Processus guidé pour l'identification des exigences de sécurité à partir de l'analyse des risques

Nabil Laoufi

le cnam

École Doctorale d'Informatique, Télécommunications et Electronique
Centre d'étude et de recherche en informatique et communications

THÈSE présentée par :

Nabil LAOUFI

soutenue le : **20 Mars 2017**

pour obtenir le grade de : **Docteur du Conservatoire National des Arts et Métiers**

Discipline/ Spécialité : **Informatique**

Processus guidé pour l'identification des exigences de sécurité à partir de l'analyse des risques

THÈSE dirigée par :
M. Jacky AKOKA Professeur émérite, CNAM
Mme. Nadira LAMMARI Maître de conférences-HDR, CNAM

RAPPORTEURS :
M. Frédéric CUPPENS Professeur, Télécom Bretagne
Mme. Zoubida KEDAD Maître de conférences-HDR, UVSQ

JURY :
Mme. Isabelle COMYN-WATTIAU, président du jury Professeur, ESSEC
Mme. Régine LALEAU Professeur, Univérsité Paris-EST
M. Manuel MUNIER Maître de conférences, UPPA

Allah عزوجل dit :

تَبَارَكَ الَّذِي نَزَّلَ الْفُرْقَانَ عَلَى عَبْدِهِ لِيَكُونَ لِلْعَالَمِينَ نَذِيرًا

{ Gloire à celui qui a révélé la Distinction à son serviteur pour qu'il

avertisse l'humanité }

[Sourate 25 - Le discernement - Al Furqane - Verset 1]

Remerciements

Ce travail de thèse m'a permis de rencontrer des personnalités formidables et enthousiasmantes de par leurs qualités humaines, leur disponibilité et leurs compétences.

Je tiens à remercier en premier lieu mes directeurs de thèse le professeur émérite Jacky AKOKA et la Maître de conferences-HDR Nadira Ilham LAMMARI pour leur encadrement et soutien tout au long de ces années. Je suis reconnaissant pour leur disponibilités et leur qualité pédagogique et scientifique. Ses remarques et critiques pertinentes m'ont conduit vers la bonne voie.

Je remercie profondément Madame Zoubida KEDAD, Maître de conferences-HDR, UVSQ et Monsieur Frédéric CUPPENS, Professeur, Télécom Bretagne qui m'ont honoré en acceptant d'être les rapporteurs de cette thèse. Les questionnements et les judicieux conseils qu'ils m'ont prodigués m'ont permis de clarifier et d'améliorer certaines parties décrites dans ce manuscrit.

Toute ma gratitude à toute personne ayant relu, corrigé et commenté mon manuscrit et ayant ainsi participé à son amélioration.

Je tiens à présenter mes remerciements les plus chaleureux à mon père LAOUFI Tayeb qui a été un grand support pour moi et de m'avoir appris à persévérer davantage durant toute la période du changement de mon statut. En particulier, je lui dois beaucoup pour avoir pris soin de relire mes chapitres de thèse et mes articles pour éliminer toutes les coquilles qui persistaient, ce qui est une contribution très importante à la qualité de ce manuscrit.

Enfin, je ne saurais terminer cette liste sans remercier mon épouse BOUZIANE Sabrina qui a cru en moi et qui m'a soutenu tout au long de ce travail ainsi que mes enfants YANIS et WASSIM.

Résumé

Toute organisation est activée par un flux physique continu et un flux décisionnel qui opèrent de symbiose pour atteindre des objectifs déterminés. Ce qui engendre l'implantation d'un système d'information fiable, opérant avec un contrôle continu et une sécurité maximale, prenant en compte le contexte interne et externe pour garder son rôle opérationnel et stratégique. Compte tenu du niveau d'exposition aux risques et de la dépendance vitale des entreprises vis-à-vis de leurs systèmes d'information, il est crucial de prêter attention aux exigences de sécurité. La réalisation d'un équilibre entre la sécurité et l'efficacité du système d'information est une tâche complexe qui exige au préalable une analyse approfondie du contexte organisationnel. Elle nécessite également l'identification, l'analyse, et la gestion des risques encourus par l'entreprise. Elle nécessite aussi la détermination des exigences de sécurité. Peu d'approches offrent un guidage permettant de dériver les exigences de sécurité à partir des risques encourus. Le but de cette thèse est de concevoir un mécanisme de guidage suggestif qui permet de dériver les exigences de sécurité à partir de l'analyse des risques. Nous proposons, pour cela, une approche fondée sur les ontologies et un ensemble de règles de correspondance. A cette fin, nous proposons le développement de quatre ontologies et un processus d'alignement entre celles-ci en utilisant des relations sémantiques cohérentes. Le processus de validation se fonde sur une étude de cas et un prototype.

Mots clés

Actifs, Contexte, Risques, Menaces, Vulnérabilités, Traitements de risques, Exigences de sécurité, Analyse des risques, Règles de correspondance, Ontologies.

Abstract

Any organization is enabled by continuous physical flow and decision flow from operating symbiosis to achieve specific objectives. Which generates the implementation of a reliable information system, operating with a continuous control and maximum security, taking in to account the internal and external environment to maintain its operational and strategic role. Given the level of risk exposure and the vital dependence of companies on their information systems, it is crucial to pay attention to security requirements. Achieving a balance between the security and effectiveness of the information system is a complex task requiring an in-depth analysis of the organizational context. It also requires the identification, analysis, and management of the risks incurred by the company. It also requires the determination of security requirements. Few approaches offer guidance to derive security requirements from the risks involved. The aim of this thesis is to design a suggestive guiding mechanism that allows to derive the security requirements from the risk analysis. We propose an approach based on ontologies and a set of correspondence rules. To achieve, we propose the development of four ontologies and an alignment process between then using consistent semantic relationships. The validation process is based on a case study and a prototype.

Keywords

Assets, Contexts, Risks, Threats, Vulnerabilities, Risks treatments, Security requirements, Risks analysis, Correspondance rules, Ontologies.

Table des matières

Chapitre III

Chapitre IV

Chapitre V

Publications et bibliographie

Annexes

Liste des figures

Liste des tableaux

Chapitre I
Introduction générale

I. Introduction générale

Dans tout projet de conception d'un système d'information, le processus de développement d'applications commence par une première étape fondamentale qui est la spécification des exigences. Les solutions proposées dans ce domaine divisent les exigences logicielles en deux familles : les exigences fonctionnelles et les exigences non fonctionnelles (Glinz, 2005). Si les exigences fonctionnelles décrivent les fonctions que l'application doit accomplir, les exigences non fonctionnelles se concentrent sur la manière dont ses fonctions sont exécutées. La sécurité est considérée comme une exigence non fonctionnelle.

Ces dernières années, l'expansion des réseaux d'une part et l'importance d'autre part de l'information, ont fortement contribué à ce que les exigences de sécurité jouent un rôle clé dans le développement d'applications ainsi que dans l'amélioration de la fiabilité des processus métiers (Firesmith, 2003b). Cependant, les exigences de sécurité ont pendant longtemps été reléguées à la deuxième place comparativement aux exigences fonctionnelles (Matoussi et Laleau, 2008). Dans le même temps, les organisations sont sujettes à de nombreuses attaques. Le bilan a de quoi inquiéter les entrepreneurs. Selon une étude du cabinet de conseil Pricewaterhouse Coopers (PwC) publiée en octobre 2015, le nombre des attaques informatiques contre des sociétés a augmenté de 38% dans le monde en douze mois. La France est plus particulièrement touchée puisque le nombre de ces attaques y a progressé de 51% en un an, avec 21 incidents par jour (Figure **1**).

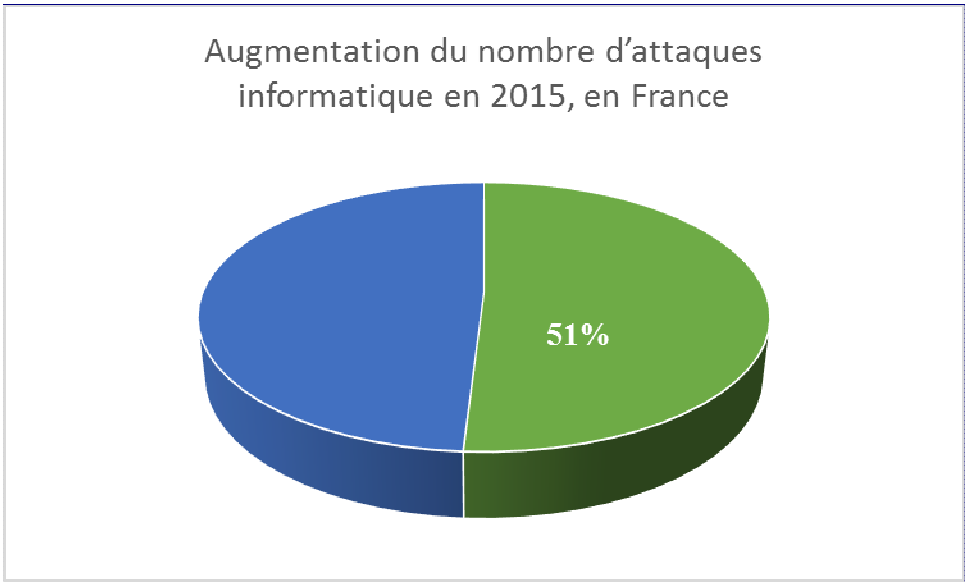


Figure 1 : Le pourcentage d'augmentation du nombre d'attaques informatique en 2015, en France (source www.PwC.com)

L'estimation des pertes financières imputables à ces incidents a bondi de 28%, soit 3,7 millions d'euros par entreprise en moyenne, selon la même étude. Les exemples des attaques informatiques de la firme Sony en 2014 aux États-Unis d'Amérique où ceux sur le site de Canal Plus en mars 2016 en France démontrent l'augmentation du nombre d'attaques informatiques. Ils montrent aussi que ces incidents proviennent de différentes sources (Figure **2**).

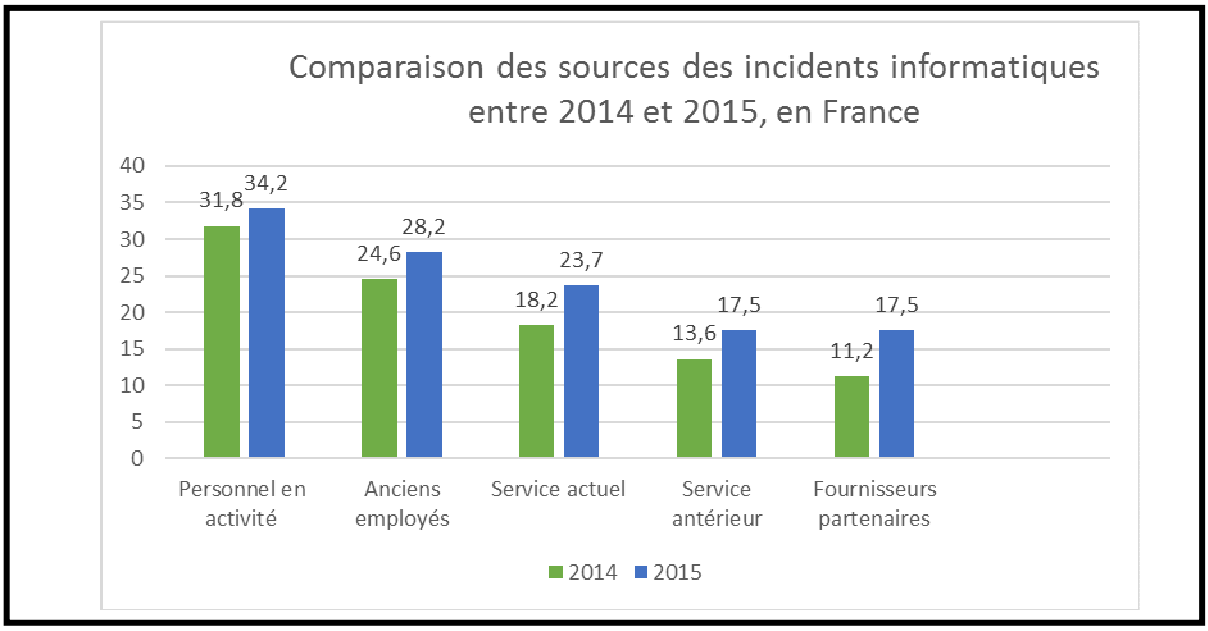


Figure 2 : Comparaison des sources des incidents informatiques entre 2014 et 2015, en France (source www.PwC.com)

En outre, la dépendance croissante des entreprises vis-à-vis de leur système d'information affaiblit leurs processus métiers. Ce qui génère des exigences de sécurité supplémentaires avec une adaptation spécifique à leurs besoins, et une recherche poussée permettant de veiller à la compatibilité avec l'existant, sur tous les plans.
À cet effet, l'ingénierie des exigences de sécurité préoccupe depuis longtemps la communauté des chercheurs et suscite un intérêt particulier en raison des pertes causées par des applications mal sécurisées ou du fait que la sécurité n'était pas intégrée dès le début du cycle de développement ou au motif qu'elle était mal spécifiée.

Selon (Van Lamsweerde,2004), il y a trois raisons qui expliquent ce fait. Tout d'abord, les premières phases du développement des logiciels donnent la priorité à l'élaboration des exigences fonctionnelles au détriment des actifs et des exigences non-fonctionnelles telle que la sécurité en vue d'obtenir un produit qui fonctionne en un court laps de temps. La deuxième raison est l'absence d'un mécanisme constructif et efficace pour l'élaboration d'exigences de sécurité d'une manière complète, cohérente et claire. La troisième raison est l'absence d'une approche précise et bien définie qui permet de produire la conception et l'implémentation des exigences de sécurité tout en assurant une prise en charge correcte de toutes les exigences et en permettant une traçabilité des exigences lors des différentes phases de développement.

Les systèmes d'information (SI) actuels doivent faire face à de nombreuses menaces susceptibles d'exploiter les vulnérabilités des actifs, les menaces sont dues soit à des méthodes d'attaques ou à des agents menaçants de violer les critères de sécurité. Les conséquences sont parfois fatales à l'organisation, mais dans tous les cas des séquelles seront visibles à court et longs termes.

Afin de limiter les impacts résultant des vulnérabilités des actifs, une politique de traitement des risques doit être mise en place, ou chaque exigence de sécurité contribue à couvrir un ou plusieurs traitements du risque ciblant le système d'information. (Figure **3**).

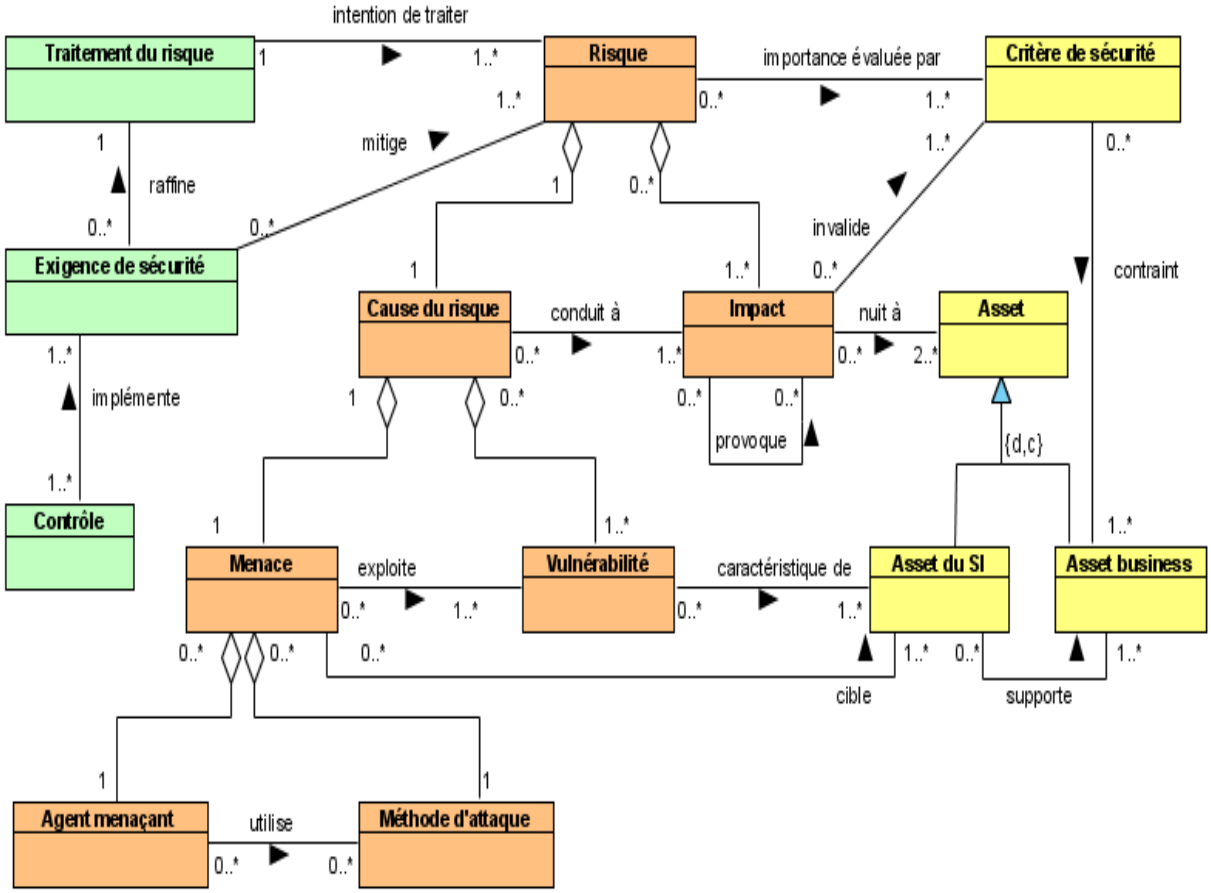


Figure 3 : Gestion des risques des systèmes d'information (Mayer, 2009).

Ces exigences de sécurité sont définies et actualisées dans le cadre d'une gestion des risques visant à améliorer la sécurisation des SI. Cette dernière est le processus par lequel les organisations identifient, analysent, traitent et contrôlent méthodiquement les risques attachés à leurs activités.
Pour de nombreuses raisons, telles que les contraintes imposées par les contrats d'assurance, les entreprises effectuent une sorte d'analyse des risques. Elles essayent d'intégrer la sécurité au sein de leurs systèmes ; mais presque toujours, elles commencent par l'identification des besoins de sécurité après la conception de l'application. Cette antériorité pose un problème de cohérence et de cohabitation entre les exigences fonctionnelles et les exigences de sécurité.
Cependant, les résultats obtenus ne sont généralement pas capitalisés sur cet effort pour développer un ensemble d'exigences de sécurité des systèmes d'information. Par conséquent, les limites actuelles dans ce domaine résultent principalement de cette incapacité à déduire clairement les exigences de sécurité à partir de l'analyse des risques. Les solutions actuelles définissent un ensemble standard d'exigences de sécurité qui ne sont généralement pas adaptées aux caractéristiques spécifiques de l'entreprise. De ce fait, elles sont très coûteuses en matière de mise en place et de mises à jour.

De ce qui précède, nous constatons que les limites actuelles de la gestion de la sécurité ne sont pas que technologiques. Ces limites résultent en partie d'une incapacité à expliciter la relation entre l'expression des exigences de sécurité et les résultats de l'analyse de risques (Vasquez, 2012). C'est dans ce cadre bien précis que s'inscrit la problématique de cette thèse.
Les recherches actuelles sur la dérivation des exigences de sécurité à partir de l'analyse de risque peuvent être enrichies en utilisant une représentation de haut niveau du domaine de la

sécurité. Les ontologies sont un outil pour parvenir à une telle représentation du fait de la possibilité du partage d'informations, de la réutilisation des connaissances du domaine et de la facilitation de la communication (Khelifa, 2014).
La littérature contient de nombreuses contributions sur l'élicitation des exigences de sécurité des systèmes d'information, mais la plupart ne sont pas liées au contexte de l'entreprise et ne proposent pas un guidage suggestif à l'utilisateur. En se basant sur ce générique de connaissances, nous évitons de partir de zéro dans la recherche de notre solution.

Le but de cette thèse est de proposer une approche guidée pour la dérivation des exigences de sécurité à partir de l'analyse des risques. Notre proposition repose sur l'utilisation de quatre ontologies où le contexte de l'entreprise, ses actifs, les risques encourus et les exigences de sécurité sont représentés. Pour construire ces ontologies et les règles de correspondance entre elles, nous avons eu recours à des sources d'information provenant du monde académique et du monde industriel.

À cette fin, nous avons passé en revue un très large éventail de normes et de standards de sécurité ainsi que les méthodes liées à l'analyse des risques. Nous avons également analysé les méthodes conduisant à la détermination des exigences en matière de sécurité afin d'en extraire les principaux concepts et les relations sémantiques de ce domaine de connaissance. Ces éléments peuplent les ontologies qui constituent les principales composantes de notre démarche d'accompagnement. Il existe différentes approches pour déterminer les types d'exigences de sécurité. Soit ils font apparaître les objectifs de sécurité à partir des buts fonctionnels, soit ils définissent les objectifs en utilisant les critères suivants : la disponibilité, l'intégrité, la confidentialité (DIC). Cette vision est plus précise. Dans ce travail, nous allons suivre la deuxième approche pour déterminer des exigences de sécurité, mais en rajoutant le critère de traçabilité de manière à répondre aux exigences réglementaires.

I.1 Contributions principales

Les contributions de notre thèse peuvent être résumées comme suit :

1. Uniformisation du vocabulaire utilisé dans le domaine, permettant une exploitation rationnelle avec le même langage par tous les concernés,
2. Construction d'une ontologie du contexte à partir de la norme ISO/CEI 27000 : 2016,
3. Construction d'une ontologie des actifs à partir des normes, standards, référentiels, méthodes d'analyse des risques et des méthodes de sécurité.
4. Mise en œuvre d'un filtrage pour l'extraction d'informations sous forme de langage naturel en exploitant les connaissances qui peuplent les ontologies des actifs et du contexte ,
5. Constitution d'une liste de scénarios de risques possibles pour un SI à partir de notre état de l'art principal,
6. Formalisation d'un scénario de risque,
7. Construction d'une ontologie des risques à partir de l'existant et l'enrichissement à partir des méthodes d'analyse de risques,
8. Mise en œuvre des fiches de caractérisation des concepts de l'ontologie des risques,
9. Extraction des règles de correspondance à partir des bases de connaissances,
10. Construction d'une ontologie des exigences de sécurité à partir de l'existant et l'enrichissement à partir des méthodes d'élicitation des exigences de sécurité,

11. Modélisation du méta modèle de sécurité,
12. Mise en œuvre et la validation de l'approche.

I.2 Organisation du mémoire

L'organisation du mémoire est structurée en deux grandes parties.

La première partie est principalement dédiée à l'état de l'art (chapitre **II**) qui présente et compare les méthodes d'analyse de risque. Ce chapitre dresse aussi un état des lieux de la recherche et présente les normes et les standards dans le domaine de la sécurité des systèmes d'information. Les différentes approches sont comparées en se basant sur des critères d'évaluation que nous avons définis. Ces comparaisons nous ont permis de dégager les limites des modèles et approches existants et d'introduire nos contributions dans ce domaine.

La seconde partie est entièrement consacrée à la description de nos contributions. Elle est composée de deux chapitres. Cette partie débute par le chapitre **III**, consacré à l'approche de la dérivation des exigences de sécurité à partir de l'analyse de risques. Nous présentons notre processus de dérivation des exigences de sécurité, nous expliquons en quoi notre approche est différente des autres approches, nous présentons notre méta modèle de sécurité. Aussi nous présentons le détail de notre approche en présentant la conception détaillée des ontologies d'une part, et expliqué les démarches que nous avons suivies pour étayer notre proposition d'autre part. Le chapitre présente aussi le méta modèle de sécurité. Le chapitre suivant (chapitre **IV**) détaille la mise en œuvre et la validation de notre approche par des calculs des relations taxonomiques et le déroulement des exemples ainsi que l'étude du cas réel d'une structure complète.

La conclusion constitue le chapitre final (chapitre **V**) de cette thèse. Cette partie résume nos contributions et propose un ensemble de perspectives.

Chapitre II
Etat de l’art

II. Etat de l'art

Il est important de commencer par clarifier les définitions des principaux concepts liés à l'analyse des risques et des exigences de sécurité. C'est l'objet du paragraphe II.1. Nous présentons ensuite au paragraphe suivant un état de l'art qui permet de capitaliser sur le savoir et les savoir-faire pratiqués dans ce domaine, en se concentrant respectivement sur les normes, les standards de sécurité, les méthodes d'analyse des risques et les méthodologies d'élicitation des exigences de sécurité.

II.1 Définitions

Les définitions des concepts du domaine sont très importantes. Nous avons constaté qu'au fur et à mesure que nous avancions dans l'étude de notre état de l'art que les définitions proposées ne sont pas homogènes, ni standardisées. C'est ainsi que, nous avons extrait des caractérisations afin de les synthétiser pour déceler les divergences et les points communs, ce qui nous permet de proposer une seule définition standard référencée dans notre démarche et qui répond parfaitement au domaine concerné.

II.1.1 Terminologies primordiales

a. Contexte

Bien que le mot « contexte » apparaisse à foison dans l'univers de l'informatique, il ne fait pas l'objet d'une définition unanime. Cela est parfaitement compréhensible étant donné qu'il n'existe pas un contexte déterminé par avance. C'est la raison pour laquelle les définitions du contexte sont nombreuses. Parmi elles, on peut citer (GERAM, 1999) : « le contexte dépend des conditions interdépendantes dans lesquelles un événement, une action, etc. a lieu ».
Dans la littérature, la définition la plus usitée est due à (Dey and Abowd, 1999) : « le contexte représente toute information qui peut être utilisée pour caractériser la situation d'une entité. Une entité est une personne, un objet ou un endroit considéré comme pertinent pour l'interaction entre un utilisateur et une application, y compris l'application et l'utilisateur ». En d'autres termes, le contexte peut être décrit comme étant constitué d'un ensemble d'attributs ayant un lien avec une finalité pour laquelle le contexte est utilisé.
Pour les linguistes et les chercheurs en langage naturel, le contexte a été utilisé pour interpréter le sens des phrases. Par exemple, si nous disons : « Je tiens à jouer avec ma sœur », il est supposé que ma sœur et moi jouons ensemble et non qu'elle est un jouet. Autrement dit, le contexte social rétrécit l'interprétation correcte d'une expression (Leech, 1981).
Il est clair que le contexte peut servir à limiter l'espace de la solution pour des problèmes liés au raisonnement automatique (Brézillon and Abu-Hakima, 1995) ou lorsqu'il y a d'énormes quantités de données. À titre d'exemple, les systèmes de recherche Web filtrent l'information en estimant sa pertinence dans des contextes déterminés d'interprétation, telle que la popularité des pages (Yahoo, Google), les catégories (recherches), les zones géographiques (Algérie), etc.….
En général, dans le domaine de l'informatique, le contexte est généralement lié aux conditions dans lesquelles les utilisateurs sont immergés (poste de travail, réseau, communication, bande passante, sécurité).
Pour la sécurité des informations, le contexte joue un rôle primordial, qu'il soit un contexte interne ou un contexte externe. Le risque et les mesures de protection changent d'après le

contexte. Exemple : on ne protège pas un serveur de banque comme un simple serveur de messagerie d'une petite entreprise de textile.

b. Actifs [1]

Pour ce concept, l'unanimité de notre état de l'art donne la même définition qui se résume ainsi : « tout élément représentant de la valeur pour l'organisme » (ISO guide 73, 2009). En d'autres termes, toute ressource qu'elle soit une personne, groupe, relation, bâtiment ou instrument à la disposition de l'entreprise ou de l'organisation pour une utilisation dans un rôle opérationnel ou de soutien (Glossary of security, 2012).

c. La gestion des risques

La gestion des risques correspond aux activités coordonnées permettant d'orienter et de contrôler un organisme en matière de risque (ISO/CEI 27000, 2016). C'est donc le processus par lequel les organisations identifient, analysent et traitent les risques, quelles que soient leurs natures ou leur origine, mais aussi pour contrôler la probabilité des événements redoutés et réduire au minimum l'impact éventuel de ces événements. Dans ce cas de figure, la gestion des risques 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 (Mayer et al, 2008).

d. Risques

La norme ISO définit le risque dans les termes suivants : « L'effet de l'incertitude sur l'atteinte des objectifs » (ISO/CEI Guide 73, 2009). Le risque est souvent caractérisé par référence à des événements et à des conséquences potentielles, ou une combinaison de ceux-ci. Il peut être quantifié en tenant compte des trois éléments : la menace, la vulnérabilité et l'impact.
Une menace peut avoir plusieurs sources, c'est la cause potentielle d'incident, qui peut résulter en un dommage au système ou à l'organisation (ISO/CEI 27002, 2013). Une menace exploite une vulnérabilité pour déclencher un événement d'attaque entraînant un risque. La vulnérabilité correspond à une faiblesse du système. L'impact est la conséquence directe ou indirecte de l'insatisfaction des besoins de sécurité sur l'organisme et/ou sur son environnement (EBIOS, 2010).

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

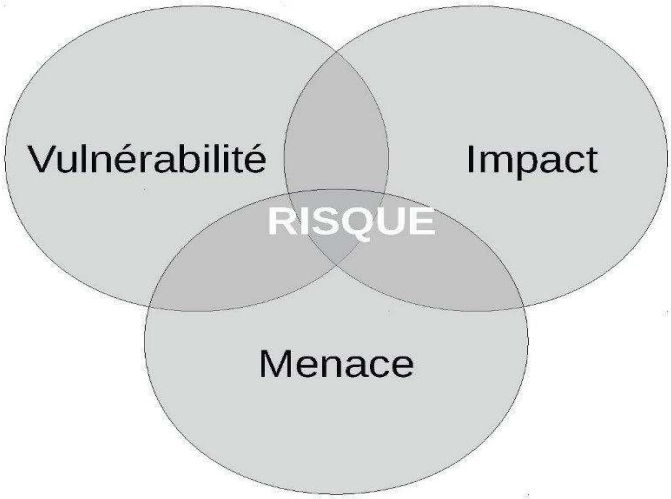


Figure 4 : Représentation du risque

Les trois concepts cités supra dans la figure 4 peuvent modifier les critères de sécurité, qui sont :

- **L'intégrité** : ce principe est de veiller à la sauvegarde de l'exactitude et l'exhaustivité de l'information et de la façon dont il est traité (ISO/CEI 27000, 2016).
- **La confidentialité** : cette condition est de veiller à ce que les informations ne soient pas divulguées ou communiquées à des personnes ou entités qui ne possédent pas les autorisations appropriées (ISO/CEI 27000, 2016).
- **La disponibilité** : cette notion est la propriété d'être accessible et utilisable sur demande par une entité autorisée (ISO/CEI 27000, 2016).
- **La traçabilité** : cette notion c'est l'assurance que les éléments considérés sont tracés et que ces traces sont conservées pour leur exploitation par les personnes autorisées.

e. Traitements des risques

Le traitement du risque est un processus de sélection et de mise en œuvre des mesures de sécurité visant à modifier le risque. Les différents traitements du risque sont :

1- **Optimisation (réduire)** : action de diminution de la probabilité, de la conséquence et d'impact qui sont associés à un risque.
2- **Prévention** : vise à prévenir l'apparition des risques en utilisant certaines mesures. Les mesures de prévention comprennent la prévention intrinsèque, l'utilisation de dispositifs de protection, d'équipements de protection individuelle, l'information pour l'utilisation et l'installation ainsi que la formation.
3- **Vivre avec (tolérable)** : c'est l'acceptation de la charge d'une perte, ou du bénéfice d'un gain ou d'un risque particulier. C'est le risque accepté dans un certain contexte et fondé sur les valeurs admises par la société.
4- **Partage (transfert)** : partage avec une autre partie du fardeau de la perte, ou le bénéfice du gain ou d'un risque particulier (Asnar, 2006).
5- **Éviter** : décision de ne pas être impliqué ou de se soustraire à un risque. C'est une décision visant à ne pas être impliquée dans une situation à risques, ou à se retirer d'une situation à risques. (ISO/CEI 17799, 2005)

f. Exigences de sécurité

Les exigences de sécurité sont des contraintes sur les systèmes de sorte que chaque contrainte met en œuvre la satisfaction d'une ou plusieurs exigences de sécurité (NIST 800-53, 2015). Une exigence est une « condition ou capacité qui doit être remplie ou possédée par un système ou un de ces composants pour satisfaire à un contrat, une norme, une spécification ou tout document imposé de façon formelle » (Kassou, 2012).
Une exigence formalisée doit être :

- Abstraite, elle est alors indépendante de la méthode de mise en œuvre ;
- Non ambiguë, elle est énoncée de manière à n'être interprétable que d'une seule manière ;
- Traçable, il est possible d'établir une relation entre la déclaration précise des besoins du client et les énoncés spécifiques de la définition du système ;
- Vérifiable, elle doit offrir un moyen de prouver que le système satisfait à son énoncé.

