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 gestion des risques pour les systèmes d'information

Au sein des entreprises, la sécurité des systèmes d'information est de plus en plus abordée à l'aide d'approches basées sur les risques. L'expérience montre que de telles études prospectives réduisent de manière considérable les pertes liées aux faiblesses de sécurité des systèmes d'information. Cette tendance est aussi perceptible dans l'évolution du métier de security officer, qui s'étend de plus en plus à celui de risk manager. Partant de ce constat et afin de mieux appréhender la gestion des risques, cet article introductif a pour but de présenter l'ensemble des concepts du domaine, ainsi que son processus, puis trois méthodes parmi les plus intéressantes du marché.

1. Introduction

Le concept de gestion des risques (ou risk management) a très certainement fait son apparition à la fin des années 50 aux États-Unis dans le domaine financier, en relation avec des questions d'assurance [1]. Par la suite, la notion de gestion des risques a été étendue à d'autres domaines, citons notamment l'environnement, la gestion de projet, le marketing, ainsi que la sécurité informatique, qui nous intéresse tout particulièrement. Cet article a pour objectif de présenter la gestion des risques de sécurité des SI (Systèmes d'Information), qui constituent uniquement une partie des risques généralement associés aux activités nécessitant un SI. Nous ne traiterons pas, par exemple, les risques ayant des causes d'ordre financier (comme des décisions en matière d'investissement) ou organisationnel (par exemple une embauche pour un poste à responsabilité). Dans la suite de cet article, la notion de « gestion des risques » se limitera donc à la « gestion des risques de sécurité liés aux SI ».

La gestion des risques est définie par l'ISO [8] comme l'ensemble des activités coordonnées visant à diriger et piloter un organisme vis-à-vis du risque. On dégage en général trois finalités à la gestion des risques pour les SI :

1. Améliorer la sécurisation des systèmes d'information.
2. Justifier le budget alloué à la sécurisation du système d'information.
3. Prouver la crédibilité du système d'information à l'aide des analyses effectuées.

Bien qu'un grand nombre ne soit plus utilisé ou confidentiel, on estime qu'il existe plus de 200 méthodes de gestion des risques. Cette multiplicité entraîne une très grande diversité dans les approches des risques de sécurité. Le but de cet article est de présenter et synthétiser les éléments de base de la gestion des risques, ainsi que trois des principales méthodes actuellement utilisées.

2. Les fondements

Pour bien appréhender la gestion des risques, ses objectifs et ses limites, il est nécessaire de comprendre en premier lieu les concepts sous-jacents et le processus employé.

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

2.1 Concepts de la gestion des risques

La gestion des risques, « dans son plus simple appareil », se compose de trois blocs interdépendants. Nous distinguons l'organisation cible de l'étude, définie par ses assets[1] et ses besoins de sécurité, puis les risques pesant sur ces assets et enfin les mesures prises ayant pour but de traiter les risques et donc d'assurer un certain niveau de sécurité.

