

---

# Défis de la sécurité de l'information

## Support à la gestion des risques de sécurité par les modèles

**Nicolas Mayer\*\* — Eric Dubois\* — Patrick Heymans\*\* — Raimundas Matulevičius\*\***

\* *Centre de recherche public Henri Tudor*  
29, Avenue John F. Kennedy  
L-1855 Luxembourg – Kirchberg, Luxembourg  
{nicolas.mayer,eric.dubois}@tudor.lu

\*\* *FUNDP - Institut d'informatique*  
rue Grandgagnage 21  
B-5000 Namur, Belgique  
{phe,rma}@info.fundp.ac.be

---

*RÉSUMÉ. Au sein des organisations, la gestion de la sécurité des systèmes d'information repose de plus en plus sur des approches basées sur les risques. Cependant, ces approches se révèlent d'une part peu adaptées à l'étude de systèmes d'information en construction et d'autre part, les produits issus des différentes étapes de gestion des risques réalisées sont généralement peu formels. Notre travail de recherche propose d'améliorer les différentes étapes de la gestion des risques à l'aide de modèles. Afin d'aboutir à cet objectif, nous proposons en premier lieu un modèle conceptuel associé au domaine de la gestion des risques de sécurité des systèmes d'informations, en y intégrant les métriques nécessaires aux raisonnements associés. Nous définissons ensuite un langage de modélisation permettant une représentation formelle de l'analyse de risques.*

*ABSTRACT. Within the organisations, information system security is more and more tackled with the help of risk management approaches. However these approaches are on one hand not well suited to be applied on information system development and on the other hand, products coming from the different risk management steps performed are generally not enough formal. Our research work proposes to improve the different risk management steps with models. In order to achieve this objective, we first define a conceptual model associated with the information system security risk management domain, and enriched with appropriate metrics for performing reasoning. We define then a modelling language for formally representing risks analysis artefacts.*

*MOTS-CLÉS : gestion des risques, sécurité, norme, modélisation.*

*KEYWORDS: risk management, security, standards, modelling.*

---

## 1. Introduction

Durant les vingt dernières années, les problèmes de sécurité ont de plus en plus impacté le développement et l'exploitation des Systèmes d'Information (SI). D'autre part, les contraintes légales au niveau de la sécurité des SI sont de plus en plus nombreuses dans beaucoup de secteurs (Basel Committee on Banking Supervision, 2002 ; AICPA, 2002). Dans ce contexte, la Gestion des Risques de Sécurité des SI (GRSSI) joue un rôle prépondérant, car elle permet aux organisations de prendre les décisions les plus adaptées à leurs besoins de sécurité au regard de leurs moyens. De nombreuses méthodes de GRSSI sont actuellement disponibles sur le marché et largement employées au sein des organismes privés ou publics. Cependant, elles présentent généralement le désavantage d'être développées pour une étude des risques d'un SI existant et considèrent donc moins l'aspect de construction de SI. De plus, si ces différentes méthodes proposent des étapes clairement définies à réaliser, les produits résultant de ces étapes sont généralement informels et peu détaillés, le plus souvent exprimés en langage naturel et parfois sous forme de tableaux. D'autre part, dans la communauté des langages formels, on trouve de plus en plus de langages, reposant la plupart sur la modélisation, qui permettent de représenter les exigences de sécurité nécessaires à un SI lors de son développement. Cependant ces langages supportent peu les raisonnements et les besoins propres à la gestion des risques. Il existe donc un manque clairement identifié de cadre formel à la GRSSI au niveau des phases amonts de développement de SI. L'objectif principal de nos travaux de recherche est ainsi de proposer un tel support à la GRSSI à l'aide d'un cadre basé sur la modélisation.

Pour atteindre cet objectif, plusieurs étapes, chacune liée à un objectif intermédiaire précis, constituent notre démarche. Tout d'abord le domaine de la GRSSI doit être identifié et clairement défini. Pour cela, la définition d'un modèle conceptuel associé au domaine de la GRSSI a été jugée nécessaire, assurant d'une part l'interopérabilité entre l'ensemble des références de la littérature du domaine et d'autre part, proposant un cadre générique au domaine de la GRSSI. La définition de ce modèle constitue le premier objectif de notre article. Ensuite, afin d'assister l'utilisateur dans les différents raisonnements qu'il est amené à effectuer au niveau de la GRSSI, il est nécessaire de définir les métriques propres au domaine. La définition des métriques associées à la GRSSI constitue le deuxième objectif de notre article. En particulier, la notion de retour sur investissement est introduite et les métriques associées identifiées. Enfin, notre troisième objectif vise à proposer un langage formel de modélisation support à la GRSSI. Afin d'optimiser la définition d'un tel langage, les langages de modélisation de la sécurité ont été analysés et comparés, dans le but d'identifier un ou plusieurs candidats potentiels à une extension à la GRSSI. Une première proposition de langage est faite, sur base du langage Secure Tropos. Dans la suite de l'article, il faut noter que pour chacun des trois objectifs introduits, une méthode de recherche est définie. L'application de cette méthode de recherche permet d'atteindre l'objectif attendu et les résultats obtenus sont présentés et analysés.

Au sein de la Section 2, nous commençons par déterminer le périmètre de la GRSSI en la situant d'abord dans le cadre général d'une problématique d'alignement business/SI. Nous précisons ensuite les notions de risque et de gestion des risques et présentons un état de l'art du domaine de la GRSSI. La Section 3 présente la définition d'un modèle conceptuel associé au domaine de la GRSSI. La Section 4 complète le modèle conceptuel du domaine à l'aide des métriques nécessaires à la GRSSI. Enfin, dans la Section 5 nous proposons un langage formel de modélisation et illustrons son usage au travers d'une étude de cas.

## **2. Objectif et présentation de la gestion des risques de sécurité**

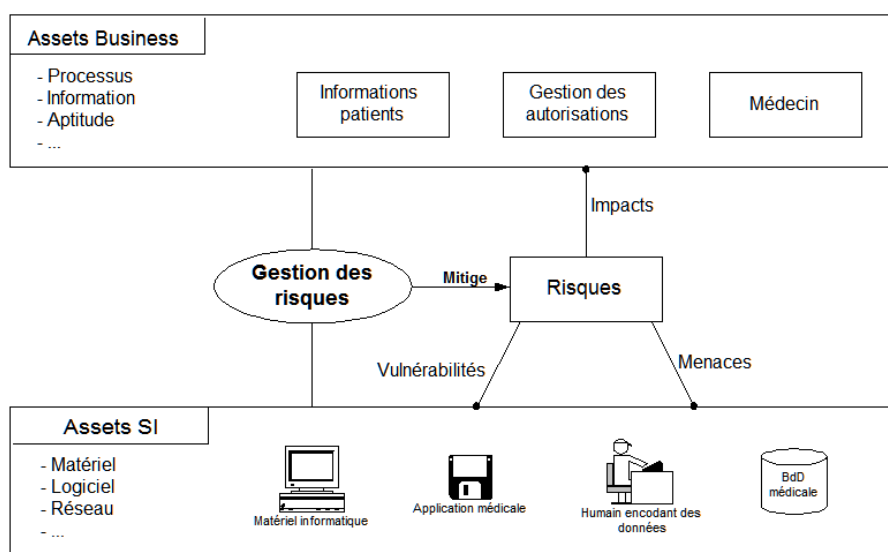
### **2.1. La sécurité et le risque de non-alignement business/SI**

Les SI jouent aujourd'hui un rôle majeur au sein des organisations et de la réussite de leur business. En supportant l'exécution des processus clés de l'organisation et le traitement des informations y afférant, le bon fonctionnement d'un SI est à la base à la fois de la compétitivité mais aussi de la capacité d'innovation d'une organisation. Un SI est défini comme « une combinaison formalisée de ressources humaines et informatiques résultant de la collecte, de la mémorisation, de la recherche, de la communication et de l'utilisation de données en vue de permettre un management efficace des opérations au sein d'une organisation » (Le Moigne, 1973).

Pour assurer l'efficacité du SI, il importe d'assurer son alignement au business qu'il supporte et à la stratégie associée (Henderson *et al.*, 1993). Toute déviation entre les objectifs business (processus à supporter et gestion de l'information) et leurs implémentations au travers du SI sont sources d'instabilité et de coûts pour une organisation. A tout moment il convient de vérifier que le SI est le réel « miroir » du business de l'organisation. Les raisons pour un non-alignement peuvent être multiples. Elles peuvent résulter d'un défaut de conception du SI (une mauvaise compréhension des processus business résulte dans la mise en place de mauvaises procédures) mais peuvent être aussi la conséquence de dysfonctionnement du SI. Parmi les causes de dysfonctionnement figurent celles liées à des défauts de sécurité. Ces défauts deviennent de plus en plus nombreux du fait de l'importance croissante jouée par les technologies de l'information et de la communication au sein des SI et surtout aux nombreuses vulnérabilités associées à ces technologies. La gestion des risques est l'outil utilisé pour assurer cet alignement au niveau de la sécurité, assurant que les mesures mises en place correspondent au besoin de sécurité requis par les processus business sous-jacent.

La gestion des risques est illustrée au niveau de la Figure 1, où l'on peut distinguer les assets liés au business et ceux au niveau du SI dont ils sont le miroir (par exemple, l'information business sur les patients peut se retrouver au niveau d'une base de données au niveau du SI). L'existence d'un risque est liée à des

vulnérabilités et menaces portant sur les assets du SI (par exemple, un accès mal intentionné à la base de données). L'impact du risque porte sur les assets business (par exemple, la divulgation des informations patients). Un risque a bien sûr un coût en terme de business non et/ou mal supporté (par exemple, le problème de réputation lié à la divulgation), mais il a aussi un autre coût lié à la réduction de ce risque c'est-à-dire aux modifications à faire au SI pour l'annuler (par exemple, les coûts liés au renforcement de la protection de la base de données).



**Figure 1.** La gestion de la sécurité dans une perspective d'alignement business/SI

## 2.2. Les risques de sécurité, couverture et limite

La définition du terme « risque » la plus généralement admise est celle proposée par le Guide 73 de l'ISO (ISO/IEC Guide 73, 2002). Le risque y est défini comme la « combinaison de la probabilité d'un événement et de ses conséquences ». En complément, la gestion des risques est définie comme les « activités coordonnées visant à diriger et piloter un organisme vis-à-vis du risque ». En fonction du contexte, la gestion des risques peut donc traiter de problèmes très différents (The Project Management Institute, 2001 ; ISO/IEC 14001, 2004). Par exemple, des risques peuvent se situer dans le domaine de la gestion de projet (ex. : maladie d'une personne clé au regard du projet), de la finance (ex. : en lien avec des investissements), de l'environnement (ex. : pollution), ou de la sécurité. Dans cet

article, nous nous focaliserons uniquement sur la gestion des risques de sécurité. Les autres types de risque, tel que financiers ou de projet, seront hors de notre scope<sup>1</sup>.

Dans la littérature, le domaine de la « sécurité » n'est pas uniformément défini. Certains auteurs, comme Firesmith (Firesmith, 2003), utilisent le terme sécurité uniquement pour ce qui concerne les actes malicieux (ou délibérés) portant atteinte au SI, et utilisent le terme sûreté (ou sûreté de fonctionnement) pour ce qui concerne les atteintes accidentelles. Ces auteurs utilisent alors la notion plus large de « survivabilité » afin de couvrir à la fois la sécurité (au sens ci-dessus) et la sûreté. Dans cet article, c'est la notion de « survivabilité » que nous couvrirons bien que nous conservions le terme de sécurité pour le désigner. Ce choix est lié à la fréquence d'utilisation du terme « sécurité » dans la littérature associée au domaine (DCSSI, 2004 ; CLUSIF, 2004 ; Alberts *et al.*, 1999 ; ISO/IEC 27001, 2005 ; Vraalsen *et al.*, 2007).