Une exigence formalisée est, en fait, le résultat du processus d'ingénierie des exigences qui est la première étape importante dans le développement d'une application. Ce processus inclut plusieurs phases dont le découpage diffère selon plusieurs définitions (Nuseibeh et Easterbrook, 2000), (Kotonya et Sommerville, 1998). Cependant, typiquement un processus d'ingénierie d'exigences est un processus itératif qui est constitué des phases d'élicitation, d'analyse, de spécification, de validation et de gestion. L'élicitation des exigences consiste en la collecte et le développement d'exigences à partir d'une variété de sources et des parties prenantes. Ces dernières peuvent être une personne ou un organisme qui peut affecter, être affecté par, où se percevoir d'être affecté par une décision ou une activité (ISO/CEI Guide 73, 2009).

g. Guidage :

Le guidage a pour but de fournit des conseils à un utilisateur et comprend un soutien dans la prise de décision, l'objectif du guidage est d'éclairer, de clarifier et de diriger les utilisateurs en utilisant l'expertise extraite des sources d'information (Silver, 1991)

Le guidage se base sur trois axes (Morana and al, 2014), qui sont :

- Les conseils décisionnels, décrivant comment soutenir les utilisateurs dans l'utilisation d'un système d'information.

- Les explications, orientent et soutiennent les utilisateurs dans l'utilisation des systèmes et dans la compréhension des résultats du système.

- Les aides à la décision soutiennent les utilisateurs dans leur processus décisionnel.

Dans les sections qui suivent, nous présentons les définitions primordiales du domaine de notre recherche et également les différentes sources d'information recensées qui nous permettent de constituer notre état de l'art.

II.2 Analyse des risques : normes, standards, référentiels et méthodologies

Il existe une grande diversité de sources qui sont orientées vers la sécurisation des systèmes d'information. Nous proposons un système de classification fondé sur notre thématique qui se résume à la dérivation des exigences de sécurité à partir de l'analyse de risque. Nous faisons la distinction entre les normes, les standards, les référentiels et les méthodologies d'analyse de risque.

Les standards de sécurité sont conçus pour fournir un environnement général permettant l'établissement et le maintien d'une politique de sécurité qui répond aux objectifs en matière de sécurité des organisations. Ils peuvent être considérés comme une prescription de bas niveau décrivant les moyens d'être utilisés par les utilisateurs pour appliquer leur politique de sécurité informatique. Dans la plupart des cas, les standards de sécurité sont mis en place par les gouvernements pour assurer un niveau de sécurité adéquat à leurs administrations.
Les normes jouent le même rôle que les standards, mais elles sont principalement orientées vers la certification. Elles sont établies par des organismes internationaux, non gouvernementaux.
Les référentiels servent à créer les fondations ainsi que les grandes lignes de toute ou d'une partie des meilleures pratiques de gestion des risques.
Enfin, **les méthodes** définissent le processus d'analyse des risques. Le processus décrit les étapes de mise en œuvre des différentes normes et standards de sécurité. Le résultat de cette classification est présenté ci-après :

- **Standards**: AS/NZS 4360, NIST 800-39, BS7799, IT Grundschutz, SS627799-2;
- **Normes**: ISO/ CEI 2700X, ISO/ CEI 13335, ISO/ CEI 31000, ISO/ CEI Guide 73:2009, ISO/ CEI 15408 ;
- **Référentiels**: COBIT5, ITIL, Risk IT;
- **Méthodologies**: EBIOS, MEHARI, OCTAVE, CRAMM, ISAMM, RMF, FTA, FMECA, HAZOP, MAGERIT, CORAS, FRAP, SRA, TARA, NIST, FAIR.

Nous décrivons ci-dessous des exemples de standards, normes, référenrtiels et méthodologies.

II.2.1 Les standards de sécurité

Les standards de sécurité jouent un rôle important dans l'analyse et la gestion des risques informatiques par leur apport dans le domaine.
Nous proposons dans cet état de l'art un aperçu des standards de sécurité les plus importants mentionnés dans la littérature spécialisée :

AS/NZS 4360 (Risk management, 2004), est un standard fournissant un guide générique pour la gestion des risques, établi en 1995, et révisé en 2004. Il a depuis été incorporé dans la norme internationale ISO/CEI 31000 : 2009 - Principes et lignes directrices.
Ce standard fournit un guide générique pour le processus de gestion des risques. Cela lui permet d'être applicable à une large gamme de systèmes, organisations et activités. Il est particulièrement utile lorsqu'il est utilisé non seulement pour la gestion des risques mais aussi comme une approche de sécurité de l'entreprise.
Il possède une structure générique pour le processus de gestion des risques qui divise les éléments du processus d'évaluation des risques en plusieurs sous-processus : "établir le

contexte ", "identifier les risques ", " analyser les risques ", "évaluer les risques" et "traiter les risques". Il dispose également de deux processus qui devraient fonctionner en parallèle avec la gestion du risque : "Suivi et examen" et "communication et consultation". Un organigramme décrivant ce procédé est présenté ci-dessous (Figure 5).

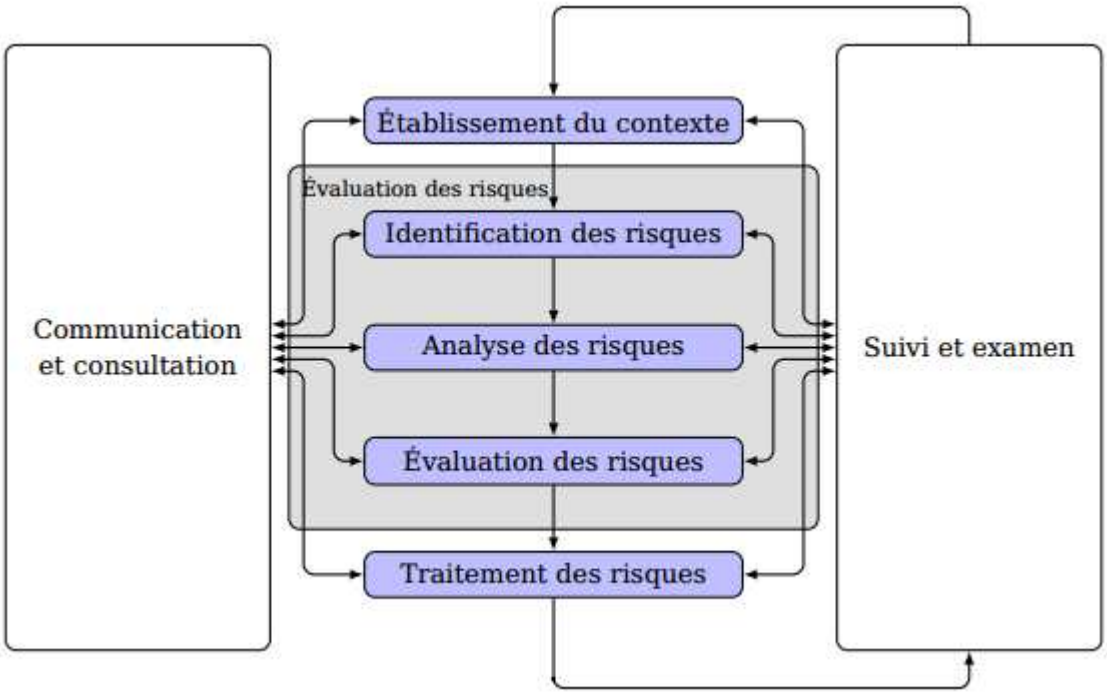


Figure 5 : Le processus de gestion des risques AS / NZS 4360 (Risk management, 2004).

BS7799 (BS7799, 2002) est un standard britannique composé des meilleures pratiques pour la gestion de la sécurité de l'information. Il offre une couverture détaillée et structurée des questions de sécurité. Ces trois parties principales sont intégrées respectivement dans les normes ISO/CEI 27001 : 2013 et ISO/CEI 27002 :2013 (Voir chapitre **II.2.2**).
La première partie, BS7799-1, contient les bonnes pratiques pour la gestion de la sécurité de l'information. Celle-ci a été adoptée par l'ISO comme ISO/CEI 17799, "Technologies de l'information - Code de pratique pour la gestion de la sécurité de l'information." en 2000. La norme ISO/CEI 17799 a ensuite été révisée en juin 2005 et a finalement été incorporée dans la série ISO 2700X.
La deuxième partie de BS7799, connue sous l'appellation BS 7799-2, est intitulée « Informations sur la sécurité des systèmes de gestion » - Spécifications et lignes directrices pour l'utilisation. Elle est axée sur la façon de mettre en œuvre un système de gestion de la sécurité de l'information en se référant à la structure de l'information de sécurité et aux contrôles identifiés. BS 7799-2 devient la norme ISO/ CEI 27001 en novembre 2005. Ce standard, présenté dans la figure 6, propose un processus en six étapes et qui se résument ainsi :

Étape 1 : Définir les informations de la politique de sécurité,
Étape 2 : Définir les champs du système de management de la sécurité de l'information (SMSI),
Étape 3 : Effectuer une évaluation des risques,
Étape 4 : Gérer le risque,

Étape 5 : Sélectionner les objectifs de contrôle et les contrôles,
Étape 6 : Déclarer l'applicabilité.

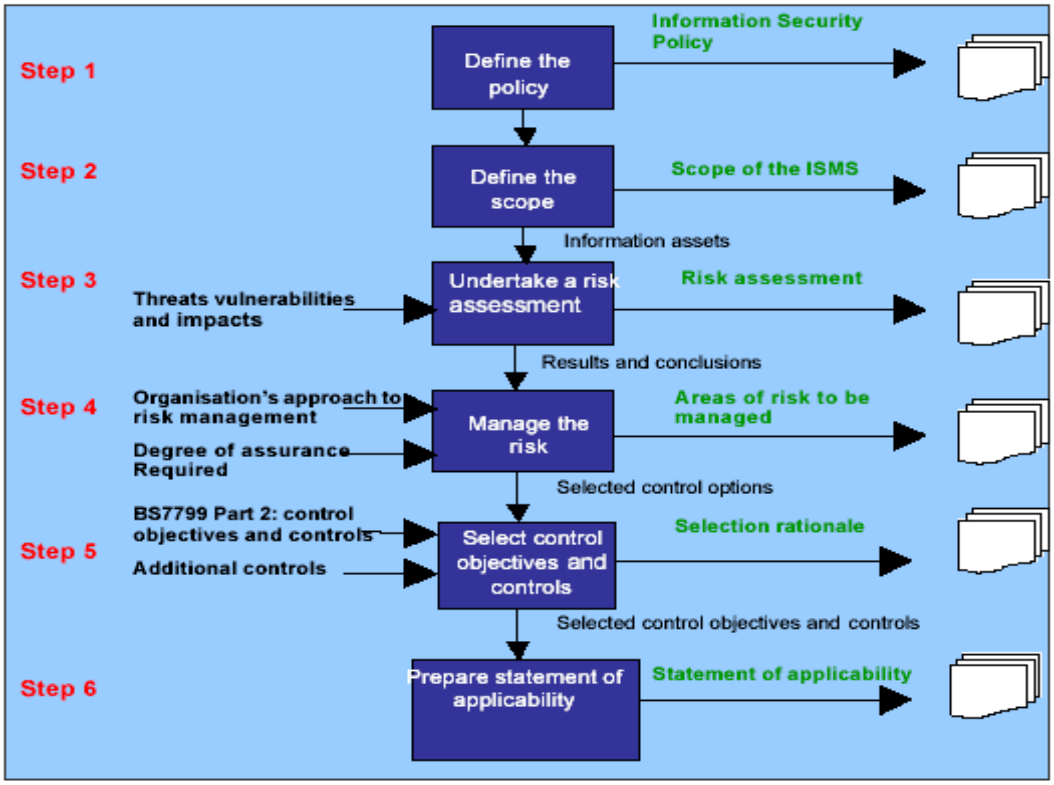


Figure 6 : Processus BS7799-2 (BS7799, 2002).

La version de BS 7799-2 2002 a présenté le Plan-Do-Check-Act (PDCA)[2]. Elle est alignée sur les normes de qualité, comme celles qui sont référencées dans ISO 9000.

Le standard BS7799, partie 3, a été publié en 2005, couvrant l'analyse et la gestion des risques. Cette partie s'aligne sur la norme ISO/CEI 27001.

IT-Grundschutz est un standard de sécurité. Il fait partie d'une série de préceptes publiés par l'Office fédéral allemand (BSI) pour la sécurité de l'information et qui décrivent "les méthodes, les processus, les procédures, les approches et les mesures relatives à la sécurité de l'information" sur la base de la norme ISO / CEI 27001 : 2013.
Ce standard offre une ligne directrice pour la réalisation d'une analyse des risques et comprend un grand nombre de contrôles de sécurité, pour mettre en place un niveau de protection relativement élevé sans avoir à effectuer une analyse détaillée des risques. L'objectif de la méthode d'évaluation des risques IT-Grundschutz est de fournir une évaluation qualitative ; elle comprend l'identification, l'analyse et l'évaluation des incidents de sécurité qui pourraient être préjudiciables à l'entreprise.
Le standard décrit un à deux niveaux d'évaluation des risques ; l'un est conçu pour atteindre un niveau « standard » de la sécurité, alors que le second peut être entrepris par des

[2] PDCA (Plan-do-check-act ou le plan-do-check-adjust) est une méthode de gestion en quatre étapes itératives utilisée dans les affaires pour le contrôle et la continuelle amélioration des processus et des produits. Il est également connu comme le Deming cercle / Cycle / roue, Shewhart Cycle, cercle de contrôle / cycle de, ou le plan-do-étude-act (PDSA). (ISO/CEI 27001, 2013)

entreprises désirant une approche personnalisée à leurs besoins. Le corps principal du standard ne décrit pas une procédure d'évaluation des risques spécifiques, mais donne lieu à des suggestions pour des garanties appropriées pour les processus métiers typiques. En revanche, les catalogues IT-Grundschutz contiennent des référentiels de scénarios de menaces et des contre-mesures de sécurité applicables à la plupart des environnements informatiques et regroupés par modules correspondant à divers environnements et informations commerciales.

Enfin, **SS627799- 2**, est un standard suédois spécifiant les exigences de sécurité pour la mise en œuvre des politiques de sécurité. Il est adapté aux besoins de chaque organisation ou à une partie de celle-ci.

Parmi les autres standards cités dans la littérature, mentionnons : GB / T22080-2008 et GB / T 220812008v de la Chine, ГОСТ P51897 de la Russie, JIS Q 27002 : 2014 du Japon et SABS7799-2 d'Afrique du Sud. Nous résumons dans le tableau ci-dessous ces standards de sécurité avec leurs objectifs.

Pays	Dénomination	Objectif
Chine	GB/T22080-2008, GB/T 22081-2008v	Techniques de sécurité - Systèmes de management de la sécurité de l'information
Russie	ГОСТ P51897	Spécification des termes et définitions pour le domaine de la gestion de risque
Royaume-Uni	BS 7799	Les bonnes pratiques, lignes directrices pour la gestion de sécurité
Suède	SS 627799-2	Spécification des exigences pour établir, mettre en œuvre, l'exploitation, la surveillance, l'examen, maintenir et améliorer un système de management de la sécurité de l'information.
Japon	JIS Q 27002 :2006	Code de bonnes pratiques pour la gestion de la sécurité de l'information
Australie/Nouvelle Zélande	AS/NZS 4360	Guide générique de gestion des risques
Afrique du sud	SABS7799-2	Lignes directrices pour la gestion de sécurité

Tableau 1 : Standards de gestion de risques.

II.2.2 Les normes de sécurité

En règle générale, les normes sont des accords documentés et acceptés communément par des pays ou à l'échelle planétaire. Ces accords internationaux sont essentiellement des spécifications précises destinées à une application répétitive et à une utilisation de façon systématique comme des lignes directrices, des règles ou des définitions de caractéristiques qui permettent d'assurer que les matériaux, produits, processus et les services sont régis par les mêmes dispositions.
L'AFNOR (Association Française de Normalisation) définit la norme comme une « donnée de référence résultant d'un choix collectif raisonné en vue de servir de base d'action pour la solution de problèmes répétitifs ».
La famille des normes internationales ainsi que les rapports techniques ISO 2700x sont dédiés, dans leur majorité, au domaine de la sécurité de l'information et du management des risques. Nous avons étudié toute cette famille et nous avons écarté les normes et les rapports techniques qui ne sont pas du même niveau d'abstraction que nos objectifs. A titre d'exemple mentionnons la cyber sécurité (ISO/CEI 27032 :2012) ou (ISO/CEI 27039 : 2015) traitant de la détection d'intrusion etc.….
Les principaux normes et rapports techniques de sécurité de l'information et du management des risques de la famille ISO2700X sont :

La norme **ISO/CEI 27000**, publiée pour la première fois en mai 2009, et révisée, en 2012 puis, en 2014 et enfin en 2016. C'est une norme conçue pour le domaine de la sécurité de l'information, contenant la définition des terminologies et des vocabulaires. Cette norme internationale est applicable à tous les types et à toutes les tailles d'organismes.

La norme **ISO/CEI 27001**, sous le titre "Technologies de l'information - Techniques de sécurité - Systèmes de gestion de sécurité de l'information - Exigences", elle succède au standard de sécurité BS 7799-2. La norme a été publiée en 2005, et révisée en 2013, elle décrit un ensemble d'exigences à respecter pour s'assurer de la pertinence du système de management de la sécurité de l'information (SMSI).

La norme **ISO/CEI 27002**, sous l'intitulé « Technologies de l'information - Techniques de sécurité -Code de bonne pratique pour le management de la sécurité de l'information» a été publiée en 2005 et révisée en 2013. Elle offre des lignes directrices en matière d'instructions organisationnelles relatives à la sécurité de l'information et des bonnes pratiques de management de la sécurité de l'information, incluant la sélection, la mise en œuvre et la gestion de mesures de sécurité, en prenant en compte le ou les environnement(s) de risques de sécurité de l'information de l'organisation.
La norme ISO 27002 :2013 est élaborée à l'intention des organisations désireuses de sélectionner les mesures de sécurité nécessaires dans le cadre du processus de mise en œuvre d'un Système de Management de la Sécurité de l'Information (SMSI) en se basant sur la norme ISO/CEI 27001 (ISO/CEI 27002, 2013).

ISO/CEI 27003 :2010, sous le titre « Technologies de l'information - Techniques de sécurité - gestion de la sécurité mise en œuvre du système d'orientation », fournit un guide de préparation et d'implémentation de la phase de planification d'un SMSI en traitant les points suivants (ISO/CEI 27003, 2010) :

- Contenu de la politique de sécurité ;

- Analyse des exigences de sécurité à partir des enjeux métiers d'affaires appliqués aux actifs ;

- Évaluation et traitement du risque ;

- Établissement du contenu et des frontières du SMSI ;

- Élaboration d'un plan de traitement des risques.

La norme **ISO/CEI 27004** : 2009, intitulée « Technologies de l'information - Techniques de sécurité - Management de la sécurité de l'information – Mesurage », décrit les lignes directrices pour l'observation et la mesure de l'efficacité des SMSI.

La norme **ISO/CEI 27005**, dont le titre est « Technologies de l'information - Techniques de sécurité - Gestion des risques liés à la sécurité de l'information », publiée pour la première fois, en 2005 et révisée, en 2008 et actualisée en 2011, décrit les systèmes de gestion associés aux risques et les moyens de les évaluer. Elle s'appuie sur les concepts généraux spécifiés dans les normes ISO/CEI 27000 et 27001. Cette norme est un processus structuré et systématique d'évaluation des risques en tenant compte de la plupart des dimensions organisationnelles.

Le processus de gestion des risques défini par cette norme comprend les étapes suivantes :

- Établissement du contexte ;
- Identification du risque ;
- Estimation du risque ;
- Évaluation du risque ;
- Traitement du risque ;
- Acceptation du risque ;
- Communication du risque.

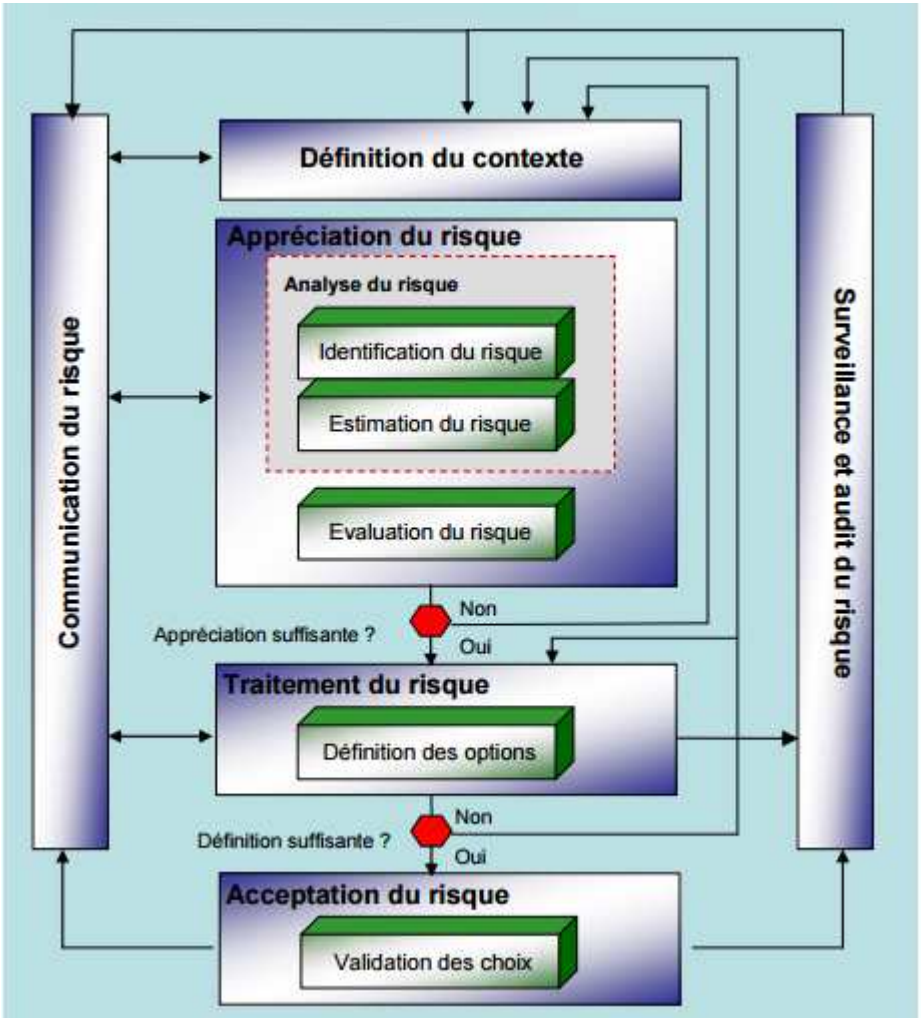


Figure 7 : Processus de gestion du risque ISO/ CEI 27005. (ISO/ CEI 27005, 2008)

La norme **ISO/CEI 27006** est intitulée « Technologies de l'information - Techniques de sécurité -Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information ». Publiée pour la première fois en 2007 et révisée en 2011, et enfin en 2015, elle spécifie les exigences et les lignes directrices pour les institutions qui certifient le système de management de la sécurité de l'information (ISO/CEI 27006, 2015).

La norme **ISO/CEI 27007** :2011 est intitulée « Technologies de l'information - Techniques de sécurité - Lignes directrices pour l'audit des systèmes de management de la sécurité de l'information ». Elle décrit des lignes directrices pour l'audit des systèmes de Management de la Sécurité de l'Information (ISO/ CEI 27007, 2011).

Le rapport **ISO/CEI TR 27008** :2011, sous le titre « Technologies de l'information - Techniques de sécurité - Lignes directrices pour les auditeurs des contrôles de sécurité de l'information, vient en appui à la norme ISO/CEI 27001. Ce rapport technique a été mis en œuvre pour renforcer la confiance dans les contrôles de sécurité de l'information.

La norme **ISO/CEI 27010**:2015, intitulée « Technologies de l'information - Techniques de sécurité - Gestion de la sécurité de l'information des communications intersectorielles et inter organisationnelles », fournit des lignes directrices en matière de partage de l'information sur

les risques de l'information, les contrôles de sécurité, les questions et / ou incidents qui couvrent les frontières entre les secteurs de l'industrie et /ou des nations, en particulier celles qui touchent les infrastructures critiques (ISO/ CEI 27010, 2015).

La norme **ISO/CEI 27011** :2008, intitulée « Technologies de l'information - Techniques de sécurité - Lignes directrices du management de la sécurité de l'information pour les organismes de télécommunications sur la base de l'ISO/CEI 27002 », est connue sous le nom X.1051 UIT. Cette norme décrit les lignes directrices du management de la sécurité de l'information pour les organismes de télécommunications sur la base de l'ISO/CEI 27002 (ISO/CEI 27011, 2008).

La norme **ISO/CEI 27013**, intitulée « Technologies de l'information - Techniques de sécurité - Guide sur la mise en œuvre intégrée d'ISO/CEI 27001 et ISO/CEI 20000-1 »[3], a été publiée pour la première fois en 2012, et révisée en 2015. La norme fournit des indications sur la mise en œuvre intégrée de la norme ISO / CEI 27001 et ISO / CEI 20000-1 pour les organisations qui ont l'intention soit de :

a) Mettre en œuvre la norme ISO/CEI 27001 lorsque ISO / CEI 20000-1 est déjà mise en œuvre, ou vice versa

b) Mettre en œuvre à la fois ISO/CEI 27001 et ISO / CEI 20000-1 ensemble ;

c) Intégrer les systèmes de gestion existants fondés sur la norme ISO / CEI 27001 et ISO/CEI 20000-1.

ISO/CEI 27013 : 2015 se concentre exclusivement sur la mise en œuvre intégrée d'un système de management de la sécurité de l'information (SMSI) tel que spécifié dans la norme ISO / CEI 27001 et un système de management de service (SMS) tel que spécifié dans la norme ISO / CEI 20000-1. (ISO/ CEI 27013, 2015)

La norme **ISO/CEI 27014** : 2013, intitulée « Technologies de l'information - Techniques de sécurité - Gouvernance de la sécurité de l'information », fournit des lignes directrices sur les concepts et les principes de la gouvernance de la sécurité de l'information, que les organisations peuvent évaluer, diriger, contrôler et communiquer les activités liées à la sécurité de l'information au sein de l'organisation (ISO/CEI 27014, 2013).

Le Rapport technique **ISO/CEI TR 27015** : 2012, intitulé « Technologies de l'information - Techniques de sécurité - Lignes directrices de gestion de la sécurité de l'information pour les services financiers », a été publié dans l'optique d'offrir un appui supplémentaire aux acteurs du secteur financier pour qu'ils puissent mettre en place un système de management de la sécurité de l'information adapté à leurs prestations de services financiers tout en renforçant la confiance de leurs clients (ISO/CEI 27015, 2012).

[3] ISO/CEI 20000, est une norme de système de management des services (SMS). Elle spécifie les exigences destinées au fournisseur de services pour planifier, établir, implémenter, exécuter, surveiller, passer en revue, maintenir et améliorer un SMS. Les exigences incluent la conception, la transition, la fourniture et l'amélioration des services afin de satisfaire aux exigences de services. (ISO/CEI 20000, 2011)

Le Rapport technique **ISO/CEI TR 27016** : 2014, sous le nom « Technologies de l'information - Techniques de sécurité - Management de la sécurité de l'information - Économie organisationnelle », fournit des lignes directrices sur la sécurité de l'information économique en tant que processus décisionnel concernant la production, la distribution et la consommation de biens et services, qui ont des utilisations différentes afin d'atteindre les objectifs d'une organisation à un coût minimal (ISO/CEI TR 27016, 2014).

Le Rapport technique **ISO/CEI TR 27019** : 2013, intitulé « Technologies de l'information - Techniques de sécurité - Lignes directrices de gestion de la sécurité de l'information fondée sur la norme ISO / CEI 27002 pour les systèmes de contrôle de processus spécifiques à l'industrie des services publics d'énergie », est destiné à aider les organisations dans l'industrie de l'énergie à interpréter et appliquer la norme ISO/IEC 27002: 2005 afin de sécuriser leurs systèmes de contrôle des processus électroniques (ISO/CEI TR 27019, 2013).

La norme **ISO/CEI 27031** : 2011, intitulée « Technologies de l'information - Techniques de sécurité - Lignes directrices pour l'information et la technologie des communications de préparation pour la continuité des activités », fournit des indications sur les concepts et les principes derrière le rôle des technologies de l'information et de la communication pour assurer la continuité des activités (ISO/CEI 27031, 2011).

La norme **ISO/CEI 27035** : 2011, intitulée « Technologies de l'information - Techniques de sécurité - Gestion de l'information des incidents de sécurité », couvre les processus de gestion de sécurité de l'information des événements, des incidents et des vulnérabilités. La norme se base sur la section de gestion des incidents de sécurité de l'information de la norme ISO / CEI 27002. Elle définit un processus en cinq (05) étapes :

- Préparer pour faire face aux incidents, par exemple préparer une politique de gestion des incidents ;
- Identifier et signaler les incidents de sécurité de l'information ;
- Évaluer les incidents et prendre des décisions sur la façon dont ils doivent être traités ;
- Répondre aux incidents, enquêter sur eux et les résoudre ;
- Apprendre les leçons - cette étape consiste à faire réellement des changements qui améliorent les processus (ISO/CEI 27035, 2011).

La norme **ISO 27799**, intitulée « Informatique de santé - Management de la sécurité de l'information relative à la santé en utilisant l'ISO/CEI 27002 », a été publiée pour la première fois en 2008, et révisée en 2016. Elle spécifie des lignes directrices permettant d'interpréter et de mettre en œuvre l'ISO/CEI 27002 dans le domaine de l'informatique de santé et constitue un complément à cette dernière.

La norme **ISO 27799 :2016** fournit des préconisations de mise en œuvre des mesures décrites dans l'ISO/CEI 27002 et les complète, le cas échéant, de façon qu'elles puissent être utilisées efficacement dans le management de la sécurité des informations de santé. La mise en œuvre de l'ISO 27799 :2016 permettra aux organismes de santé et aux autres dépositaires d'informations de santé de garantir le niveau minimal requis de sécurité approprié aux conditions de leur organisme et de protéger la confidentialité, l'intégrité et la disponibilité des informations personnelles de santé dans leurs activités de soin (ISO 27799, 2016).