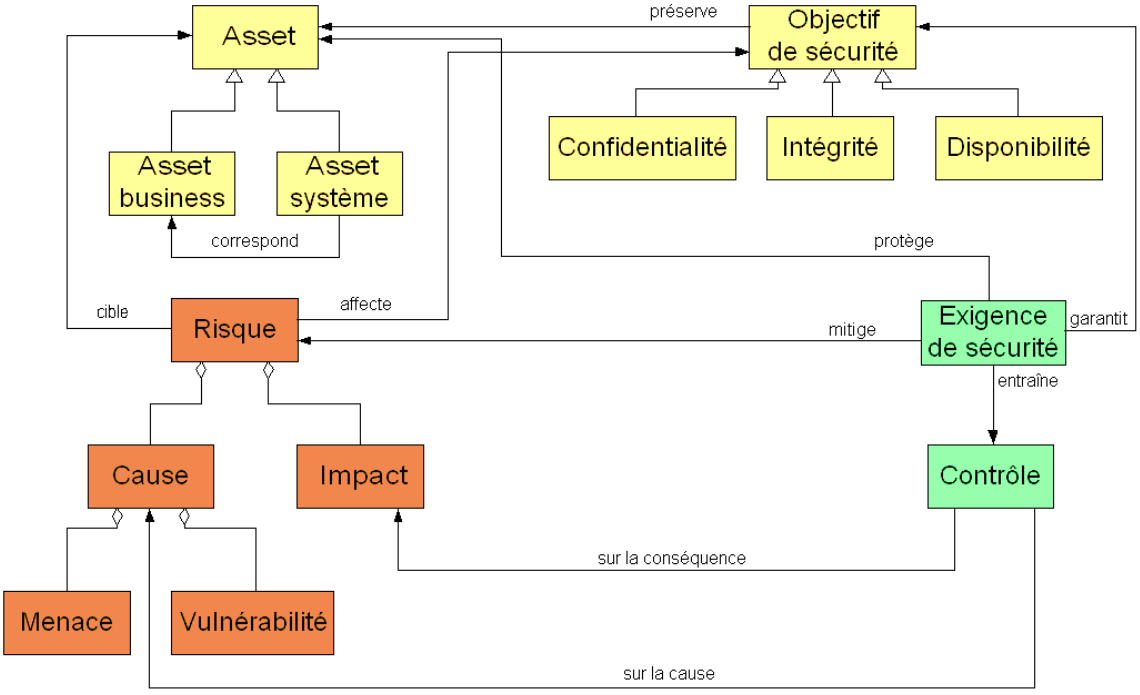


Figure 1: Les concepts de la gestion des risques

Les assets sont définis comme étant l'ensemble des biens, actifs, ressources ayant de la valeur pour l'organisme et nécessaires à son bon fonctionnement. On distingue ici les assets du niveau business des assets liés au SI. Du côté des assets business, on retrouve principalement des informations (par exemple des numéros de carte bancaire) et des processus (comme la gestion des transactions ou l'administration des comptes). Les assets business de l'organisme sont bien souvent entièrement (ou presque) gérés au travers du SI, ce qui entraîne une dépendance de ces assets vis-à-vis de ce dernier. C'est ce que l'on appelle les « assets système ». On retrouve dans les assets système les éléments techniques, tels les matériels, les logiciels et les réseaux, mais aussi l'environnement du système informatique, comme les utilisateurs ou les bâtiments. C'est cet ensemble qui forme le SI. Le but de la gestion des risques est donc d'assurer la sécurité des assets, sécurité exprimée la plupart du temps en termes de confidentialité, intégrité et disponibilité, constituant les objectifs de sécurité.

[1] Asset est un anglicisme couramment utilisé dans le domaine.

Ces assets à protéger sont soumis à des risques de sécurité. Le guide 73 de l'ISO [8] définit un risque par la combinaison de la probabilité d'un événement et de ses conséquences. Cette définition est généralement étendue et on définit un risque à l'aide de ce que l'on nomme « l'équation du risque » :

RISQUE = MENACE * VULNÉRABILITÉ * IMPACT

Cette équation est celle qui est la plus couramment utilisée et la plus reconnue dans le domaine de la gestion des risques. Elle joue un rôle fondamental dans l'identification et l'évaluation du risque.

Pour bien comprendre la notion de risque, il est important de se pencher sur chacune de ses composantes. Tout d'abord la menace, la source du risque, est l'attaque possible d'un élément dangereux pour les assets. C'est l'agent responsable du risque. Ensuite, la vulnérabilité est la caractéristique d'un asset constituant une faiblesse ou une faille au regard de la sécurité. Enfin l'impact représente la conséquence du risque sur l'organisme et ses objectifs. La menace et la vulnérabilité, représentant la cause du risque, peuvent être qualifiées en termes de potentialité. L'impact peut, quant à lui, être qualifié en termes de niveau de sévérité.

Afin de mitiger ces risques et de protéger les assets, une politique de traitement des risques est mise en place. Elle sera constituée d'exigences de sécurité permettant de répondre aux risques. Ces exigences de sécurité vont ensuite entraîner la mise en place de contrôles (ou contre-mesures) de sécurité à implémenter, afin de satisfaire aux exigences. Les contrôles sont de deux types :

- Sur la menace ou la vulnérabilité, afin de limiter la cause du risque ;
- Sur l'impact, afin de limiter la conséquence du risque.

2.2 Le processus de gestion des risques

Après avoir mis en évidence les concepts intervenant dans la gestion des risques, on peut identifier un processus de haut niveau couvrant ses activités. Ce processus est presque toujours appliqué dans les méthodes pratiques de gestion des risques, comme nous le verrons par la suite.