Le dénominateur commun à l'ensemble des approches de GRSSI est la notion d'objectifs de sécurité à atteindre (ou propriété de sécurité à respecter) afin d'assurer un niveau raisonnable de protection pour les assets de l'organisation. Les assets sont généralement définis comme étant tout ce qui possède de la valeur pour l'organisation et donc nécessitant d'être protégé. Ces assets sont directement liés aux processus et informations associés au business de l'organisation. Ainsi, dans un contexte de SI donné, les assets de l'organisation sont implémentés au travers de matériels, de logiciels et de composants réseaux, aussi bien que par des personnes ou des équipements jouant un rôle dans le SI (ex. : employé encodant des données, ou encore le conditionnement d'air de la salle serveur). Tous ces éléments sont sujets à des risques et ces risques doivent être évalués au regard des propriétés de sécurité du SI pouvant être endommagées. Ces propriétés incluent principalement la confidentialité, l'intégrité et la disponibilité des informations et/ou des processus d'une organisation (ISO/IEC 13335-1, 2004) :

– La confidentialité est la propriété qu'une information ne soit pas disponible ou divulguée à un individu, une entité ou un processus non autorisé ;

– L'intégrité est la propriété de préserver la précision et la complétude des assets. La précision peut être menacée par une mise à jour ou modification (non-autorisées ou indésirables). La complétude peut être menacée par une altération ou une suppression ;

– La disponibilité est la propriété d'être accessible et utilisable sur demande par une entité autorisée.

---

<sup>1</sup> Cette hypothèse ne signifie en aucun cas que ces différents types de risque sont totalement décorrélés. Bien au contraire, ils sont souvent reliés, comme par exemple une augmentation des risques de sécurité pouvant entraîner des risques financiers et de projet accrus pour une organisation. Notre objectif est ici de traiter uniquement les risques de sécurité principalement pour une question de faisabilité.

D'autres critères tels l'authenticité ou la non-répudiation (ISO/IEC 13335-1, 2004) peuvent être ajoutés en fonction du contexte, mais ils sont généralement considérés comme secondaires.

Comme admis précédemment, nous considérons que les atteintes à ces propriétés proviennent de causes accidentelles ou délibérées. Par exemple, la divulgation d'une information confidentielle peut être réalisée délibérément par une personne malintentionnée ou accidentellement, en raison d'une faute dans un programme ou d'une erreur d'un employé.

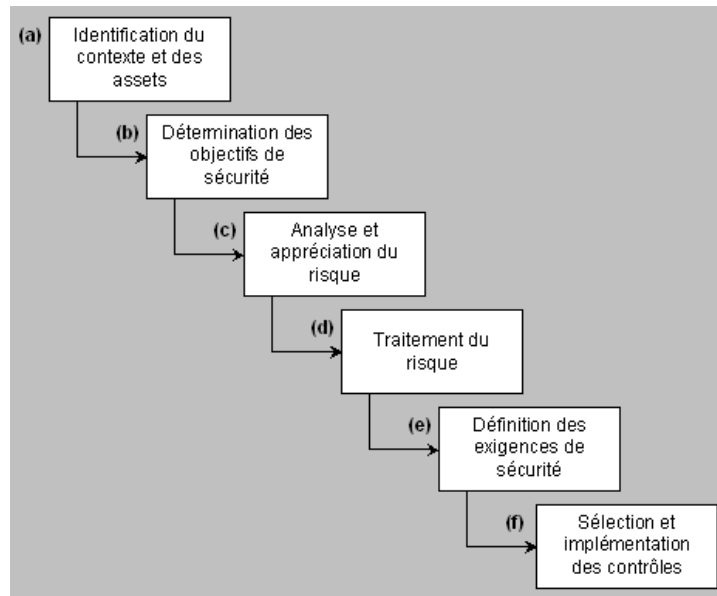
En conclusion, l'objectif de la GRSSI est de protéger les éléments essentiels d'un SI de toute atteinte à sa sécurité (en termes de confidentialité, intégrité et disponibilité) pouvant se déclarer de manière accidentelle ou délibérée.

### **2.3. *Processus de la gestion des risques de sécurité des SI***

L'utilisation d'une approche de GRSSI a trois avantages principaux (Stoneburger, 2002) :

- L'amélioration de la sécurité du SI
- La justification de l'allocation de budget pour la sécurité du SI
- L'évaluation du niveau de confiance que les clients et partenaires peuvent avoir dans le SI

Afin d'aboutir à ces résultats, les activités de gestion des risques suivent généralement un processus classique, repris comme base dans la majorité des standards et méthodes (DCSSI, 2004; Stoneburger, 2002; AS/NZS 4360, 2004). Cependant, chaque méthode n'accorde pas la même importance aux différentes activités de ce processus. Certaines, par exemple, sont plus centrées sur l'analyse des risques (DCSSI, 2004; CLUSIF, 2004; Alberts *et al.*, 1999) quand d'autres (BSI – Germany, 2004; ISO/IEC 17799, 2005) suggèrent d'appliquer des exigences standards de sécurité pour atteindre un niveau de sécurité satisfaisant. Le processus peut être résumé en six étapes principales (Figure 2) :



**Figure 2.** *Processus de GRSSI*

Le processus commence par une étude du *contexte et des assets* de l'organisation cible. Dans cette étape (a), l'organisation et son environnement sont décrits et une vue d'ensemble du SI, s'il est déjà en place, est proposée en y identifiant les assets business qui y sont implémentés. Par exemple, on peut illustrer un résultat de cette étape à l'aide d'un exemple extrait du domaine médical (Dubois *et al.*, 2006) : les informations patients enregistrées dans une base de données médicale du SI sont associées à des assets de niveau business de l'organisation étudiée, qu'il va donc falloir protéger.

Ensuite, il est nécessaire de déterminer les *objectifs de sécurité* (b) qui vont indiquer le niveau de protection requis pour les assets de l'organisation identifiés comme indiqué précédemment. Les objectifs de sécurité sont le plus souvent définis en termes de confidentialité, intégrité et disponibilité des assets. Au niveau de notre exemple, la confidentialité des informations patient doit être garantie.

L'étape principale du processus est l'*analyse des risques* (c), qui identifie quels risques portent atteinte aux assets de l'organisation et menacent les objectifs de sécurité. L'analyse des risques consiste en l'identification des risques et l'estimation de leurs niveaux de manière qualitative ou quantitative. On parle d'*appréciation du risque* (ISO/IEC Guide 73, 2002) une fois que les risques sont évalués au regard des objectifs de sécurité définis lors de l'étape (b). Par exemple, la base de données dans laquelle sont enregistrées les informations des patients peut être la cible d'un pirate tentant d'utiliser les vulnérabilités courantes du protocole TCP/IP afin

d'accéder aux données confidentielles. Ce risque a un niveau estimé suffisamment haut pour être considéré comme important vis-à-vis des objectifs de sécurité et devant donc être mitigé.

Une fois l'appréciation des risques effectuée, le risque doit être traité. En premier lieu, on va prendre une décision sur le type de *traitement de risque* (d), comme le réduire à l'aide de contrôles sur le SI ou le transférer à un tiers (par exemple, au travers de la prise d'une assurance). Dans le cas de notre exemple, la mise en place de contrôles est le choix retenu.

Des *exigences de sécurité* peuvent alors être déterminées afin de mitiger le risque (e). Pour notre exemple, des contrôles techniques peuvent être choisis afin de réduire le risque, comme mettre en place du filtrage et de la détection d'intrusion sur le réseau du SI.

Les exigences sont finalement instanciées en *contrôles de sécurité* (f), c'est-à-dire des contre-mesures spécifiques au SI, implémentables au sein de l'organisation. Dans notre exemple, un firewall ainsi qu'un IDS (Intrusion Detection System) pourront être sélectionnés et implémentés au sein du SI.

#### **2.4. Etat de l'art de la gestion des risques de sécurité des SI**

Afin d'être à même de réaliser notre premier objectif de définition d'un modèle du domaine de la GRSSI, un état de l'art complet couvrant intégralement le domaine a été réalisé. L'accent a notamment été mis sur les références fournissant des renseignements sur les concepts et la terminologie. La littérature en lien avec le domaine de la GRSSI étant étendue et variée, nous l'avons regroupée sous forme de quatre familles distinctes, permettant de couvrir l'ensemble du domaine. La première famille de documents concerne les **standards de gestion des risques**. Ce sont des références de haut niveau présentant de manière générale la gestion des risques et se situant en amont des différentes approches et méthodes liées à des domaines spécifiques (sécurité, environnement...).

- ISO/IEC Guide 73 (ISO/IEC Guide 73, 2002) : Ce guide définit le vocabulaire de la gestion des risques et les lignes directrices de son utilisation dans les standards de l'ISO. Il est principalement focalisé sur la terminologie.
- AS/NZS 4360 (AS/NZS 4360, 2004) : Ce standard commun à l'Australie et à la Nouvelle-Zélande fournit un guide générique de gestion des risques. Le document propose une vue d'ensemble de la terminologie et du processus de gestion des risques.

La seconde famille de références est constituée de **standards de sécurité IT** ou étendue au SI. Les documents de cette famille sont focalisés sur les aspects de sécurité de manière générale, mais parfois des concepts en lien avec la gestion des risques sont également présentés.

- ISO/IEC 27001 (ISO/IEC Guide 27001, 2005) : L'objectif de ce standard est de fournir un modèle pour établir, implémenter, utiliser, contrôler, revoir, maintenir et améliorer un Système de Management de la Sécurité de l'Information (SMSI), qui est la partie liée à la sécurité du système global de gestion d'une organisation.
- ISO/IEC 13335-1 (ISO/IEC 13335-1, 2004) : Ce standard est le premier de la série des ISO/IEC 13335, qui traite de la planification, de la gestion et de l'implémentation de la sécurité IT. La partie 1 présente un intérêt particulier au regard de nos objectifs, car il définit les concepts et modèles de la sécurité IT qui peuvent être appliqués à différentes organisations.
- Common Criteria (Common Criteria, 2006) : Les Critères Communs (standardisés en version 2.3 sous ISO/IEC 15408) fournissent un ensemble commun d'exigences, à la fois pour les fonctions de sécurité des produits et systèmes IT, mais aussi pour les mesures d'assurance leurs étant appliquées et étant vérifiables dans le cadre d'une évaluation.
- NIST 800-27 Rev A / NIST 800-30 (Stoneburner *et al.*, 2004 ; Stoneburner *et al.*, 2002) : Au sein de la série de publications proposée par le National Institute of Standards and Technology (NIST), la série 800 traite de la sécurité informatique. Dans cette série, NIST 800-27 et NIST 800-30 sont les standards reliés au domaine de la GRSSI introduit en Section 2.2.

Les **méthodes de GRSSI** constituent la troisième famille de notre état de l'art. En 2004, une étude du CLUSIR RHA (Club Sécurité des Systèmes d'Information de la région Rhône Alpes) dénombrait plus de 200 méthodes de gestion des risques (Club Sécurité des Systèmes d'Information de la région Rhône Alpes, 2004). Dans ce cadre, nous avons sélectionné un sous-ensemble de méthodes représentatif de l'état actuel du marché. Notre choix s'est décidé à l'aide de conférences sur la thématique, comme la journée CLUSSIL 2005<sup>2</sup> traitant « du bon usage des méthodes dans l'analyse de risques » ou d'études récentes comme le rapport de l'ENISA visant à répertorier les méthodes de gestion et d'appréciation des risques de sécurité (ENISA, 2006).

- OCTAVE (Alberts *et al.*, 1999) : OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) est une approche d'évaluation des risques de sécurité de l'information développée par le Software Engineering Institute de la Carnegie Mellon University.
- CRAMM (Insight Consulting, 2003) : CRAMM est une méthode anglaise de GRSSI développée par CCTA<sup>3</sup> en 1985 et actuellement maintenue par Insight Consulting.

---

<sup>2</sup> <http://www.clussil.lu>

<sup>3</sup> Central Computer and Telecommunications Agency

- EBIOS (DCSSI, 2004) : La méthode d'origine française EBIOS est développée et maintenue par la Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI).
- MEHARI (CLUSIF, 2004) : MEHARI est une méthode de GRSSI développée par le CLUSIF et construite sur les bases de deux autres méthodes : MARION (CLUSIF, 1998) et MELISA (Direction des Constructions Navales, 1989), ces dernières n'étant actuellement plus maintenues.
- CORAS (Vraalsen *et al.*, 2007) : CORAS est un projet européen qui a développé un framework accompagné d'un outil, dans le but d'analyser et d'apprécier les risques de systèmes dont la sécurité est critique.

Enfin, la dernière famille concerne les **cadres conceptuels de sécurité** développés dans le cadre de recherches dans le domaine du génie logiciel.

- Haley *et al.* (Haley *et al.*, 2006) et Moffett et Nuseibeh (Moffett *et al.*, 2003) proposent un cadre focalisé sur le développement des exigences de sécurité.
- Firesmith (Firesmith, 2003) présente un ensemble de modèles interconnectés qui fournissent les bases théoriques de la sûreté, de la sécurité et de la « survivabilité ».