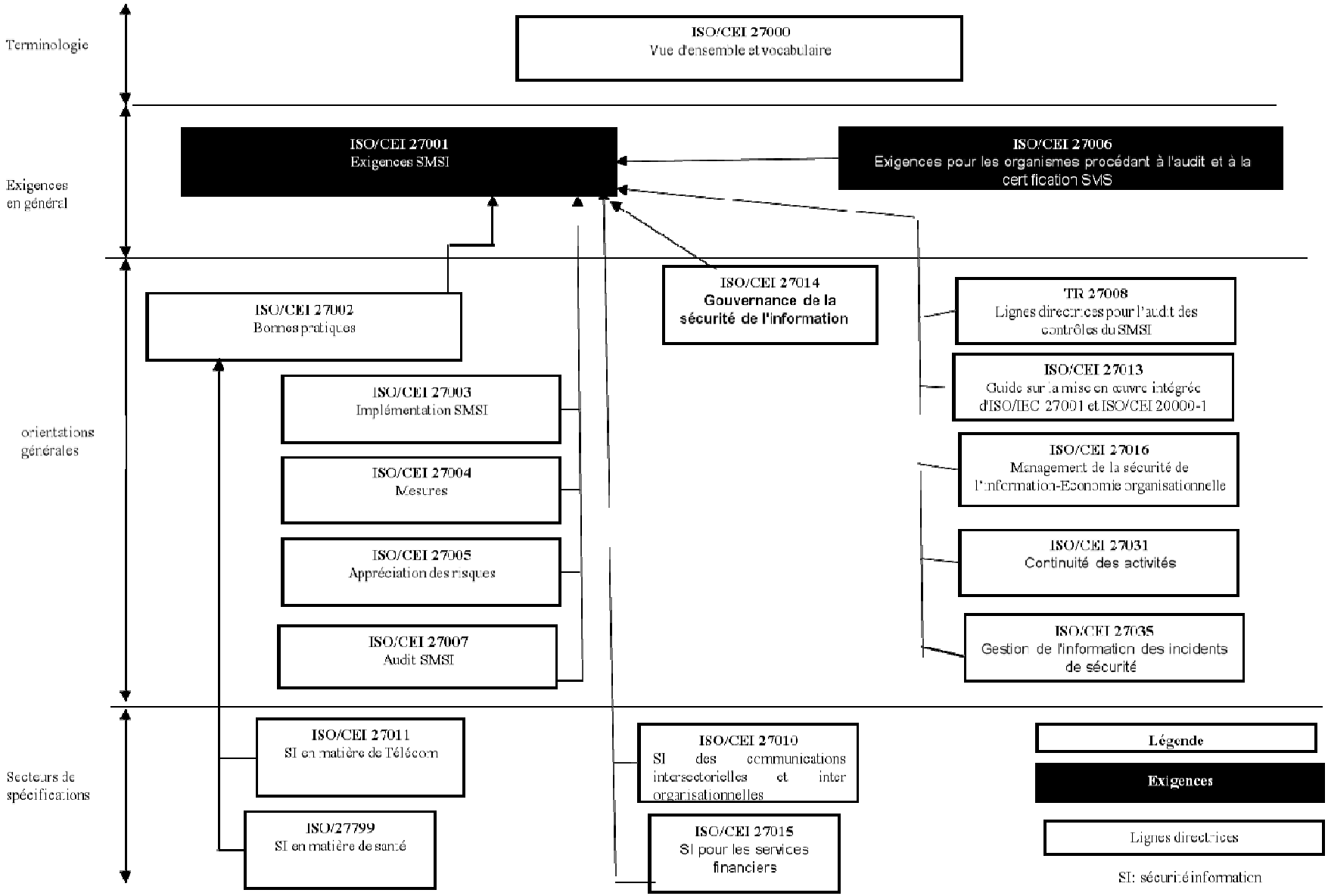


Figure 8 : Famille des normes de sécurité 2700X.

La norme **ISO 31000**, 2009, établit un ensemble de principes permettant une analyse efficace de la gestion des risques. Le but de cette norme est de fournir des principes et des lignes directrices du management des risques ainsi que les processus de mise en œuvre aux niveaux stratégiques et opérationnels. Elle ne vise pas à promouvoir l'uniformisation du management du risque au sein des organismes, mais plutôt à harmoniser la myriade d'approches, de standards et de méthodologies existant en matière de management des risques. La famille des normes ISO 31000 comprend :

- ISO 31000 :2009 – Management du risque -Principes et lignes directrices ;

- CEI[4] 31010 :2009 - Gestion des risques - Techniques d'évaluation des risques ;
- ISO Guide 73 : 2009 - Management du risque –Vocabulaire ;
- ISO/TR[5] 31004 : 2013- Management du risque - Lignes directrices pour l'implémentation de l'ISO 31000.

ISO/TR 31004 : 2013, est un rapport technique qui est destiné à aider les organisations à intégrer la gestion des risques dans leur processus de gestion de l'organisation en suivant les onze points suivant :

1. La gestion des risques créée de la valeur et la préserve ;
2. La gestion des risques fait partie intégrante de tous les processus de l'organisation ;
3. La gestion des risques fait partie de la prise de décision ;
4. La gestion des risques traite explicitement des incertitudes ;
5. La gestion des risques est systématique, structurée et en temps opportun ;
6. La gestion des risques est fondée sur les meilleures informations disponibles ;
7. La gestion du risque est adaptée en fonction des ressources disponibles ;
8. La gestion du risque prend des facteurs humains et culturels en compte ;
9. La gestion des risques est transparente et sans exclusion ;
10. La gestion des risques est dynamique, itérative et sensible au changement ;
11. La gestion des risques facilite l'amélioration continue de l'organisation.

La norme **ISO/CEI 15408** (Common Criteria, 2012), connue sous le label des critères communs, est née d'un partenariat entre le Canada, les États-Unis et l'Europe. Elle est consacrée à l'évaluation des systèmes et de la sécurité du logiciel. La prolifération des critères communs démontre l'importance de la gestion des risques informatiques. Les critères communs possèdent des bases de connaissances suivantes :

- Ensembles de Profils de protection ;
- Ensembles de menaces potentielles ;
- Ensembles de politiques de sécurité potentielles ;
- Ensembles des hypothèses de sécurité potentielles ;
- Ensembles des exigences de sécurité et d'assurances.

[4] CEI, Commission électrotechnique internationale. Elle est complémentaire de l'Organisation internationale de normalisation (ISO), dédiée au domaine électrotechnique.

[5] ISO/TR, Rapport technique.

La norme **ISO/CEI 17799**, issue du standard britannique BS 7799, offre des lignes directrices et des recommandations pour le management de la sécurité. Le principe général de celle-ci est, de mettre en œuvre, entretenir et améliorer la gestion de la sécurité de l'information au sein d'un organisme. Les objectifs esquissés fournissent une orientation générale sur les buts acceptés communément (ISO/CEI 17799, 2005).

ISO Guide 73 : 2009, intitulée « Management du risque – Vocabulaire » fournit les définitions de termes génériques relatifs au management du risque, a pour but est d'encourager une compréhension commune homogène et une approche cohérente de la description des activités relatives au management du risque, ainsi qu'une utilisation uniforme de la terminologie du management du risque dans les processus et cadres organisationnels en rapport avec ce domaine. L'ISO Guide 73 :2009 sert à l'usage des :

- Personnes chargées du management des risques ;

- Personnes impliquées dans les activités d'ISO et CEI ;

- Personnes chargées de rédiger des normes, guides, procédures et codes de bonnes pratiques relatives au management du risque.

Le tableau suivant résume les principales normes de sécurité de l'information ou on peux destingue quatre grand axe :

- Normes avec vue générale et vocabulaire (ISO guide 73, ISO/CEI 27000)
- Normes qui proposent des exigences de sécurité de matière générale (ISO/CEI 15408, ISO/CEI 27001, ISO/CEI 27006)
- Normes qui proposent des orientations générales en matière de sécurité (ISO/CEI 27001 au 7, ISO/CEI 27013, ISO/CEI 27031,27035, ISO 31000)
- Normes destiné à des secteurs spécialisés (ISO/CEI 27011, ISO/CEI 27799)

Nom	Fondement	Objectif
ISO/CEI Guide73	ISO 31000:2009	Définition des termes relatifs au management du risque
ISO/CEI 15408	Orange book, ITSEC,CTCPEC	Évaluation et certification
ISO/CEI 17799	BS7799-1	Lignes directrices et des recommandations SMSI
ISO/CEI 27000	/	Vue d'ensemble et vocabulaire
ISO/CEI 27001	BS 7799-2	Systèmes de gestion de sécurité de l'information – Exigences
ISO/CEI 27002	ISO/ CEI 27001	Code de bonne pratique pour le management de la sécurité de l'information
ISO/CEI 27003	ISO/ CEI 27001	Mise en œuvre du système d'orientation
ISO/CEI 27004	ISO/ CEI 27001	Management de la sécurité de l'information – Mesurage
ISO/CEI 27005	ISO/ CEI 13335	Gestion des risques liés à la sécurité de l'information
ISO/CEI 27006	/	Exigences pour les organismes procédant à l'audit et à la certification des SMSI
ISO/CEI 27007	ISO/ CEI 27006	Lignes directrices pour l'audit des SMSI
ISO/CEI 27011	ISO/ CEI 27001	Lignes directrices du management de la sécurité de l'information pour les organismes de télécommunications sur la base de l'ISO/CEI 27002
ISO/CEI 27013	ISO/ CEI 27001 ISO/CEI 20000	Guide sur la mise en œuvre intégrée d'ISO/CEI 27001 et ISO/CEI 20000-1
ISO/CEI 27031	ISO/CEI 27001	Lignes directrices pour l'information et la technologie des communications de préparation pour la continuité des activités
ISO/CEI 27035	ISO/CEI 27001	Gestion de l'information des incidents de sécurité
ISO/ CEI 27799	ISO/ CEI 27001	Gestion de la sécurité de l'information en matière de santé
ISO 31000	AS/NZS 4360	Management du risque, principes et lignes directrices

Tableau 2 : Résumé des principales normes de sécurité de l'information.

II.2.3 Les référentiels

Les référentiels sont des encadrements souvent adaptés pour résoudre des problèmes de sécurité spécifiques. Ils rassemblent un ensemble détaillé de tâches qui définissent la stratégie et les procédures qui doivent être mises en œuvre pour gérer les démarches de sécurité de l'information. Ces processus permettent de constituer un plan détaillé suivant lequel, on peut construire une démarche qui gère les menaces et réduit les vulnérabilités tout en attribuant des priorités de traitement.
Les référentiels de sécurité les plus connus sont :

COBIT 5 (Control Objectives for Information and related Technology) (ISACA, 2012) a été développé à l'origine pour fournir des lignes directrices en matière de gouvernance informatique. Ce référentiel s'adresse à la fois aux métiers et aux domaines fonctionnels des systèmes d'information. Il prend en considération les intérêts relatifs à l'informatique des parties prenantes internes et externes des entreprises de toutes tailles, dans n'importe quel secteur d'activité.
COBIT 5 est fondé sur 5 principes :

- Principe 1 – répondre aux besoins des parties prenantes;
- Principe 2 – couvrir l'entreprise étendue ;
- Principe 3 – appliquer un référentiel unique et intégré ;
- Principe 4 – faciliter une approche holistique ;
- Principe 5 – séparer la gouvernance de la gestion.

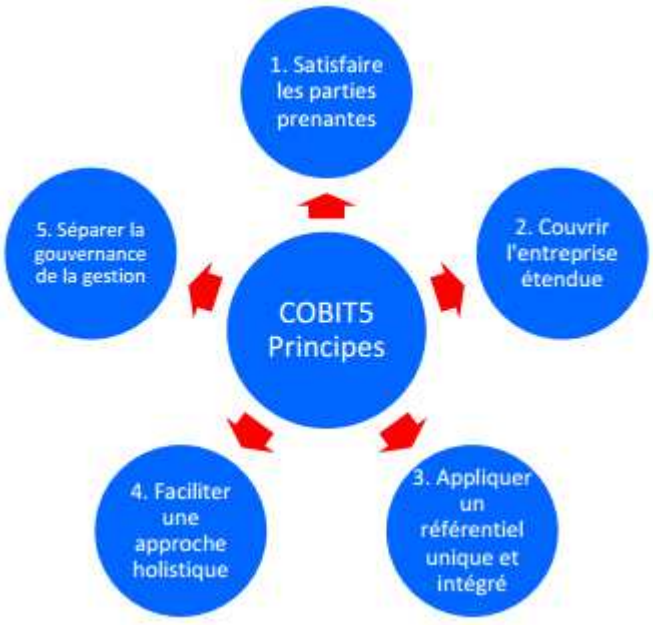


Figure 9 : Principe du référentiel COBIT5 (ISACA, 2012).

COBIT 5, identifie trente-sept (37) processus. Ce sont des ensembles organisés de pratiques et d'activités permettant d'atteindre des résultats des objectifs généraux liés aux technologies informatiques. Ils sont regroupés en cinq (05) domaines :

1. **Évaluer, diriger et surveiller** : Ce domaine compte cinq (05) processus. Il permet de s'assurer du respect des grandes règles de gouvernance. Il comprend les activités suivantes :

- Assurer la définition et l'entretien d'un référentiel de gouvernance ;
- Assurer le partage des bénéfices ;

- Assurer l'optimisation du risque;
- Assurer l'optimisation des ressources;
- Assurer aux parties prenantes la transparence.

2. **Aligner, planifier et organiser** : Ce domaine compte treize (13) processus. Ils constituent les bases de la gestion de l'informatique.

- Gérer le référentiel de gestion des ressources informatiques ;
- Gérer la stratégie;
- Gérer l'architecture de l'entreprise;
- Gérer l'innovation;
- Gérer le portefeuille;
- Gérer le budget et les coûts ;
- Gérer les relations humaines;
- Gérer les relations;
- Gérer les accords de service ;
- Gérer les fournisseurs;
- Gérer la qualité;
- Gérer le risque;
- Gérer la sécurité.

3. **Bâtir, acquérir et implanter** : Ce domaine comprend dix (10) processus. Le but de ce domaine est d'améliorer les processus de définition et de mise en place des applications informatiques :

- Gérer les programmes et les projets ;
- Gérer la définition des exigences ;
- Gérer l'identification et la construction des solutions ;
- Gérer la disponibilité et la capacité ;
- Gérer le changement organisationnel;
- Gérer les changements;
- Gérer l'acceptation du changement et de la transition ;
- Gérer la connaissance;
- Gérer les actifs;
- Gérer la configuration.

4. **Livrer, servir et soutenir** : Ce domaine comprend six (06) processus. L'objectif est de perfectionner le fonctionnement de l'exploitation informatique et notamment :

- Gérer les opérations;
- Gérer les demandes de services et les incidents ;
- Gérer les problèmes;
- Gérer la continuité;
- Gérer les services de sécurité ;
- Gérer les contrôles des processus d'affaires.

5. **Surveiller, evaluer et mesurer** : Ce domaine comprend trois (03) processus. Il détaille les bases du contrôle des systèmes d'information dont le contrôle interne et comprend :

- Surveiller, évaluer et mesurer la performance et la conformité ;

- Surveiller, évaluer et mesurer le système de contrôle interne ;
- Surveiller, évaluer et mesurer la conformité aux exigences externe.

ITIL (Infrastructure Library Information Technology) (Hochstein et al, 2005) est un ensemble des meilleures pratiques dans la gestion des services informatiques, développés par l'Office of Government Commerce du Royaume-Uni. Il se concentre principalement sur les processus de services informatiques. Depuis 2005, ITIL a évolué grâce à la norme ISO / CEI 20000. Le référentiel aborde les points suivants :

- Organisation et l'amélioration du système d'information ;
- Réduction des risques;
- Augmentation de la qualité des services informatiques.

ITIL propose un référentiel de développement structuré en processus et centré sur le client. Le client est en effet au cœur de l'approche. C'est le point fondateur de la démarche, en facilitant le dialogue clients/fournisseurs (internes et/ou externes) et en réutilisant des pratiques ayant déjà été testées, ITIL cherche à améliorer l'organisation des SI. Le deuxième principe du référentiel est de s'assurer de la fiabilité des projets dès la phase de conception du système, et enfin de maîtriser les processus. En effet, la qualité de service est fondée sur les processus. Chaque projet ITIL suit les cinq (05) étapes suivantes :

1. Définition du rôle
   - Définition de la raison d'être du service informatique ;
   - Établissement des buts et des objectifs.
2. Accroissement de la prise de conscience ;
   - Communication sur les bénéfices du service informatique ;
   - Apport d'une information générale;
   - Circulation de l'information par des séminaires, rencontres, feuillets ou circulaires.
3. Planification
   - Exécution d'une analyse des besoins ;
   - Définition détaillée des besoins;
   - Quantification de la charge de travail du nouveau service ;
   - Élaboration de directives concernant la façon dont le service fonctionnera – sa structure et ses relations par rapport à la structure organisationnelle ;
   - Spécification des mesures des objectifs de performance ;
   - Conception du processus, y compris le support pour celui-ci ;
   - Élaboration d'un plan de mise en œuvre.
4. Mise en œuvre
   - Définition des besoins en formation ;
   - Description des bénéfices, coûts et problèmes possibles ;
   - Développement et validation du processus ;
   - Installation des logiciels et de l'équipement ;
   - Personnalisation des outils informatiques de distribution ;
   - Mise à l'épreuve du processus.

- Création d'inventaires pour les logiciels et les équipements ;
- Rédaction de documents de référence ;
- Formation du personnel;
- Exécution des tests d'acceptation;
- Déploiement et mise en œuvre.

5. Revue et contrôle préalables à la mise en œuvre
   - Adéquation des besoins avec la réalité – vérification que les services fournissent ce que les utilisateurs attendent ;
   - Comparaison des niveaux d'activité réels avec les prévisions ;
   - Évaluation de la satisfaction du personnel à l'égard du service ;
   - Révision de l'efficacité et de la rentabilité ;
   - Détermination des bénéfices;
   - Révision de la gestion du projet ;
   - Préparation des rapports de révision ;
   - Exécution régulière de contrôles;
   - Surveillance, révision et ajustement de l'efficacité du service.

Le référentiel **Risk IT** a été construit en complément de COBIT 5 et définit un ensemble de bonnes pratiques pour identifier, gouverner et gérer les risques des systèmes d'information de l'entreprise. Risk IT, fournit une vue d'ensemble des risques informatiques. Il permet de gérer et de proposer aux entreprises d'identifier et de régenter les risques informatiques (ISACA, 2009). Il se compose de trois (03) domaines, de neuf (09) processus et de quarante-sept (47) bonnes pratiques comme le montre la figure suivante :

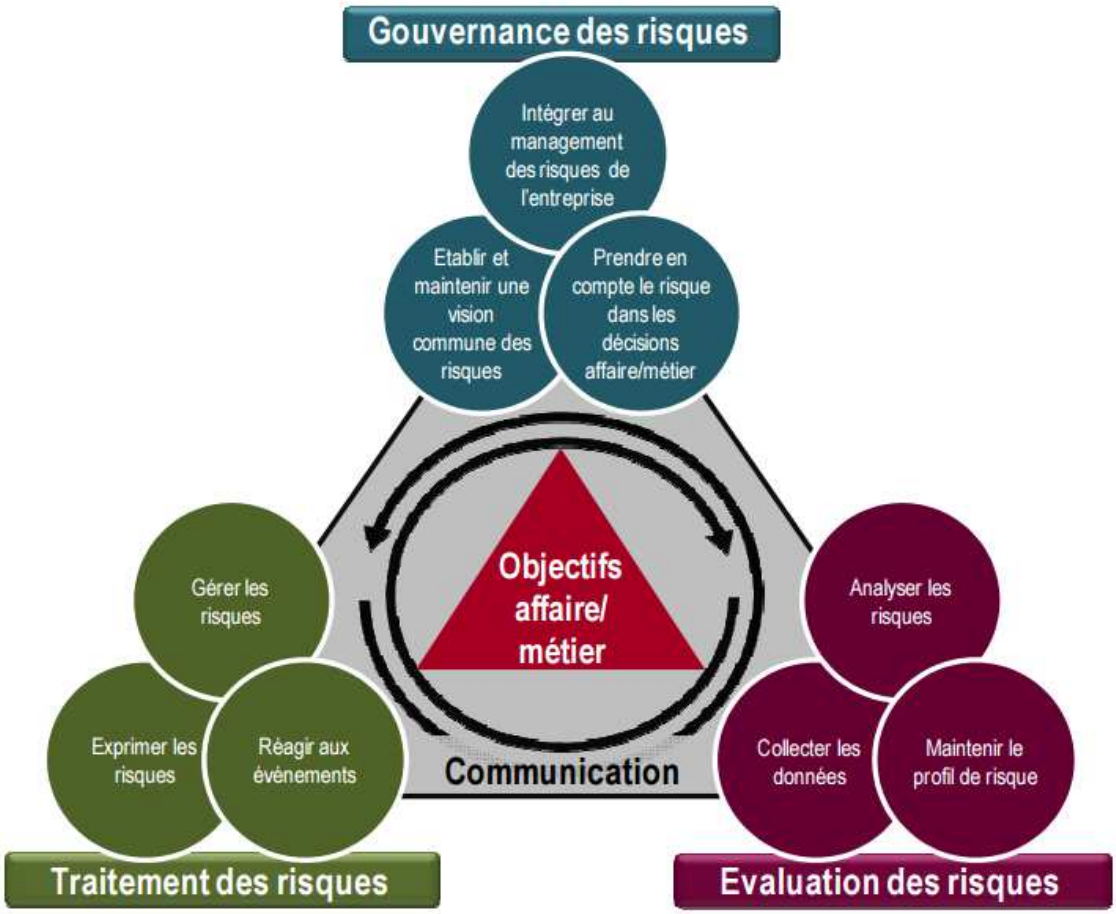


Figure 10: Principe de Risk IT (ISACA, 2009).

Selon notre constat, une faiblesse du référentiel est liée au fait qu'il ne décrit pas l'évaluation du risque avec des détails techniques suffisants.

II.2.4 Les méthodologies d'analyse des risques

Actuellement, il existe de nombrables méthodes de gestion et d'analyse des risques qui sont déclinées à travers le monde. L'étude approfondie de leurs concepts et de leurs processus nous a permis de constater qu'elles sont plus ou moins bien finalisées, plus ou moins documentées ou tout simplement sans aide précieuse pour nos recherches.
Cependant, il est important de souligner que certaines méthodes font référence dans leur domaine et sont les plus utilisées dans la conduite d'une démarche de gestion des risques. Elles sont considérées comme des guides méthodologiques, informels ou semi formels. Chacune de ces méthodes a été développée pour répondre à un besoin spécifique. Les méthodologies de gestion des risques sont nombreuses. Nous avons écraté les méthodes d'analyse de risque qui ne disposent pas d'assez de documentation pour mieux les étudier. Les méthodologies retenues dans notre état de l'art sont :

MAGERIT (Metodología de Análisis y GEstión de Riesgos de los Sistemas de Información) est une méthodologie espagnole pour l'analyse des risques, élaborée, en 1997 par le Conseil Supérieur Espagnol d'Administration Electronique (CSAE). Elle met en œuvre le processus de gestion des risques de la norme ISO 31000. Son application se fait "dans un cadre précis permettant aux organes de prendre des décisions en tenant compte des risques découlant de l'utilisation des technologies de l'information" (Magerit V3, 2012).

L'objectif de la méthode est comme suit :

1) Faire connaître aux parties prenantes les risques encourus par les systèmes d'information, ainsi que les besoins en matière de sécurité et les traitements de risques qui existent ;
2) Offrir une méthode systématique d'analyse des risques ;
3) Aider à décrire et à planifier les mesures appropriées tout en gardant les risques sous contrôle.

En outre, elle vise à préparer l'organisation pour le processus d'évaluation, de vérification, de certification ou d'accréditation. La méthodologie MAGERIT est soutenue par le ministère espagnol des administrations publiques et se compose de trois livres qui sont brièvement décrits ci-après :
Le premier livre comprend les lignes directrices de la méthode d'analyse des risques.Les chapitres du livre décrivent la méthode d'évaluation des risques à partir de plusieurs points de vue, ce qui implique pour chacun un certain niveau de granularité et d'abstraction. Citons par exemple les aspects pratiques résultant de l'expérience. Tout cela est complété par les chapitres qui décrivent comment appliquer une telle évaluation des risques aux systèmes en cours de développement. Tout d'abord, la méthode est décrite à un niveau élevé, adaptée à la gestion. Elle facilite l'évaluation des risques et doit être intégrée d'une manière conforme à une stratégie de gestion des risques. Ensuite, le processus est décrit à un niveau opérationnel, en spécifiant exactement quelles activités devraient être entreprises pour chaque phase, ainsi que la description des produits et des intrants nécessaires. Les deuxième et troisième livres se concentrent presque exclusivement sur les détails techniques, les référentiels et techniques qui peuvent être utilisés par l'équipe d'analyse quand on procéde à l'évaluation.

NIST (National Industry Security Program) (NIST, 2015) documente une approche globale d'analyse des risques. Elle offre un framework et un plan décrivant étape par étape la mise en œuvre de la gestion des risques des systèmes d'information. Il fournit quatre publications (800-30, -37, -39 et -53) couvrant les activités de gestion des risques.
L'objectif de la publication spéciale NIST 800-30 est «de fournir des orientations pour l'évaluation des risques des systèmes et des organismes d'information fédéraux » (Stoneburner et al, 2007). Ce processus d'orientation permet l'identification des facteurs de risques spécifiques, permettant aux organisations de déterminer le niveau inacceptable des risques.
NIST Special Publication 800-37 est lié au cadre de gestion des risques (RMF) (Christopher, 2010), qui fournit un processus structuré intégrant la sécurité de l'information et des activités de gestion des risques dans le cycle de vie du développement du système.
NIST Spécial Publication 800-39 « fournit, une approche structurée et flexible pour gérer le risque, avec les détails spécifiques de l'évaluation, intervention et de suivi du risque sur une base continue fournie par l'appui d'autres normes et directives de sécurité NIST ».
Enfin, NIST Spécial Publication 800-53 (Révision 4) « fournit une approche plus holistique de la sécurité de l'information et la gestion des risques, en fournissant aux organisations des contrôles de sécurité nécessaires pour renforcer leurs systèmes d'information » (NIST, 2015).

OCTAVE, (Operationally Critical Threat, Actif and Vulnerability Evaluation) est une méthode, développée et publiée par le Software Engineering Institute (SEI) de la Carnegie Mellon University à travers son programme CERT. Elle est reconnue dans le domaine de la sécurité des systèmes d'information notamment par la (Federation of computer Emergency & Response Team -CERTS).
Elle dispose de trois versions : OCTAVE, OCTAVE-S et OCTAVE-Allegro (OCTAVE, 1999).

La méthode OCTAVE est utilisée dans les grandes entreprises (plus de 300 employés) et fournit les lignes directrices pour la conduite de la sécurité intérieure.
La méthode **OCTAVE-S** a été développée pour les petites entreprises (moins de 100 employés) et suppose que les personnes chargées de l'évaluation des risques sont connues, les exigences de sécurité, les menaces et les pratiques de sécurité de l'organisation aussi, et ils ne nécessitent pas de mener des entrevues, des sondages et des ateliers.
La méthode **OCTAVE-Allegro** est la dernière version. Elle est orientée vers l'évaluation des risques de sécurité de l'information. Elle décrit les étapes et fournit des feuilles de calcul des risques et des questionnaires, comme des guides et des modèles pour évaluer les risques de l'organisation ou plus précisément, ses actifs.
OCTAVE-Allegro fournit un framework d'évaluation des risques, composé de quatre phases :

1- Définir les paramètres : Établir les critères d'évaluation.
2- Définir les profils d'actifs : Établir les profils des actifs informationnels et identifier les intervenants.
3- Identifier les menaces : Identifier les domaines de préoccupation et les scénarios de menaces.
4- Identifier et atténuer les risques : Identifier les risques, analyser les risques, et choisir une approche face aux risques.

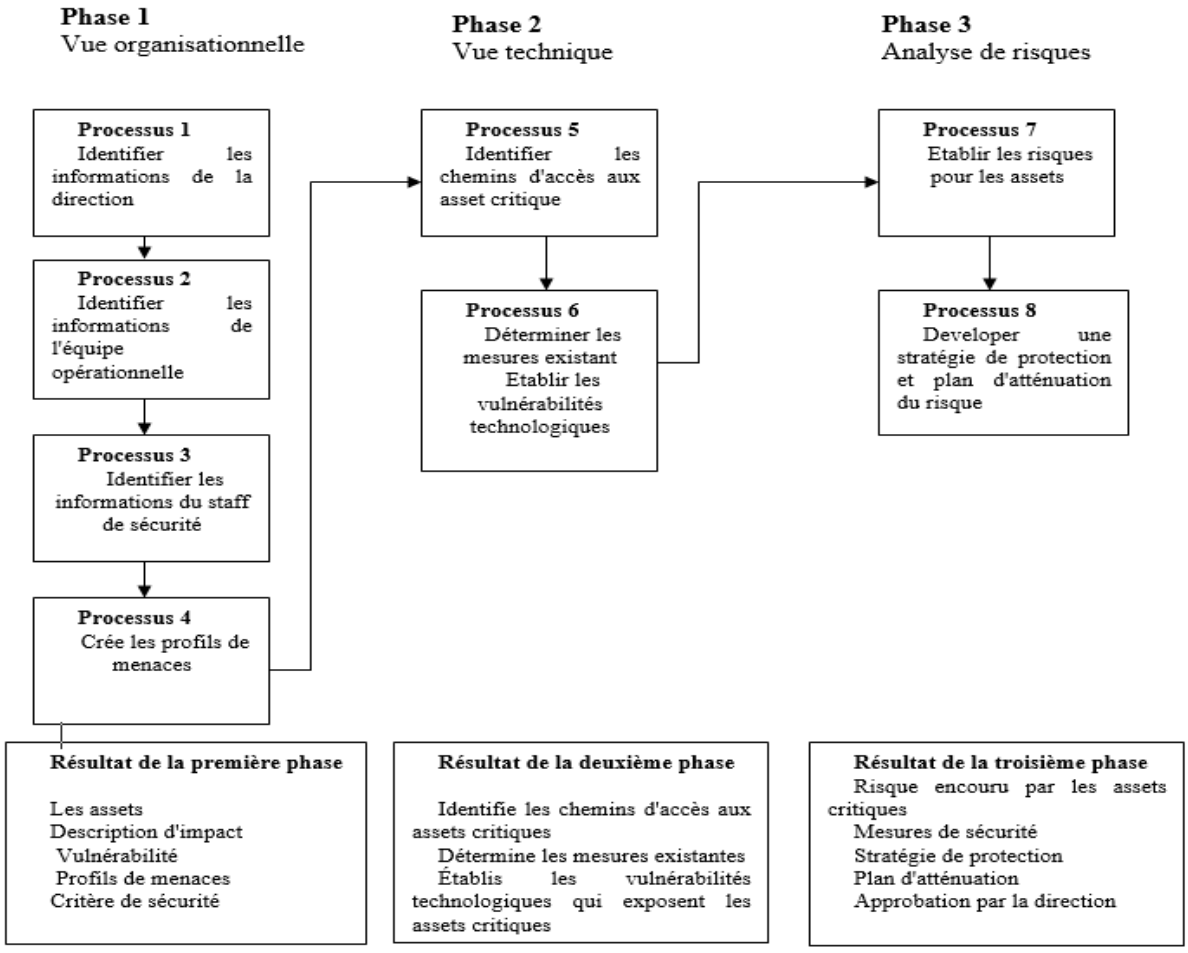


Figure 11 : Phases Octave-allegro (OCTAVE, 1999).