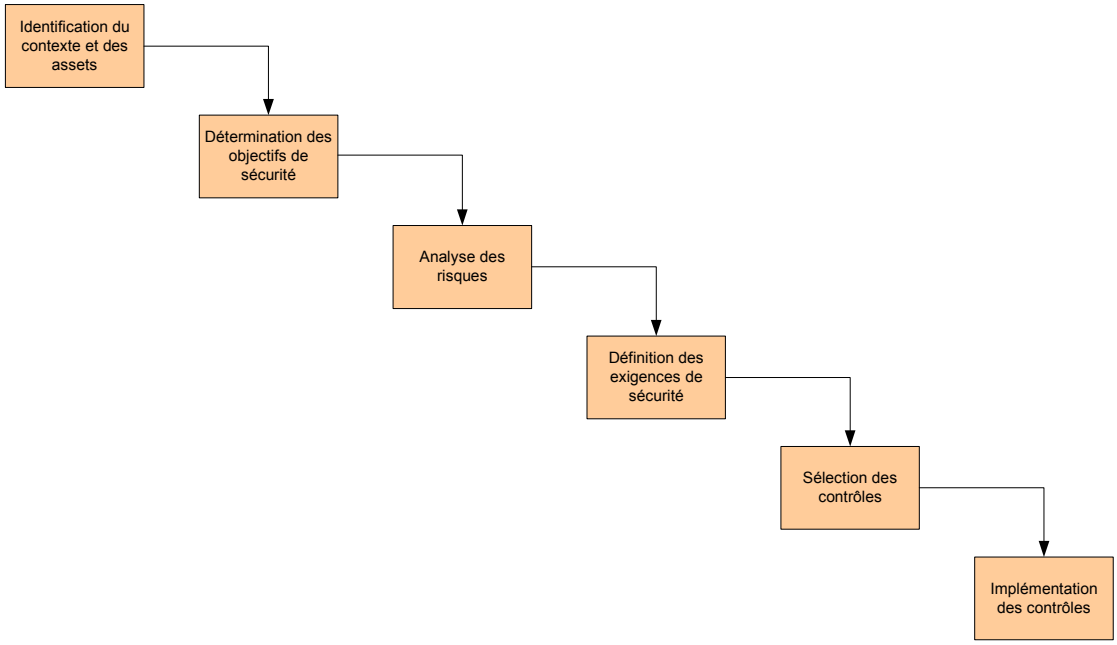


Figure 2: Le processus de gestion des risques

La première étape d'une démarche de gestion des risques consiste en l'identification du domaine et des assets. Dans cette partie, il est question de prendre connaissance avec l'organisation, son environnement, son SI et de déterminer précisément les limites du système sur lequel va porter l'étude de gestion des risques. Une fois notre système borné, on procède en premier lieu à l'identification des assets business constituant la valeur de l'organisation. Ensuite, le lien sera fait entre ces assets business et les assets système, sur lesquels on identifiera et corrigera les risques d'un point de vue technique et organisationnel.
Ex. : Un site de e-commerce dispose d'une base de données clients, présente sur un serveur de son parc informatique et contenant les informations bancaires de ces derniers.

La détermination des objectifs de sécurité vise à spécifier les besoins en termes de confidentialité, intégrité et disponibilité des assets, en particulier au niveau business. Le lien entre les assets business et les assets système étant fait en amont, on retrouve donc les besoins en sécurité au niveau du système.
Ex. : La base de données clients a donc un fort besoin de confidentialité, lié à la sensibilité des informations qu'elle contient.

L'analyse des risques constitue le coeur de la démarche de gestion des risques. Elle a pour finalité l'identification et l'estimation de chaque composante du risque (menace/vulnérabilité/impact), afin d'évaluer le risque et d'apprécier son niveau, dans le but de prendre des mesures adéquates (parfois, cette étape est également appelée « appréciation du risque » [8]). Il y a deux grandes écoles pour l'identification des risques : soit en réalisant un audit du système et de ses différents acteurs [5], soit à partir de bases de connaissances prédéfinies [3,4]. Pour l'estimation des risques, il est possible en théorie de les quantifier à l'aide de distributions de probabilités sur les menaces et les vulnérabilités, ainsi qu'en estimant les coûts occasionnés par les impacts. En pratique, il

se révèle difficile de donner des valeurs absolues et on se contente bien souvent d'une échelle de valeurs relatives, par exemple, allant de 1 à 4. Cette estimation permet de faire un choix, représenté sur la figure 3, dans le traitement du risque, avant de passer à la détermination des exigences de sécurité.