### 3. Interopérabilité des référentiels de gestion des risques de sécurité des SI

Comme nous l'avons vu dans la section précédente, le domaine de la GRSSI présente une diversité importante, tant au niveau des aspects méthodologiques proposés que des concepts et de la terminologie employée. La diversité méthodologique représente généralement un avantage du marché pour les utilisateurs. En effet, chaque utilisateur peut, en fonction de sa sensibilité et de ses besoins, choisir la méthode qui lui convient, en tenant compte des objectifs à atteindre, du coût de déploiement de la méthode, des compétences requises, du type d'approche, etc. Par opposition, la diversité conceptuelle et terminologique représente un frein pour l'utilisateur. En effet, il devient difficile de voir clairement la portée de chaque méthode. De plus, l'interopérabilité entre les méthodes s'en retrouve diminuée et il n'est pas aisé de comparer les résultats obtenus entre deux méthodes ou d'utiliser plusieurs méthodes de manière séquentielle sur une même étude de cas. Améliorer l'interopérabilité entre les différents référentiels de GRSSI est donc un challenge important et nécessaire afin d'augmenter la maturité du domaine.

D'autre part, en considérant notre objectif de définition d'un langage de modélisation pour la GRSSI, un modèle du domaine est nécessaire, afin de déterminer les concepts à intégrer au langage. Ce modèle du domaine devra être d'une part représentatif et inspiré de l'ensemble des approches du marché et d'autre part compatible avec ces dernières. Afin d'aboutir à ces résultats, une méthode de



fournie dans un glossaire séparé et obtenue en réutilisant et, si besoin, en améliorant les définitions les plus pertinentes trouvées lors de l'étape 1.

Afin de borner l'ensemble de concepts de départ à étudier, nous nous concentrons en premier lieu sur le concept central de risque, dont un extrait de l'analyse est présenté dans ce papier. Les risques étant fortement dépendants (i) des besoins de sécurité associés aux assets de l'organisation et (ii) des traitements des risques sélectionnés, les concepts propres à ces éléments seront également étudiés au départ. Naturellement ces premiers éléments d'étude seront précisés, complétés et affinés par la suite, lors du déroulement de la méthode de recherche. Il est à noter que les deux étapes devront être réalisées non pas séquentiellement, mais de manière itérative et incrémentale. Ainsi, l'ensemble final de concepts considéré sera celui disponible dans le tableau produit en fin d'étape 1. Néanmoins, l'ensemble de concepts obtenus peut encore être réduit ou augmenté par la suite, principalement en cas de besoins spécifiques d'utilisateurs ou d'émergence de nouveaux concepts à considérer.

### **3.2. Construction du tableau d'alignement des concepts**

Nous illustrons notre méthode de recherche par un exemple d'analyse associé au concept central de risque. La priorité est mise sur l'étude de la définition du concept et de ses composants associés. Les autres caractéristiques du risque présentées, comme par exemple les métriques associées ou les activités à réaliser, ne sont pas considérées à ce stade (voir Section 4 et 5). Les résultats obtenus sont résumés dans le tableau 1. L'étude exhaustive du concept de risque (Mayer *et al.*, 2007) ainsi que de l'ensemble des autres concepts considérés est disponible dans le rapport technique suivant (Mayer *et al.*, 2006b).

#### **3.2.1. Standards de gestion des risques**

Comme déjà évoqué au sein de la Section 2.2, le Guide 73 de l'ISO (ISO/IEC Guide 73, 2002) propose la définition suivante de risque :

**Risk:** *combination of the probability of an event and its consequence.*

Une définition proche est donnée par la norme AS/NZS 4360 (AS/NZS 4360, 2004). Ces deux sources extraites des standards de gestion des risques montrent qu'un risque est composé de deux éléments interdépendants : une cause (appelée aussi « *event* ») et une conséquence. Cette considération est donc valide pour tous les domaines de risque. Nous allons maintenant confronter cette définition avec celles extraites du domaine de la sécurité, l'objectif étant évidemment d'affiner l'analyse.

#### **3.2.2. Standards de sécurité**

Au sein des standards de sécurité, la norme ISO/IEC 13335 (ISO/IEC 13335-1, 2004) définit le risque au sein de son glossaire :

**Risk:** *the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization.*

A l'image de la norme ISO/IEC 13335, l'utilisation du terme « risque » dans les standards de sécurité montre une définition plus précise que celles proposées dans les standards de gestion des risques, mais néanmoins compatibles. Le risque comme défini dans les standards de sécurité est en fait une spécialisation du risque défini dans les standards de gestion des risques. Le concept « risque » est ainsi aligné entre ces sources au sein du tableau 1. Cependant la précision de ses composants est améliorée. La conséquence du risque diffère uniquement en terme de label, parfois appelée impact, conséquence ou nuisance, mais la sémantique sous-jacente reste la même. Cependant la cause du risque est présentée comme une composition d'éléments différents en fonction des sources étudiées. L'étude des méthodes de GRSSI permet de préciser ces composants.

### 3.2.3. Méthodes de GRSSI

La définition de risque est différente dans chaque méthode de GRSSI. Par exemple, la méthode EBIOS (DCSSI, 2004) propose la définition suivante :

**Risk:** *Combination of a threat and the losses it can cause, i.e.: of the opportunity, for a threat agent using an attack method, to exploit one or more vulnerabilities of one or more entities and the impact on the essential elements and on the organisation.*

Pour la méthode OCTAVE (Alberts *et al.*, 1999) :

**Risk:** *[...] It breaks down into three basic components: asset, threat, and vulnerability.*

En premier lieu, les méthodes de GRSSI renforcent dans leur ensemble la conclusion obtenue au niveau des standards de gestion des risques, qui identifient une partie causale et une conséquence au risque. Cependant, une grande diversité est présente à une granularité plus fine, au niveau des composants du risque. D'une manière générale, une tendance se dégage : la partie causale du risque est composée de deux éléments les plus souvent appelés « menace » et « vulnérabilité ».

### 3.2.4. Cadres conceptuels de sécurité

Firesmith propose une définition très précise de « risque » (Firesmith, 2003), composée de la définition de risque de sûreté et risque de sécurité. Ces définitions sont regroupées dans la définition de risque de « survivabilité » :

**Survivability risk** *is the potential risk of harm to an asset due to the sum (over all relevant hazards and threats) of the negative impact of the harm to the asset (i.e., its criticality) multiplied by the likelihood of the harm occurring.*

Cette définition montre une fois encore les deux parties du risque, caractérisé par sa cause et sa conséquence. De plus, en investiguant les définitions et modèles associés à cette référence, on remarque que la cause du risque dépend d'une menace

(pour le domaine de la sécurité) ou d'un danger (pour le domaine de la sûreté) et de l'existence de vulnérabilité (au niveau sûreté ou sécurité).

### 3.2.5. Tableau d'alignement de risque et de ses composants

Les résultats de cette section sont résumés dans le tableau 1. Ce dernier montre une proposition d'alignement du concept de risque et de ses sous-composants. Cinq concepts sont présentés ici, numérotés de (1) à (5), car n'ayant pas de label pour le moment. Un label et une définition à ces concepts sont proposés lors de la construction du modèle du domaine de la GRSSI (Section 3.3). L'ensemble des concepts analysés et l'intégralité du tableau est disponible dans le rapport technique (Mayer *et al.*, 2006b). Il faut également noter que l'illustration précédente (Section 3.2.1 à 3.2.4) montre uniquement une itération de l'étape 1 de la méthode de recherche. Le tableau d'alignement final est obtenu après plusieurs itérations de cette méthode dans le but de vérifier, valider et améliorer les résultats obtenus. Il est à noter que le même type de travail a été effectué pour les relations entre concepts, les résultats étant également disponible dans un rapport technique (Mayer *et al.*, 2006a).

Référence	(1)	(2)	(3)	(4)	(5)
ISO/IEC Guide 73	Risk	Event	Consequence	Source	/
AS/NZS 4360	Risk	Event	Consequence Impact	Source of risk	Cause
ISO/IEC 27001	Risk	/	Impact	/	Vulnerability
ISO/IEC 13335	Risk	/	Impact	/	Vulnerability
Common Criteria	Risk	/	/	Threat	Vulnerability
NIST 800-27 NIST 800-30	Risk	/	Impact	Threat	Vulnerability
EBIOS	Risk	Threat	Impact	/	Vulnerability
MEHARI	Risk Risk scenario	Cause	Consequence	/	Vulnerability
OCTAVE	Risk	/	Consequence Impact	Threat	Vulnerability
CRAMM	Risk	/	Impact	Threat	Vulnerability
CORAS	Risk	/	Unwanted incident	Threat scenario	Vulnerability
Haley <i>et al.</i> Moffet et Nuseibeh	Risk	/	Impact	Threat	Vulnerability
Firesmith	Risk	/	Harm	Hazard Threat	Vulnerability

**Tableau 1.** Alignement de cinq concepts de la GRSSI

### 3.3. Le domaine de la GRSSI

L'étape 2 de la méthode de recherche proposée (Figure 3) démarre par l'assignation d'un label pour chaque concept associé à chaque colonne du tableau d'alignement. Elle prend en compte la pertinence des labels proposés au sein des référentiels étudiés ainsi que leur fréquence. Concernant les concepts du tableau 1, la proposition retenue est la suivante :

- (1) Risque
- (2) Cause du risque
- (3) Impact
- (4) Menace
- (5) Vulnérabilité

Une définition est ensuite proposée pour chaque concept. L'ensemble du modèle du domaine de la GRSSI peut être partagé en trois groupes de concepts : (i) les concepts relatifs aux assets; (ii) les concepts relatifs aux risques; et (iii) les concepts relatifs aux traitements du risque. On distingue ces différents groupes de concept au niveau du modèle conceptuel. Les définitions proposées pour chaque concept résultent de l'alignement des termes de la littérature étudiée en lien avec la GRSSI.

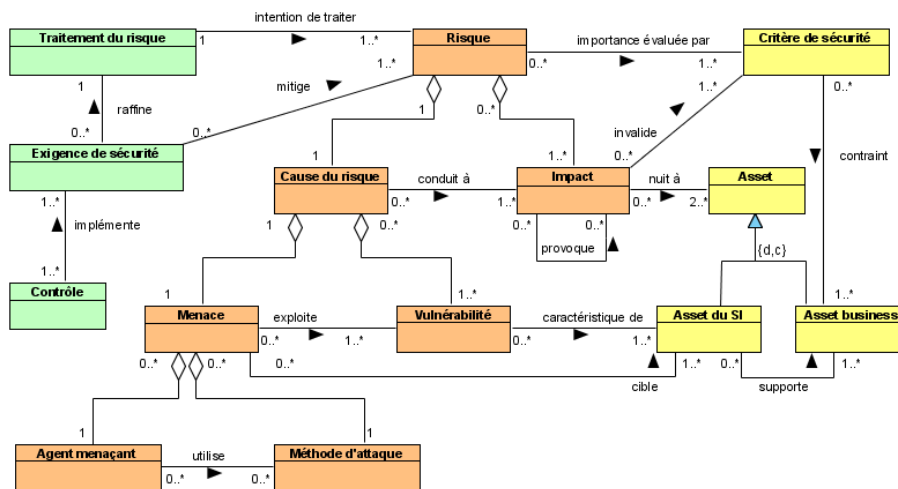


Figure 4. Modèle du domaine de la GRSSI

Les **concepts relatifs aux assets** décrivent quels sont les assets importants à protéger ainsi que les critères qui garantissent leur sécurité. Les concepts sont :

**Asset** – tout ce qui a de la valeur pour l'organisation et qui est nécessaire à la réalisation de ses objectifs.

*Exemple : liste de noms ; processus de remboursement médical ; système d'exploitation ; ordinateur ; réseau Ethernet ; employé encodant des données ; administrateur système ; conditionnement d'air de la salle serveur*

**Asset business** – information, processus, capacité et aptitude inhérent au business de l'organisation, qui a de la valeur pour l'organisation et qui est nécessaire à la réalisation de ses objectifs.

*Exemple : liste de noms ; processus de remboursement médical ; compétences de diagnostic médical*

**Asset du SI** – un composant ou une partie du SI, support aux assets business, qui a de la valeur pour l'organisation et qui est nécessaire à la réalisation de ses objectifs. Un asset du SI peut être un composant du système IT, comme un matériel, un logiciel ou un composant réseau, mais aussi des personnes ou des équipements jouant un rôle dans le SI et donc dans sa sécurité. Il est parfois pertinent pour conduire une étude macroscopique de définir un système en tant qu'asset du SI, composé de divers assets du SI correspondant aux autres types décrits ci-dessus.