L'objectif de la phase1 est d'établir les critères de mesure du risque, d'identifier les principaux secteurs de l'organisation concernés (finances, clients, production, sécurité, etc .).

Dans cette phase, sont aussi définis les critères généraux des mesures de risques et les effets qui peuvent résulter des menaces. Ces critères seront pris en compte tout au long du processus de gestion des risques.

Le but de la phase 2 est de développer un profil d'actifs qui décrit pour chacun d'eux, leurs caractéristiques uniques, leurs qualités, leur valeur, où ils sont stockés, traités et transportés. Ce profil ne devrait pas donner lieu à une information ambiguë, et veille à ce que les exigences de sécurité pour cet actif soient clairement définies. En outre, dans ce profil, les paramètres sont définis, comme le responsable et les niveaux de confidentialité, l'intégrité et la disponibilité ainsi que l'identification de ce qui est le plus important.

Durant la phase 3 on procède à l'identification et à la documentation de ses menaces qui pèsent sur les actifs. Ensuite, on identifie les scénarios de menaces, plus précisément les menaces recensées dans l'étape précédente, puis on les associe à des scénarios de menaces. Un scénario est une situation de menace unique pour un actif. La probabilité est utilisée pour déterminer plus précisément quels scénarios sont plus susceptibles d'être réalisés.

Enfin, lors de la phase 4, on procède à l'identification des risques sur la base des informations fournies dans la zone ci - dessus, ainsi que l'élaboration de stratégie d'atténuation (Pyka, 2013).
Pour OCTAVE-Allegro, la formule de calcul du risque est la suivante :

L'impact est la conséquence négative de la menace.

FAIR (Factor Analysis of Information Risk) (FAIR, 2006), est une méthode d'analyse des risques quantitatifs développée par plusieurs groupes, dont l'Open Group et l'ISACA. Cette méthode propose un processus composé de dix étapes, réparties dans quatre (04) phases :

Phase 1 : Identifier les composants de scène (actifs et menaces)

1. Identifier les actifs à risque ;
2. Identifier les menaces encourues par les actifs à risque.

Phase 2 : Évaluer la fréquence des événements de perte

3. Estimation de la fréquence des menaces probables de l'événement ;
4. Estimer l'importance de la menace ;
5. Estimer les contrôler robustes ;
6. Dériver les vulnérabilités ;
7. Calculer les pertes fréquente de l'événement.

Phase 3 : Évaluer l'ampleur probable des pertes

8. Estimer les pires pertes ;
9. Estimer les pertes probables.

Phase 4 : Dérivation sur les risques

10. Dériver et atténuer les risques.

FAIR met l'accent sur l'objectivité. Elle présente un grand nombre de termes et de formules. La documentation fournit les critères, des diagrammes et des explications pour se familiariser avec eux. La méthode a été conçue pour remédier aux faiblesses dans la pratique de la sécurité. Elle permet aux entreprises de parler le même langage sur le risque, appliquer l'évaluation des risques à un actif de l'organisation, voir les risques organisationnels dans leur totalité et comprendre combien de temps et d'argent seront affectés au profil de sécurité de l'organisation. Elle est conforme à la norme ISO/CEI 27001.

La méthode **CORAS** est définie comme un cadre fondé sur un modèle pratique pour l'évaluation des risques sans ambiguïté pour les systèmes critiques (Vraalsen et al, 2005). Elle fournit un langage graphique pour la modélisation du risque. Elle a été mise au point par le conseil norvégien de la recherche et de l'UE. Elle est fondée sur le standard australo-néo-zélandais : AS / NZS 4360 : 2004.
L'analyse des risques de sécurité de la méthode CORAS se compose de huit étapes différentes où les quatre premières étapes se concentrent sur la création du contexte et les quatre dernières étapes sont sur le risque : l'identification, l'estimation, l'évaluation et les traitements possibles du risque.

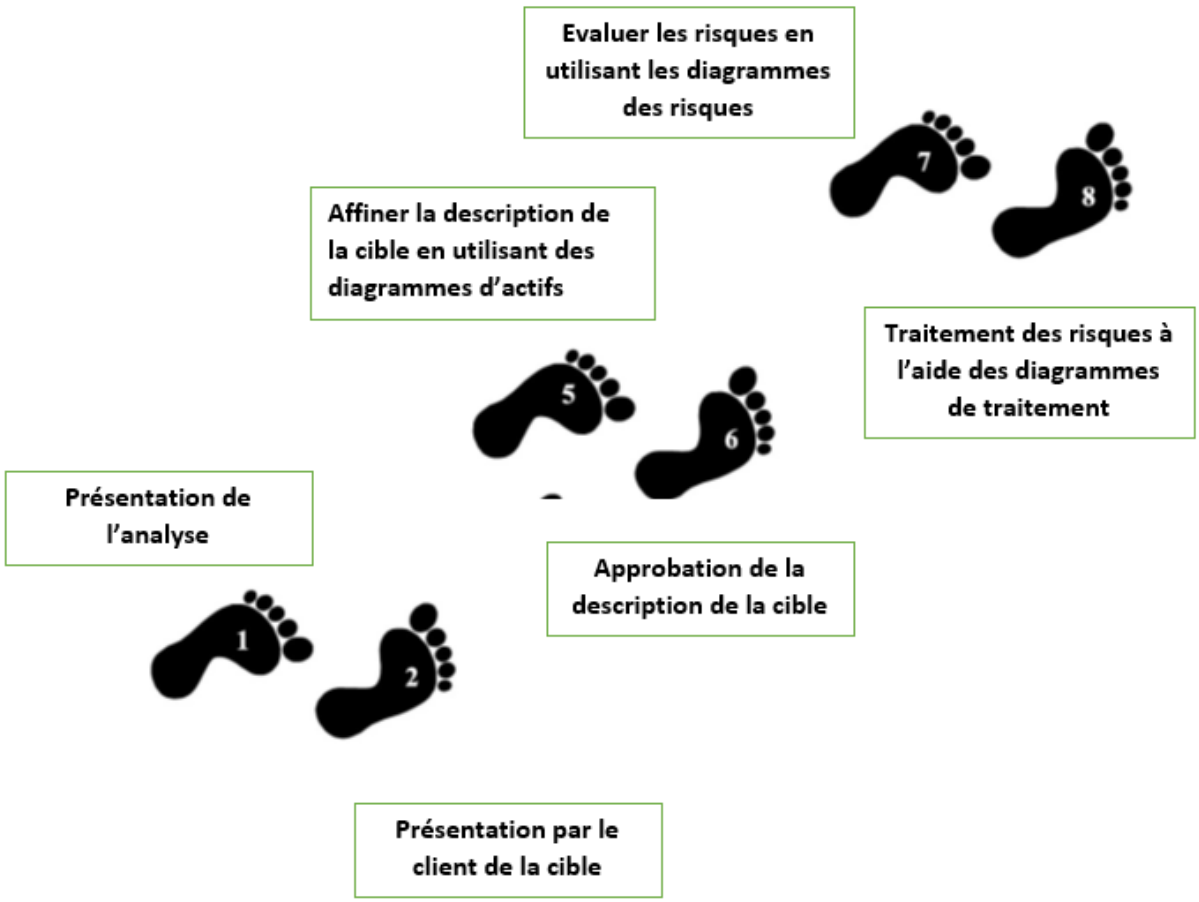


Figure 12 : Étapes de CORAS (Vraalsen et al, 2005).

CRAMM (Central Computer and Telecommunications Agency Risk Analysis and Management Method) (CRAMM, 2003) est utilisée pour justifier des investissements de sécurité. La méthode met l'accent sur les dimensions techniques de la sécurité. Elle utilise une matrice de risques combinant les menaces sur les actifs et les informations de vulnérabilité.

Un avantage de la méthode est qu'elle est supportée par un outil puissant. Mentionnons que CRAMM a été développé principalement pour les grandes organisations.

Cette méthode couvre les différentes menaces et vulnérabilités auxquelles le système d'information est exposé, qu'elles soient délibérées ou accidentelles. L'entreprise doit évaluer ses risques mais également décider du niveau de sécurité voulue pour chaque menace. Le processus de CRAMM suit les étapes :

1. Identification et évaluation des actifs en matière de coût et d'impact en cas de compromission des éléments qui constituent le système d'information de l'entreprise (les équipements, les applications, les données…) ;
2. Évaluation de la criticité des menaces et des vulnérabilités du système d'information ;
3. Choix de contre-mesures à mettre en place.

EBIOS (Expression des Besoins et identification des objectifs de Sécurité) (EBIOS, 2010) est une méthode développée en 1995, et revue en 2010, par la DCSSI (Direction centrale de la Sécurité des systèmes d'Information). Cette méthode française vise à l'évaluation et le traitement des risques. Elle se compose de cinq (05) guides (phases) qui sont : "Étude du contexte". "Expression des besoins de sécurité", "Étude des menaces", "Identification des objectifs de sécurité" et enfin "détermination des exigences de sécurité".

Figure 13 : Processus de gestion des risques EBIOS (EBIOS, 2010).

EBIOS est semblable à NIST SP 800-30. Elle est compatible avec les normes ISO /CEI 13335, ISO/CEI 15408(critères communs), ISO/CEI 17799 et ISO/CEI 27005.

FRAP (Facilitated Risk Assessment Process) (Peltier, 2005) est une méthode orientée vers les non-experts. Elle est prévue pour fournir une analyse qualitative des risques. Les parties prenantes jouent un rôle important au cours de la phase d'évaluation. Elle se compose de trois phases : définition de l'évaluation, l'identification des risques et de leur niveau, et la génération de rapports. Elle est axée sur les entreprises nécessitant très peu d'aide extérieure. L'une de ses faiblesses est la dépendance à l'égard du « facilitateur ».

MEHARI (Méthode Harmonisée d'Analyse des Risques) (CLUSIF, 2004) est une méthodologie française développée par une organisation de sécurité de l'information sans but lucratif (CLUSIF). MEHARI fait usage d'une méthode fondée sur la connaissance des procédures de support semi-automatiques pour l'évaluation des risques. Elle offre la possibilité d'évaluer et de gérer les risques liés aux scénarios de risque grâce à des formules d'évaluation directe et le choix des moyens de les réduire. Les bases de connaissances sont disponibles comme un classeur (pour Excel ou Open Office) capable de mener la qualification et la quantification de tous les éléments de risque. La démarche MEHARI comprend trois phases:

La phase préparatoire
Cette phase consiste à étudier le périmètre de l'étude et le contexte, de classer l'ensemble des actifs du SI, d'identifier les événements pouvant impacter le bon déroulement du SI et d'évaluer la gravité de cet impact pour l'entreprise. Cette phase permet de générer le Plan Stratégique de Sécurité (PSS). Ce dernier fixe les objectifs de sécurité, c'est-à-dire le niveau de sécurité requis en matière de critère de sécurité pour chaque actif identifié. Il fixe également les métriques permettant d'évaluer le niveau de gravité d'un risque. Il définit la politique de sécurité ainsi que la charte d'utilisation du SI pour ses utilisateurs.

La phase d'analyse des risques
Cette phase permet de détecter les scénarios de risques qui peuvent remettre en cause un des objectifs de sécurité de l'organisation. Il s'agit d'élaborer des scénarios de risque et d'effectuer un diagnostic des services de sécurité. Une évaluation des risques (probabilité, impact) est réalisée, permettant par la suite d'exprimer les besoins de sécurité, et les mesures nécessaires au traitement du risque. Cette phase permet de générer le Plan Opérationnel de Sécurité (POS) qui définit les mesures de sécurité qui doivent être mises en œuvre.

La phase de planification du traitement des risques
Cette phase consiste à analyser les scénarios de risque afin d'identifier et décider du traitement à adopter. Cette phase permet de générer le Plan Opérationnel d'Entreprise (POE) qui assure le suivi de la sécurité par l'élaboration d'indicateurs sur les risques identifiés et le choix des scénarios de risque contre lesquels il faut se prémunir.

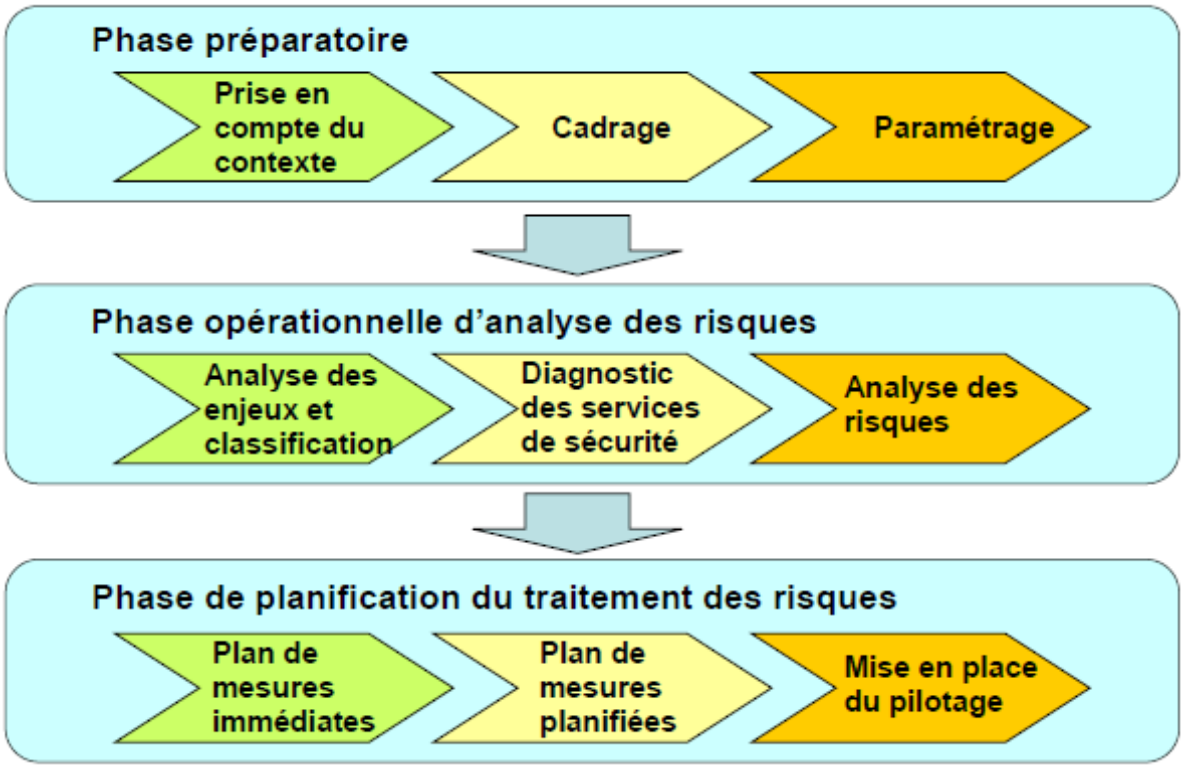


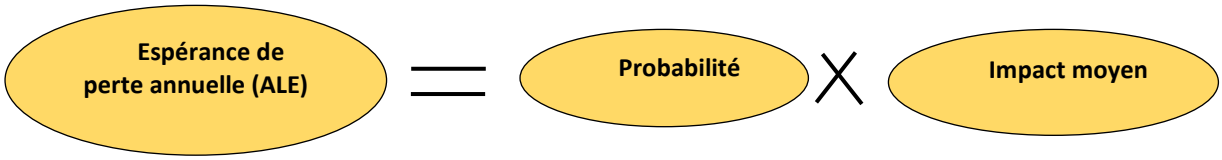
Figure 14 : Les grandes phases de la méthode MEHARI (CLUSIF, 2004).

SRA (Structured Risk Analysis) (McEvoy, 2002), est une méthode structurée pour identifier et classer les risques. Elle met l'accent sur un « attaquant moyen », sans prendre en considération les scénarios d'attaque. La méthode ne nécessite pas d'outils dédiés et elle est facile à utiliser. Certains auteurs estiment qu'elle manque de profondeur par rapport à d'autres méthodologies.

La méthodologie **TARA** (Threat Agent Risk Assessment) (TARA, 2011) a été développée par la firme Intel. C'est une méthode dédiée à la lutte contre un grand nombre d'attaques sur l'infrastructure informatique. Elle privilégie les risques critiques et se concentre sur les profils d'attaquants. Elle décrit comment utiliser les bases de données de vulnérabilité. TARA est une méthode qualitative offrant une des techniques de visualisation. Elle repose sur trois (03) bibliothèques qui sont :

- Bibliothéque des agents d'attaque (Threat agent library (TAL));
- Bibliothèque d'exposition commune (Common exposure library (CEL)) ;
- Bibliothèque des méthodes et objectifs (Methods and objectives library (MOL))

ISAMM (Information Security Assessment and Monitoring Method) (ISAMM, 2002) est une méthodologie de gestion de la sécurité de l'information utilisant une approche quantitative pour la détermination des risques, où les risques évalués sont exprimés par leur espérance de perte annuelle (ALE), en unités monétaires. ALE étant la perte ou le coût annuel prévu en cas de menace ou d'un groupe de menaces.



La méthode peut être utilisée pour identifier les actifs et les menaces, afin d'évaluer la probabilité et l'impact des menaces que représentent les risques, et pour donner un appui permettant de décider si un risque est acceptable ou non. Elle donne un soutien à la sélection des contrôles de sécurité afin de traiter les risques non acceptables et enfin à soutenir le processus de communication des risques. ISAMM se compose de quatre (04) étapes : "Détermination de la portée", "Évaluation des menaces et la conformité", "Validation de la conformité et de la menace" et "Rapport du résultat de calcul". La méthode offre un support pour la norme ISO/CEI 27001.

FMECA (Failure Mode, Effects and Criticality Analysis) (FMECA, 1993) est une technique permettant d'identifier les modes de défaillance et leur criticité. Son principal objectif est d'évaluer les risques et de donner la priorité aux efforts de contrôle associés.

HAZOP (Hazard and Operability Analysis) (Rune, 2007) est une méthode utilisée avec succès dans les systèmes critiques de sécurité industriels. Elle fournit une analyse structurée permettant aux organisations d'identifier les écarts critiques du comportement prévu. Initialement conçue pour analyser la sécurité des systèmes critiques, HAZOP a été modifiée pour identifier les menaces de sécurité.

FTA (Fault Tree Analysis) (Clifton, 1999) est une méthode visant à analyser les questions de sûreté / sécurité du système. FTA identifie les conditions qui peuvent conduire un système pour atteindre un état non-souhaitable. C'est une méthode d'analyse des arbres des défaillances. Elle permet de décrire de manière déductive les choix de combinaisons possibles qui donnent lieu à une défaillance. La méthode est particulièrement utile dans les phases de conception.

Soulignons le fait que le développement de chacune de ces méthodes a été réalisé pour répondre à un besoin spécifique. En outre, elles ont des objectifs différents (Sans, 2002). Cependant,les solutions proposées demeurent pertinentes pour l'identification et la gestion des risques sans toutefois être suffisantes pour le déclenchement des exigences de sécurité..

II.2.5 Les méthodes d'élicitation des exigences de sécurité

Les assujettissements aux exigences d'un système d'information se composent en exigences fonctionnelles et non fonctionnelles. Les exigences fonctionnelles décrivent ce que le système doit faire, tandis que les exigences non fonctionnelles définissent la façon dont le système doit être (Jureta et al, 2008). Pour arriver à maintenir le fonctionnement, les exigences de sécurité contribuent à couvrir un ou plusieurs risques ciblant le SI. Il existe plusieurs méthodes que nous regroupons en six catégories :

1- Les approches multilatérales ;
2- Les approches fondées sur UML ;
3- Les approches axées sur les buts ;
4- Les approches à base des abuses frames ;
5- Les approches fondées sur l'analyse des risques ;
6- Les approches fondées sur des critères communs.

Le premier groupe utilise des **approches multilatérales**, telles que MSRA (G¨urses, 2006), SQUARE (Travis et al, 2010), SIREN (Toval et al, 2001), IRIS (Shamal et al, 2010), et MOSIS. (Lammari et al, 2011) .
Le but de **MSRA** (Multilateral Security Requirements Analysis) est d'analyser la sécurité et les besoins de la vie privée de toutes les parties prenantes, en exploitant tous les points de vue. Son accent est mis sur la sécurité multilatérale et l'ingénierie de besoins orientée vers la réconciliation des exigences contradictoires.

SQUARE (Security quality requirements engineering methodology) est une méthodologie qui définit les exigences de sécurité. Elle est fondée sur les meilleures pratiques dans l'ingénierie des exigences. Elle met en évidence sept différents types de besoins de sécurité : contrôle d'accès, protection physique, politique de sécurité, non-répudiation, récupération du système, détection des attaques et des dispositifs de protection. SQUARE est probablement la méthode intégrant la sécurité d'ingénierie des exigences des processus de développement de logiciels la plus complète (Travis et al, 2010). Toutefois,elle n'est pas fondée sur l'évaluation du risque et ne propose pas de guidage à l'utilisateur.
SIREN (Simple Reuse of Software Requirements) (Toval et al, 2001) vise à l'identification des caractéristiques d'un système et le logiciel qui pourrait être réutilisé pour réduire l'effort de développement. La méthode est fondée sur les exigences réutilisables. Le but du développement avec les exigences réutilisables est d'identifier les systèmes qui pourraient être utilisés (totalement ou partiellement) avec un nombre minimal de modifications, réduisant ainsi l'effort total de développement. Ainsi, si une condition de système est réutilisée, le processus de développement subséquent peut être accéléré. Bien que beaucoup de techniques plus complexes pour la réutilisation des exigences existent, SIREN est une solution simple et pratique.
IRIS (Integrating Requirements and Information Security) est un méta-modèle des exigences de sécurité ayant comme base la réutilisation. La méthodologie est fondée sur quatre sous-modèles :

1-Sous-modèles des **tâches**,

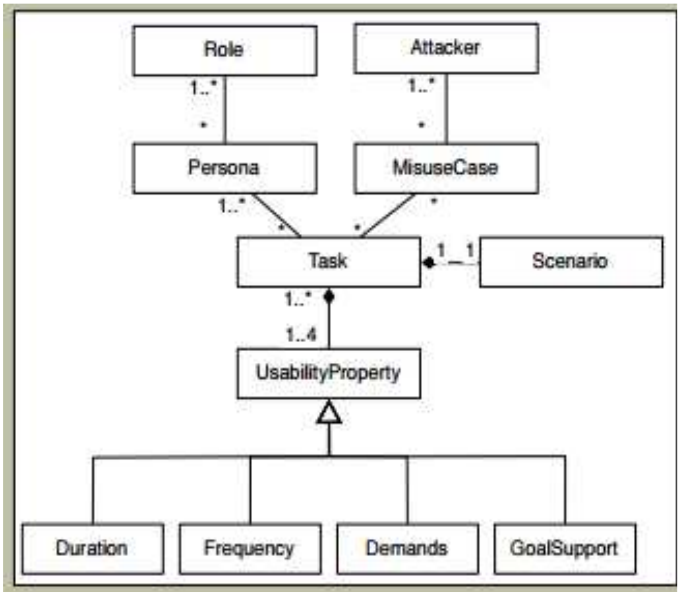


Figure 15 : Sous-modèle des tâches (Shamal et al, 2010).

Ce méta-modèle des tâches identifie les attaquants et les menaces grâce à la caractérisation du rôle alloué aux personnels.Une tâche est composée d'un scénario textuel décrivant comment le personnage réalise un travail associé au système. Chaque tâche agrège une ou plusieurs personnes et, pour chaque personnage associé, des attributs d'utilisabilité sont spécifiés. Ces attributs sont définis du point de vue de la personnalité, et décrivent le degré de la tâche qui répond aux objectifs implicites d'efficacité et de la satisfaction (Shamal et al, 2010).

2- Sous-modèle **d'analyse de risque**,

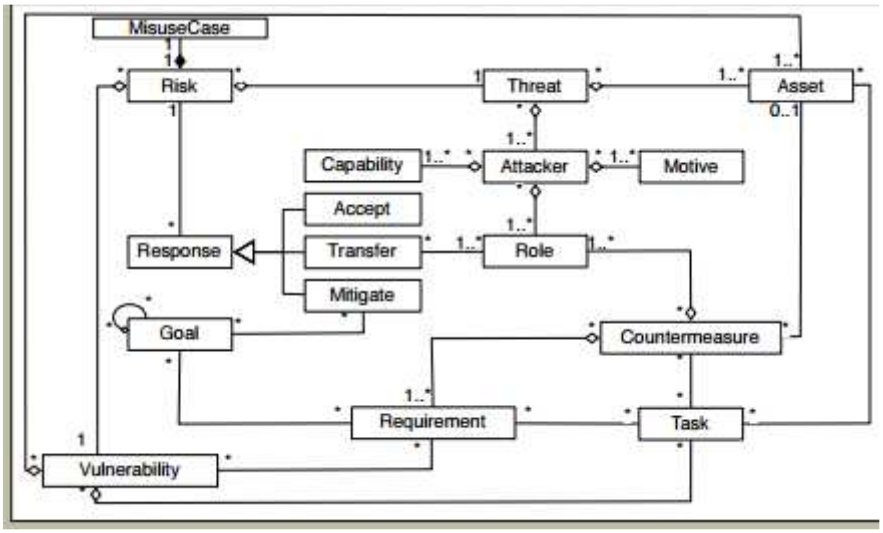


Figure 16 : Sous-modèle d'analyse de risque (Shamal et al, 2010).

Ce méta-modèle incorpore les éléments contribuant à la définition des risques et également les concepts d'atténuation des risques. L'attaquant possède des motivations et profite de la liste des menaces, rôles et capacités qui détiennent. Le risque à des types de traitement de risque (accepte, transfert, et atténue). L'application des exigences pour protéger les vulnérabilités des actifs se traduit par des contre-mesures.

3- Sous-modèle des actifs,

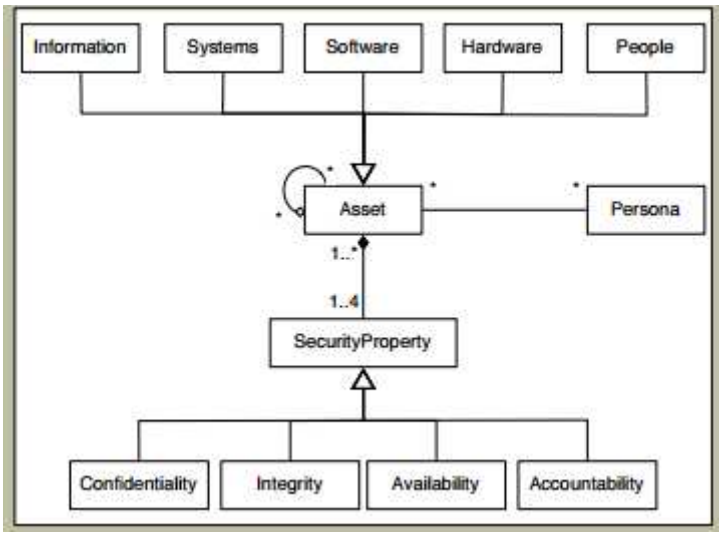


Figure 17 : Sous-modèle d'actif (Shamal et al, 2010).

Ce méta-modèle propose une classification des actifs et montre leurs relations avec les critères de sécurité.

- Sous modèle **d'objectifs** (Goal).

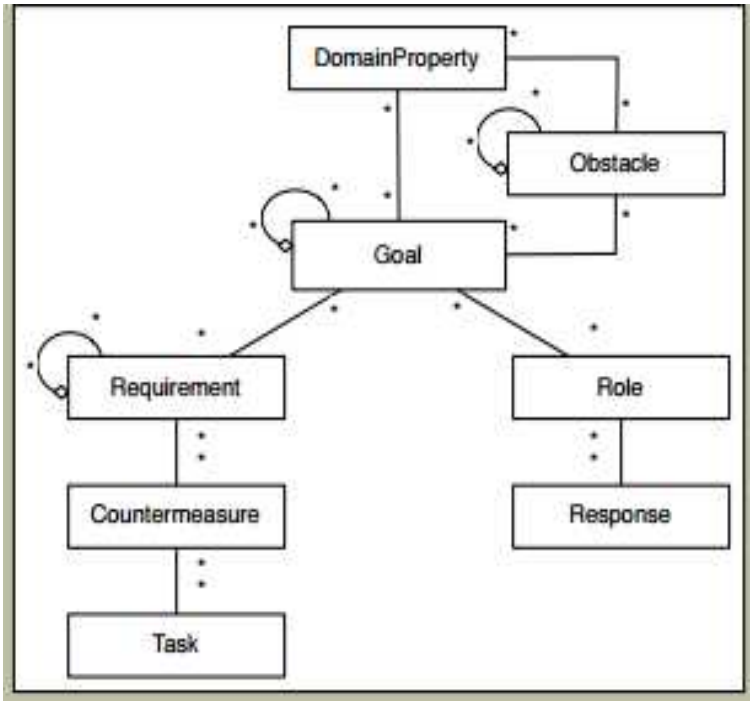


Figure 18 : Sous-modèle d'objectifs(Shamal et al, 2010).

Ce méta modèle explique les relations qui existe entre les objectifs et les autres concepts de la solution.

MOSIS (Modeling Secure Information Systems) (Lammari et al, 2011) est fondée sur l'ingénierie dirigée par les modèles. Il s'agit de construire un modèle de conception du SI et de le dériver successivement à l'aide de règles de transformation. Ces règles opèrent sur des méta-modèles de SI sécurisés. La représentation des propriétés de sécurité nécessitent la possibilité d'intégrer dans ces méta-modèles:

1) Les processus de gestion pour lesquels les SI servent de supports ;
2) Les besoins fonctionnels et non fonctionnels que les SI vont prendre en charge ;
3) La structure de l'organisation dans laquelle le SI est exploitée.

MOSIS est un méta-modèle composé de trois modèles : l'organisation, les processus métiers et les exigences.

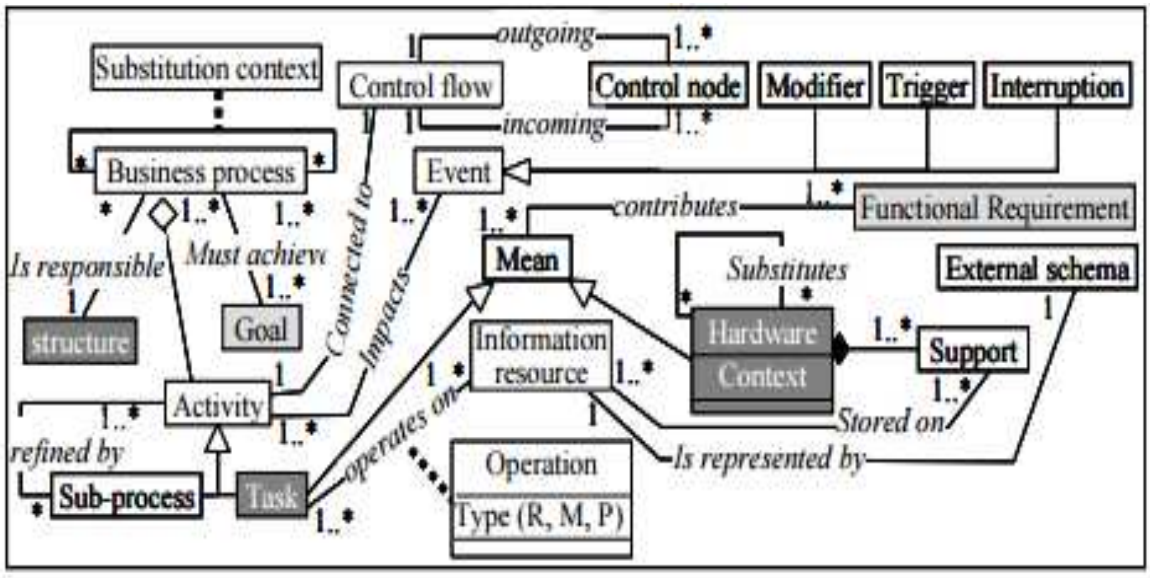


Figure 19 : Méta-modèle MOSIS (Lammari et al, 2011.