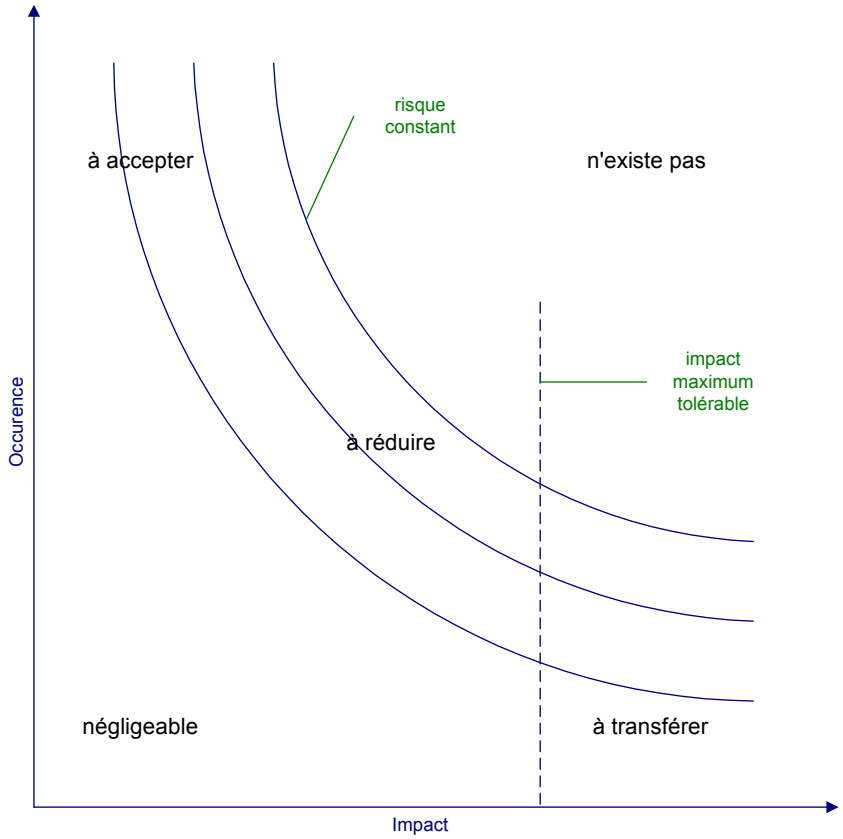


Figure 3 : Les différentes zones de risque

D'une manière générale [7], on considère que :

- Les risques ayant une occurrence et un impact faible sont négligeables.
- Les risques ayant une forte occurrence et un impact important ne doivent pas exister, autrement une remise en cause des activités de l'entreprise est nécessaire (on évite le risque, avoidance en anglais)
- Les risques ayant une occurrence forte et un impact faible sont acceptés, leur coût est généralement inclus dans les coûts opérationnels de l'organisation (acceptation du risque).
- Les risques ayant une occurrence faible et un impact lourd sont à transférer. Ils peuvent être couverts par une assurance ou un tiers (transfert du risque).
- Enfin, les autres risques, en général majoritaires, sont traités au cas par cas et sont au centre du processus de gestion des risques ; l'objectif, étant de diminuer les risques en les rapprochant au maximum de l'origine de l'axe (mitigation du risque à l'aide de contrôles).

Ex. : L'analyse des risques montre un certain nombre de scénarios ayant un niveau de risque inquiétant pour la base de données clients. Un des risques identifiés est l'accès aux données par un utilisateur non-autorisé à travers le réseau. Cela aurait pour

conséquence de nuire à la confidentialité des données. Ce risque nécessite d'être traité par des contrôles de sécurité.

Une fois l'analyse des risques effectuée, la définition des exigences de sécurité permettra de réduire les risques identifiés. Comme précédemment, en fonction des méthodes, cette étape pourra être effectuée avec l'assistance de référentiels [9,10], ou aiguillée par la connaissance d'experts système/sécurité. La définition des exigences de sécurité, de par son importance et sa complexité, est souvent effectuée de manière incrémentale et par raffinement successif. En effet, on conseille bien souvent de débuter par des exigences générales, qui définiront l'intention de contrer les risques identifiés (de niveau stratégique), pour les raffiner ensuite en des exigences plus précises (vers le niveau opérationnel). Toutefois les exigences sont censées être génériques et applicables à tout SI. Il faut également rappeler que ces exigences de mitigation des risques porteront à la fois sur le système informatique (comme le besoin d'encryption des mots de passe), mais aussi sur son environnement (par exemple, « l'utilisateur du système ne doit pas dévoiler son mot de passe à un tiers »).
Ex : Le serveur doit être protégé, dans sa globalité, des intrusions éventuelles. De même, on décide de mettre en place un contrôle d'accès adéquat sur la base de données. Une authentification à distance, plus forte que l'authentification actuelle par login/password, est nécessaire. Toutefois le coût et la simplicité d'utilisation de la solution choisie doivent rester à un niveau acceptable.