*Exemple : système d'exploitation ; ordinateur ; réseau Ethernet ; employé encodant des données ; administrateur système ; conditionnement d'air de la salle serveur*

**Critère de sécurité** (aussi appelé propriété de sécurité) – propriété ou contrainte sur les assets business caractérisant leur besoin de sécurité. Les critères de sécurité sont utilisés en tant qu'indicateurs afin d'évaluer l'importance du risque. Généralement, les critères de sécurité sont confidentialité, intégrité et disponibilité, mais parfois, en fonction du contexte, d'autres critères plus spécifiques peuvent être ajoutés tels que l'authenticité ou la non-répudiation. Les objectifs de sécurité d'un SI sont définis en utilisant les critères de sécurité sur les assets business.

*Exemple : confidentialité d'une liste de noms ; intégrité du processus de remboursement médical*

Les **concepts relatifs aux risques** présentent comment le risque lui-même est défini, quels sont les principes majeurs qui doivent être pris en compte lorsque l'on définit les risques probables. Les concepts sont :

**Risque** – la combinaison d'une menace avec une ou plusieurs vulnérabilités, aboutissant à un impact négatif nuisant à un ou plusieurs assets. Menace et vulnérabilités font partie de la cause du risque et l'impact est la conséquence du risque.

*Exemple : un pirate informatique utilisant de l'ingénierie sociale sur un membre du personnel de l'organisation, en raison d'un manque de sensibilisation du personnel, aboutissant à un accès non-authorized sur des postes informatiques et une perte de confidentialité et d'intégrité sur des informations sensibles ; un voleur pénétrant dans l'immeuble de l'organisation en raison d'absence de contrôle d'accès physique, volant des documents contenant des informations sensibles et provoquant ainsi une perte de confidentialité*

**Impact** – la conséquence négative potentielle d'un risque qui peut nuire aux assets d'un SI ou d'une organisation, quand une menace (ou la cause du risque) est réalisée. L'impact peut être décrit au niveau des assets du SI (destruction de données, défaillance d'un composant) ou au niveau des assets business, où il invalide les critères de sécurité, comme par exemple : perte de confidentialité, perte d'intégrité, indisponibilité... Un impact peut provoquer d'autres impacts (appelés impacts indirects), comme par exemple une perte de confidentialité sur des informations sensibles qui peut engendrer une perte de la confiance des clients.

*Exemple : découverte du mot de passe utilisateur (niveau SI) ; perte de la confidentialité des informations personnelles (niveau business)*

**Cause du risque** – la combinaison d'une menace avec une ou plusieurs vulnérabilités

*Exemple : un pirate informatique utilisant de l'ingénierie sociale sur un membre du personnel de l'organisation, en raison d'un manque de sensibilisation du personnel ; un voleur pénétrant dans l'immeuble de l'organisation en raison d'absence de contrôle d'accès physique*

**Vulnérabilité** – caractéristique d'un asset du SI ou d'un groupe d'assets du SI, qui constitue une faiblesse ou une faille au regard de la sécurité. Elle peut être accidentellement ou intentionnellement exploitée par une menace.

*Exemple : manque de sensibilisation du personnel ; absence de contrôle d'accès physique ; absence de détection incendie*

**Menace** – attaque ou incident potentiel, qui cible un ou plusieurs assets du SI et qui peut engendrer une nuisance aux assets. Une menace est généralement composée d'un agent menaçant et d'une méthode d'attaque. (Note : Parfois il peut tout de même être plus pertinent de décrire un risque à l'aide d'une menace globale, sans distinction précise entre l'agent menaçant et la méthode d'attaque, comme pour une crue ou une défaillance de composant).

*Exemple : un pirate informatique utilisant de l'ingénierie sociale ; crue ; défaillance de composant*

**Agent menaçant** – un agent qui peut potentiellement nuire aux assets du SI. Un agent menaçant déclenche une menace et est la source du risque. Il peut être caractérisé par son type (généralement humain ou naturel/environnemental) et par sa manière d'agir (accidentelle ou délibérée). Dans le cas d'une cause accidentelle, il peut également être caractérisé par son exposition et les ressources disponibles et dans le cas d'une cause délibérée, il peut être caractérisé par son expertise, ses ressources disponibles et sa motivation.

*Exemple : membre du personnel avec peu de capacités techniques et de temps mais une forte motivation pour lancer une attaque ; pirate informatique avec de fortes compétences techniques, bien équipé et une forte motivation liée à l'argent qu'il peut gagner ; climat très humide durant trois mois de l'année ; virus*

**Méthode d'attaque** - moyen standard par lequel un agent menaçant mène une attaque.

*Exemple : intrusion de système ; vol de média ou de document ; ingénierie sociale ; défaillance de composant*

Les **concepts relatifs aux traitements du risque** décrivent quelles mesures, exigences et contrôles doivent être définis et implémentés dans le but de mitiger les risques potentiels. Les concepts sont :

**Traitement du risque** – expression de l'intention de traiter les risques identifiés. Il satisfait un besoin de sécurité, exprimé en termes génériques et fonctionnels, et peut être raffiné par des exigences de sécurité. Les différents traitements du risque sont :

- Evitement du risque – décision de ne pas être impliqué ou de se soustraire à un risque.
- Réduction du risque – action de diminution de la probabilité, de la conséquence, ou des deux, associées à un risque.
- Transfert du risque – partage avec une autre partie de la charge de la perte liée à un risque.
- Prise du risque – acceptation de la charge de la perte liée à un risque

*Exemples : des contrôles doivent être mis en place afin d'éviter les intrusions réseau ; l'accès physique aux salles doit être protégé ; prise d'une assurance afin de couvrir la perte de service ; acceptation d'une indisponibilité du service durant une heure*

**Exigence de sécurité** – le raffinement d'une mesure de traitement du risque pour mitiger le risque. Chaque exigence de sécurité contribue à couvrir un ou plusieurs traitements du risque ciblant le SI. (Note : Généralement, les exigences de sécurité sont utilisées afin de raffiner les décisions de réduction de risque.)

*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 ; un contrôle d'accès physique doit être effectué ; les salles doivent être protégées contre les départs de feu*

**Contrôle** (ou contre-mesure) – un moyen d'améliorer la sécurité, spécifié par une exigence de sécurité et implémenté pour s'y conformer. Les contrôles de sécurité peuvent être des processus, des politiques, des appareils, des pratiques ou toute action ou composant du SI et de son organisation qui agit afin de réduire les risques.

*Exemple : firewall ; procédure de sauvegarde ; gardien à l'entrée du bâtiment*

#### **4. Optimisation du retour sur investissement de la sécurité**

L'objectif central de la gestion des risques est de permettre un alignement business/IT au niveau de la sécurité du SI (Section 2.1). Au cœur de la gestion des risques et plus particulièrement de l'analyse et de l'appréciation du risque, on

retrouve donc la mesure du risque et de ses composantes, appelée estimation des risques. Plusieurs approches à l'estimation du risque sont envisageables et utilisées parmi les différents référentiels et méthodes de gestion des risques :

- Estimation "ad-hoc" des risques

On retrouve dans cette catégorie les méthodes et référentiels très pauvres en termes de mesure des concepts de la GRSSI. On y trouve des approches se focalisant sur l'identification des risques, où peu d'indications (voire pas du tout) sont données quant à l'estimation du risque (Stoneburner *et al.*, 2002).

- Estimation qualitative des risques

L'estimation qualitative des risques est certainement à l'heure actuelle la plus répandue dans l'industrie (DCSSI, 2004 ; CLUSIF, 2004 ; Alberts *et al.*, 1999). Elle propose une échelle de niveaux (avec des entiers tels 1 – 2 – 3 – 4 ou des termes tels bas – moyen – haut) pour décrire qualitativement les concepts à mesurer. Le principal avantage de l'estimation qualitative est sa facilité de compréhension par toutes les parties concernées, mais un désavantage est la dépendance à un choix subjectif de l'échelle.

- Estimation quantitative des risques

Les approches quantitatives de gestion des risques proposent de mesurer précisément les concepts de la GRSSI. La qualité de l'estimation dépend de la précision et de la complétude des mesures numériques et de la validité des modèles utilisés. Par exemple, on va évaluer en terme financier les assets ou en terme de durée d'indisponibilité les risques liés à la disponibilité (Insight Consulting, 2003). L'historique des incidents constitue une des sources principales de données des estimations quantitatives. L'avantage de ce type d'approche est bien entendu sa précision, mais le coût et le manque d'informations utiles constitue son principal désavantage.

A noter enfin qu'un nouveau type d'estimation émerge, appelé estimation semi-quantitative. Elle consiste à estimer les risques à l'aide d'une échelle, dont les niveaux seraient définis à l'aide d'informations quantitatives (ex: niveau d'impact 1 : perte entre 100€ et 1000€, niveau d'impact 2 : perte entre 1000€ et 10000€, etc.) Dans une méthode de gestion des risques donnée, les différents types d'approche peuvent être associés. Par exemple, une estimation qualitative peut être utilisée en premier afin d'obtenir une estimation grossière des risques, puis une estimation quantitative peut fournir des informations complémentaires sur les risques majeurs identifiés.

Il est généralement admis que les deux facteurs principaux de la GRSSI à considérer, en lien avec l'alignement business/SI recherché, sont le niveau de sécurité (ou de réduction de risque) et le coût associé, comme le montre, par exemple, la définition suivante tirée du CISA Review Manual 2006 (ISACA, 2006): *"Risk management is the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives, and deciding what countermeasures, if any, to take in reducing risk to an acceptable*

*level, based on the value of the information resource to the organization.*" Il en découle donc un de nos objectifs de recherche : l'amélioration et l'automatisation de la GRSSI afin d'atteindre le meilleur « Retour sur Investissement de la Sécurité » ou ROSI (Return On Security Investment). Définir des métriques pertinentes associées aux concepts identifiés de la GRSSI est naturellement une base pour un tel objectif, principalement pour effectuer l'estimation puis l'appréciation du risque. Notre but est donc de définir d'une manière systématique les métriques pertinentes à utiliser dans le cadre de la GRSSI et de les intégrer à notre modèle conceptuel de la GRSSI. Il est fondamental de noter que le résultat attendu n'est pas la définition d'un nouveau cadre concret d'analyse des risques avec des métriques définies précisément (à l'image des méthodes de GRSSI). Notre objectif est focalisé sur l'identification, à un niveau abstrait, des métriques pertinentes pour la GRSSI. A partir de cette étude, il serait possible à tout un chacun de définir son propre ensemble de métriques concrètes, qualitative, quantitative ou autre, à inclure au sein d'une méthode donnée ou d'un outil logiciel.

#### **4.1. Méthode de recherche**

Afin d'atteindre notre objectif de définition des métriques pertinentes pour la GRSSI et le raisonnement autour du ROSI, la méthode de recherche que nous proposons (Figure 5) est basée sur deux approches complémentaires. La première est le paradigme *Goal Question Metric* (GQM) (Basili *et al.*, 1994). Cette approche est utilisée afin d'éliciter les métriques d'une manière top-down, en partant des objectifs généraux du domaine de la GRSSI. Les résultats obtenus sont l'ensemble des métriques nécessaires pour effectuer de la GRSSI et atteindre le meilleur ROSI. Cependant cette définition des métriques reste subjective et doit être validée. La seconde approche, utilisée en tant que validation, est basée sur une étude des méthodes et référentiels de GRSSI. Cette approche est bottom-up, utilisant une analyse des sources (méthodes ou référentiels) existantes de GRSSI, afin d'identifier les métriques actuellement utilisées. Les sources étudiées sont celles exploitées lors de la définition du domaine de la GRSSI (Section 3) qui disposent d'une partie méthodologique. Les documents ne traitant que de terminologie sont évidemment exclus de cette étude. L'analyse commence par une identification des différentes étapes de chaque source effectuant de la mesure de concept. Ensuite, nous collectons les caractéristiques de chaque métrique identifiée au sein d'un tableau. Les métriques identifiées lors de cette seconde étape devraient bien entendu être compatibles avec les métriques définies lors de la première étape à l'aide de l'approche GQM. Si une métrique non identifiée à l'aide du framework GQM est relevée au sein d'une approche de GRSSI, il est alors nécessaire d'évaluer sa pertinence. L'étude GQM doit être revue et améliorée en tenant compte de ce nouvel élément ou une justification d'exclusion de cette métrique doit être formulée, principalement en se basant sur les objectifs et les caractéristiques propres de chaque méthode de GRSSI, qui peuvent être différents d'une approche à l'autre, et la pertinence de cette métrique vis-à-vis de nos objectifs. Les résultats finaux (Figure 8) sont intégrés en tant qu'attributs du modèle conceptuel GRSSI présenté en Figure

4. Dans la suite, bien que les résultats soient présentés d'une manière séquentielle, il faut bien noter que ces étapes ont été conduites de manière itérative et incrémentale.