Le deuxième groupe de méthodes est composé d'approches fondées sur UML, y compris les Misuse cases (Sindre et al, 2005), les Abuses cases (McDermott et Fox, 1999), SecureUML (Lodderstedt et al, 2002), et UMLsec (Jurjens, 2002).

Misuse cases représente des comportements indésirables qui ont été exclus du système en cours de développement. Cette méthode propose des solutions en rajoutant des nouvelles relations, menace et atténue.

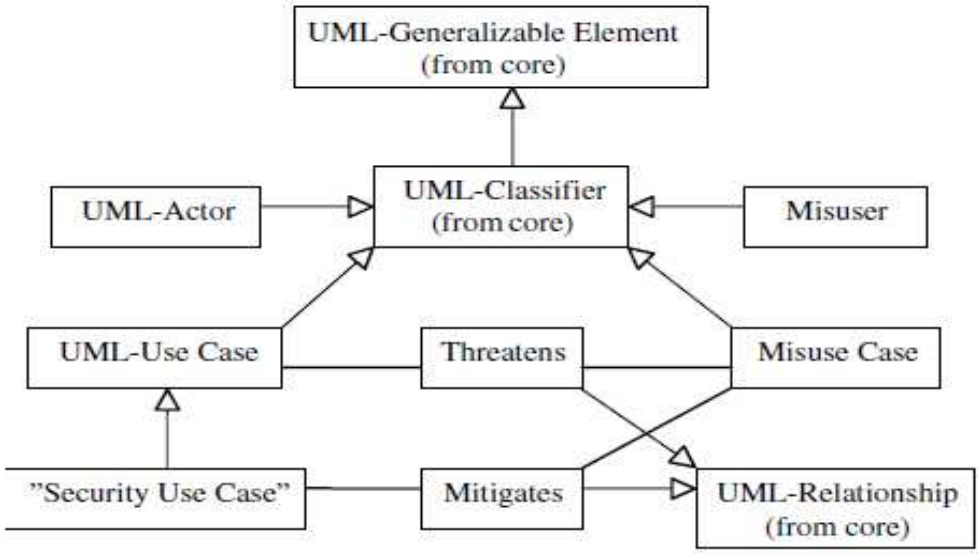


Figure 20 : Méta modèle Misuse cases (Sindre et al, 2005).

Misuse case est une séquence d'actions comprenant des variantes d'un système ou autres entités qui peuvent rentrer en interaction avec l'abuseur et causer un dommage à certains intervenants. L'abuseur est un acteur qui initie misuse case, soit intentionnellement ou non. Le cas d'utilisation atténue les misuse cases. C'est une contre-mesure contre un cas de mauvaise utilisation.

Misuse case menace le cas d'utilisation et exploite les faiblesses du cas d'utilisation est nuit au bon fonctionnement du cas d'utilisation.

Les **Abuses cases** se concentrent sur les interactions néfastes. Cette méthode est utilisée pour montrer l'interaction complète entre un système et un ou plusieurs acteurs, où les résultats de l'interaction sont nuisibles à l'une ou l'autre, l'un des acteurs, ou l'un des intervenants dans le système. L'abus est l'interaction entre un acteur et le système qui résulte un préjudice réel.
Un diagramme des Abuse case utilise les mêmes notations que le diagramme des cas fondés sur UML. L'abuse case est représenté sous forme d'arborescence comprenant :

- La racine qui représente le système ;
- Les feuilles qui représentent les ressources ou les composants du système qui sont les cibles de la cause de l'abus ;
- Les nœuds intérieurs qui représentent les sous-systèmes (applications et individu) ;
- Chaque chemin de la racine à une feuille qui montre que le sous-système, les applications et les classes peuvent être utilisés à mauvais escient afin d'influer sur la feuille et nœud.

SecureUML se concentre sur la conception des politiques de contrôle d'accès fondés sur les rôles afin de répondre aux objectifs de confidentialité et d'intégrité, à l'exclusion de la disponibilité. Ces politiques peuvent être considérées comme des exigences de sécurité. La méthode est une extension du méta modèle d'UML. Les concepts de la politique de contrôle d'accès RBAC[6] sont directement représentés dans ce méta-modèle. Il a été conçu initialement dans le cadre d'une recherche dont l'objet est de proposer une approche garantissant la sécurité dans l'e–commerce. SecureUML se concentre initialement sur le contrôle d'accès.

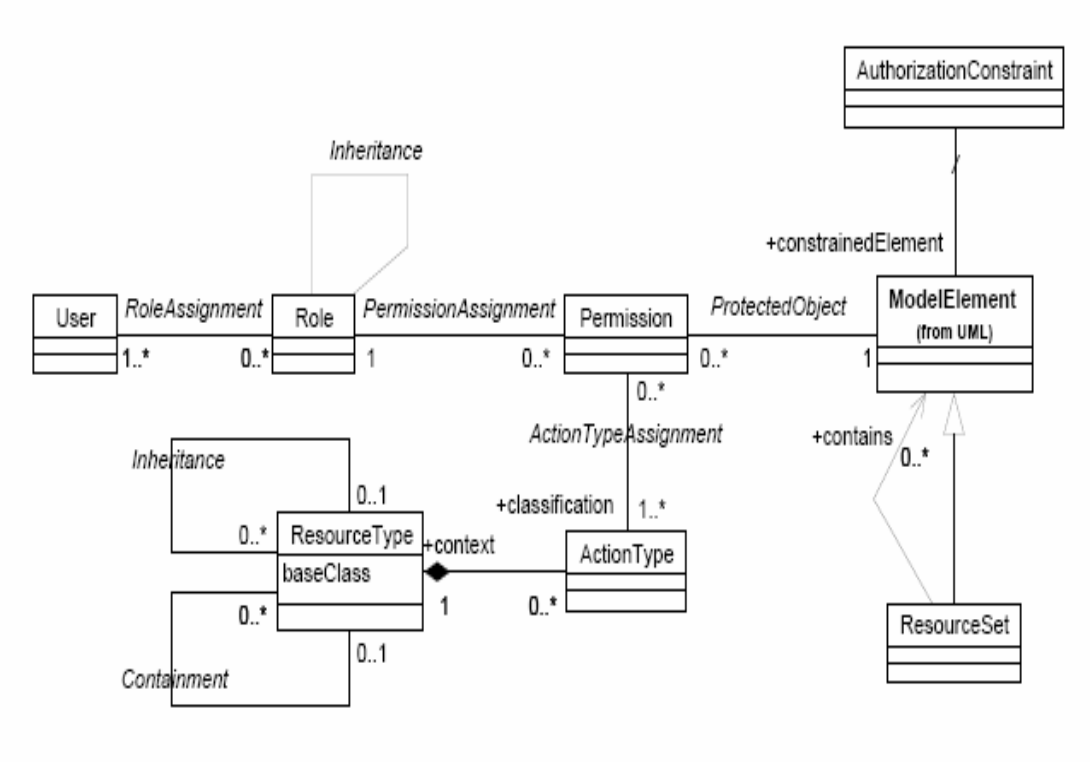


Figure 21 : Méta – Modèle SecureUML (Lodderstedt et al, 2002).

6 RBAC, Modèle de contrôle d'accès fondé sur le rôle auquel l'utilisateur est attaché.

UMLSec est une extension du modèle UML qui autorise l'expression d'informations de sécurité au moyen de diagrammes UML dès la phase de spécification des besoins d'une application. Le profil UMLSec est établi au moyen des trois mécanismes d'extension qui sont les stéréotypes, les valeurs marquées ou TaggedValues (rattachées aux stéréotypes) et les contraintes qui servent à raffiner la sémantique des éléments stéréotypés.

Bien qu'intéressantes, ces approches nécessitent la plupart du temps une maîtrise du langage qui leur est associé.

Le troisième groupe de méthodes comprend des approches axées sur les buts tels que KAOS (Matulevičius et al, 2007), Secure i *(Yu et al, 2006), Secure Tropos (Matulevicius et al, 2008), et GBRAM (Anton et al, 2000).

KAOS (Keep All Objectives Satisfied) est une méthode d'ingénierie des exigences qui résulte des travaux de recherche menés à l'Université de Louvain, en collaboration avec l'Université d'Oregon. KAOS est une méthode d'élicitation et de spécification des besoins fonctionnels et non fonctionnels, incluant la sécurité. L'élicitation des besoins se fait par raffinement des buts (goals). Le résultat de ce raffinement est une instanciation du méta-modèle des buts. D'autres diagrammes sont aussi utilisés pour la spécification des besoins, laquelle est décrite à l'aide du diagramme des cas d'utilisation UML. Ce dernier est obtenu au moyen du mécanisme d'opérationnalisation des buts. Notons que, bien que KAOS offre la possibilité de décrire dans le modèle des buts, les buts fonctionnels, les buts de sécurité ainsi que les attributs, elle ne propose cependant qu'un algorithme de traduction des besoins fonctionnels en cas d'utilisation. Elle ne permet pas de dériver les cas de sécurité.

SECURE I * est une extension de i * framework. Elle se concentre sur l'alignement des exigences de sécurité avec d'autres exigences fonctionnelles et non fonctionnelles. L'approche est fondée sur un méta-modèle de concepts de sécurité contenant quelques notions importantes et leurs relations. Les notions importantes sont : les acteurs, les actifs, les menaces et les vulnérabilités qui ne peuvent pas être représentées par les notations de modélisation de i *. Les acteurs sont des entités qui ont (ou cherchent) des objectifs de sécurité. Ces derniers sont l'expression de la décision de traiter les menaces selon des modalités prescrites. Les acteurs peuvent posséder ou déléguer l'autorisation d'utilisation des actifs à d'autres acteurs.

SECURE TROPOS est une approche fondée sur TROPOS, une méthodologie décrivant la relation entre les systèmes de contexte et d'informations organisationnelles. Elle adopte le i* modèle comme une référence pour la modélisation des acteurs, des objectifs, des ressources, des tâches et des relations entre eux. Il permet le développement de logiciels sécurisés. À cette fin, elle utilise les notions d'acteur, but, Soft-but, tâche, ressource, contrainte de sécurité, objectif sécurisé, tâche sécuriser, et des ressources sécurisées.

GBRAM (Goal-Based Requirements Engineering Analysis Method) est une méthode d'analyse des besoins fondée sur des objectifs en utilisant les buts (Goals) et les scénarios pour formuler des politiques de sécurité grâce à un ensemble de questions standard. GBRAM compte deux activités : l'analyse des buts et le raffinement des buts. L'analyse des buts consiste à explorer les sources d'information pour identifier les buts, les organiser et les classifier. L'intérêt de GBRAM est qu'elle fait la distinction entre les buts de réalisation (les buts fonctionnels) et les buts de maintenance (les buts non-fonctionnels). L'activité de raffinement de buts quant à elle concerne l'évolution des buts à partir du moment où ils sont

identifiés jusqu'au moment où ils sont traduits en exigences opérationnelles. Tout au long de l'activité de raffinement de buts, GBRAM définit la relation de précédence qui consiste à trouver les buts qui précèdent les autres. Tous les concepts de GBRAM (buts, agents, parties prenantes...) sont spécifiés seulement sous une forme textuelle dans des schémas de buts, sans qu'ils ne fournissent aucune notation graphique.

Le quatrième groupe de méthodes utilise des approches à base des abuses frames, y compris abuse frames (Lin et al, 2003), SEPP (Hatebur et al, 2007), et SREF (Haley et al, 2008).

Abuse frames est une méthode qui correspond aux anti-exigences. Ces dernières expriment les intentions d'un utilisateur malveillant, tandis que l'abuse frames représente l'analyse des menaces de sécurité encourues.

SEPP (Security Engineering Process using Patterns) est un processus d'ingénierie de sécurité fondée sur les frameworks de problèmes de sécurité. Ces frameworks sont disposés dans un système de modèle, ce qui permet de structurer, de caractériser, analyser et résoudre les problèmes de sécurité et logiciels du système.

SREF (Security Requirements Engineering Framework) est une approche fondée sur la construction d'un contexte pour le système en utilisant une notation orientée problème afin de représenter les besoins de sécurité, et pour développer et évaluer les arguments de satisfaction pour les besoins de sécurité. SREF est un processus comptant quatre étapes intégrant les exigences ordinaires et les exigences de sécurité.

Le cinquième groupe de méthodes est composé d'approches fondées sur l'analyse des risques, y compris Tropos Goal-Risk Framework (Asnar et al, 2007), et ISSRM (Mayer, 2009).

Tropos Goal-Risk Framework évalue les risques en tenant compte des relations de confiance qui peuvent exister entre les acteurs. La confiance est définie comme « probabilité subjective qui définit l'attente d'un acteur sur le comportement rentable d'un autre acteur". L'objectif de Tropos Goal-Risk Framework est d'évaluer le risque d'événements incertains sur les stratégies d'organisation et d'évaluer l'efficacité des traitements. A cette fin, elle a étendu la méthode Tropos en rajoutant trois (03) couches à l'existant, et qui sont : l'objectif, l'événement et le traitement.

Enfin, l'objectif de la méthode **ISSRM** (Information Risk Management Security System), est de proposer un processus d'analyse des risques qui est composé de six (06) étapes (Mayer et al, 2008) :

- Étude du contexte et des actifs de l'organisation cible : dans cette étape, l'organisation et son environnement sont décrits en une description globale du système d'information réalisé ;
- Détermination des objectifs de sécurité : les objectifs de sécurité sont le plus souvent définis en matière de critères de sécurité des actifs ;
- Analyse des risques : identifie quels risques portent atteints aux actifs 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/CEI Guide 73, 2002) une fois que les risques sont évalués au regard des objectifs de sécurité définis lors de l'étape précédente ;

- Traitement de risque : dans cette étape on associe un type de traitement au risque (le réduire à l'aide de contrôles sur le SI ou le transférer à un tiers,……) ;
- Les exigences sont finalement instanciées en contrôles de sécurité, c'est-à-dire des contre-mesures spécifiques au SI ;
- Implémentation des exigences de sécurité au sein de l'organisation (Mayer et al, 2008).

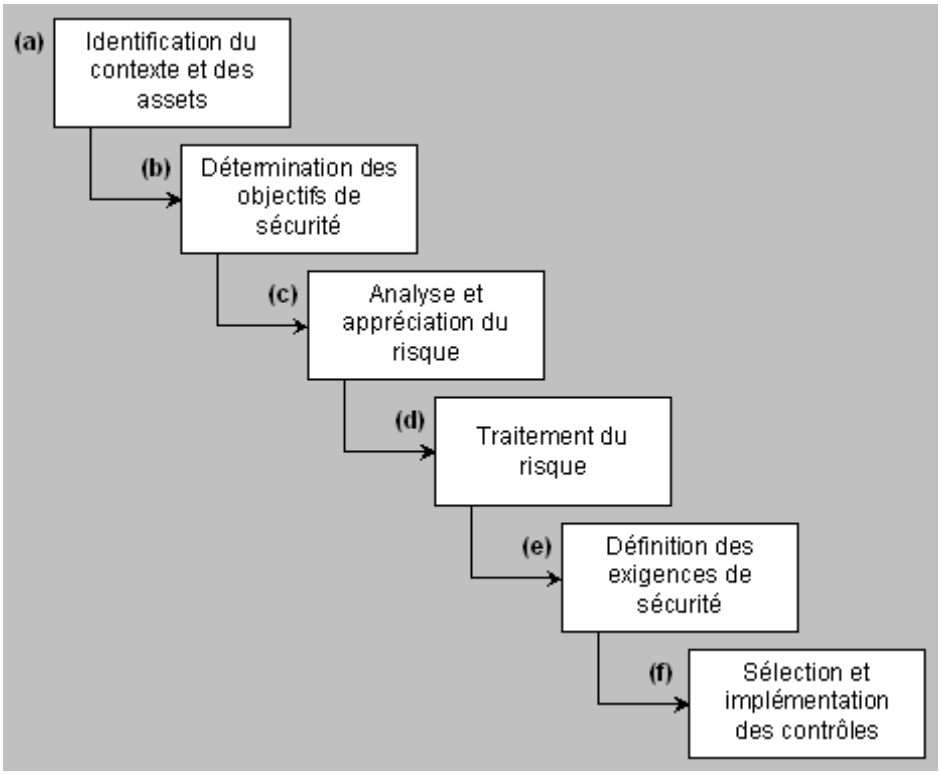


Figure 22 : Processus ISSRM (Mayer et al, 2008).

Enfi, le dernier groupe de méthodes est composé d'approches fondées sur des critères communs, dont CC (Common Criteria, 2012) et SREP (Mellado, 2006).

CC est l'abréviation de critères communs pour l'évaluation de la sécurité de la technologie de l'information. C'est une norme internationale (ISO/CEI 15408) pour l'évaluation des produits de sécurité de l'information menant à une certification de la sécurité. La méthode se compose de lignes directrices et de spécifications, assurant un ensemble de standards et d'exigences de sécurité et un niveau d'assurance de la sécurité.

SREP (Security Requirements Engineering Process) met l'accent sur le développement des dimensions de la sécurité au début de la phase de développement dans le cycle de vie du SI. Comme indiqué par les auteurs, "il décrit comment intégrer des critères communs dans le modèle du cycle de vie du SI ainsi que l'utilisation des ressources référentielles de sécurité ".

Nous avons présenté dans les sous-chapitres précédents les techniques et les différentes méthodologies particulières et nous avons fait état de l'efficience de leurs concepts et processus de gestion des risques. Il semble évident de capitaliser sur les référentiels de connaissances et les données pertinentes pour construire les ontologies prévues comme base de notre solution.

Dans la section suivante, nous procédons à la comparaison des méthodes présentées dans notre état se l'art pour faire ressortir les points positifs et les faiblesses en matière de guidage dans la dérivation des exigences de sécurité.

II.3 Comparaison

Le but de ce paragraphe est d'examiner avec attention notre état de l'art et de présenter une comparaison générale permettant de mettre en exergue les avantages et les limites des méthodes présentées. Soulignons le fait que certaines comparaisons ont fait l'objet de publications dans la littérature spécialisée et dont les principaux résultats sont présentés ci-dessous.

1) **Comparaison des méthodes d'analyse de risque** :

(Vorster et al, 2005) et (Behnia, 2012) proposent respectivement une enquête et un framework pour comparer les différentes méthodologies d'analyse des risques. (Tomhave, 2014) a analysé plusieurs méthodes d'analyse des risques, y compris l'ISO /CEI 31000, COBIT 5, MAGERIT, NIST SP 800-30, OCTAVE et FAIR. Dans leurs travaux, ils ont utilisé plusieurs critères afin de comparer ces méthodes, notamment le type, le coût, le fait qu'elle soit outillée ou non, les compétences spéciales requises, la flexibilité, le temps de monter en puissance. Cette comparaison avait pour but de guider les utilisateurs dans le choix d'une des méthodes étudiées.

(Ionita, 2013) présente et compare une liste exhaustive de méthodes qui ont été inventoriées par l'Agence européenne de sécurité des réseaux et de l'information (European Network and Information Security Agency, 2013) et par plusieurs auteurs dont (Zambon et al, 2011). Les critères de comparaisons utilisés sont : l'identification de la phase d'utilisation de la méthode, la date de sortie, la répartition géographique, le modèle conceptuel correspondant, etc.).

En ce qui nous concerne, nous avons comparé les méthodes d'analyse de risque du point de vue de notre problématique (guidage par rapport au cycle de développement du SI, base de connaissances utilisée par les méthodes pour l'identification des risques, méthode d'estimation du risque et l'artefact utilisé pour l'identification des risques). Le tableau ci-dessous présente cette comparaison :

Nom	Type d'évaluation du risque	Fondement	Base de connaissances	Cycle couvert	Artefact utilisé
EBIOS	Quantitative	ISO/CEI 15408, 27005 et ISO 31000	Type de sources de menaces Type d'impacts Type d'actifs supports Menaces et vulnérabilités génériques Mesures de sécurité génériques	**	Processus
MEHARI	Quantitative	ISO/CEI 27001, 27002,27005	Actifs secondaires Scénarios de Risques Mesures de sécurité	**	Processus
OCTAVE	Quantitative	ISO 31010	Type d'actifs Vulnérabilités Menaces	**	Processus
CRAMM	Qualitative	BS7799 ISO/CEI 27001, 27002	Actifs Vulnérabilités Menaces	*	Processus
RMF	Qualitative	NIST Special Publication 800-39	/	*	Processus
FTA	Qualitative	/	/	*	Processus Arbre
FMECA	Quantitative	/	/	*	Processus
HAZOP	Qualitative	/	Menaces	*	Processus
MAGERIT	Qualitative Quantitative	ISO 31000	Scénario de risques	*	Processus
FAIR	Qualitative	ISO/CEI 27001	Actifs Menaces	**	Processus Taxonomie
COBIT	/	ISO / CEI 20000 ISO/CEI 27001	/	/	Processus
ITIL	/	ISO / CEI 20000	/	/	Processus
Risk IT	Qualitative	ISO 31000	Risques	*	Processus
CORAS	Qualitative Quantitative	AS/NZS 4360 ISO 31000	Actifs Risques	**	Processus Langage graphique
ISAMM	Quantitative	ISO/CEI 27001	Actifs Menaces	*	Processus
NIST	Qualitative	/	/	*	Processus
FRAP	Qualitative	/	Risques	**	Processus
SRA	Quantitative	/	Risques	*	Processus
TARA	Qualitative	/	Agents d'attaques Objectifs de sécurité	*	Processus

Tableau 3 : Comparaison des méthodes d'analyse de risques

**: Couverture limitée à une seule phase de développement.*

***: Couverture deux ou plusieurs phases de développement, mais pas la totalité.*

En résumé, le tableau de comparaison nous amène au constat suivant :

- **Absence**
    - ❖ d'approche couvrant le cycle de développement en totalité.
- **Diversité**
    - ❖ des bases de connaissances pour identifier les risques;
    - ❖ des fondements sous-jacents aux méthodes d'analyse de risque;
    - ❖ des types d'évaluation du risque.

2) **Comparaison des méthodes d'élicitation des exigences de sécurité** :

(Moffett et al, 2004) ont fait une distinction entre le noyau d'élicitation des exigences de sécurité et les artefacts de soutien. Les noyaux d'élicitation des exigences consistent en actifs, menaces et principes de contrôle. Les contrôles sont constitués d'objectifs, d'exigences, et des composants du système et de la structure.
(Firesmith, 2003a) propose une taxonomie qui conduit à un modèle d'information. Cette taxonomie est utilisée par (Fabian et al, 2010) comme un modèle comparatif pour les concepts fondamentaux utilisés dans leur framework.
Une autre comparaison sur les méthodes d'exigence de sécurité peut être trouvée dans (Salini et al, 2008). Cette comparaison se concentre principalement sur les méthodes de gestion des risques en mettant l'accent sur une conformité aux Critères Communs.
(Tondel et al, 2008) propose une comparaison sur les méthodes d'exigence de sécurité. Toutefois, la portée est limitée.
(Souag et al, 2013) présente une étude de cartographie systématique des ontologies d'exigences de sécurité et de leur utilisation pour la définition des besoins de
sécurité. Ces ontologies incluent des méthodes de risque ainsi que les approches d'exigences de sécurité. Une liste des exigences de sécurité des approches est présentée par la plupart des auteurs cités ci-dessus.

En ce qui nous concerne, nous présentons dans le tableau suivant la comparaison des méthodes d'élicitation des exigences de sécurité, en utilisant les critères suivants : source d'élicitation des exigences utilisées par ces méthodes, la couverture de leur guidage par rapport au cycle de développement du SI, ainsi que les artefacts utilisés.

Nom	Élicitation des exigences de sécurité	Cycle couvert	Artefact utilisé
SecureUML	Patterns de sécurité	*	Méta Modèle
UMLSec	Patterns de sécurité	*	Méta Modèle
Misuse Cases	Base de connaissances des menaces	*	Modèle Processus
Abuse Cases	Base de connaissances des menaces	*	Modèle Processus
MSRA	/	*	Processus
SIREN	Patterns de sécurité	*	Processus
MOSIS	Patterns de sécurité	*	Méta modèle
IRIS	Patterns de sécurité	*	Méta modèle
GBRAM	/	*	Représentation textuelle
Secure Tropos	/	**	Langage Notation graphique
Secure I*	/	*	Langage
KAOS	/	*	Langage
ISSRM	Base de connaissances menaces et vulnérabilités	**	Processus Méta modèle
Abuses frames	Scénarios de menaces	**	Référentiel
SEPP	Patterns de sécurité	*	Référentiel
SREF	Référentiel de sécurité	*	Processus
Tropos Goal-Risk Framework	Référentiel de sécurité	*	Langage Notation graphique
CC	Patterns de sécurité	**	Processus
SREP	Patterns de sécurité	**	Processus

Tableau 4 : Comparaison des méthodes d'élicitation des exigences de sécurité.
**: Couverture limitée à une seule phase de développement.*
***: Couverture deux ou plusieurs phases de développement, mais pas la totalité.*

En résumé, le tableau de comparaison nous amène au constat suivant :

- **Absence**
  - ❖ d'approche couvrant le cycle de développement en totalité.
- **Diversité**
  - ❖ des sources utilisées pour l'élicitation des exigences de sécurité;
  - ❖ des artefacts utilisés pour éliciter les exigences de sécurité.

Nous avons présenté jusqu'à maintenant une comparaison de chaque famille de méthodes dans leurs spécialités respectives (analyse de risque et l'élicitation des exigences de sécurité). Dans le tableau qui suit, nous proposons une comparaison sur la base des critères suivants (qui représentent les limites des méthodes présentées dans l'état de l'art) :

- Passage des risques vers les exigences de sécurité ;
- Guidage (voir partie définition Chapitre II).

Nom	**Guidage**	**Passage des risques vers les exigences de sécurité**
SecureUML	*	/
UMLSec	*	/
Misuse Cases	*	/
Abuse Cases	*	/
MSRA	*	/
SIREN	*	/
MOSIS	*	/
IRIS	*	/
GBRAM	*	/
Secure Tropos	**	/
Secure I*	*	/
KAOS	*	/
ISSRM	**	Partiel et informel
Abuse frames	*	/
SEPP	*	/
SREF	*	/
Tropos Goal-Risk Framework	*	Partiel et informel
CC	**	Partiel et informel
SREP	**	Partiel et informel
EBIOS	*	Partiel et informel
MEHARI	*	Partiel et informel
OCTAVE	*	Partiel et informel
CRAMM	*	/
RMF	*	/
FTA	*	/
FMECA	*	/
HAZOP	*	/
MAGERIT	*	Partiel et informel
FAIR	*	Partiel et informel

COBIT	/	/
ITIL	/	/
Risk IT	*	/
CORAS	*	/
ISAMM	*	/
NIST	*	/
FRAP	*	/
SRA	*	/
TARA	*	/

Tableau 5 : Comparaison des méthodes de l'état de l'art par rapport à notre problématique.
**: Guidage faible **: Guidage moyen*

Notons que quelques méthodes ont tenté d'établir un lien entre l'analyse des risques et l'elicitation des exigences de sécurité. C'est le cas de la méthode ISSRM qui tente un alignement avec des méthodes d'élicitation des exigences telles que : Secure Tropos, Misuse Cases, SecureUML, Mal activity, KAOS [(Matulevicˇius et al, 2008) (Soomro et al, 2012), (Chowdhury, 2012), (Chowdhury, 2014), /(Graa and al, 2011]. Cependant, en plus du fait que ces méthodes exigent de l'utilisateur une maîtrise de la notation, elles héritent du même niveau de guidage que les méthodes d'origine, sauf la dérniere approche ou elle rajoutait un niveau de guidage de plus afin d'obtenir les règles de politiques de sécurité.

En résumé, notre étude de l'état de l'art fait ressortir le constat suivant :

- **Absence**
  - ❖ de guidage total pour l'élicitation des exigences de sécurité;
  - ❖ de règles de passage entre les risques encourus et les exigences de sécurité qui les couvrent;
  - ❖ d'approche couvrant le cycle de développement en totalité.
- **Diversité**
  - ❖ des sources utilisées pour l'élicitation des exigences de sécurité;
  - ❖ des artefacts utilisés pour éliciter les exigences de sécurité;
  - ❖ des bases de connaissances pour identifier les risques;
  - ❖ des fondements sous-jacents aux méthodes d'analyse de risque;
  - ❖ des types d'évaluation du risque.

Dans le chapitre qui suit, nous présentons notre approche globale de dérivation des exigences de sécurité à partir de l'analyse des risques.

Chapitre III

Approche de dérivation des exigences de sécurité à partir de l'analyse des risques

III. Approche de dérivation des exigences de sécurité à partir de l'analyse des risques

III. 1 Notre approche

La sécurisation du système d'information est fondamentale pour permettre son exploitation dans des conditions optimales et par-delà, assurer sa pérennité. Notre démarche se positionne dans cette vision en proposant un mécanisme de guidage suggestif qui permet d'obtenir un plan d'exigence de sécurité à partir des sources fournies par l'entreprise. À notre connaissance et d'après le résultat de nos recherches, il n'y a pas d'approche offrant un tel mécanisme de guidage. Comme nous pouvons le constater dans les paragraphes qui suivent, le passage en revue des nombreuses contributions sur la sécurité des systèmes d'information démontre que celles-ci se concentrent majoritairement sur les aspects techniques de la question. Plusieurs approches traitent le sujet de façon fragmentaire et proposent l'extraction à un haut niveau d'abstraction des exigences de sécurité.

(Fabian et al, 2010) propose une synthèse complète des approches des exigences de sécurité (SRE) par rapport aux menaces et aux risques. (Schmidt, 2009) intègre l'environnement comme la connaissance du domaine, améliorant ainsi la définition de SRE personnalisé. (Gandotra et al, 2009) décrit une nouvelle technique, nommée technique hybride, qui combine les cas d'abus et les arbres d'attaques pour aider à identifier les menaces et les représenter dans les exigences de sécurité. Une fois identifiées, les menaces sont prioritaires et les techniques d'atténuation peuvent être définies comme des exigences de sécurité concrètes. (SANS Institute, 2003) propose un modèle (Capability Maturity- CMM) pour l'obtention des exigences de sécurité. Ce modèle est composé de cinq niveaux et de onze zones de traitement. L'évaluation de la maturité de ces zones de traitement est l'un des résultats de ce modèle. Pour chaque zone de traitement, un ou plusieurs objectifs sont définis. (Haley et al, 2006) met l'accent sur les jointures nécessaires entre les exigences de sécurité fonctionnelles et non-fonctionnelles. (Soler, 2008) décrit un modèle d'exigence de sécurité pour l'entreposage a base des rôles, les niveaux de sécurité et les compartiments de sécurité de l'utilisateur.