Le dernier niveau de raffinement est constitué par la sélection des contrôles (ou contre-mesures) de sécurité. Les contrôles sont l'instanciation des exigences de bas niveau pour le système cible étudié. Ici sont définis les choix techniques des solutions de sécurité, influencés par le système déjà en place, les compétences disponibles, les coûts de mise en oeuvre…
Ex : On sélectionne l'ajout d'un IDS au firewall déjà en place. De plus, on décide de mettre en place une politique de password plus exigeante constituée d'un login/password ainsi que d'un code de contrôle distribué à l'utilisateur lors de son inscription. Une authentification par carte à puce est trop contraignante.

Une fois les contrôles sélectionnés, il reste alors à les implémenter dans le SI et à éventuellement les tester et les évaluer. Il subsiste alors indéniablement une part de risques traités partiellement ou non, qui constitue ce que l'on appelle le risque résiduel.
Ex : Le service informatique de la société mettra en place l'IDS et le prestataire chargé de la maintenance du site Web développera un nouveau portail supportant l'authentification désirée.

Ce processus est communément admis par les différentes méthodes de gestion des risques. Par contre, la terminologie est souvent très différente, d'une méthode ou norme à une autre. La comparaison du processus de plusieurs méthodes nécessite alors une bonne analyse, mais dans l'ensemble, le schéma présenté précédemment est suivi. Toutefois, quelques méthodes se distinguent en présentant une trame quelque peu différente ou étendue (tout en gardant bien souvent comme base l'inamovible processus générique présenté). Citons notamment le BS 7799-2:2002 [11] qui voit la gestion des risques

comme un processus suivant le paradigme PDCA ou d'autres méthodes utilisant la gestion des risques dans une démarche de conception de système [6].

3. La gestion des risques en pratique

Même après en avoir dégrossi les fondements, la notion de risque reste un concept difficile à appréhender. La complexité des organisations actuelles associée aux enjeux business forcent à ne pas s'en remettre exclusivement à ses subjectivités, en résumé à sa perception « intellectuelle », mais plutôt à faire confiance à des méthodes formelles éprouvées. En un mot : « Nul besoin de ré-inventer la roue en matière d'analyse des risques ». Mieux vaut plutôt profiter du travail effectué et des guides à disposition.

Tel que décrit précédemment, plus de 200 méthodes de gestion/analyse des risques sont déclinées actuellement à travers le monde. Ces dernières sont plus ou moins bien finalisées, plus ou moins faciles d'accès ou tout simplement inconnues ! A ce titre, le Club Informatique des Grandes Entreprises Françaises (CIGREF) a récemment rappelé, en regard du domaine de la sécurité des SI, que « l'abondance de normes et de méthodes est souvent source de confusion ». Il ne faut, en effet, pas se perdre dans le dédale des méthodes et tenter d'aller à l'essentiel sur cette thématique.

Mais comment faire son choix au milieu de la jungle des référentiels d'analyse des risques ? Une première aide précieuse est fournie via la présentation, en amont, des fondements caractérisant les concepts et processus de la gestion des risques pour les SI. Ces concepts transcrivent le cadre de compréhension nécessaire pour appréhender sereinement la matière. En effet, à partir de ces informations, le choix peut alors se faire, de manière progressive et en fonction du contexte.

Pour réduire le champ du choix au coeur des méthodes formelles, certaines sont actuellement très populaires, faisant référence dans leur domaine. A ce titre, nous avons choisi de détailler EBIOS® [3], MEHARI™ [4] et OCTAVE^{SM} [5] qui remplissent efficacement leur rôle dans la conduite d'une démarche de gestion des risques.

EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité)

Il s'agit d'une méthode développée et maintenue par la DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information). Cette méthode, créée en 1995, se compose de cinq guides (Introduction, Démarche, Techniques, Outillages pour l'appréciation des risques et Outillages pour le traitement des risques) et d'un logiciel support. Sa diffusion est gratuite [3]. La méthode a pour objectif la formalisation d'objectifs de sécurité adaptés aux besoins du système audité (et de son contexte).