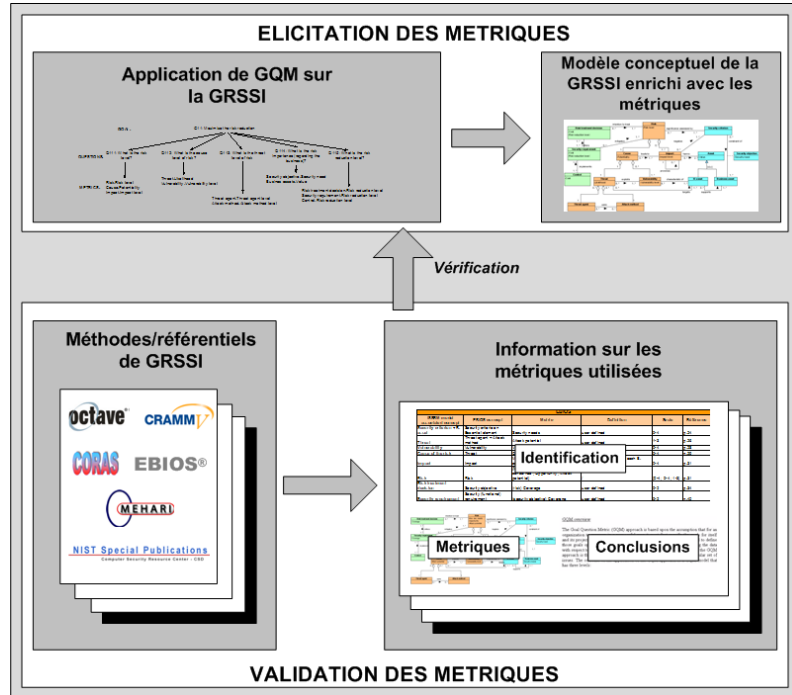


Figure 5. Méthode de recherche des métriques de la GRSSI

## 4.2. Approche Goal-Question-Metric pour l'élicitation des métriques de la GRSSI

### 4.2.1. Présentation de l'approche GQM

L'approche GQM se base sur l'hypothèse que pour qu'une métrique soit pertinente, il est nécessaire de spécifier en premier lieu les objectifs sous-jacents à l'utilisation de cette métrique, puis relier à ces objectifs les données qui vont permettre de définir les objectifs au niveau opérationnel et enfin fournir le cadre permettant d'interpréter les données au regard des objectifs définis (Basili *et al.*, 1994). La finalité de l'application de l'approche GQM est la spécification d'un système de mesure répondant à une problématique. Le résultat est un modèle GQM qui comporte trois niveaux :

1. Niveau conceptuel, ou "Objectifs" : Un objectif est défini pour un objet tel un produit, un processus ou une ressource

2. Niveau opérationnel, ou "Questions" : Un ensemble de questions est utilisé afin de caractériser la manière d'évaluer qu'un objectif spécifique est en train de se réaliser
3. Niveau quantitatif, ou "Métriques" : Un ensemble de données est associé à chaque question dans le but d'y répondre de manière quantitative

Un modèle GQM est donc une structure hiérarchique (Figure 6) démarrant par un objectif. Cet objectif est raffiné en plusieurs questions. Enfin chaque question est raffinée en métriques. A noter qu'une même métrique peut être utilisée afin de répondre à des questions différentes.

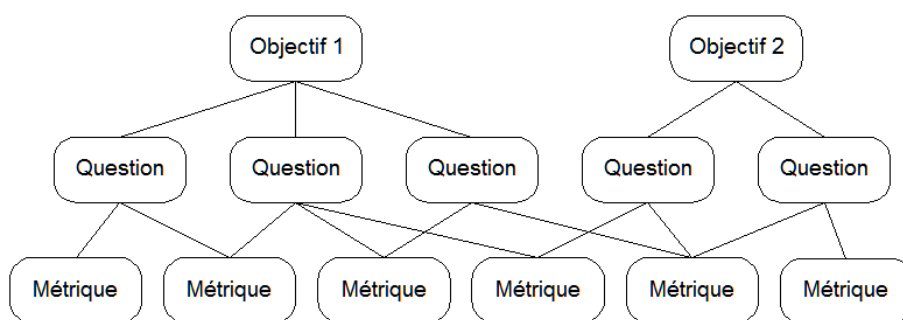


Figure 6. Exemple de modèle GQM (inspiré de (Basili et al., 1994))

#### 4.2.2. Application de l'approche GQM sur le domaine de la GRSSI

Le principal objectif de la GRSSI est d'obtenir le meilleur ROSI (ISACA, 2006 ; Stoneburner *et al.*, 2002). En effet, l'introduction de la gestion des risques au sein de la sécurité des SI a permis de ne plus voir la sécurité comme simplement un problème technique, elle a permis d'aligner la sécurité avec le niveau stratégique de l'entreprise. Le CLUSIF propose un état de l'art (CLUSIF, Groupe de travail ROSI, 2004) autour de la notion de ROSI. Il n'y a pas de consensus clair autour de la définition de ROSI, mais deux propositions se distinguent :

La première relativise les coûts de la sécurité par rapport aux bénéfices qu'elle apporte :

$$\text{ROSI} = (\text{Bénéfices} - \text{Coûts}) / \text{Coûts}$$

La seconde est orientée incidents et mesure le ROSI à l'aide de la « Prévission de Pertes Annuelles » de la sécurité ou ALE (Annual Loss Expectancy). Cette prévision de perte annuelle exprime l'évaluation des pertes annuelles à partir du coût financier d'un incident et de sa fréquence de survenance :

$$\text{ROSI} = \text{ALE 1} - \text{ALE 2} - \text{coût annuel des contrôles}$$

Avec ALE 1 = ALE avant mise en place de contrôles de sécurité

$ALE_2 = ALE$  après mise en place de contrôles de sécurité  
 $ALE = \sum Coûts_i \times Fréquence\ de\ survenance_i$   
 $i$  : incident de sécurité ;  $\Sigma$  : la somme annuelle des incidents de sécurité prévisibles

En considérant ces deux définitions, la proposition suivante reste valide pour le domaine de la GRSSI : **afin de maximiser le ROSI, il est nécessaire de maximiser la réduction des risques tout en minimisant le coût de traitement des risques associé.** Les objectifs de notre étude GQM sont donc « Maximiser la réduction des risques » et « Minimiser le coût de traitement des risques », qui seront respectivement à la base des modèles GQM obtenus (Figure 7, A et B).

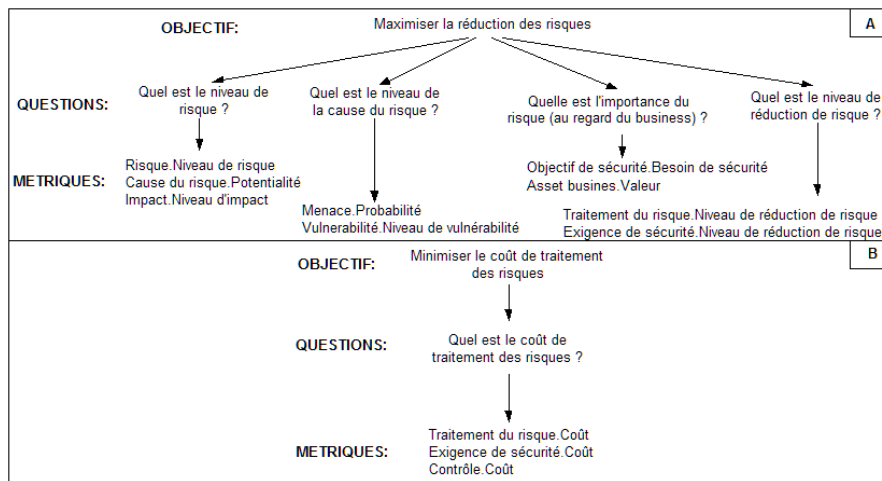


Figure 7. Modèles GQM issus de l'application de l'approche GQM au domaine de la GRSSI

L'application de l'approche GQM sur le domaine de la GRSSI a permis d'identifier un ensemble de métriques portant sur les concepts du domaine précédemment défini (Section 3.3). Au sein du modèle GQM (Figure 7), on présente les métriques de la manière suivante : *ConceptDomaineGRSSI.Métrique*, comme par exemple *Menace.Probabilité* indiquant que *Probabilité* est une métrique du concept de *Menace*. Il est ainsi possible de reporter sur le modèle conceptuel du domaine de la GRSSI (Figure 4) l'ensemble de ces métriques sous la forme d'attributs. On remarque particulièrement sur notre modèle GQM le besoin d'introduction d'un nouveau concept, qui prend la forme d'une classe d'association sur notre modèle conceptuel (Figure 8). Il définit l'application d'un critère de sécurité sur un asset business. Ce concept est appelé « Objectif de sécurité » et est particulièrement intéressant pour définir le besoin de sécurité, qui est une métrique identifiée de la

GRSSI. On pourra définir par exemple le besoin de sécurité en confidentialité (critère de sécurité) d'une information client (asset business).

#### 4.3. Etude des méthodes et référentiels de GRSSI pour la validation des métriques

L'analyse des méthodes et référentiels de GRSSI, afin de valider les métriques obtenues lors de l'application de l'approche GQM sur le domaine de la GRSSI, a été réalisée sur six sources différentes : EBIOS (DCSSI, 2004), MEHARI (CLUSIF, 2004), OCTAVE (Alberts *et al.*, 1999), CRAMM (Insight Consulting, 2003), NIST 800-30 (Stoneburner *et al.*, 2002) et CORAS (Vraalsen *et al.*, 2007). Nous présentons au sein de ce paragraphe uniquement l'analyse détaillée de la méthode EBIOS, les autres sources ayant été analysées d'une manière identique. Le document ayant servi de référence à l'analyse d'EBIOS est le suivant : EBIOS – Expression des Besoins et Identification des Objectifs de Sécurité – Section 3 – Techniques (DCSSI, 2004).

La première étape de notre analyse consiste en une identification des différentes mesures de concepts réalisées lors du déroulement de la méthode. Les métriques utilisées seront représentées en *italique* et les concepts associés en **gras**.

- Définir les *besoins de sécurité* des **éléments essentiels** à l'aide des **critères de sécurité** les contraignant.
- Définir le *potentiel d'attaque* des **agents menaçants** couplés aux **méthodes d'attaque**.
- Définir le *niveau* des **vulnérabilités** associées aux agents menaçants sélectionnés.
- Définir l'*opportunité* des **menaces** en se basant sur le niveau des vulnérabilités associées ou directement.
- Définir les **impacts** des risques, équivalents au maximum des *besoins de sécurité concernés*.
- Définir le niveau des **risques**, composé par l'*opportunité*, le *potentiel d'attaque* et le maximum des *besoins de sécurité concernés*.
- Définir la *couverture* des risques par les **objectifs de sécurité** sélectionnés.
- Définir la *couverture* des objectifs de sécurité par les **exigences de sécurité** sélectionnées.

Une fois l'ensemble des tâches mettant en œuvre une mesure de concept identifié, les métriques associées sont analysées à l'aide du tableau suivant (Tableau 2) dans lequel seront répertoriées les informations suivantes : concept du domaine de la GRSSI concerné, concept EBIOS équivalent, nom de la métrique, nom choisi pour cette métrique lors de l'utilisation de GQM, manière dont la métrique est définie ou calculée, échelle ou unité de la métrique.

