1. Il est alors possible de rechercher si chaque risque identifié en amont présente un objectif de sécurité visant à le mitiger, afin d'assurer la complétude de l'étude. Cette étape initie le traitement des risques.

Une fois les objectifs de sécurité définis, une FEROS (Fiche d'Expression Rationnelle des Objectifs de Sécurité) peut être rédigée, ayant pour but de formaliser tous les éléments nécessaires à l'acceptation de la mise en oeuvre d'un système par une autorité. A noter que ce document est obligatoire dans le cas de systèmes traitant des informations classifiées de défense et recommandé dans les autres cas [15].

#### Étape 5 : Détermination des exigences de sécurité

La liste des exigences de sécurité est établie. Elles représentent les moyens d'atteindre les objectifs de sécurité et donc de traiter précisément les risques. Nous devons ensuite justifier la complétude des exigences de sécurité vis-à-vis des objectifs de sécurité. De même que pour les objectifs de sécurité, une liste très complète d'exigences de sécurité est fournie. Celle-ci s'appuie, entre autres, sur les exigences de la norme ISO 17799 [13], des Critères Communs [14] (ISO 15408), mais également sur un complément d'exigences propres à la méthode. Tout autre référentiel de meilleures pratiques peut également être intégré (ex : *IT-Grundschutz Manual* [9] du BSI allemand…).
Au terme de cette étape, il restera à implémenter les mesures concrètes, spécifiées par les exigences de sécurité et alignées avec les contraintes de l'entreprise (réglementation, budget, temps, compétences et ressources disponibles…).

## 4. Certification ISO 27001: les perspectives d'utilisation d'EBIOS

La norme ISO 27001 [2] définit un modèle pour mettre en place un Système de Management de la Sécurité de l'Information (SMSI ou encore Information Security Management System (ISMS)). Ce modèle doit être basé sur une approche de gestion des risques, définissant un ensemble de mesures de sécurité. Il permet d'assurer qu'une organisation de la sécurité de l'information est en place et s'inscrit dans un processus d'amélioration continue. Pour cela, la norme reprend le cycle « PDCA » de Deming (Figure 2), instancié à la sécurité des SI.

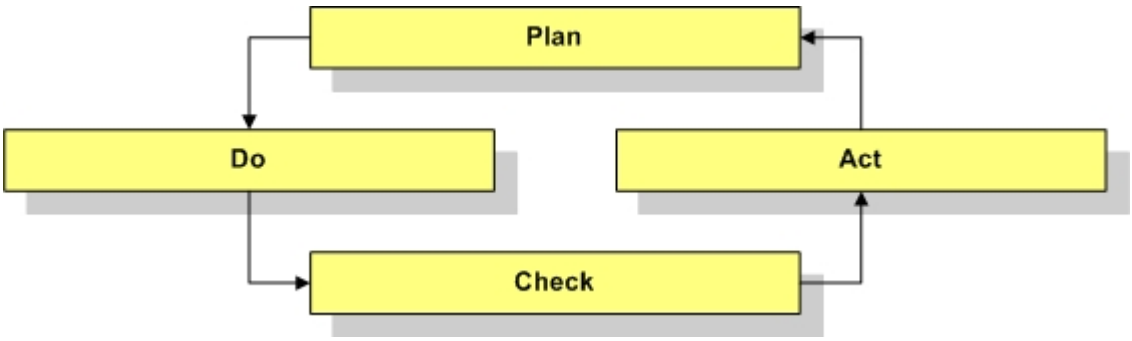


**Figure 2: Le cycle PDCA**

***Plan*** : définir le cadre de l'ISMS, apprécier et spécifier le traitement des risques de sécurité des SI
***Do*** : implémenter et maintenir les mesures
***Check*** : vérifier que les mesures fonctionnent conformément à l'étape « *Plan* » et identifier les améliorations possibles de l'ISMS

***Act*** : mettre en œuvre les améliorations identifiées pour l'ISMS

La norme n'imposant aucune méthode pour l'appréciation des risques, chaque organisme préparant la certification est libre de choisir celle qu'il souhaite utiliser. EBIOS rentre dans ce cadre et offre un certain nombre d'avantages en vue d'une démarche de certification ISO 27001, aussi bien au niveau méthodologique (méthode support à la démarche spécifiée dans la norme, identification structurée des besoins, justification du choix des objectifs et contrôles de sécurité…), qu'au niveau des résultats (méthode compatible avec la liste de contrôles fournie dans l'annexe A de la norme, résultats réutilisables en vue des itérations successives de l'ISMS…).