Parmi les méthodes décrites dans notre état de l'art principal (voir chapitre **II**), EBIOS propose de déduire les exigences de sécurité en fonction du contexte général de l'organisation, mais sans totalement en faire la liaison directe avec l'analyse des risques. La relation entre l'analyse des risques et les exigences de sécurité est souvent mentionnée dans cette méthode sans pourtant qu'elle propose un lien formel. (Van Lamsweerde, 2004) propose une approche axée sur les obstacles malveillants, appelés anti-objectifs, considérés comme des menaces pour les objectifs de sécurité. Les exigences de sécurité sont obtenues comme des contre-mesures en tenant compte des anti-exigences et vulnérabilités. (Naved, 2014) fournit une approche d'analyse des processus métiers pour obtenir les exigences de sécurité. (Allen et al, 2012) décrit une approche qui permet aux organisations de tirer des mesures de sécurité pour les logiciels à partir des pratiques standards en matière de sécurité de l'information. (Wagner et al, 2009) propose un modèle de sécurité Web spécifiant les exigences de sécurité au début du développement du système, en utilisant des mécanismes de réutilisation. Enfin, (Hernandez-Ardieta et al, 2012) propose une méthodologie permettant la construction de « cibles de sécurité contenant un problème de sécurité précis et les exigences de sécurité qui neutralisent les menaces identifiées ».

Malgré l'apport important de ces contributions dans le traitement de ce domaine sensible, nous constatons qu'aucune d'elles ne fournit une aide tangible pour la dérivation des exigences de sécurité à partir des sources d'information.

Ce chapitre décrit notre approche. Dans cette démarche, nous proposons un mécanisme de guidage suggestif qui nous permet d'obtenir un plan d'exigence de sécurité d'entreprise à partir des rapports d'audits (s'ils existent) ou des cahiers des charges de conception du SI. Pour cela, nous avons conçu :

- Un processus de dérivation des plans d'exigences de sécurité pour les entreprises composée de trois phases (phase de contexte, phase d'analyse des risques et phase de dérivation des exigences de sécurité),
- Un méta modèle de sécurité,
- Quatre ontologies (contexte, actifs, risques et exigences de sécurité),
- Une liste des scénarios de risques extraits de notre état de l'art,
- Un modèle de construction d'un scénario de risque,
- Des fiches de caractérisation des concepts des ontologies,
- Des règles de correspondance entre les ontologies des risques et des exigences de sécurité. Ces règles sont représentées dans une base de connaissances résultant des meilleures pratiques dans le domaine de la sécurité. Elles aident à assurer la cohésion de l'alignement sémantique entre les ontologies des risques et des exigences de sécurité.

Nous présentons ci-dessous les grandes lignes de notre démarche. L'approche détaillée est décrite au dans le sous chapitre **III.9**.

III.2 Processus de dérivation des plans d'exigences de sécurité

Nous proposons un mécanisme de guidage suggestif qui nous permet d'obtenir un plan d'exigence de sécurité d'entreprise à partir des rapports d'audits (s'ils existent) ou de cahiers des charges de conception du SI.

Le processus de dérivation des plans d'exigences de sécurité est composé de trois (03) phases, chaque phase est décomposée en plusieurs étapes : (voir figure **23**)

1- Phase d'analyse du contexte ;

- Identification et extraction des éléments du contexte et des actifs de l'entreprise,
- Détermination des critères de sécurité associés aux actifs de l'entreprise.

2- Phase d'analyse des risques

- Identification des scénarios de risques
- Identification des risques,
- Caractérisation des risques.

3- Phase de dérivation des exigences de sécurité

- Dérivation des exigences de sécurité,
- Caractérisation des exigences de sécurité.

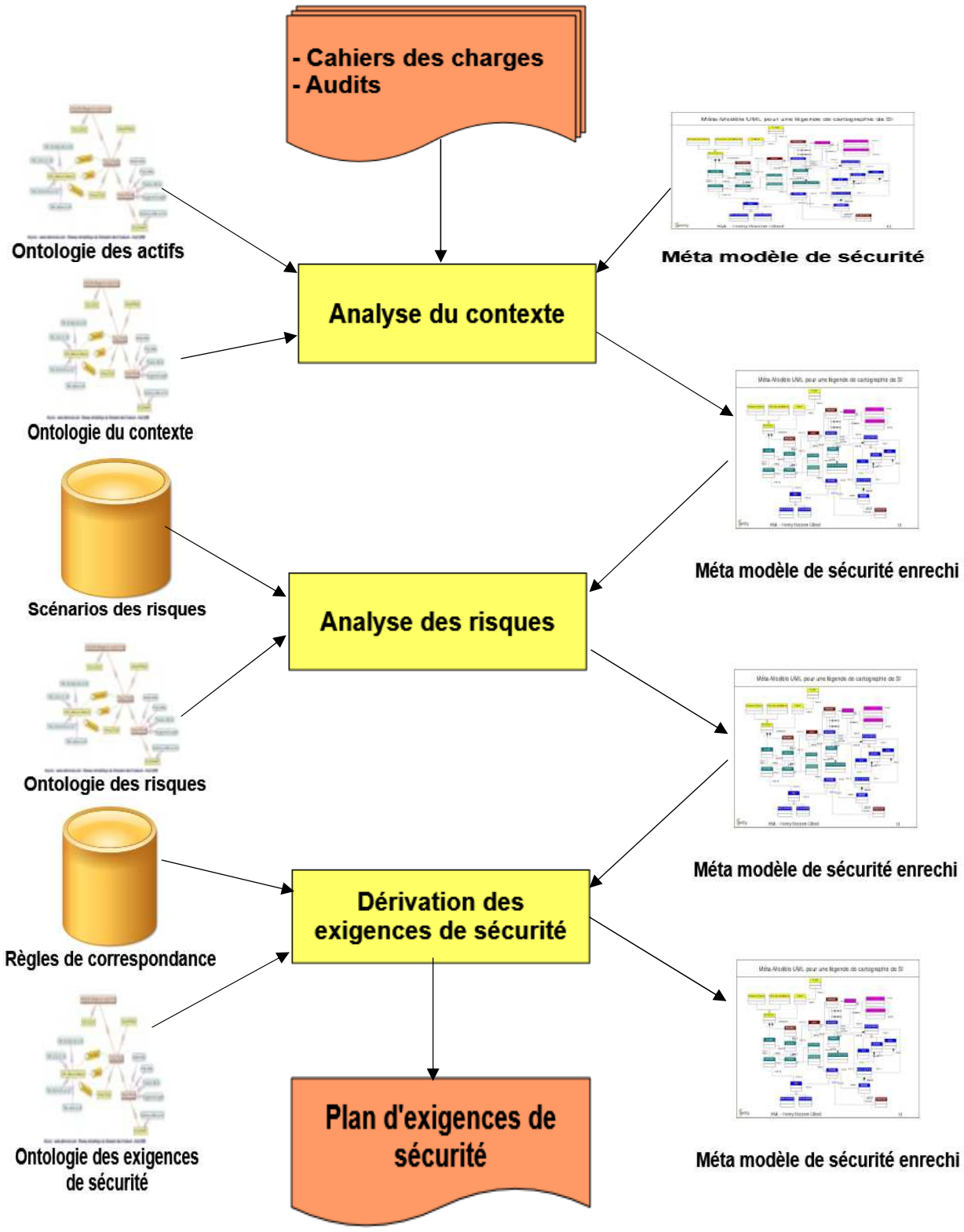


Figure 23 : Processus de dérivation des exigences de sécurité.

III.3 En quoi c'est différent des autres approches

Nous procédons dans notre approche à l'extraction de toutes les définitions disponibles dans notre état de l'art principal en utilisant leurs noyaux de sens permettant l'uniformisation du vocabulaire avec l'ambition modeste d'une forte homogénéité dans les usages des termes.

Notre solution prend en compte le contexte de l'organisme.

Notre démarche dérive les exigences de sécurité à partir de l'identification et de l'estimation des risques encourus par l'organisation en prenant en compte les critères de sécurité dès que la phase de spécification des besoins a été lancée. Un guidage est proposé à l'utilisateur dans toutes les phases du processus de dérivation des exigences de sécurité.

L'approche est fondée sur le développement de quatre ontologies à partir de la sélection, l'uniformisation, l'intégration et la mise en conformité des sources d´informations hétérogènes, qui ont été créées ou adaptées pour le traitement de la sécurité des systèmes d´information.

Notre approche réutilise des bases de connaissances existantes dans la littérature spécifique comme les listes des scénarios des risques. L'ajout, la suppression ou la modification d'un nœud ou d'une feuille des ontologies est possible dans notre solution sans pour autant modifier l'approche en totalité.

Dans le cas d'absence des entrées dans notre processus de dérivation, nous pouvons dérouler les scénarios des risques de notre base de connaissances pour obtenir un plan de sécurité générique.

Notre approche propose plus de formalisme que les autres sources et plus de guidage pour la dérivation des exigences de sécurité. Elle crée une nouvelle dynamique en proposant de lier les éléments du contexte d'une organisation au plan de sécurité implémenté.

Enfin, elle réutilise des bases de connaissances existantes, permet de bâtir une politique de sécurité globale qui prenne en compte les opérations d'ajout, de modification et de suppression d'un ou plusieurs concept (s) sans pour autant modifier l'approche en totalité.

III.4 Méta modèle de la sécurité

Le processus de dérivation proposé (figure **23**) démarre par l'obtention des informations nécessaires à la caractérisation de l'organisation.

La première phase prend en compte les concepts suivants :

(1) **Le contexte** : tous que joue un rôle primordial à l'organisation, qu'il soit un contexte interne ou un contexte externe.
(2) **Les actifs :** tout élément représentant de la valeur pour l'organisme.
(3) **Les critères de sécurité** : caractéristiques d'assurances.

La deuxième phase s'articule autour de l'identification du scénario du risque associé à la phase d'analyse du contexte. Le scénario en question inclut un ou plusieurs risque(s). Ce risque-là est identifié et caractérisé. Une fois l'appréciation des risques effectuée, le risque doit être traité, ce qui implique la prise de décision sur le type de traitement de risque, notamment le réduire à l'aide de contrôles sur le SI ou le transférer à un tiers.

La troisième phase consiste à la dérivation des exigences de sécurité afin de mitiger les risques encourus par l'organisme. Au fur et à mesure que l'on exploite cette démarche grâce à la réussite de l'implémentation des exigences de sécurité, on peut avoir des patterns de sécurité sous forme d'un plan de sécurité de l'organisation.

L'ensemble est représenté sous forme d'un modèle de sécurité. Ce modèle est enrichi par les instances de chaque phase du processus de dérivation des exigences de sécurité.

Le méta modèle a été construit sur la base des modèles ontologiques, il peut être partagé en trois groupes de concepts :

(i) Les concepts relatifs à la phase d'analyse du contexte :

Cette partie du méta-modèle est très importante elle nous permet de caractériser les concepts d'une organisation et de déterminer les critères de sécurité des actifs qui l'on compose et au final de lier le plan de sécurité à l'organisation.

(ii) Les concepts relatifs à la phase d'analyse des risques ;

Cette partie exploitée les instances de la phase du contexte dans le méta modèle de sécurité pour construire les scénarios des risques encourus par l'organisation, de ces scénarios en extrait les risques encourus par l'organisme et en associent un type de traitement.

(iii) Les concepts relatifs à la phase de dérivation des exigences de sécurité.

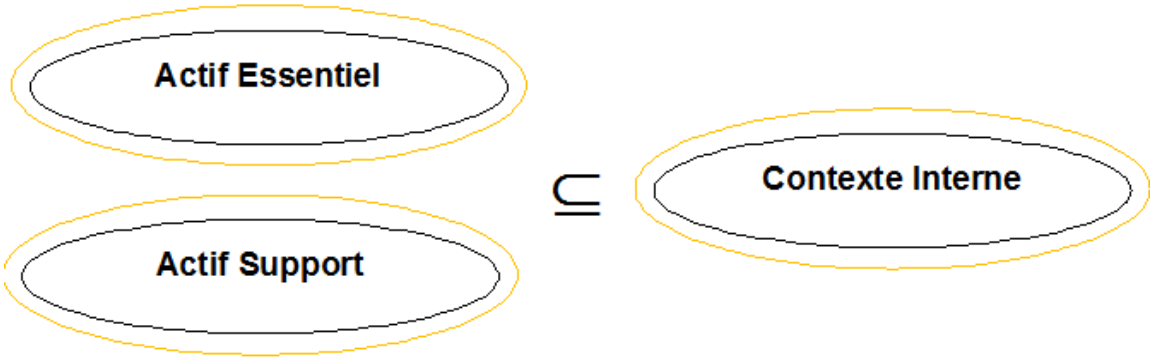
Cette partie consiste au raffinement d'une mesure de traitement du risque pour mitiger le risque. Chaque exigence de sécurité contribue à couvrir un ou plusieurs traitements du risque ciblant le SI. Le plan de sécurité peut être constitué des politiques, des processus, des pratiques ou toute action ou composant du SI et de son organisation qui agit afin de réduire les risques.

Nous présentons, dans la partie suivante nos contributions additionnelles relatives au méta modèle de sécurité en rapport avec notre démarche globale.

- Les vulnérabilités sont des propriétés des actifs supports comme, nous l'avons montré lors de la présentation de notre état de l'art général (EBIOS, MEHARI, …). Toutefois, il faut noter aussi que les vulnérabilités sont une des composantes du risque. Il y a une relation entre le concept de risque et le concept d'actif support qu'on dénomme menace (Menace).
- Les critères de sécurité sont proposés pour les actifs essentiels de l'organisation (voir modèle des actifs ISSRM). Chaque relation possède un poids défini d'après la situation d'exploitation de l'actif essentiel. Cette valeur est tirée des méthodes citées dans notre état de l'art pour la construction de l'ontologie des actifs. (voir chapitre **III.6**)
- Les actifs font partie du contexte. cette affirmation n'apparaît dans aucun document compulsé lors de nos recherches et n'est pas démontrée formellement au sein des concepts étudiés. On dit que l'ensemble des actifs sont inclus dans l'ensemble du contexte, si tous les éléments des actifs sont aussi éléments du contexte.

Actifs ⊆ Contexte si et seulement si Actifs ∩ Contexte = Actifs ;
Actifs ⊆ Contexte si et seulement si Actifs ∪ Contexte = Contexte

Ces deux équations mathématiques sont facilement vérifiables dans notre cas.



- Le contexte joue un rôle prépondérant dans la proposition des exigences de sécurité. A titre d'exemple mentionnons le fait que l'on ne propose pas de créer un département de sécurité informatique (Security Department) pour une petite entreprise agricole de cinq (05) personnes.

Le lien et l'interdépendance entre le contexte et les exigences de sécurité est constatable tout au long du déroulement de nos exemples de validation et également dans le déroulement du cas réel étudié par notre approche.

Du fait que ces deux concepts sont rarement formalisés dans les démarches orientées sécurité et afin de formaliser le lien entre le contexte et les exigences de sécurité, nous rajoutons deux concepts du contexte (ressources, connaissances) dans la fiche de caractérisation des

exigences de sécurité (voit tableau **19**) et nous proposons une association dénommée “influence” dans le méta-modèle de sécurité.

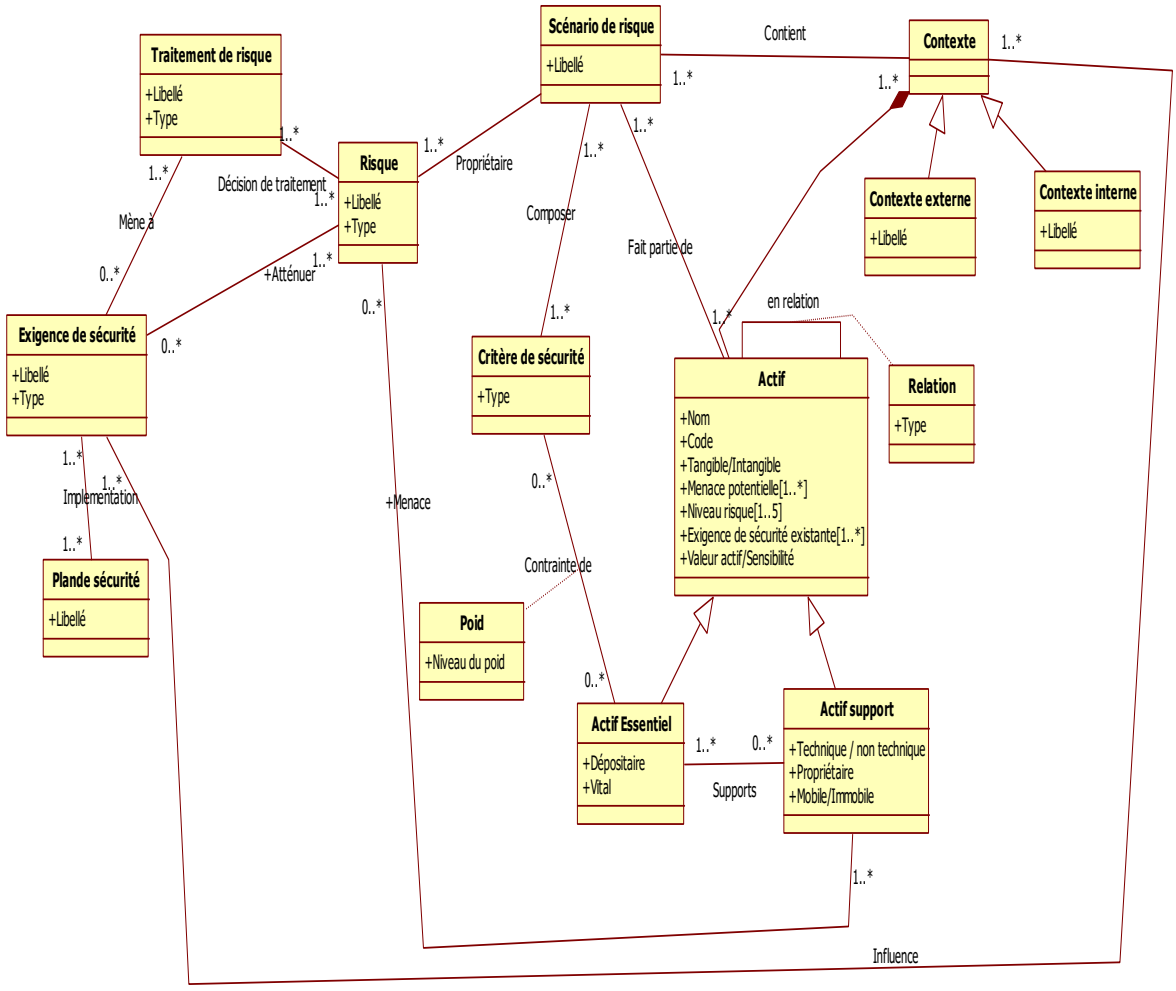


Figure 24 : Méta modèle de sécurité.

III.5 Description détaillée des différentes étapes de l'approche

III.5.1 Construction des ontologies (contexte, actifs, risques et exigences de sécurité)

III.5.1 Construction de l'ontologie

Une ontologie est une relation de concepts permettant de partager un ensemble de connaissances d'un domaine donné. Exploitable par les systèmes informatiques, elle permet d'expliciter et d'interpréter les termes nécessaires pour partager la connaissance liée à ce domaine. Deux types de conception existent :

i) Conception manuelle

Cette conception se base sur des fondements philosophiques et suit des procédés de modélisation collaboratifs. Ils mènent à la conception d'ontologies dites légères et d'ontologies dites lourdes (ces ontologies se distinguent par la présence ou non d'axiomes). Cependant, ce procédé de génération est très coûteux en temps et pose surtout des problèmes de maintenance et de mise à jour.

ii) Conception reposant sur des apprentissages

Face à la masse croissante de documents présents sur le Web et aux avancées technologiques dans le domaine de la recherche d'informations, il existe de nouveaux travaux portant sur la recherche des procédés de construction plus automatiques. Ces mécanismes mènent généralement à la conception d'ontologies dites légères. Dans (Maedche et al, 2001), différents types d'approches sont distingués en fonction du support sur lequel elles se basent : à partir des textes, de dictionnaires, de bases de connaissances, de schémas semi structurés et des schémas relationnels. Les méthodologies de construction d'ontologies les plus connues, sont :

La méthode **KACTUS** (modelling Knowledge About Complex Technical systems for multiple USe) (KACTUS, 1996). Sa mise en œuvre intervient dès la phase de conceptualisation d'une nouvelle application. L'ontologie qui suit la phase de développement représente les connaissances structurées de l'application. La méthode donne la possibilité de réutiliser d'autres ontologies existantes. Elle repose sur trois phases :

Phase 1 : Extraction des termes et des tâches à effectuer ;

Phase 2 : Organisation des termes en concepts, relations, attributs, etc..

Phase 3 : Hiérarchisation des connaissances en passant par un affinement.

La méthode **METHONTOLOGY** (Fernández-López et al, 1997) s'applique à clarifier les différentes phases de la construction en respectant les activités de gestion de projets, de développement et des activités de support.

La phase de spécification permet de fournir le domaine, les limites et le but de l'ontologie. Lors de la phase d'acquisition des connaissances, la liste des sources de connaissance est obtenue. Cette phase fournit une description de la façon de réaliser l'acquisition des connaissances. La phase de conceptualisation est consacrée à la description du problème et de ces solutions. Elle conceptualise les connaissances acquises. La phase d'intégration permet la réutilisation des définitions déjà intégrées dans d'autres ontologies en évitant de repartir de zéro. Enfin, une évaluation est effectuée afin d'éviter d'éventuelles erreurs. La figure **25** présente le processus de la méthode.

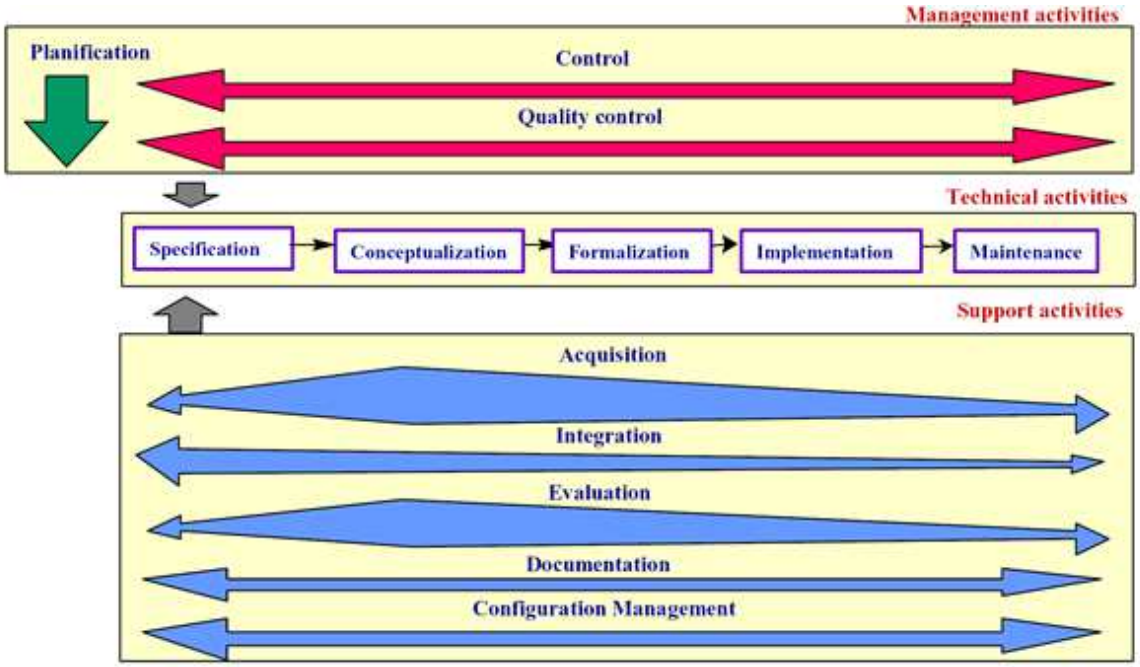


Figure 25 : METHONTOLOGY-Processus de développement d'ontologie (Fernández-López et al, 1997).

La méthode **On-To-Knowledge** (Staab, et al, 2001) tient compte du domaine d'application de l'ontologie en construction. La figure **26** représente le processus de la méthodologie. Cette dernière se présente en cinq étapes. La première étape porte sur l'identification du problème à résoudre alors que les quatre dernières portent sur le développement de l'ontologie :

- Étape 1 : Étude de faisabilité : identifier le problème, les opportunités et les solutions potentielles ;
- Étape 2 : Phase de Kickoff : spécification des besoins de l'ontologie ;
- Étape 3 : Raffinement :
  - Raffiner la taxonomie et extraire les axiomes ;
  - Implémenter l'ontologie.

- Étape 4 : Évaluation

- Vérifier les spécifications des besoins (étape 2);
- Tester l'ontologie dans le cadre de son environnement d'application.

- Étape 5 : Maintenance de l'ontologie.

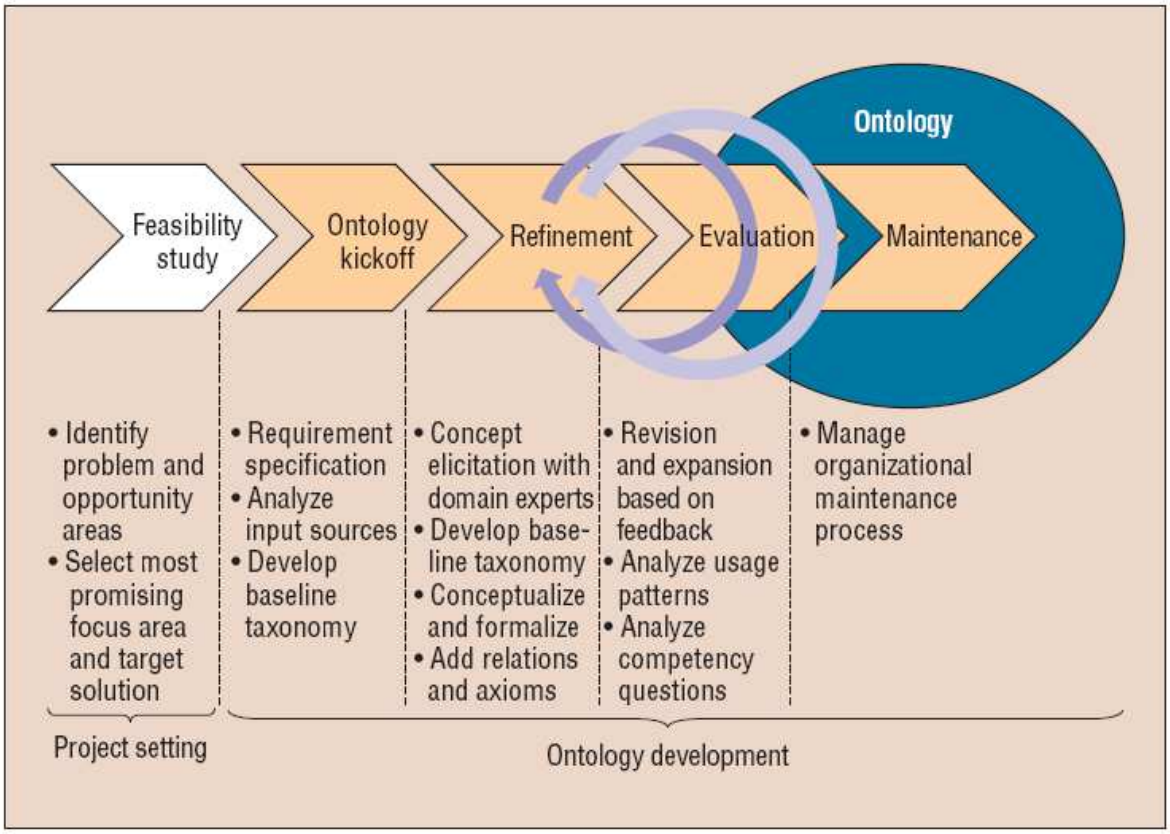


Figure 26 : On-To-Knowledge -Processus de développement d'ontologie (Staab, et al, 2001).

La méthodologie **Neon** (Suárez-Figueroa et al, 2012) est fondée sur l'utilisation de neuf (09) scénarios, (voir sous chapitre **III.5.2**) qui prennent en charge les différents aspects du processus de développement de l'ontologie. Ils prennent en charge aussi la réutilisation et l'évolution dynamique d'ontologie dans des environnements distribués, où la connaissance est introduite par différentes personnes (experts de domaine, les praticiens) à différents stades du processus de construction de l'ontologie.
Cette méthode comprend les composants suivants :

• Le NeOn Glossaire, qui identifie et définit les processus et activités potentiellement impliqués dans la construction de l'ontologie.

• Les scénarios pour la construction des ontologies. Chaque scénario est décomposé en différents processus et activités prises parmi celles qui figurent dans le NeOn Glossaire.

• Deux modèles de cycle de vie de l'ontologie qui spécifient comment organiser les processus et les activités du NeOn Glossaire.

• Un ensemble de directives méthodologiques prescriptives pour les processus et les activités.

Afin de choisir une méthode de construction d'ontologies, nous avons étudié les états comparatifs existants, tels que celui de (Rousseye et al, 2013) qui propose une comparaison des méthodes de construction d'ontologies sur la base des interrogations suivantes :

1- Modularité : La méthode génère-t-elle des ontologies modulaires ?

2- Intégration : La méthode propose-t-elle d'intégrer des ontologies entre elles ?

3- Réutilisation : la méthode propose-t-elle de réutiliser des ressources lors de la création des ontologies ?

4-Patrons de Conception : La Méthode propose-t-elle d'utiliser des patrons de conception (PC) ?

Dans cette comparaison, les auteurs soulignent que la méthode **NeOn** semble la plus complète. Elle propose neuf (09) scénarios possibles permettant de construire une ontologie. Ces scénarios, décrits ci-dessous, sont applicables même pour les autres méthodologies

III.5.2 Scénarios de construction d'ontologie (Suárez-Figueroa et al, 2012)

Dans cette section, nous présentons les scénarios les plus courants qui peuvent se dérouler pendant la construction d'une l'ontologie. Cette liste n'est pas exhaustive.

• **Scénario 1** : de la spécification à la mise en œuvre. Le réseau de l'ontologie est développé à partir de zéro, et qui se conçoit sans la réutilisation des ressources de connaissances disponibles.

• **Scénario 2** : réutilisation et ré-ingénierie des ressources non ontologiques. Ce scénario couvre le cas où les développeurs d'ontologies doivent analyser des ressources non ontologiques et décider, selon les exigences de l'ontologie qu'ils doivent construire, quelles ressources non ontologiques peuvent être réutilisées pour assembler cette dernière. Le scénario couvre également la tâche de ré-ingénierie des ressources sélectionnées des ontologies.

• **Scénario 3** : réutilisation des ressources ontologiques. Ici, les développeurs optent pour la réutilisation des ressources ontologiques (ontologies dans son ensemble, les modules de l'ontologie, et / ou l'état de l'ontologie).

• **Scénario 4** : réutilisation et ré-ingénierie des ressources ontologiques. Ici, les développeurs utilisent à la fois la réutilisation et le ré-ingénierie des ressources ontologiques.

• **Scénario 5** : réutilisation et la fusion des ressources ontologiques. Ce scénario se déroule seulement dans les cas où plusieurs ressources ontologiques existent dans le même domaine, alors ils seront sélectionnés pour réutiliser leurs connaissances.

• **Scénario 6** : réutilisation, la fusion et le ré-ingénierie des ressources ontologiques. Ce scénario est semblable au scénario 5. Cependant, ici les développeurs décident de ne pas utiliser l'ensemble de ressources fusionnées, tel qu'il est.