EBIOS					
Concept du domaine de la GRSSI	Concept EBIOS	Métrique	Métrique du méta-modèle de la GRSSI	Définition	Echelle/unité
Objectif de sécurité (Critère de sécurité + Asset business)	Critère de sécurité sur Elément essentiel	Besoin de sécurité	Besoin de sécurité	Défini par l'utilisateur	0-4
Menace	Agent menaçant et méthode d'attaque	Potentiel d'attaque	Probabilité	Défini par l'utilisateur	1-3
Vulnérabilité	Vulnérabilité	Niveau de vulnérabilité	Niveau de vulnérabilité	Défini par l'utilisateur	0-4
Cause du risque	Menace	Opportunité	Potentialité	f(Niveau de vulnérabilité)	0-4
Impact	Impact	Besoins de sécurité concernés	Niveau d'impact	max(Besoin de sécurité) pour chaque asset business	0-4
Risque	Risque	{Besoins de sécurité concernés ; Opportunité ; Potentiel d'attaque}	Niveau de risque	/	{0-4 ; 0-4 ; 1-3}
Traitement du risque	Objectif de sécurité	Couverture (des risques)	/	Défini par l'utilisateur	0-2
Exigence de sécurité	Exigence de sécurité (fonctionnelle)	Couverture (des objectifs de sécurité)	/	Défini par l'utilisateur	0-2

**Tableau 2.** Analyse des métriques de la méthode EBIOS

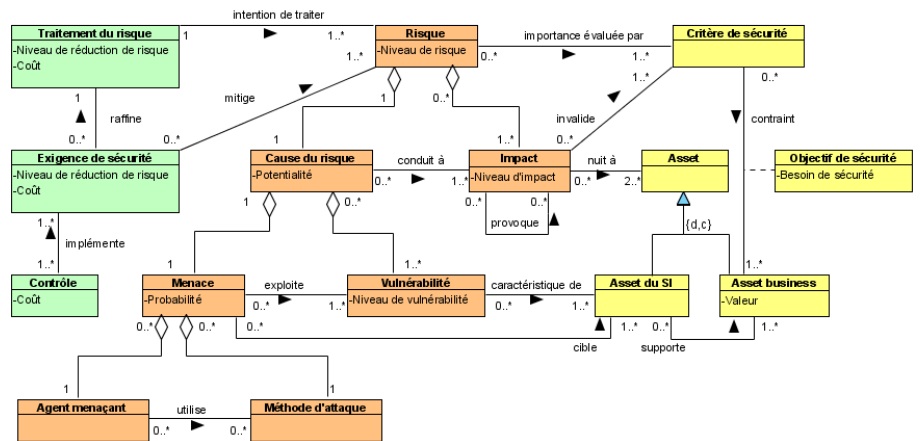
On peut donc voir, par exemple, que le concept de « Cause du risque » du domaine de la GRSSI, appelé « Menace » dans la méthode EBIOS, est mesuré à l'aide d'une métrique nommée « Opportunité ». Cette métrique est équivalente à la métrique de « Potentialité » proposée pour le domaine de la GRSSI (Figure 7A) et elle est définie au sein de la méthode comme étant fonction du niveau des vulnérabilités associées. Enfin, une échelle qualitative de 0 à 4 est suggérée. Un modèle de référence pour les métriques de la méthode EBIOS peut être produit, reprenant les concepts du domaine de la GRSSI et les métriques proposées dans EBIOS en tant qu'attribut de ces concepts, permettant ainsi de comparer plus facilement les métriques d'EBIOS par rapport aux métriques élicitées lors de l'application de l'approche GQM.

On remarque que l'ensemble des métriques proposé par EBIOS est proche de celui que nous proposons (Figure 7). Au niveau des concepts relatifs aux assets et aux risques, les métriques identifiées au sein d'EBIOS sont équivalentes à celles identifiées sur les modèles GQM. La différence principale entre les résultats des deux études se situe au niveau des concepts relatifs aux traitements du risque. L'étude GQM a identifié les métriques de niveau de réduction de risque et de coût des traitements, tandis que l'analyse d'EBIOS a révélé les métriques de couverture du risque par les traitement du risque et de couverture des traitements par les exigences de sécurité. En effet, le résultat principal attendu suite à l'utilisation de la méthode EBIOS est une couverture complète des risques par les différents niveaux de traitement du risque, plus que l'atteinte du meilleur ROSI. Les métriques de couverture (des risques et des objectifs de sécurité au sens EBIOS) ne représente donc pas des métriques de premier ordre au regard de nos objectifs et ne nécessitent donc pas d'être intégrées à notre modèle conceptuel (Figure 8). Cependant elles restent tout de même pertinentes et potentiellement utilisable au sein d'une méthode concrète, principalement en tant qu'indicateurs montrant qu'aucun risque n'a été

oublié. De plus, bien que ces deux métriques ne soient pas intégrées à notre modèle conceptuel, elles peuvent apporter une aide à l'implémentation de la maximisation de la réduction de risque, car indiquant l'état actuel des risques considérés (traités ou non) à un moment donné.

**4.3. Proposition d'enrichissement du modèle conceptuel de la GRSSI par les métriques associées**

En conclusion de notre étude sur les méthodes existantes, on remarque que chaque type de concept est généralement mesuré : concepts relatifs aux assets, concepts relatifs aux risques et concepts relatifs aux traitements du risque. Cependant, les métriques sont proposées à différents niveaux d'abstraction (niveau générique asset ou spécifique asset business, niveau du concept de risque ou niveau de ses sous-composants, traitement du risque ou contrôle...) A partir de notre application de GQM au domaine de la GRSSI, de l'étude des différents référentiels et méthodes existants et du modèle conceptuel de la GRSSI, notre proposition de métriques est la suivante (Figure 8) :



**Figure 8. Modèle conceptuel de la GRSSI enrichi par les métriques associées**

Au niveau des concepts relatifs aux assets, il est intéressant de déterminer la valeur des assets business ainsi que le besoin de sécurité associé à chaque objectif de sécurité. Les concepts relatifs aux risques sont mesurés à l'aide du niveau de risque pour le concept de risque, de la potentialité pour la cause du risque et le niveau d'impact pour l'impact et enfin de la probabilité de la menace et le niveau de vulnérabilité des vulnérabilités. Finalement, au niveau des concepts relatifs aux traitements du risque, les traitements du risque et les exigences de sécurité sont estimés en termes de niveau de réduction de risque et de coût et les contrôles uniquement en termes de coût.

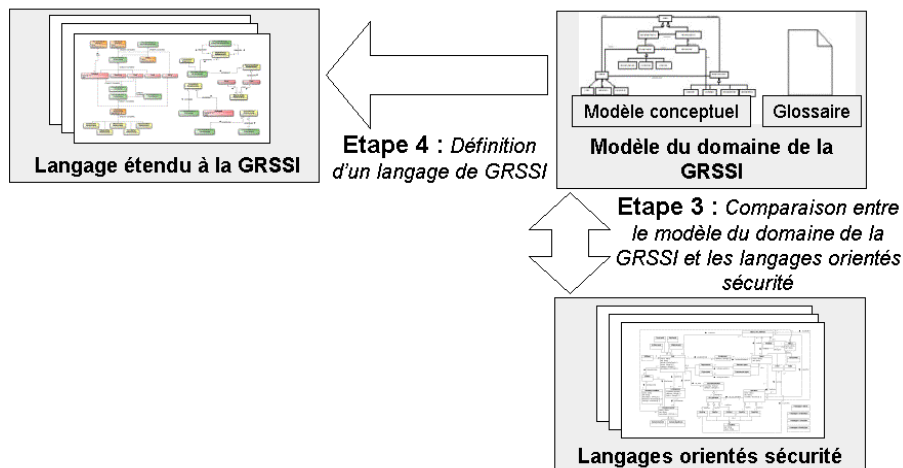
Plusieurs particularités se dégagent de cet ensemble de métriques. Tout d'abord, le concept de contrôle ne dispose pas d'un attribut de niveau de réduction des risques, à l'image du concept de traitement du risque ou d'exigence de sécurité. En prenant un exemple d'exigence de sécurité et de contrôles associés, l'explication est évidente : à l'exigence de sécurité « Effectuer du filtrage réseau » sont associés les contrôles « Firewall » et « Mise à jour du firewall ». On remarque alors qu'il est impossible d'attribuer un niveau de réduction de risque propre au contrôle « Mise à jour du firewall ». Seule la mesure de la réduction de risque au niveau des exigences de sécurité et des traitements du risque ont un sens. La deuxième particularité principale de l'ensemble proposé de métriques est que tous les composants du risque ont une métrique permettant de mesurer leur niveau à l'exception d'agent menaçant et de méthode d'attaque. En effet, seule leur composition (menace) est mesurable et cette hypothèse a été vérifiée lors de l'étude des méthodes existantes. Seules certaines caractéristiques sont identifiées indépendamment entre les agents menaçants et les méthodes d'attaques, utilisable ensuite en tant qu'indicateurs de la probabilité de la menace, tel le niveau de compétence d'un agent menaçant ou le type de méthode d'attaque (naturel, humain...) En vue de l'implémentation du modèle conceptuel au sein d'un outil, les contraintes OCL (Warmer *et al.*, 2003) présentes seront identifiées par la suite, permettant ainsi une nouvelle validation de l'exactitude et de la pertinence de ces métriques. Ce travail est actuellement en cours.

## **5. Support à la gestion des risques par les modèles**

Une fois l'ensemble des concepts de la GRSSI identifié (Section 3) et les métriques associées définies (Section 4), une proposition de langage de modélisation peut être réalisée en lien avec notre objectif principal de support à la gestion des risques par les modèles.

### **5.1. Méthode de recherche**

La méthode de recherche suivante complète la méthode proposée à la Section 3.1 (Figure 3) par deux étapes. Notre point d'entrée est donc le modèle du domaine de la GRSSI. A noter que nous avons complété ce dernier à l'aide des métriques nécessaires à la GRSSI (Figure 5).



**Figure 9.** Méthode de recherche permettant de définir un langage de GRSSI

Les étapes sont les suivantes :

**Etape 3 – Comparaison entre le modèle du domaine de la GRSSI et les langages orientés sécurité :** De nombreux langages de modélisation ont déjà été proposés afin de modéliser les aspects liés à la sécurité des SI. Ces langages ont été comparés avec le modèle du domaine de la GRSSI. Pour chaque langage, son méta-modèle ainsi que les définitions des concepts fournies seront examinées, dans le but d'identifier les concepts du modèle du domaine de la GRSSI supportés et ceux manquant. Lors de cette étape, des informations pertinentes peuvent être également identifiées afin d'améliorer le modèle du domaine, ce qui explique la flèche à double sens de l'étape 3. Les principaux résultats attendus sont :

- la validation (ou non) de l'hypothèse qu'aucun langage ne supporte complètement la GRSSI
- l'évaluation du domaine de couverture de chaque langage de modélisation au regard des concepts de la GRSSI
- l'identification des améliorations (extensions/révisions) à apporter aux langages pour les rendre adaptés à la GRSSI

**Etape 4 – Définition d'un langage de GRSSI :** Notre objectif final est de fournir un support de modélisation à la GRSSI sous forme d'un (voire plusieurs) langages. La conformité de ses éléments avec le domaine de la GRSSI est garantie par l'étape précédente. La définition d'un langage de modélisation formel implique la définition d'une syntaxe et d'une sémantique (Harel *et al.*, 2004) afin de supporter le raisonnement automatique et d'éviter les ambiguïtés. Il faut également prendre en

compte d'autres propriétés telles les mécanismes de structuration du langage ou la pertinence des symboles graphiques (Moody, 2006a ; Moody, 2006b).

### 5.2. Comparaison entre le modèle du domaine de la GRSSI et les langages orientés sécurité

Plusieurs langages de modélisation développés pour les phases amonts de développement de SI sont aujourd'hui disponibles. Ces derniers nous intéressent particulièrement afin de couvrir notre objectif de prise en compte de la sécurité au plus tôt dans le développement de SI. Au sein de ces langages, certains sont plus spécifiquement focalisés sur la sécurité et donc plus proches de nos besoins : Secure Tropos (Mouratidis *et al.*, 2002), Misuse Cases (Sindre *et al.*, 2005), Abuse Case (McDermott *et al.*, 1999), Abuse Frames (Lin *et al.*, 2004) ou KAOS étendu à la sécurité (van Lamsweerde, 2004). Cet ensemble de langage représente notre panel de langages à comparer avec le modèle du domaine de la GRSSI.