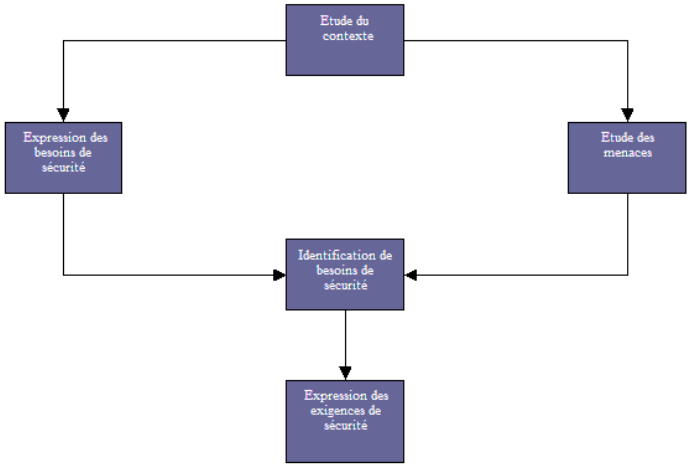


Figure 4 : Démarche EBIOS globale

EBIOS appréhende les risques de sécurité en tenant compte des trois blocs interdépendants des concepts de gestion présentés en amont. La méthode travaille par construction du risque, adoptant une prise en compte du contexte de l'organisation cible, en privilégiant le périmètre du SI, les éléments essentiels, les fonctions et les informations (correspondant aux assets business), et enfin les entités (assets système). La seconde phase de la méthode permet de dégager les besoins via une grille des services souhaités de sécurité (respect des critères « Confidentialité, Intégrité, Disponibilité »).

Le risque adapté à l'organisation est ainsi construit et renforcé par la prise en compte relative des vulnérabilités et des menaces s'appliquant sur les assets et jugées critiques. De l'interdépendance entre ces phases se décline ensuite naturellement la définition des exigences de sécurité de haut-niveau (appelées ici « objectifs ») puis de bas-niveau (appelées « exigences »), conformément à ISO 15408 [9] et ISO 17799 [10]. Cette dernière phase permet de sélectionner les bonnes contremesures strictement adaptées aux besoins de l'organisation. Tous les concepts présentés dans la première partie sont donc présents, malgré des différences de terminologie.

Quant au processus de gestion des risques, les phases 5 et 6 vues précédemment ne sont pas réellement développées, ce qui ne permet pas de valider véritablement le cycle théorique dans son ensemble. Dans ce cas, certains considèrent alors EBIOS exclusivement comme une méthodologie d'analyse des risques.

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)

Cette méthode d'évaluation du risque [5] est publiée par le Software Engineering Institute (SEI) de la Carnegie Mellon University, reconnue dans le domaine de la sécurité des SI (fédération des Computer Emergency & Reponse Team – CERTS). Les fondements mêmes de cette méthode reposent sur la possibilité de réaliser une analyse des risques de l'intérieur de l'organisation, exclusivement avec des ressources internes. Pleinement orientée vers les grands comptes, une version OCTAVE-S (Small) peut, cependant, facilement se décliner au sein d'une petite structure économique.

OCTAVE est une méthode d'évaluation des vulnérabilités et des menaces sur les actifs opérationnels. Une fois ces derniers identifiés, la méthode permet de mesurer les menaces et les vulnérabilités pesant sur eux.

Les trois phases suivantes déclinées au coeur d'OCTAVE, respectent l'analyse progressive des trois blocs des concepts de gestion des risques présentés en amont :

- La phase 1 (vue organisationnelle) permet d'identifier les ressources informatiques importantes, les menaces associées et les exigences de sécurité qui leur sont associées.
- La phase 2 (vue technique) permet d'identifier les vulnérabilités de l'infrastructure (ces dernières, une fois couplées aux menaces, créant le risque).
- La phase 3 de la méthode décline le développement de la stratégie de sécurité et sa planification (protection et plan de réduction des risques).

On retrouve également dans cette méthode l'ensemble des concepts présentés en première partie. Concernant le processus, la même remarque faite précédemment, pour EBIOS, est valable : les deux dernières étapes sont peu ou pas abordées, la méthode se voulant être principalement une méthode d'analyse des risques.