• **Scénario 7** : réutilisation des « design patterns » pour la construction de l'ontologie.

• **Scénario 8** : restructuration des ressources ontologiques. Ce scénario est utilisé pour l'ontologie modulaire afin de les intégrer dans le réseau de l'ontologie en cours de construction.

• **Scénario 9** : localisation des ressources ontologiques. Adapter l'ontologie à d'autres langues, produisant ainsi une ressource ontologique multilingue.

Il est à noter que ces scénarios peuvent être combinés entre eux, et quelle que soit leur combinaison, elle devrait inclure, obligatoirement le scénario 1, parce que ce dernier est constitué des activités de base qui doivent être effectuées dans tout développement de l'ontologie.

Pour notre part, nous utilisons ces scénarios de construction des ontologies pour élaborer nos (04) quatre ontologies.
Nous commençons par la construction de l'ontologie des actifs, cette ontologie va nous permettre d'identifier les concepts qui ont de la valeur pour l'organisation. Ensuite nous contruisons l'ontologie du contexte afin de lier l'organisation au plan de sécurité générique. Nous terminons par la construction des ontologies des risques et des exigences de sécurité qui, nous mènent au développement du plan de sécurité.

III.6 Ontologie des actifs

Pour construire notre ontologie des actifs, nous procédons à l'étude des différentes contributions relatives à la classification des actifs dans le domaine de la gestion des risques. Cette étude approfondie se prolonge par les méthodes d'analyse de risque et également les normes et les standards de sécurité.

Nous établissons pour chaque approche sélectionnée une représentation ontologique légère sous forme de modèle UML (Unified Modeling Language) et un tableau qui propose les synonymes et les instances tirées des approches elles-mêmes. Cette démarche nous permet d'obtenir les liens ontologiques entre les concepts, mais elle nous permet aussi de détecter des conflits potentiels entre actifs. Cette détection de conflits offre un meilleur guidage dans la spécification des scénarios de risques associés.

Il existe des règles de transformation des modèles UML en ontologie (Héon et al, 2008). Ces règles, nous les appliquons au résultat final pour avoir l'ontologie des actifs (voir annexe **A**).

III.6.1 Etat de l'art pour la construction de l'ontologie des actifs

L'analyse des travaux relatifs à la construction de l'ontologie des actifs, nous amènet à opérer une sélection sur la base d'un filtrage des approches présentées dans le chapitre **II.** Ce filtrage consiste à ne considérer que les approches qui proposent une classification ainsi qu'une définition des actifs en même temps (voir tableau **6**). Nous procédons aussi à une classifications des actifs issus des publications récentes et qui ne sont pas mentionnées dans notre état de l'art principal. Pour chaque méthode séléctionnée, nous présentons, après le filtrage cité supra, un modèle d'actif.
Cette démarche à la particularité de nous aider au final à avoir le modèle global de notre ontologie des actifs avec les associations et les attributs qui le composent.

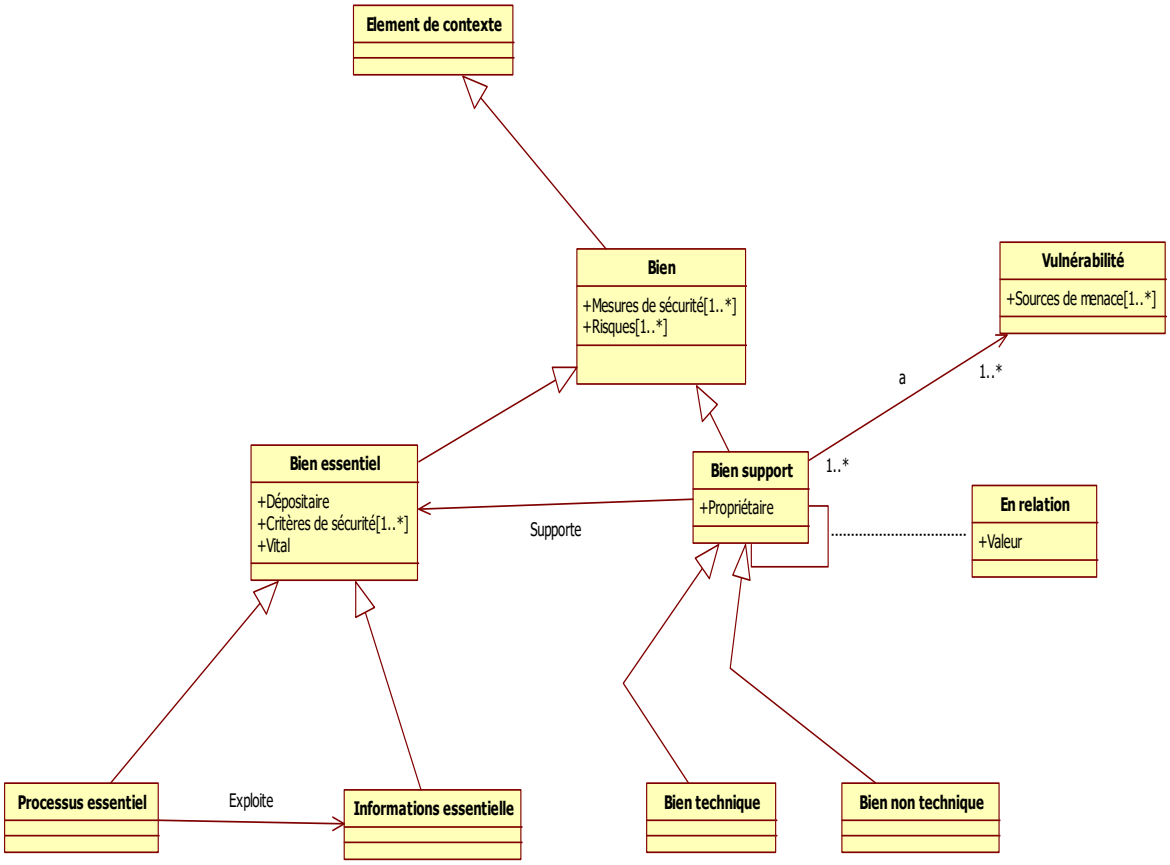
Nom	Définition	Proposer une classification
EBIOS	« Toute ressource qui a de la valeur pour l'organisme et qui est nécessaire à la réalisation de ses objectifs »	Oui
MÉHARI	« Sont les sujets principaux du risque »	Oui
OCTAVE	« Tout ce qui a de la valeur à une organisation »	Non
CRAMM	« Tout ce qui a de la valeur à une organisation »	Oui
ISSRM	« Tout ce qui possède de la valeur pour l'organisation et donc nécessitant d'être protégé »	Oui
SQUARE	/	Non
SECURE TROPOS	/	Non
KAOS	/	Non
MAGERIT	« Les actifs sont des ressources du système, ils sont nécessaires à l'organisation pour fonctionner correctement et d'atteindre les objectifs proposés par gestionnaire »	Oui
FAIR	« Actif, c'est toutes les données, périphériques ou un autre composant de l'environnement qui soutient les activités liées à l'information, qui peut être accessible de manière illicite, utilisée, divulguée, modifiée, détruite, et / ou de vol, résultant en une perte »	Non
CORAS	/	Non
HAZOP	/	Non
MISUSE CASES	« Les actifs sont des ressources avec grande potentialité et valeur pour le système »	Non
ABUSE CASES	/	Non
AS/NZS 4360	/	Non
BS7799/	« Tout ce qui a de la valeur à une organisation »	Non
COBIT5	« Quelque chose de valeur soit tangible ou intangible qui est digne pour être protégé, y compris les personnes, l'information, l'infrastructure, les finances et la réputation »	Oui
ITIL	« Toute ressource ou aptitude »	Oui
ISO/CEI 15408	Entité qui possède une valeur que le propriétaire de la TOE[7] a placée.	Non
ISO/CEI 27001	« Tout élément représentant de la valeur pour l'organisme »	Oui

Tableau 6 : Filtrage de l'état de l'art.

Nous présentons ci-dessous un état de l'art relatif à la construction de l'ontologie des actifs. Parmi les méthodes qui répondent aux critères de filtrage cités supra, citons :

[7] TOE Target of Evaluation

La méthode **EBIOS** catégorise les actifs en "biens essentiels" et "biens supports". La première catégorie représente le patrimoine informationnel ou les "biens immatériels", que l'on souhaite protéger, c'est-à-dire ceux pour lesquels le non-respect de la disponibilité, de l'intégrité, de la confidentialité, voire d'autres critères de sécurité, mettraient en cause la responsabilité du dépositaire[8]. La seconde catégorie concerne des biens techniques ou non-techniques, supports aux biens essentiels précédemment identifiés. On note que ces biens supports possèdent des vulnérabilités que des sources de menaces pourront exploiter, pouvant ainsi atteindre aux biens essentiels.
Une fois les biens supports identifiés, il convient de "rattacher" un propriétaire pour chacun d'eux, nommément ou fonctionnellement identifié. En effet, la personne qui en a la responsabilité sera sans doute là plus à même d'analyser ses vulnérabilités, et c'est elle qui sera garante de l'application de mesures de sécurité (voir le modèle suivant).



Propriété valeur ϵ [Inclusion, interconnexions,…….]

Figure 27 : Modèle des biens EBIOS.

Pour enrichir notre ontologie des actifs par les synonymes et les instances qui existent dans les descriptions textuelles dans la méthode EBIOS, nous avons élaboré le tableau suivant :

[8] Le dépositaire : service commercial ; bureau d'études ; directeur adjoint.

Concepts	Synonymes	Exemples
Bien	Actif	Actif essentiel ; Actif support.
Actif essentiel	Patrimoine informationnel ; Biens immatériels	Processus essentiel ; Informations essentielles.
Actif support		Actif technique ; Actif non technique.
Processus essentiel		Établir les devis (estimation du coût global d'un projet, négociations avec les clients…) ; Créer des plans et calculer les structures ; Créer des visualisations ; Gérer le contenu du site Internet.
Informations essentielles		Cahier des charges ; Catalogues techniques ; Contrat (demande de réalisation) ; Devis ; Dossier technique d'un projet ; Informations société (contacts, présentation…) ; Page Web.
Actif technique		Réseau interne ; Sous réseau Ethernet ; Sous réseau Wifi ; Système d'information
Actif non technique		Locaux ; Personnels ; Organisations

Tableau 7: Synonymes et exemples extrait de la méthode EBIOS.

Dans la méthode **MEHARI,** les actifs sont le sujet principal du risque. Il est bien clair dès lors, que les conséquences et la gravité de la survenance du risque dépendent de la nature de ces actifs et donc que cette nature doit faire partie de la caractérisation du risque. Les actifs sont classifiés en deux catégories, "actifs primaires" et "actifs secondaires ou actifs de supports".
Un actif primaire peut être composé d'un actif de type service, ou d'un actif de type donnée et information, ou enfin d'un actif de type processus de gestion.
Les vulnérabilités sont associées aux actifs secondaires. Le modèle de la figure suivante indique cette liaison :

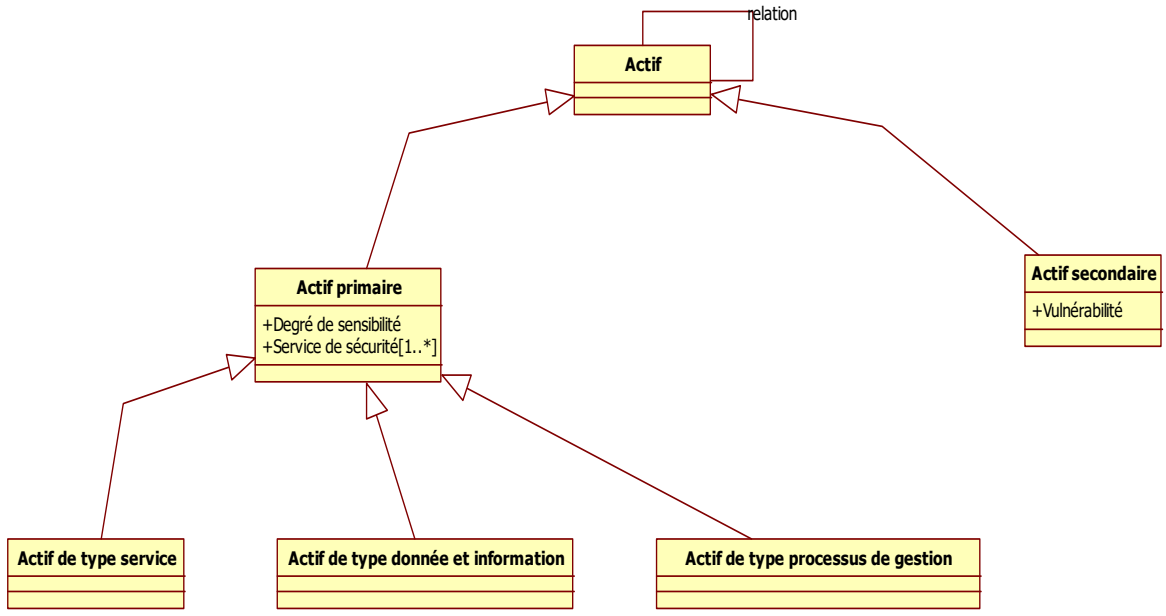


Figure 28 : Modèle des actifs MEHARI.

Pour enrichir notre ontologie des actifs par les synonymes et les instances qui existent dans les descriptions textuelles dans la méthode MEHARI, nous avons élaboré le tableau suivant :

Concepts	**Synonymes**	**Exemples**
Actif	Actif	Actif primaire ; Actif secondaire
Actif primaire	Besoins fonctionnels ; Actif primaire	Actif de type service ; Actif de type donné ; Actif de type processus de gestion
Actif secondaire	Objets concerts ; Support ; Actif secondaire	
Actif de type service		
Actif de type donné		
Actif de type processus de gestion		
Actif non technique		

Tableau 8 : Synonymes et exemples extrait de la méthode MEHARI

La méthode **CRAMM** classe les actifs en trois catégories: actifs informations, actifs applications et actifs physiques (équipements, personnels, locaux). Les actifs possèdent des objectifs de sécurité à respecter comme la disponibilité, l'intégrité, la confidentialité, voire d'autres critères de sécurité, qui mettraient en danger l'organisation.

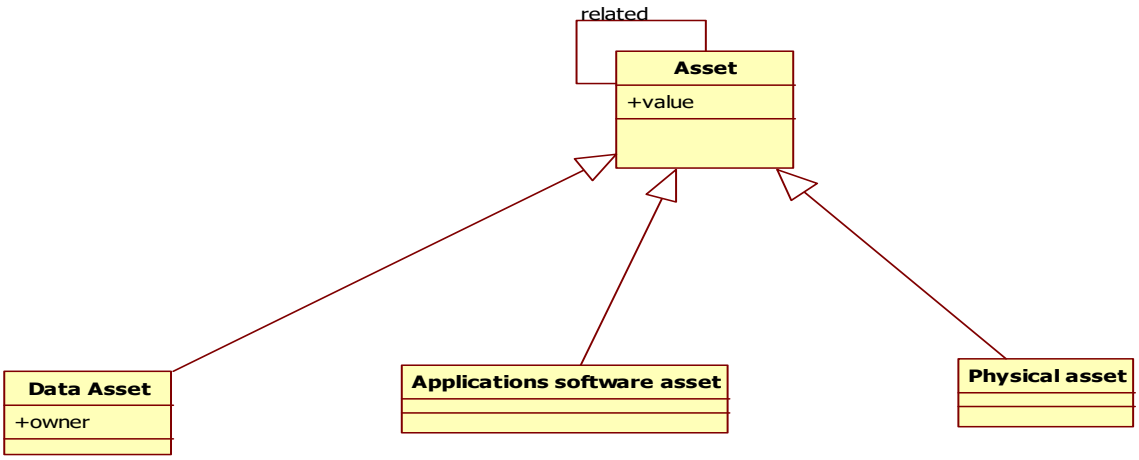


Figure 29 : Modèle des actifs CRAMM.

Nous avons tirer les instances suivantes à partir du texte du la méthode CRAMM :

Concepts	**Synonymes**	**Exemples**
Asset	Actif	Actif donné ; actif application; actif physique
Actif donné		
Actif application software		
Actif Physique		Équipements ; Buildings ; Personnel

Tableau 9 : Exemples extrait de la méthode CRAMM

Pour la méthode **MAGERIT**, activo en espagnol ou actif, est une composante d'un système d'information qui peut être l'objet d'attaques délibérées ou accidentelles qui peuvent avoir des conséquences pour l'organisation. Les actifs comprennent : les actifs essentiels et les autres actifs.
Il existe deux types d'actifs essentiels dans un système d'information :

- L'information qu'il gère
- Les services qu'il fournit.

Les actifs essentiels marquent les conditions requises de sécurité pour tous les autres actifs.

Les autres actifs concernés et qui peuvent être identifiées, sont:

- Les données qui matérialisent l'information.
- Les services auxiliaires nécessaires pour organiser le système.
- Les applications informatiques (logiciel)
- Le matériel informatique (hardware) qui héberge les données, les applications et les services.
- Les supports d'information, qui stockent les données.
- L'équipement auxiliaire qui complète l'équipement informatique.
- Les réseaux de communication qui échangent les données.
- Les installations.
- Les personnes.

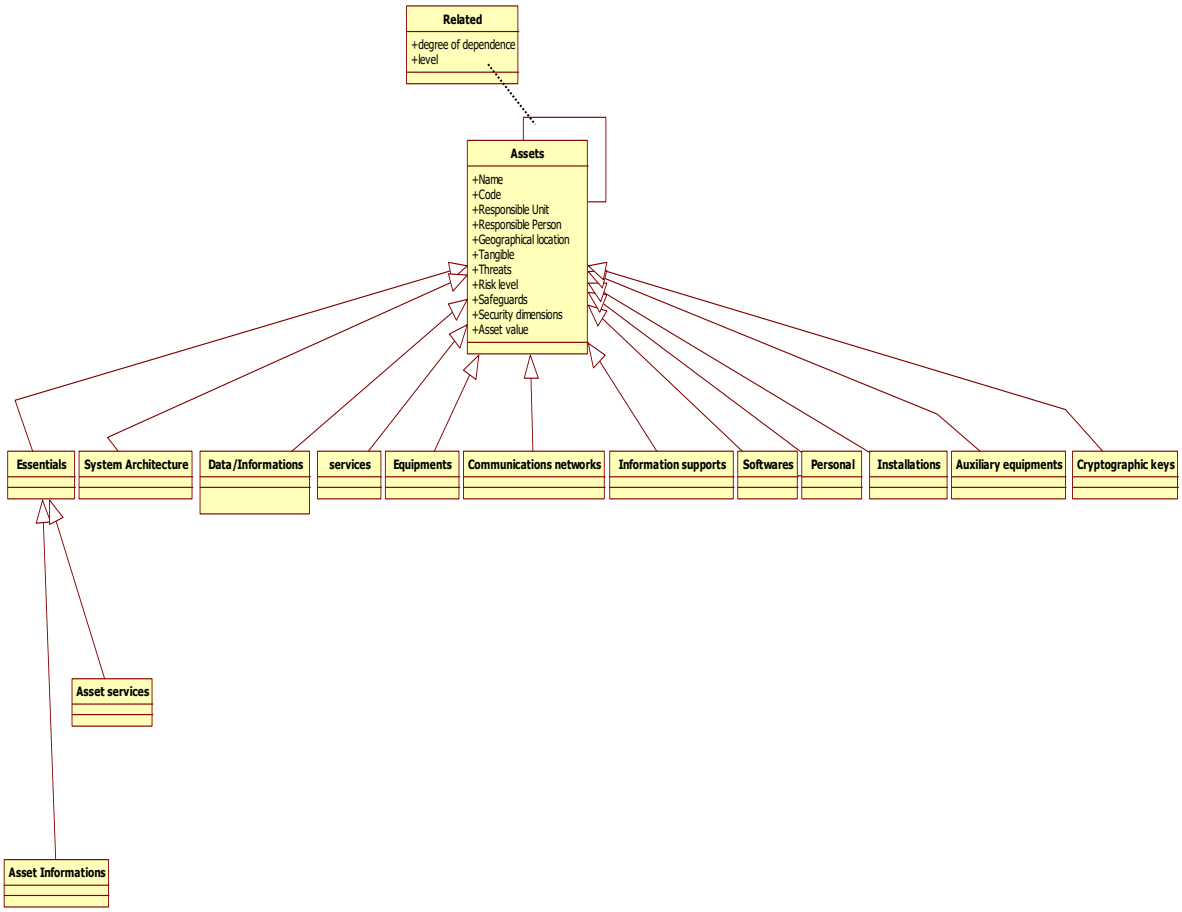


Figure 30 : Modèle des actifs MAGERIT.

Pour le référentiel **COBIT**, un actif est quelque chose qui a de la valeur, soit tangible soit intangible et qui mérite d'être protégé. A titre d'exemple mentionnons le personnel, les données, les infrastructures, les finances et la réputation.

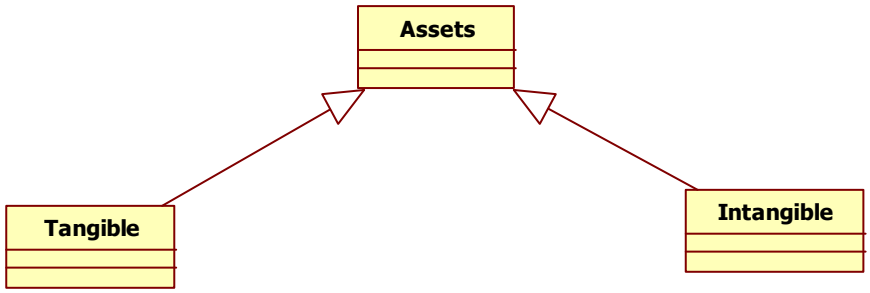


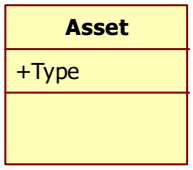
Figure 31 : Modèle des actifs COBIT.

Nous avons obtenu les instances suivantes à partir du texte du référentiel COBIT :

Concepts	**Synonymes**	**Exemples**
Asset	Actif	Tangible ; Intangible
Tangible		Personnes; Infrastructure
Intangible		Finance ; Réputation ; Information

Tableau 10 : Exemples extrait du référentiel COBIT5.

Pour le référentiel **ITIL**, un actif est toute ressource ou aptitude. Les actifs d'un fournisseur de services regroupent tout ce qui peut contribuer à fournir un service. Les actifs peuvent appartenir à une des catégories suivantes : gestion, organisation, processus, connaissances, personnel, information, applications, infrastructure et capital financier. Nous trouvons aussi un type d'actif client, de service et stratégique.



Type ϵ [actif client, actif service, actif stratégique]

Figure 32 : Modèle d'actif ITIL.

Nous avons obtenu les instances suivantes à partir du texte du référentiel ITIL :

Concepts	**Synonymes**	**Exemples**
Asset	Actif	Management ; Organisation ; processus ; Connaissance Personnelle ; donnée ; Software ; Infrastructure ; capital financier

Tableau 11 : Exemples extrait du référentiel ITIL.

Pour la méthode **ISSRM**, « les actifs sont directement liés aux processus et informations associés au business de l'organisation. Ainsi, dans un contexte d'un SI donné, les actifs de l'organisation sont implémentés à travers les matériels, les logiciels et les composants réseaux, aussi bien que par des personnes ou des équipements jouant un rôle dans le SI ».
ISSRM classifie les actifs comme suit :

Actif business – « information, processus, capacité et aptitude inhérents au business de l'organisation, qui a de la valeur pour l'organisation et qui est nécessaire à la réalisation de ses objectifs ».
Actif SI – « un composant ou une partie du SI, support aux actifs business, qui a de la valeur pour l'organisation et qui est nécessaire à la réalisation de ses objectifs. Un actif SI, peut-être un composant du système d'information, 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 ».

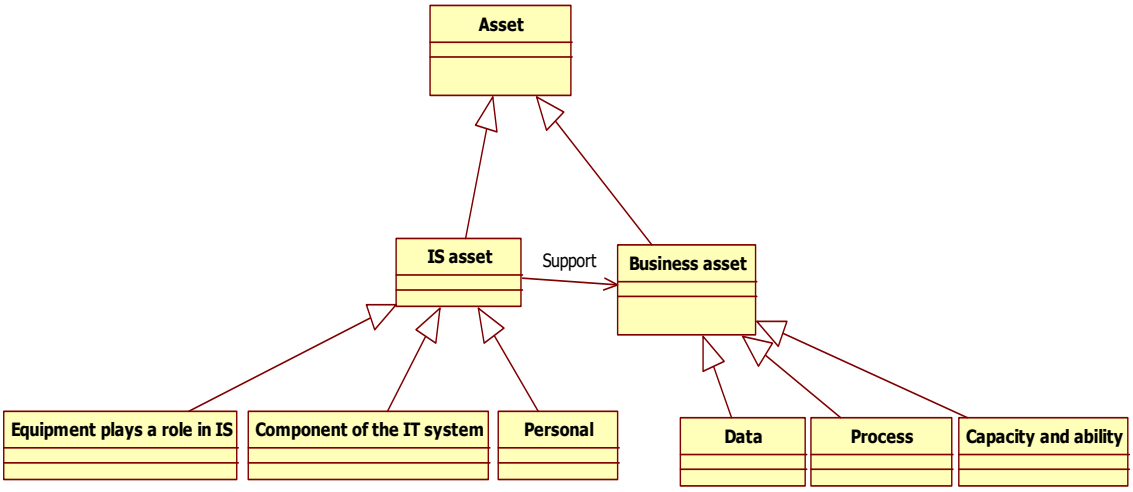


Figure 33 : Modèle des actifs ISSRM.

Pour enrichir notre ontologie des actifs par les synonymes et les instances qui existent dans les descriptions textuelles dans la méthode ISSRM, nous avons élaboré le tableau suivant :

Concepts	**Synonymes**	**Exemples**
Asset	Actif	Actif SI ; Actif Business
Actif Business	Actif métier	Données ; Processus ; Capacité et aptitude
Actif SI		Composant du système IT ; Personnel ; Équipement jouant un rôle dans SI
Composant du système IT		Ordinateur ; Réseau Ethernet ; Système d'exploitation
Équipement jouant un rôle dans SI		Conditionnement d'air de la salle serveur
Personnel		Administrateur système ; Employé encodant des données
Donnée		Liste de noms
Processus		Processus de remboursement médical
Capacité et aptitude		Compétences de diagnostic médical

Tableau 12 : Exemples extrait de la méthode ISSRM.

La norme **ISO/CEI 27001** donne une classification des actifs comme suit :
- Les actifs infrastructures (bâtiments, magasins, tours, etc.) ;
- Les actifs physiques (matériel informatique, matériel de communications, machinerie lourde) ;
- Les actifs logiciels (applications, code logiciel, outils de développement, logiciel de fonctionnement, etc.) ;
- Les actifs informations (informations de base de données, documentation juridique, manuels, les documents organisationnels, etc.) ;
- Les actifs services (transport, climatisation, communications, etc.) ;
- Les actifs personnes (management, compétences, expérience, etc.) ;
- L'imperceptible (réputation, l'image, etc.) ;
- Les actifs clients.

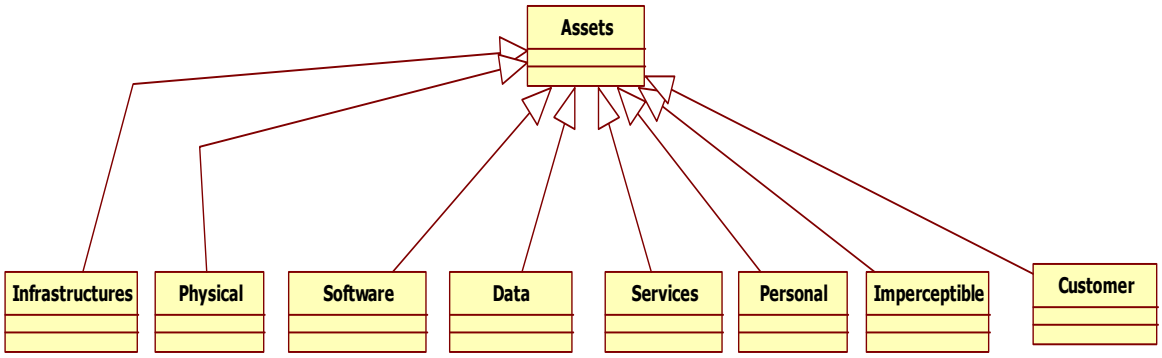


Figure 34 : Modèle des actifs ISO/CEI 27001.

Il existe d'autres approches relatives à la construction de l'ontologie des actifs. Citons notamment :

(Bhattacharjee et al, 2013) décrit une méthodologie formelle pour l'évaluation des risques de l'entreprise (A Formal Methodology for Enterprise Information Security Risk Assessment). Cette solution propose une classification en deux catégories des actifs, une primaire et l'autre support. Les actifs primaires sont ceux qui sont essentiels à la survie d'une entreprise. Ils sont de deux types : (i) Les processus métiers et d'activités, et (ii) les actifs d'information. Un processus métier est défini comme « un ensemble d'activités interactives qui transforment des entrées en sorties ». D'autre part, les actifs d'information comprennent des documents et des dossiers qui sont essentiels pour l'exécution des opérations commerciales.
Les actifs supports sont ceux qui aident à mener à bien les processus métiers d'une entreprise. Il existe six catégories différentes d'actifs supports :

- (i) Materiel;
- (ii) Logiciel;
- (iii) Réseau;
- (iv) Personnel;
- (v) Site;
- (vi) Structure organisationnelle.

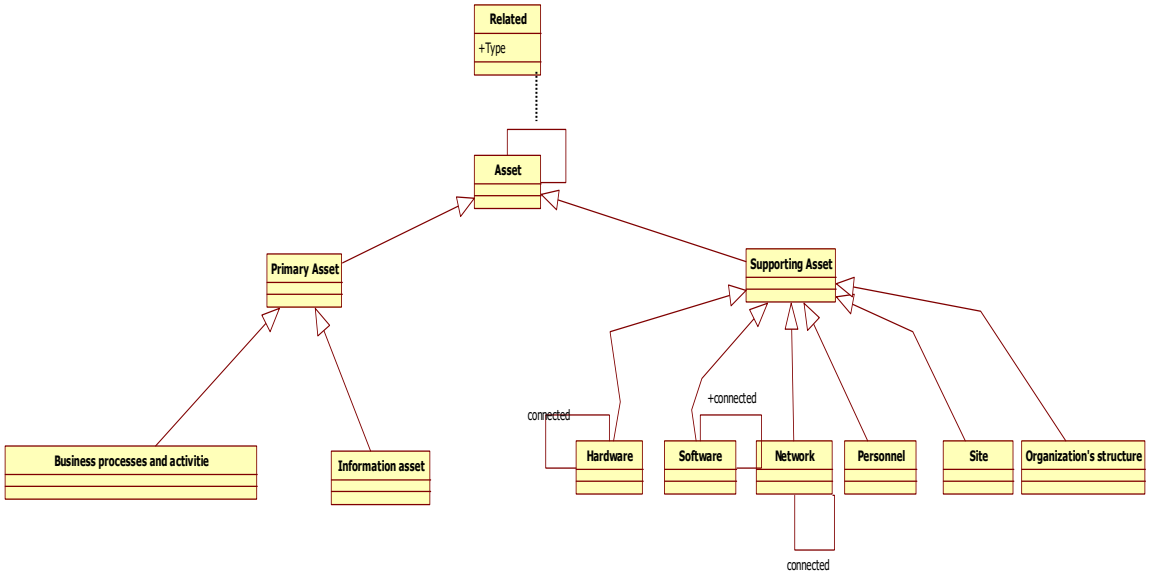


Figure 35 : Modèle des actifs d'après (Bhattacharjee et al, 2013).