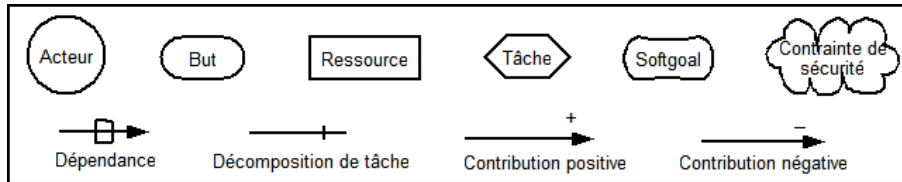


Figure 10. Légende du langage Secure Tropos

Pour chaque langage, un tableau de comparaison est produit, mettant en évidence le niveau de support du langage par rapport au domaine de la GRSSI. Le tableau 3 présente par exemple les résultats obtenus suite à l'étude du langage Secure Tropos (Mouratidis *et al.*, 2004 ; Mouratidis *et al.*, 2007), qui repose principalement sur les concepts d'acteur, de but de ressource, de tâche, de softgoal et de contraintes de sécurité, ainsi que sur les relations de dépendances de décomposition de tâche et de contributions (Figure 10). Ces éléments de langage sont illustrés par la suite à l'aide des exemples proposés Figure 11 et Figure 12. Au niveau du tableau de comparaison, la colonne « Synonymes » rassemble le ou les termes utilisés spécifiquement pour désigner un concept donné du domaine de la GRSSI au sein de la littérature du langage étudié, tandis que la colonne « Élément de langage » indique quel(s) élément du langage (ou du méta-modèle de ce dernier) permet de le représenter au sein des modèles.

Modèle du domaine de la GRSSI		Secure Tropos	
		Synonymes	Éléments du langage
Concepts relatifs aux	Asset	/	Acteur, But, Tâche, Ressource et Softgoal
	Asset business		

<b>assets</b>	Asset du SI		
	Critère de sécurité	Propriété de protection, Caractéristique de sécurité	Softgoal, Contrainte de sécurité
<b>Concepts relatifs aux risques</b>	Risque	/	/
	Impact	/	Contribution négative
	Cause du risque	/	Menace
	Menace	/	But, Tâche
	Vulnérabilité	/	/
	Agent menaçant	Attaquant	Acteur
	Méthode d'attaque	/	Tâche ayant un lien <i>attacks</i>
<b>Concepts relatifs aux traitements du risque</b>	Mesure de traitement du risque	/	/
	Exigence de sécurité	Objectif de protection, Entités sécurisées	Acteur, But, Tâche, Ressource et Softgoal
	Contrôle	/	/

**Tableau 3.** *Alignement entre Secure Tropos et le modèle du domaine de la GRSSI*

Ce travail d'alignement a donc été réalisé pour l'ensemble des langages de modélisation de la sécurité. La conclusion principale est qu'il n'existe à l'heure actuelle aucun langage proposant un support complet à la GRSSI. Bien que certains langages incluent plusieurs concepts en lien avec la GRSSI, ces approches ne sont pas complètes au regard du domaine. Cette analyse a, de plus, mis en évidence la pertinence de chaque langage vis-à-vis des différentes phases du processus de GRSSI. Certains langages ont par exemple approché le domaine de la GRSSI en considérant plus particulièrement les agents menaçants et les méthodes d'attaques (Sindre *et al.*, 2005 ; McDermott *et al.*, 1999) et se sont ensuite focalisés sur les différents contrôles applicables, sans effectuer une analyse des risques. D'un autre côté, les langages sont généralement dédiés à certaines phases du cycle de développement système. Par exemple, certains langages comme Secure Tropos mettent essentiellement l'accent sur le niveau business qu'on retrouve au sein de la GRSSI (asset business, critères de sécurité, exigences de sécurité...) tandis que d'autres, plus focalisés sur l'architecture du système, couvrent des concepts comme les assets du SI, les vulnérabilités et les contrôles, comme KAOS. Enfin, les tableaux d'alignement de chaque langage nous permettent d'assurer l'interopérabilité entre ces langages du point de vue de la GRSSI. Comme notifié précédemment, des langages sont plus adaptés que d'autres pour supporter certaines étapes de la GRSSI.

Les langages peuvent donc être utilisés de manière complémentaire et les différents tableaux d'alignement constituent une référence afin d'assurer l'interopérabilité entre les langages au niveau des concepts de la GRSSI.

### **5.3. Proposition de langage pour la GRSSI basée sur Secure Tropos**

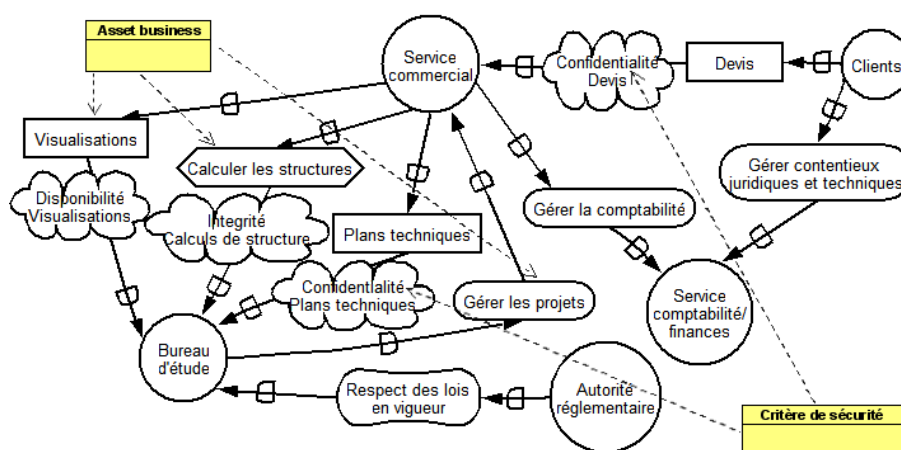
Le langage Secure Tropos représente un candidat intéressant en vue d'une extension de langage visant à supporter la GRSSI (voir étape 4 Figure 9), d'une part par le nombre de concepts déjà supportés, mais également par rapport à certaines caractéristiques qui lui sont propres. Par exemple, Secure Tropos prend particulièrement en compte les aspects liés aux exigences non-fonctionnelles, dont la sécurité fait partie. Les mécanismes du langage qui en découlent traduisent cet aspect, on peut citer en particulier les contributions positives et négatives (Figure 10) permettant d'évaluer différentes architectures.

Actuellement, une description formelle du langage de Secure Tropos, étendu à la gestion des risques est un travail en cours. Cependant, notre travail s'articulant autour d'études empiriques et d'expérimentations régulières de nos travaux sur des études de cas théoriques ou concrètes, afin d'en tirer au plus tôt les retours d'expérience, nous avons proposé une extension ad-hoc du langage de Secure Tropos (Dubois *et al.*, 2006 ; Mayer *et al.*, 2005). Il repose sur l'utilisation classique du langage pour les étapes du processus de gestion des risques déjà supportées en termes de concepts de la GRSSI (Figure 11), ainsi que sur une proposition d'extension par de nouveaux éléments pour les concepts absents du langage initial (Figure 12).

L'exemple suivant, qui est une adaptation de l'étude de cas de la méthode EBIOS (DCSSI, 2004), est un exemple illustratif de l'utilisation de Secure Tropos dans le cadre de la GRSSI. Il présente une société fictive d'ingénierie en architecture, qui réalise des plans d'usines ou d'immeubles. Au cœur de ses activités, elle calcule des structures, élabore des plans de visualisation pour les clients, élabore des plans techniques pour les architectes et établit des devis.

Les différentes activités de l'entreprise sont introduites à l'aide d'un modèle Secure Tropos. La société est composée de plusieurs départements représentés sous la forme d'*acteurs* : le bureau d'étude, le service commercial et le service comptabilité/finances, les deux derniers étant en relation avec des clients. Ces acteurs présentent un ensemble de dépendances entre eux. Le bureau d'étude dépend du service commercial afin d'assurer la gestion des projets. Le service commercial dépend du service comptabilité/finances pour gérer la comptabilité. Les clients dépendent du service comptabilité/finances pour gérer les contentieux juridiques et techniques. Ces trois relations, qui peuvent être réalisés de plusieurs manières, représentent des dépendances de *but*. Une dépendance de *tâche* est quant à elle utilisée lorsque qu'un acteur doit réaliser une activité. Le service commercial dépend du bureau d'étude pour le calcul de structure, le calcul de structure étant une activité précisément définie et où aucune alternative dans sa réalisation n'est

possible. Les acteurs présentent aussi des dépendances au niveau de *ressources*, de type physique ou informationnel, à fournir. Le service commercial dépend du bureau d'étude pour la fourniture des plans techniques et des visualisations et les clients dépendent du service commercial qui doit leur fournir des devis. Enfin, un dernier acteur est considéré : l'autorité réglementaire qui impose le respect des lois en vigueur. Cette dépendance est représentée par un *softgoal*, caractérisé (par opposition à un but) par une absence de critère clair de satisfaction, le respect des lois n'étant pas précisément défini à ce niveau et n'ayant donc pas de critère clair de satisfaction. Secure Tropos introduit enfin le concept de *contrainte de sécurité*. Une contrainte de sécurité est définie comme une restriction en lien avec la sécurité (comme la confidentialité, l'intégrité ou la disponibilité) qui va influencer l'analyse et le design du SI en construction. On retrouve plusieurs contraintes de sécurité pesant sur la société, comme le respect de la confidentialité des devis ou encore l'intégrité des calculs de structure.

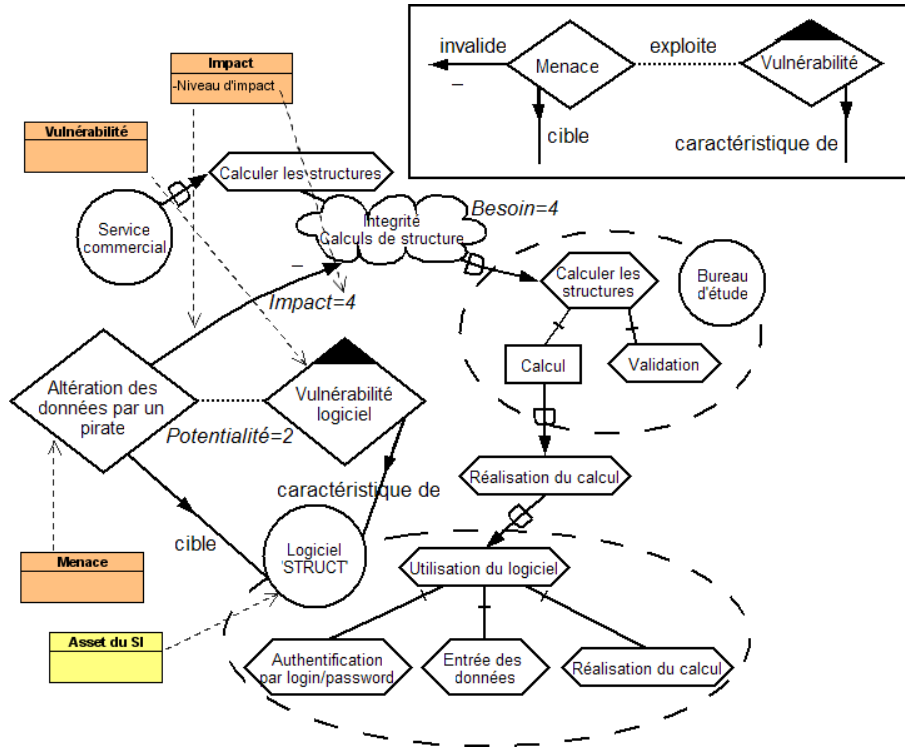


**Figure 11.** Modélisation des actifs business et des objectifs de sécurité associés

L'étape de détermination des objectifs de sécurité (étape (b) Figure 2) peut être supportée par Secure Tropos. L'ensemble des concepts de GRSSI nécessaire est représenté : asset business ainsi que critère de sécurité (Figure 11). Par exemple, les ressources, tâches et buts identifiés tels, respectivement, les visualisations, le calcul de structures et la gestion de projet, représentent des assets business. Sont identifiés ensuite les critères de sécurité qui s'appliquent, qui sont modélisés à l'aide des contraintes de sécurité du langage de Secure Tropos<sup>4</sup>. On remarque donc que l'étape

<sup>4</sup> Les exemples d'assets business et de contraintes de sécurité sont visualisés à l'aide de leur classe respective, pointant par des flèches pointillées sur les instances associées. Ils ne font

(b) du processus de GRSSI (Figure 2) est intégralement supportée par Secure Tropos.