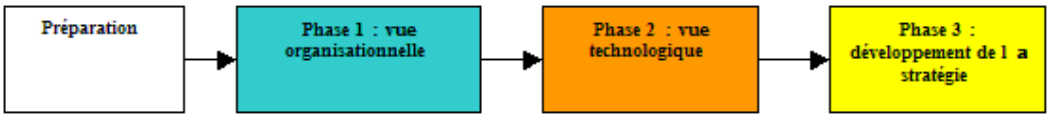


Figure 5 : Les phases principales d'OCTAVE

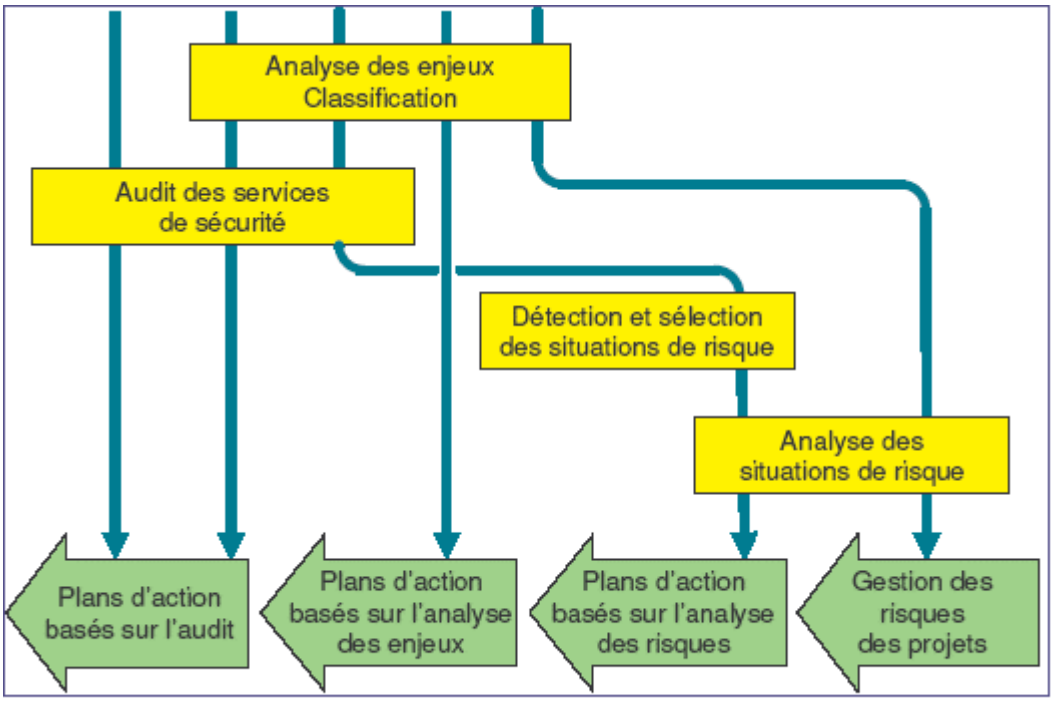
MEHARI (Méthode Harmonisée d'Analyse de RIsques)

MEHARI demeure une des méthodes d'analyse des risques les plus utilisées actuellement. Elle est dérivée de deux autres méthodes d'analyse des risques (MARION et MELISA). MEHARI est maintenue en France par le CLUSIF (Club de la Sécurité des Systèmes d'Information Français) [4], via notamment le Groupe de Travail dédié à cette méthode.

MEHARI se présente comme une véritable boîte à outils de la sécurité des SI, permettant d'appréhender le risque de différentes manières au sein d'une organisation, et composée de plusieurs modules. Ces derniers, indépendamment de la démarche sécurité choisie, permettent notamment :

- D'analyser les enjeux de la sécurité (en décrivant les types de dysfonctionnements redoutés) et, corrélativement, de classifier les ressources et informations selon les trois critères sécurité de base (Confidentialité, Intégrité, Disponibilité).
- D'auditer les services de sécurité, de manière à prendre en compte l'efficacité de chacun, son contrôle, et de synthétiser les vulnérabilités.
- D'analyser les situations de risques, permettant d'évaluer les potentialités et les impacts intrinsèques, ainsi que les facteurs d'atténuation de risque, puis, enfin, de déduire un indicateur de gravité de risque.