EBIOS intervient principalement dans la première étape de l'ISMS (*Plan*), mais également dans les trois étapes suivantes (*Do, Check, Act*) :

Étape 1 – *Plan* : indispensable à cette étape, EBIOS supporte efficacement l'ensemble des actions, notamment la définition du périmètre, l'appréciation des risques et la spécification du traitement des risques

Étape 2 – *Do* : EBIOS contribue à l'élaboration du plan de traitement des risques et à la communication relative aux risques

Étape 3 – *Check* : EBIOS fournit le référentiel d'audit et l'étude est réactualisée pour mettre à jour le niveau de risques

Étape 4 – *Act* : la réitération et la traçabilité d'EBIOS permettent une amélioration continue de l'ISMS

En support à la méthode et pour approfondir ces points, des documents spécifiques à l'utilisation d'EBIOS pour la mise en place d'un ISMS et son exploitation dans le cadre d'une préparation à la certification ISO 27001 sont disponibles sur le site [4] :

« Mise en œuvre dans le cadre d'une démarche ISO 27001 »

« Mise en place d'un système de gestion de la sécurité des systèmes d'information à l'aide de la méthode EBIOS »

## 5. Conclusion

L'utilisation des méthodes de gestion des risques est devenue systématique pour les entreprises soucieuses de leur sécurité. EBIOS, en tant que véritable boîte à outil de la gestion des risques, contribue à de nombreuses démarches de sécurité permettant d'élaborer le socle de la SSI (schéma directeur, politique de sécurité, tableaux de bord) et de rédiger des spécifications de sécurité (FEROS, profil de protection, cible de sécurité, politique de certification ou d'autres formes de cahiers des charges et plans d'action). La méthode EBIOS présente l'avantage de structurer une démarche complète de construction du risque, à partir de l'existant de l'organisation concernée. Associées à cette démarche, les bases de connaissance, remises à jour constamment, ainsi qu'un logiciel "open source" disponible gratuitement, fournissent un support rapide et efficace. La méthode EBIOS est souvent présentée en "concurrence", avec d'autres méthodes de gestion des risques SSI. Cependant, au-delà des comparaisons, EBIOS propose une démarche singulière de construction des risques, dégagée de toute préoccupation commerciale, et s'adaptant à tout type d'organisation, qu'elle soit privée ou publique.

Avec l'émergence de la norme ISO 27001, dans la lignée de l'ISO 9001 pour la qualité et de l'ISO 14001 pour l'environnement, le nombre de certificats 27001 ne cesse d'augmenter, et le domaine de la normalisation de la SSI s'organise ainsi pour créer un

cadre homogène de normes adaptées à ces évolutions (série 2700x, nouveaux groupes de travail 4 et 5 de l'ISO/JTC1/SC27…). Il convient, dès lors, à tout niveau de l'entreprise, de tenir compte de ces développements ; c'est notamment le rôle du RSSI, en première ligne, qui se doit aussi de connaître les outils à sa disposition, pour assurer la mise en place, la maintenance et l'amélioration continue de la sécurité de l'information de manière globale. De fait, les méthodes phares de gestion des risques de sécurité, telle qu'EBIOS, retiennent plus que jamais l'attention.

# BIBLIOGRAPHIE

[1] Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS), Direction centrale de la sécurité des systèmes d'information, Février 2004, http://www.ssi.gouv.fr/fr/confiance/ebiospresentation.html.
Contact : ebios.dcssi@sgdn.pm.gouv.fr
[2] ISO 27001:2005, Information Technology, Security Techniques, Information Security Management Systems – Requirements
[3] J.-P. Humbert, N. Mayer, La gestion des risques pour les systèmes d'information, MISC 24, Mars-Avril 2006
[4] http://www.ssi.gouv.fr
[5] http://www.cases.lu
[6] CFSSI (Centre de Formation à la Sécurité des Systèmes d'Information), http://www.formation.ssi.gouv.fr/
[7] ENST (École Nationale Supérieure des Télécommunications), http://www.enst.fr/
[8] FIDENS, http://www.fidens.fr/
[9] BSI - Germany, IT-Grundschutz Manual, 2004, http://www.bsi.bund.de/english/gshb/
[10] Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) v2.0, Carnegie Mellon - Software Engineering Institute, October 2001. http://www.cert.org/octave/
[11] Méthode Harmonisée d'Analyse de Risques (MEHARI), Principes et mécanismes, CLUSIF, Version 3, Octobre 2004. http://www.clusif.asso.fr/
[12] CCTA Risk Analysis and Management Method (CRAMM), http://www.cramm.com/
[13] ISO/IEC 17799:2005, Information Technology – Security techniques - Code of Practice for Information Security Management. http://www.iso.org/
[14] Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005, http://www.commoncriteriaportal.org
[15] Meilleures pratiques pour la gestion des risques SSI : Utilisation spécifique de la méthode EBIOS pour rédiger une FEROS, Direction centrale de la sécurité des systèmes d'information, Avril 2005.