**Figure 12.** Modélisation de l'analyse d'un risque

La Figure 12 est une vue que l'on peut obtenir lors du déroulement de l'étape d'analyse des risques (étape (c) Figure 2). Un zoom est effectué sur la tâche 'Calculer les structures' contrainte par le critère d'intégrité (Figure 11). On a ensuite représenté les assets au niveau du SI qui supportent cette tâche, ici par exemple le logiciel nommé 'STRUCT' et les activités réalisées au sein de cet acteur. Afin de supporter pleinement cette étape, de nouveaux éléments ont été ajoutés au langage Secure Tropos. On a introduit le concept de menace, représenté par un losange (ex : Altération des données) ainsi que le concept de vulnérabilité, représenté par un losange dont le coin supérieur est noirci (ex : Vulnérabilité logiciel). Conformément à notre modèle conceptuel de la GRSSI (Figure 4), la menace a pour cible un asset du SI (ex : le logiciel 'STRUCT') et la vulnérabilité est une caractéristique d'un asset

pas partie intégrante du modèle mais sont représentés à titre illustratif. Cette remarque s'applique également à la Figure 12.

du SI (ex : également le logiciel 'STRUCT'), ces relations étant symbolisées par des flèches dont la pointe est au milieu de l'arc. L'exploitation de la vulnérabilité par la menace est représentée à l'aide d'un trait pointillé. Enfin, l'impact, qui permet de composer le risque associé à la menace et la vulnérabilité sus-citée, est représenté par une contribution négative pointant sur la contrainte de sécurité concernée. Sont ici explicitées les attributs suivants du modèle conceptuel : le besoin de sécurité associé à l'objectif de sécurité formé par le critère de sécurité sur l'asset business concerné, la potentialité d'exploitation de la vulnérabilité par la menace, ainsi que le niveau d'impact qui en découle.

## 6. Conclusion

Au sein de cet article, nous avons présenté les résultats de nos travaux, visant à améliorer la GRSSI par l'utilisation d'un langage de modélisation, permettant à la fois une approche plus formelle et analytique de l'analyse de risques tout en permettant également le déroulement de cette analyse aussi bien a-posteriori sur un SI existant ou a-priori sur un système en construction. Pour aboutir à notre objectif de développement d'un langage de modélisation, nous avons identifié trois sous-objectifs. Nos deux premiers sous-objectifs ont été atteints : la définition d'un modèle du domaine de la GRSSI (Section 3) et l'intégration à ce dernier des métriques nécessaires à la GRSSI et à l'atteinte du meilleur ROSI (Section 4). Notre troisième sous-objectif de proposition d'extension d'un langage formel lié à la sécurité (Section 5) est actuellement partiellement complété. Nous avons proposé et illustré une proposition basée sur l'extension de Secure Tropos, mais celle-ci doit encore être améliorée et validée.

Les résultats obtenus offrent déjà un certain nombre de bénéfices. En relation avec les deux premiers sous-objectifs, l'alignement des différents concepts de la littérature, propres au domaine de la GRSSI, permet d'atteindre un premier niveau d'interopérabilité entre les différentes normes et méthodes. L'interopérabilité entre ces différents référentiels présente naturellement des avantages, autorisant l'utilisation de ces derniers de manière complémentaire. Notre action au niveau du modèle du domaine de la GRSSI constitue également un intérêt pour les travaux de normalisation de la sécurité des SI. Notre contribution a par exemple été utilisée pour des propositions d'amélioration de normes au niveau ISO, traitant de la terminologie de la GRSSI ainsi que des activités à réaliser lors d'une étude de GRSSI.

Notre objectif d'extension formelle d'un ou plusieurs langages de modélisation afin de supporter la GRSSI demeure aujourd'hui notre principal défi. Des études de cas et des expérimentations sont actuellement en cours. Elles se situent à la fois sur une utilisation du langage en support aux méthodes classiques de GRSSI (sur SI existant) et dans le cadre de construction de nouveaux SI. Le but de ces expérimentations est de profiter au plus tôt des retours d'expérience sur l'utilisation

de ce type de langage dans le domaine de la GRSSI. Nos travaux sont notamment expérimentés dans le cadre d'une démarche de préparation à la certification ISO/IEC 27001, visant à l'établissement et à la gestion d'un système de management de la sécurité de l'information.

Le travail présenté dans cet article couvre uniquement la partie de notre travail de recherche relatif à la définition d'un langage de modélisation. Une partie outillage est également en cours de développement, afin d'intégrer notre langage au sein d'un outil logiciel. Enfin, sur le plan méthodologique, plusieurs de nos résultats ont déjà été présentés (Dubois *et al.*, 2006 ; Mayer *et al.*, 2005) et, à ce niveau, notre recherche porte actuellement sur une formalisation de ces résultats à l'aide d'un cadre de formalisation basé sur les fragments de méthode (Mirbel *et al.*, 2005).

## 7. Bibliographie

- AICPA (ed.), *Summary of Sarbanes-Oxley Act*, 2002.
- Alberts C. J., Dorofee A. J., *Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE)*, Carnegie Mellon University - Software Engineering Institute, 1999.
- AS/NZS 4360, *Risk management*, SAI Global, 2004.
- Basel Committee on Banking Supervision, *International Convergence of Capital Measurement and Capital Standards. A Revised Framework*, Bank for International Settlements Press & Communications, CH-4002 Basel, Switzerland, 2002.
- Basili V. R., Caldiera G., Rombach H. D., « The Goal Question Metric Approach », *Encyclopedia of Software Engineering*, John Wiley & Sons, Inc., p. 538-532, 1994.
- BSI - Germany, *IT-Grundschutz Manual*, 2004.
- Club Sécurité des Systèmes d'Information de la région Rhône Alpes, « Point sur les méthodes », 2004. <http://www.clusir-rha.fr/>.
- CLUSIF, *MARION (Méthodologie d'Analyse des Risques Informatique et d'Optimisation par Niveau)*, 1998.
- CLUSIF, *MEHARI (Information risk analysis and management methodology) V3, Concepts and Mechanisms*, France, 2004.
- CLUSIF, Groupe de travail ROSI, « Retour sur investissement en sécurité des systèmes d'information : quelques clés pour argumenter », 2004.
- Common Criteria, *Common Criteria for Information Technology Security Evaluation version 3.1*, 2006.
- DCSSI, *EBIOS - Expression of Needs and Identification of Security Objectives*, France, 2004.
- Direction des Constructions Navales, *MELISA (Méthode d'Evaluation de la Vulnérabilité Résiduelle des Systèmes d'Information)*, 1989.

- Dubois E., Mayer N., Rifaut A., Rosener V., « Contributions méthodologiques pour l'amélioration de l'analyse des risques », in T. Ebrahimi, F. Leprévost, B. Warusfel (eds), *Enjeux de la sécurité multimédia (Traité IC2, série Informatique et systèmes d'information)*, Hermes, p. 79-131, 2006.
- ENISA, « Inventory of risk assessment and risk management methods », 2006.
- Firesmith D. G., Common Concepts Underlying Safety, Security, and Survivability Engineering, Technical note CMU/SEI-2003-TN-033, Software Engineering Institute, Pittsburgh, Pennsylvania, 2003.
- Haley C. B., Moffett J. D., Laney R., Nuseibeh B., « A Framework for Security Requirements Engineering », *Proceedings of the 2006 international workshop on Software engineering for secure systems*, ACM Press, New York, NY, USA, p. 35-42, 2006.
- Harel D., Rumpe B., « Meaningful Modeling : What's the Semantics of "Semantics" ? », *Computer*, vol. 37, n° 10, p. 64-72, 2004.
- Henderson J. C., Venkatraman N., « Strategic Alignment : Leveraging Information Technology for Transforming Organizations », *IBM Systems Journal*, vol. 32, n° 1, p. 4-16, 1993.
- Insight Consulting, *CRAMM (CCTA Risk Analysis and Management Method) User Guide version 5.0*, SIEMENS, 2003.
- ISACA, *CISA Review Manual 2006*, Information Systems Audit and Control Association, 2006.
- ISO 14001, *Environmental management systems - Requirements with guidance for use*, International Organisation for Standardisation, Geneva, 2004.
- ISO/IEC 13335-1, *Information technology - Security techniques - Management of information and communications technology security - Part 1 : Concepts and models for information and communications technology security management*, International Organisation for Standardisation, Geneva, 2004.
- ISO/IEC 17799, *Information technology - Security techniques - Code of Practice for Information Security Management*, International Organisation for Standardisation, Geneva, 2005.
- ISO/IEC 27001, *Information technology - Security techniques - Information security management systems - Requirements*, International Organisation for Standardisation, Geneva, 2005.
- ISO/IEC Guide 73, *Risk management - Vocabulary - Guidelines for use in standards*, International Organisation for Standardisation, Geneva, 2002.
- Le Moigne J.-L., *Les systèmes d'information dans les organisations*, Presses Universitaires de France, 1973.
- Lin L., Nuseibeh B., Ince D., Jackson M., « Using Abuse Frames to Bound the Scope of Security Problems », *Proceedings of the Twelfth IEEE International Conference on Requirements Engineering (RE'04)*, IEEE Computer Society, Washington, DC, USA, p. 354-355, 2004.

- Mayer N., Genon N., Design of a Modelling Language for Information System Security Risk Management – Elicitation of relationships between concepts and meta-model of each source, Technical report, University of Namur, 2006a.
- Mayer N., Heymans P., Matulevičius R., Design of a Modelling Language for Information System Security Risk Management, Technical report, University of Namur, 2006b.
- Mayer N., Heymans P., Matulevičius R., « Design of a Modelling Language for Information System Security Risk Management », in C. Rolland, O. Pastor, J.-L. Cavarero (eds), *Proceedings of the First International Conference on Research Challenges in Information Science (RCIS'07)*, Ouarzazate, Morocco, p. 121-132, 2007.
- Mayer N., Rifaut A., Dubois E., « Towards a Risk-Based Security Requirements Engineering Framework », *Proceedings of the Eleventh International Workshop on Requirements Engineering Foundations for Software Quality (REFSQ'05)*, IEEE Computer Society, Washington, DC, USA, p. 148-157, 2005.
- McDermott J., Fox C., « Using Abuse Case Models for Security Requirements Analysis », *Proceedings of the Fifteenth Annual Computer Security Applications Conference (ACSAC '99)*, IEEE Computer Society, Washington, DC, USA, p. 55, 1999.
- Mirbel I., Ralyté J., « Situational method engineering: combining assembly-based and roadmap-driven approaches », *Requir. Eng.*, vol. 11, n° 1, p. 58-78, 2005.
- Moffett J. D., Nuseibeh B., A Framework for Security Requirements Engineering, Technical report, Department of Computer Science, University of York, UK, 2003.
- Moody D., « Dealing with "Map Shock" : A Systematic Approach for Managing Complexity in Requirements Modelling », *Proceedings of the Twelfth International Workshop on Requirements Engineering Foundations for Software Quality (REFSQ'06)*, IEEE Computer Society, Washington, DC, USA, p. 148-157, 2006a.
- Moody D., « What Makes a Good Diagram ? Improving the Cognitive Effectiveness of Diagrams in IS Development », *Proceedings of the Fifteenth International Conference in Information Systems Development*, IEEE Computer Society, Washington, DC, USA, p. 148-157, 2006b.
- Mouratidis H., Giorgini P., « Enhancing Secure Tropos to effectively deal with security requirements in the development of multiagent systems », *Proceedings of the First International Workshop on Safety and Security Multiagent Systems*, AAMAS, 2004.
- Mouratidis H., Giorgini P., *Social Modeling for Requirements Engineering*, accepted for publication in MIT Press, chapter Extending i\* and Tropos to model security, 2007.
- Mouratidis H., Giorgini P., Manson G., Philp I., « A Natural Extension of Tropos Methodology for Modelling Security », *Proceedings of the Agent Oriented Methodologies Workshop (OOPSLA'02)*, 2002.
- Sindre G., Opdahl A. L., « Eliciting security requirements with misuse cases », *Requir. Eng.*, vol. 10, n° 1, p. 34-44, 2005.
- Stoneburner G., Goguen A., Feringa A., *NIST Special Publication 800-30 : Risk Management Guide for Information Technology Systems*, National Institute of Standards and Technology, Gaithersburg, 2002.

Stoneburner G., Hayden C., Feringa A., *NIST Special Publication 800-27 Rev. A : Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*, National Institute of Standards and Technology, Gaithersburg, 2004.

The Project Management Institute, *Project Management Body of Knowledge*, 2001.

van Lamsweerde A., « Elaborating Security Requirements by Construction of Intentional Anti-Models », *Proceedings of the 26th International Conference on Software Engineering (ICSE '04)*, IEEE Computer Society, Washington, DC, USA, p. 148-157, 2004.

Vraalsen F., Mahler T., Lund M. S., Hogganvik I., den Braber F., Stølen K., « Assessing enterprise risk level : The CORAS approach », in D. Khadraoui, F. Herrmann (eds), accepted in *Advances in Enterprise Information Technology Security*, Idea group, 2007.

Warmer J., Kleppe A., *The Object Constraint Language : Getting Your Models Ready for MDA*, Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 2003.