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



Source CLUSIF

Figure 6 : Démarche MEHARI globale

MEHARI présente une grande diversité dans l'utilisation de ses modules. Trois approches se détachent plus particulièrement :

- En se basant sur une analyse détaillée des risques, il est possible de mettre en oeuvre des plans de sécurité. Cette démarche se décline au niveau stratégique, mais aussi opérationnel. Le premier niveau permet la cohérence des besoins et du contexte de l'ensemble de l'organisation. Le second niveau définit les unités business autonomes au coeur de l'organisation et en charge des décisions nécessaires en matière de sécurité.
- En se basant sur l'audit de sécurité, ou plus précisément après un diagnostic de l'état de sécurité, la réalisation de plans d'actions est facilitée. En effet, des faiblesses relevées découlent alors, directement, les actions à entreprendre.
- Dans le cadre de la gestion d'un projet particulier, tenir compte de la sécurité, en se basant, de nouveau, sur l'analyse des risques, et ainsi faciliter l'élaboration de plans d'action. Les besoins de sécurité sont alors directement intégrés aux spécifications du projet, et à intégrer dans le plan de sécurité global de l'entité concernée.

Cette méthode s'aligne avec les deux premières en termes de couverture du processus de gestion des risques.

4. Conclusion

La notion de risque, qui demeure intangible, reste difficile à appréhender : « Les risques désignent un futur qu'il s'agit d'empêcher d'avenir » [12]. Les risques en relation avec la sécurité se doivent de reposer sur des techniques et des méthodologies particulières. Ces

méthodes permettent de prendre en compte toutes les facettes du risque, une démarche déterminante afin de ne pas oublier des concepts essentiels : « En France 100% des grandes entreprises effectuent ce type d'analyses de risques, via une méthodologie formelle » (CIGREF). Dans cet article, seules ont été proposées des méthodes orientées « Analyse des risques », majoritaires dans le domaine en raison de la complexité inhérente à cette partie, mais de nombreux guides existent également pour les autres étapes [2]. Concernant le choix d'une méthode, la question est complexe et pourrait faire l'objet d'un article à elle seule. Outre l'étendue de la couverture de la méthode, quelques critères de choix à retenir peuvent être le type d'approche (audit ou analyse à l'aide de bases de connaissances), leur origine (secteur privé, universitaire, militaire…), leur facilité d'utilisation, leur gratuité, des sources ouvertes, etc. (cette liste étant loin d'être exhaustive). Il demeure que les analyses non formelles, dans un contexte sécurité, sont très rares et généralement non exhaustives. La force des concepts et du processus de gestion des risques présentés en amont est globalement vérifiée au coeur des différentes méthodes décrites. De fait, il serait dommage de ne pas profiter de ces véritables guides méthodologiques pour parfaire votre sécurité !

Bibliographie

[1] Dubois, J.-C., L'analyse du risque : une approche conceptuelle et systémique, Chenelière-McGrawHill, 1996. ISBN : 2-89461-066-1

[2] IT Baseline Protection Manual, BSI - Germany, October 2003. http://www.bsi.bund.de/english/gshb/

[3] 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

[4] Méthode Harmonisée d'Analyse de Risques (MEHARI), Principes et mécanismes, CLUSIF, Version 3, Octobre 2004.
http://www.clusif.asso.fr/

[5] Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE), Carnegie Mellon - Software Engineering Institute,
Juin 1999. http://www.cert.org/octave/

[6]Ebrahimi T., Leprévost F., Warusfel B., Les enjeux de la sécurité multimédia Vol.1 (traité IC2, série Informatique et SI), Chapitre : Contributions méthodologiques pour l'amélioration de l'analyse des risques, Hermes, 2005. ISBN : 2-7462-1207-2

[7] Bosworth, Seymor and Michael E. Kabay, Computer Security Handbook, 4th edition, Chapter 47, John Wiley & Sons, 2002.
ISBN: 0-471-41258-9

[8] ISO/IEC Guide 73:2002, Risk management – Vocabulary – Guidelines for use in standards.

[9] Common Criteria for Information Technology Security Evaluation, Version 2.2 (également ISO 15408), 2004.
http://www.commoncriteriaportal.org

[10] ISO/IEC 17799:2005, Information Technology – Security techniques - Code of Practice for Information Security Management

[11] BS 7799-2:2002, Information security management systems – Specification with guidance for use
[12] Ulrich Beck, La Société du risque – Sur la voie d'une autre modernité, Flammarion - Champs 2003, 522 pages. ISBN : 2-08-080058-2.