Pour enrichir notre ontologie des actifs par les synonymes et les instances qui existent dans les descriptions textuelles dans de la contribution académique précédente, nous avons élaboré le tableau suivant :

Concepts	**Synonymes**	**Exemples**
Asset	Actif	Actif primaire, Actif support
Actif primaire		Processus métiers et activités, - Actif Information
Actif support		Structure organisationnelle
Processus métiers et activités	Actifs services	
Actif Information		.
Hardware		
Software		
Réseau		
Personnel		Employés ; contractuels
Site	Locale	
Structure Organisationnel		

Tableau 13 : Synonymes et exemples extrait de (Bhattacharjee et al, 2013).

L'approche **ISRA** (Information Security Risk Assessment) (Shameli-Sendi et al, 2016) propose une taxonomie des actifs. Ces derniers sont classés comme suit :

a. Actif information,
b. Actif donnée,
c. Actif physique,
d. Actif software,
e. Actif hardware,
F. Actif personnel.

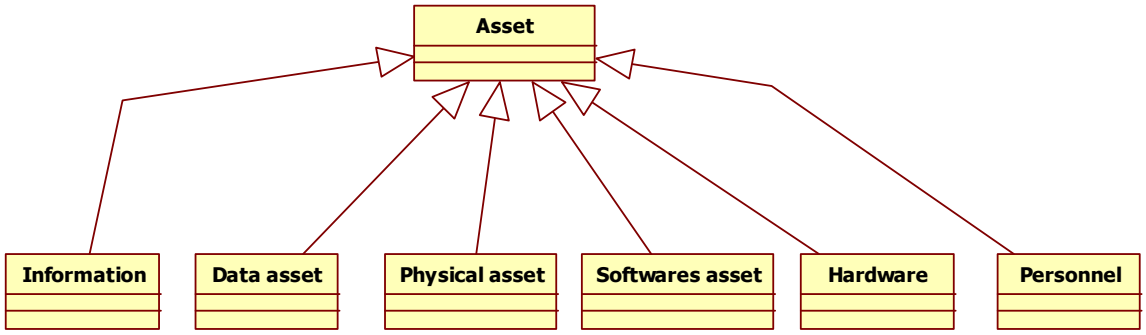


Figure 36 : Modèle des actifs ISRA (Shameli-Sendi et al, 2016).

Nous présentons ci-dessous une ontologie des actifs extraite de (Ramanauskaite et al, 2013). Celle-ci décrit à la fois les actifs comme étant tangibles et intangibles. Les actifs intangibles sont divisés en données et logiciels, tandis que ceux tangibles sont sous la forme mobile et immobile.

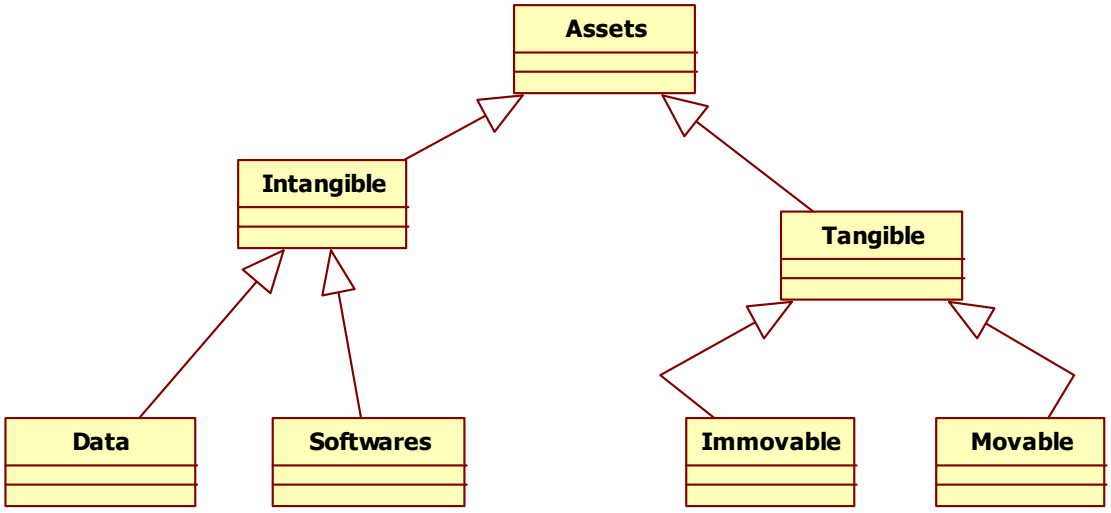


Figure 37 : Modèle des actifs d'après (Ramanauskaite et al, 2013).

Nous avons obtenu les instances suivantes à partir de l'étude précédente :

Concepts	**Synonymes**	**Exemples**
Asset	Actif	Actif intangible, actif tangible
Actif tangible		Actif mobile, actif immobile
Actif intangible		Actif donné, actif software
Actif Donné		
Actif software		
Actif mobile		
Actif immobile		

Tableau 14 : Exemples extrait de (Ramanauskaite et al, 2013).

III.6.2 Construction de notre ontologie des actifs

La construction de notre ontologie s'effectue à l'aide de la méthodologie **METHONTOLOGY** pour une application générique. Nous rappelons que cette méthode s'applique à clarifier les différentes étapes de la construction en respectant des activités de gestion de projets (planification, assurance qualité), et de développement (spécification, conceptualisation, formalisation, implémentation, maintenance). Nous précisons que les scénarios utilisés pour la construction de l'ontologie sont extraits de la méthode **NeOn**.

III.6.2.1 Spécification

Une ontologie ne peut être construite qu'après avoir réalisé la phase de spécification. Il s'agit d'établir un document informel de spécification des besoins. Au niveau de ce document, nous décrivons l'ontologie à construire à travers les aspects suivants :

Domaine de connaissance : domaine sécurité des systèmes d'information.

Objectif : Permettre la caractérisation des actifs extraits des audits et des inputs des organisations.

Utilisateurs : Praticiens et chercheurs du domaine.

Sources d'information : Méthodes, normes et standards de sécurité ainsi que les publications scientifiques spécialisées.

III.6.2.2 Acquisition des connaissances

Le but de cette phase est de mettre en lumière la liste des sources de connaissances et de décrire le processus d'acquisition. Dans notre cas, nous avons établi un état de l'art complet du domaine concerné (voir section **III.5.1**).

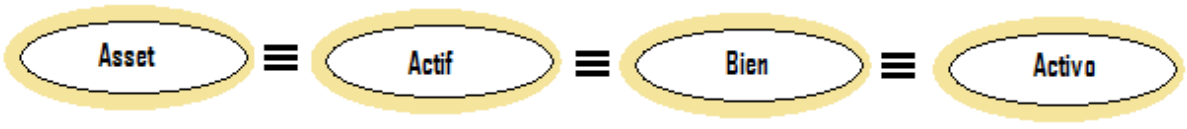
III.6.2.3 Construction

Pour concrétiser cette étape, nous appliquons les scénarios 1, 2 et 6 mentionnés dans le sous chapitre **III.5.2** et repris ci-après :

- **Scénario 1** : de la spécification à la mise en œuvre. Le réseau de l'ontologie est développé à partir de zéro, et qui se conçoit sans la réutilisation des ressources de connaissances disponibles.
- **Scénario 2** : Réutilisation et ré-ingénierie des ressources non ontologiques.
- **Scénario 6** : Réutilisation, fusion et ré ingénierie des ressources ontologiques.

a. **Premier niveau de l'ontologie**

Le fait de croiser les connaissances édictées par des différentes méthodes de notre état de l'art pour la construction de l'ontologie des actifs, le résultat de nos recherches et les données de la documentation spécialisée, nous a permis de contribuer à répondre à notre objectif. Nous pouvons donc affirmer que :



La deuxième étape consiste à fusionner et prendre les attributs d'actif dans toutes les méthodes citées supra et que nous jugeons utiles pour notre ontologie (cette étape est la même pour tous les concepts de notre ontologie) :

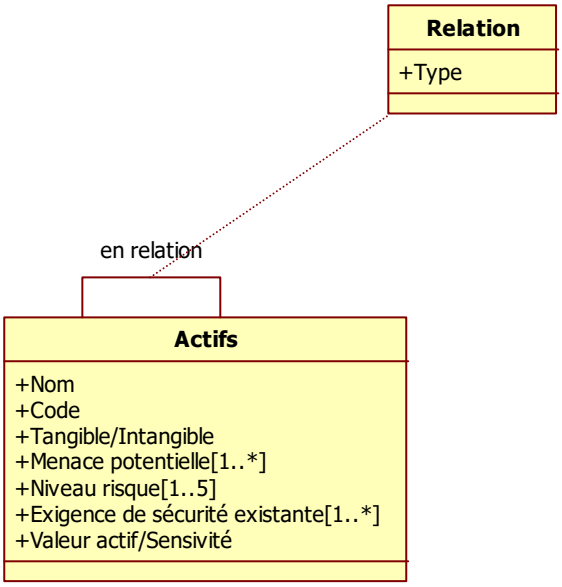


Figure 38 : Premier niveau de l'ontologie des actifs.

Un actif peut avoir des relations avec d'autres actifs comme les relations d'inclusion ou d'interconnexions. Il peut aussi avoir des attributs extraits de l'état de l'art dédié à la construction de l'ontologie des actifs (voir sous chapitre **III.6.1).**

b. Deuxième niveau de l'ontologie

Nous optons pour une solution à plusieurs niveaux d'abstraction. Pour cela, nous privilégions les solutions prévoyant de tenir compte du fait que l'actif est composé de deux parties, même si chacune d'elles utilise une appellation propre. Les connaissances dans cette partie donnent le résultat suivant :

L'appellation que nous avons choisie est : actif essentiel et actif support.

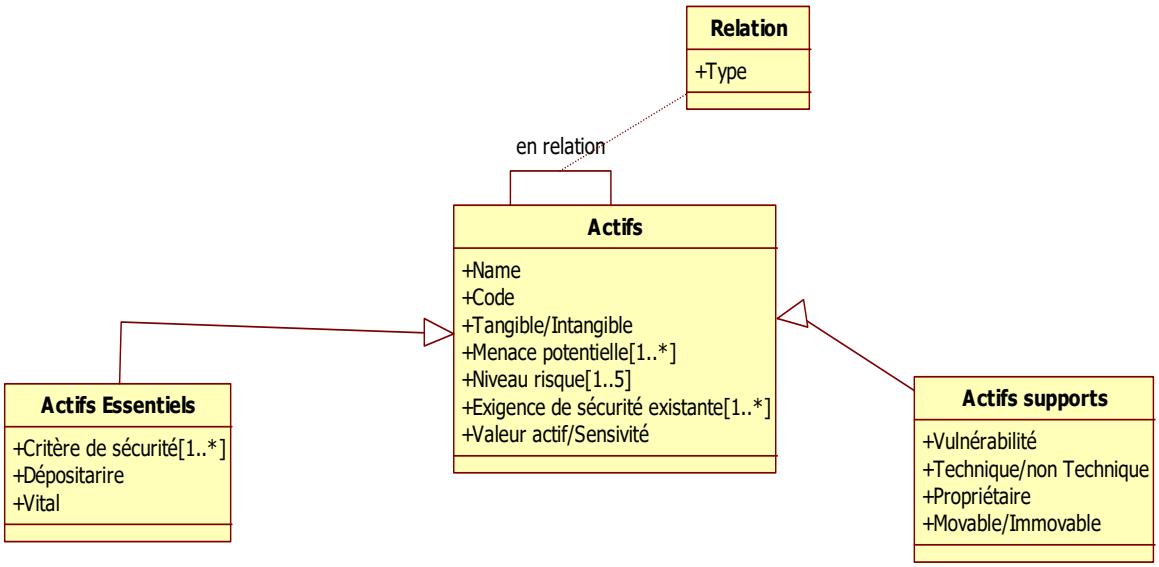


Figure 39 : Deuxième niveau d'abstraction de l'ontologie des actifs.

A noter que vulnérabilité est une propriété d'un actif support, technique ou non technique. De même il peut-être soit mobile ou immobile. Les critères de sécurité s'appliquent sur les actifs essentiels. L'actif support possède un propriétaire tandis que les actifs essentiels possèdent un dépositaire (voir méthode EBIOS).

c. Troisième niveau de l'ontologie

Nous comparons les concepts qui reste d'un point de vue sémantique et, nous effectuons une vérification à l'aide de notre base de connaissances pour juger de l'utilité ou non du concept.

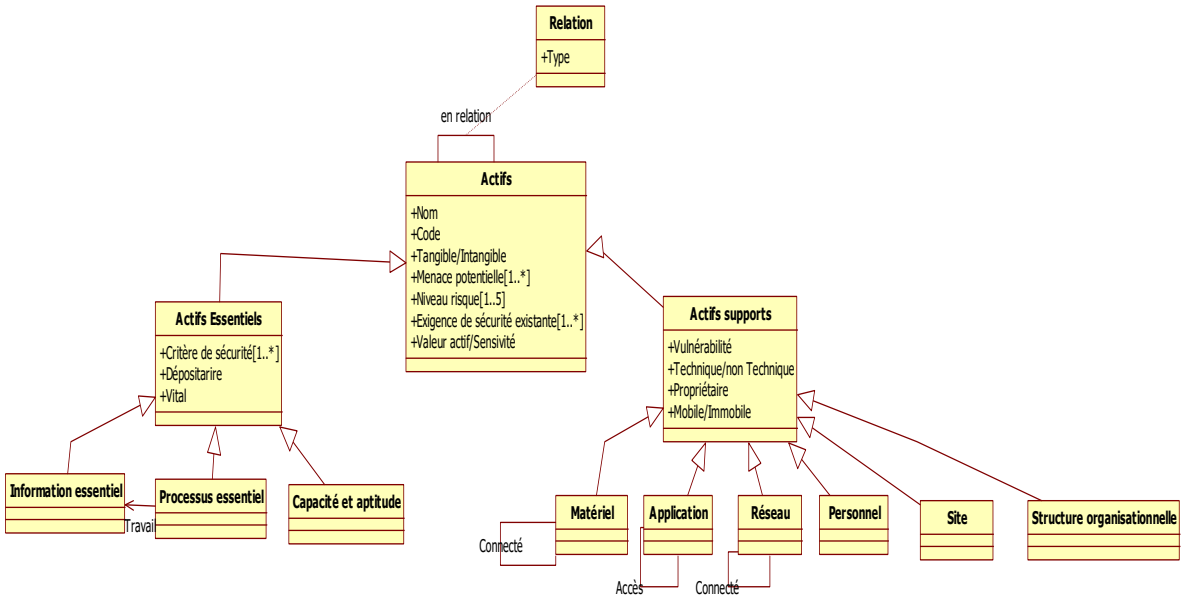


Figure 40 : Modèle de l'ontologie des actifs.

A noter que si :
- L'actif support est technique ⇒ Actif ϵ [matériel, application, réseau] ;
- L'actif support est non technique ⇒ Actif ϵ [personnel, site, structure organisationnelle]
- L'actif support est mobile ⇒ Actif ϵ[matériel, application, réseau, personnel] ;
- L'actif support est immobile ⇒ Actif ϵ [structure organisationnelle]

Le modèle de l'ontologie des actifs obtenu est fondé sur les concepts des principales méthodes d'analyse des risques actuelles. Il a été enrechi par les synonymes et les instances extraits des textes de ces méthodes. Cette ontologie légère qui est représentée sous forme de modèle est la plus riche et la plus complète par rapport à l' existant. Elle englobe tous les concepts étudiés pour les actifs.

III.7 Ontologie du Contexte

De façon semblable à la construction de l'ontologie des actifs, nous puisons les connaissances essentielles dans notre état de l'art principal (chapitre **II**). Toutefois, étant donné que ce concept n'a pas été beaucoup traité ou modélisé par les méthodes citées supra, nous avons effectué une revue approfondie des contributions dans ce domaine pour enrichir et conforter notre ontologie du contexte.

Nous présentons pour chaque méthode un modèle du contexte. Au final, cette démarche nous aide à faire apparaître le modèle global de notre ontologie du contexte avec les associations et les attributs qui la composent.

III.7.1 Etat de l'art relatif à la construction de l'ontologie du contexte

La méthode EBIOS considère que le contexte est composé de deux catégories. L'une est externe et comprend tout ce qui est environnement social, culturel, politique, légal, réglementaire, financier, technologique, économique, naturel et concurrentiel, au niveau international, national, régional ou local. Elle considère aussi les facteurs et les tendances ayant un impact déterminant sur les objectifs ainsi que les relations avec les parties prenantes externes, leurs perceptions et leurs valeurs.
L'autre catégorie, interne, comprend la description générale de l'organisme, les aptitudes en matière de ressources, missions, les valeurs, les métiers ..., (Voir figure **41**)

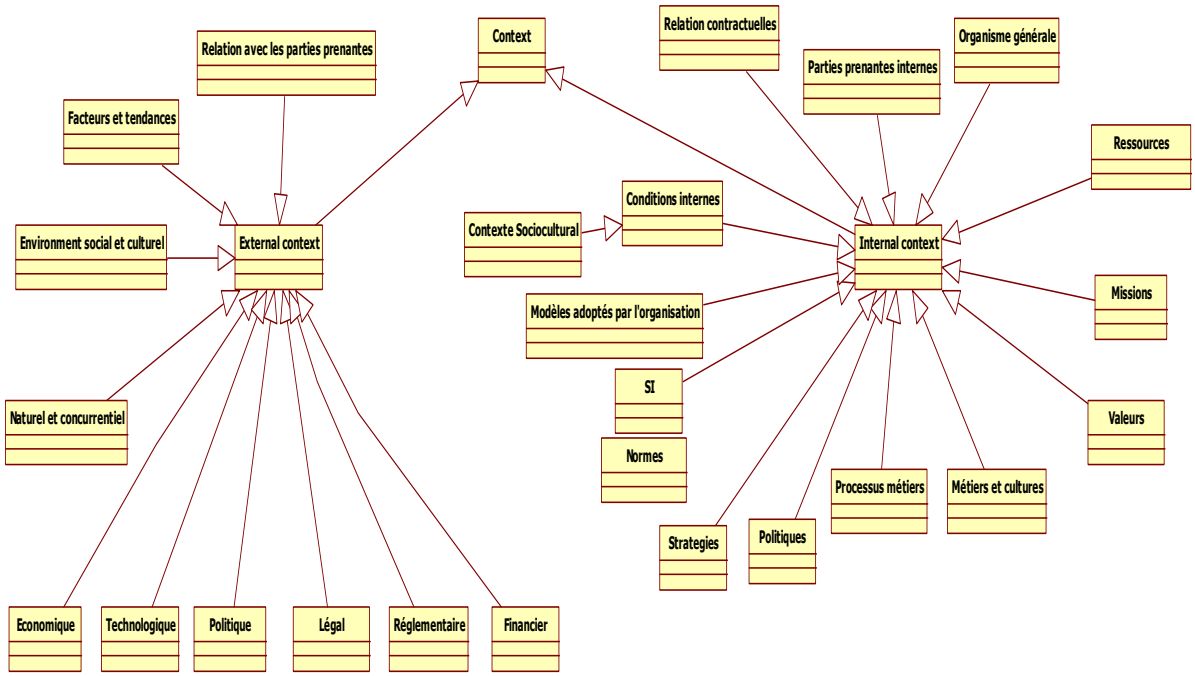


Figure 41 : Modèle du contexte d'après EBIOS.

MAGERIT fait la différence entre le contexte interne et les autres concepts qui constituent l'ensemble du contexte. Pour cette méthode, le contexte interne est composé des politiques

internes ainsi que des intervenants internes et du patronat ou leur représentant, tel que présenté à la figure suivante :

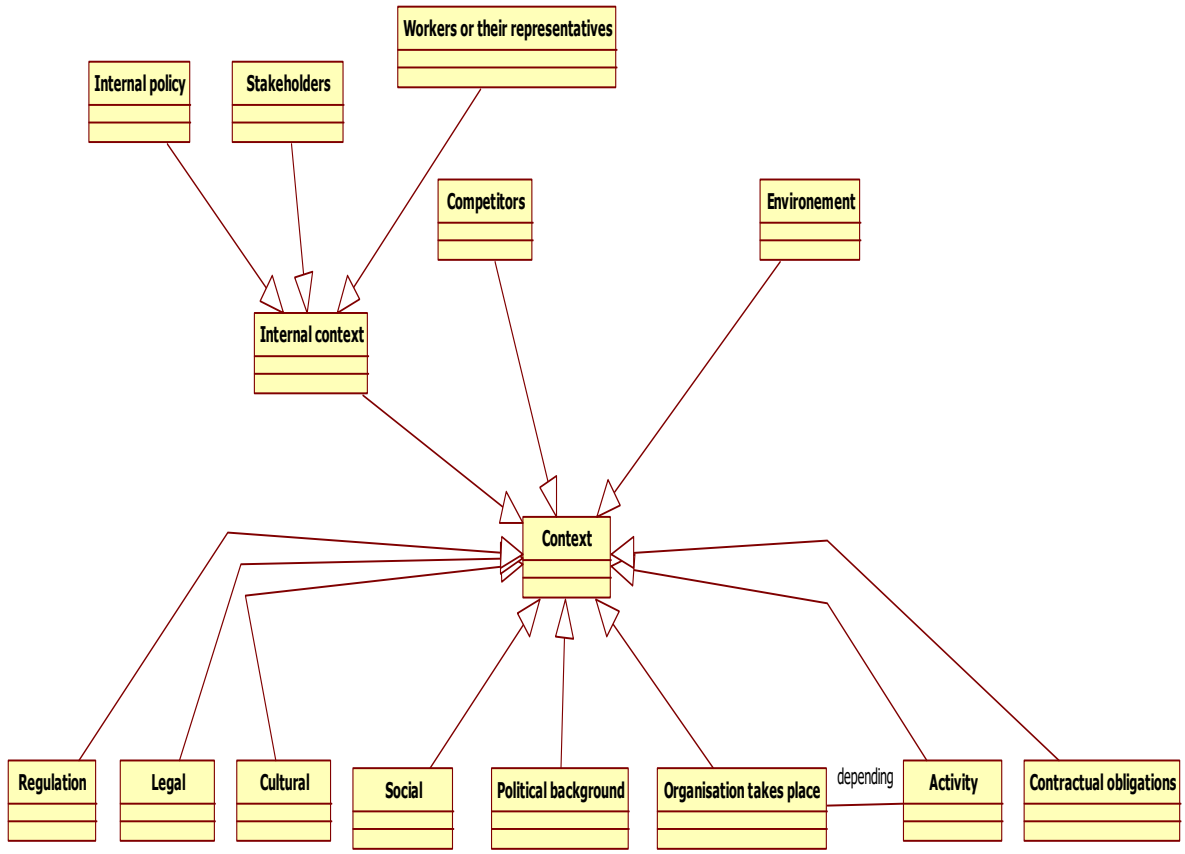


Figure 42 : Modèle du contexte d'après MAGERIT.

La norme **ISO 9001** : 2015 (ISO 9001, 2015) définit une série d'exigences concernant la mise en place d'un système de gestion du management de la qualité dans un organisme, quels que soient sa taille et son secteur d'activité.
Dans sa dernière version, la norme ajoute un chapitre dédié au contexte où elle le présente comme un concept qui joue un rôle primordial dans l'organisation.
D'après cette norme, le contexte est composé de deux catégories, l'une est interne où l'on retrouve les valeurs internes, la culture interne et les connaissances acquises en interne, mais aussi une autre qui traite du contexte externe (voir figure **43**).

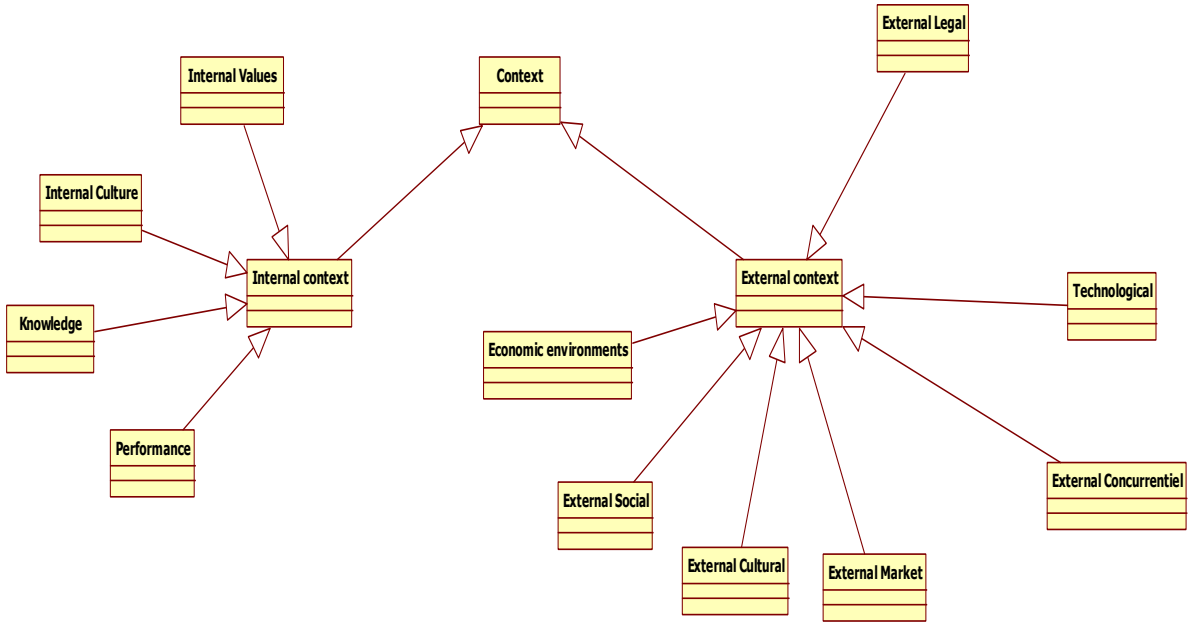


Figure 43 : Modèle du contexte d'après ISO 9001 :2015.

L'ISO/CEI 27000 :2016 offre les définitions d'usage courant dans la famille de normes du système de management de la sécurité de l'information. La présente norme internationale est applicable à tous les types et à toutes les tailles d'organismes.
Cette norme propose d'après les définitions des concepts du domaine, une classification du contexte très intéressante du fait qu'elle est orientée déjà sécurité. Elle catégorise le contexte en deux catégories l'une interne et l'autre externe.
Le contexte externe qui correspond à l'environnement extérieur dans lequel l'organisation cherche à atteindre ses objectifs. Cela peut inclure :

- Les aspects culturels, sociaux, politiques, juridiques, réglementaires, financiers, technologiques, économiquse, naturels ainsi que l'environnement concurrentiel, qu'il soit international, national, régional ou local ;
- Les principales tendances ayant un impact sur les objectifs de l'organisation ;
- Les relations avec et les perceptions et les valeurs des parties prenantes externes ;

Le contexte interne inclue :

- la gouvernance, la structure organisationnelle, les rôles et les responsabilités
- Les politiques, les objectifs et les stratégies qui sont en place pour les atteindre ;
- Les capacités, comprises en matière de ressources et de connaissances (par exemple capital, temps, les gens, les processus, les systèmes et les technologies);
- Les systèmes d'information, les flux d'informations et les processus de prise de décision (à la fois formel et informel) ;
- Les relations avec et les perceptions et les valeurs des parties prenantes internes ;
- La culture de l'organisation ;
- Les normes, directives et modèles adoptés par l'organisation ;
- La forme et l'étendue des relations contractuelles ».

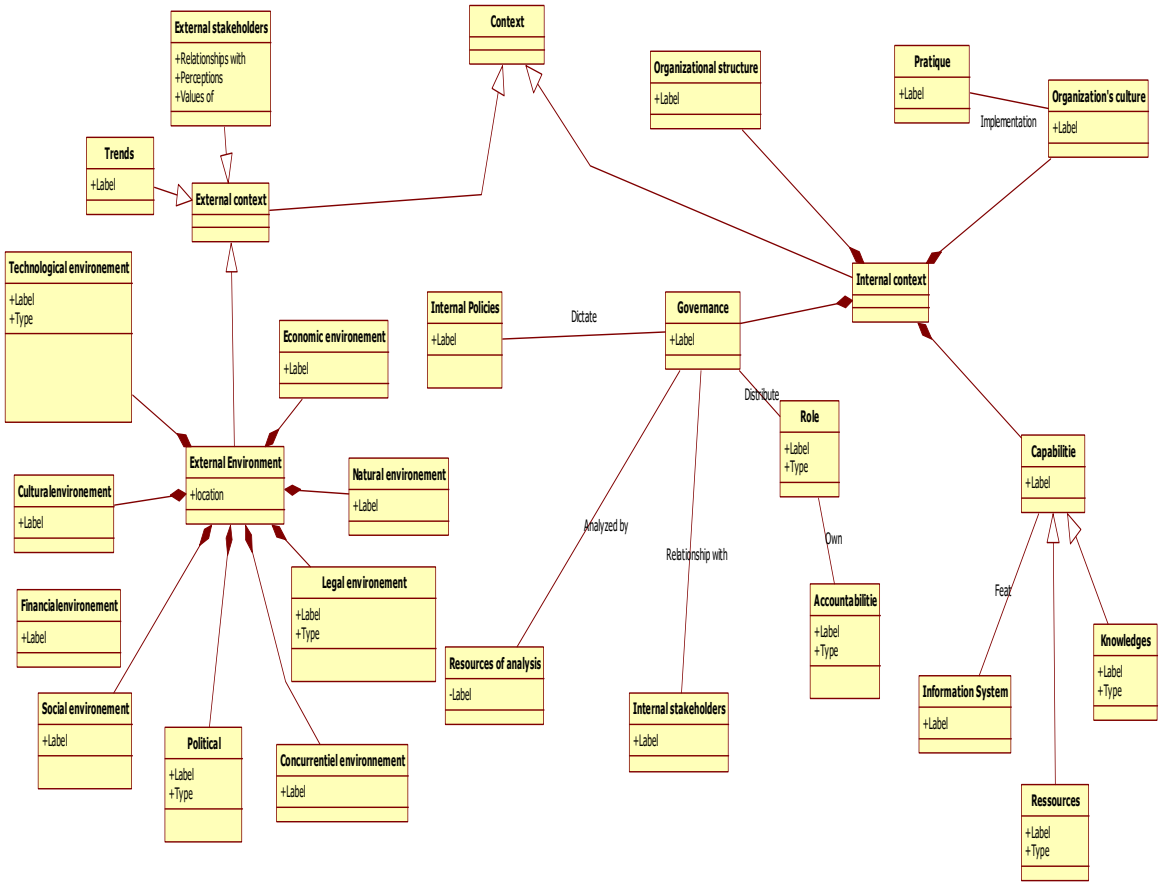


Figure 44 : Modèle du contexte d'après ISO/CEI 27000 :2016.

Dans la partie qui suit, nous proposons d'autres modèles de classification du contexte extraits de la littérature.

1. Le modèle du contexte CONON

Le modèle du contexte CONON, est développé sur la base :

- d'une ontologie de haut niveau qui capture les caractéristiques des entités générales du contexte et,
- des ontologies spécifiques de domaine et les caractéristiques de chaque sous domaine.

Il classe le contexte en quatre sous groupes (localisation, personne, activité et entité).

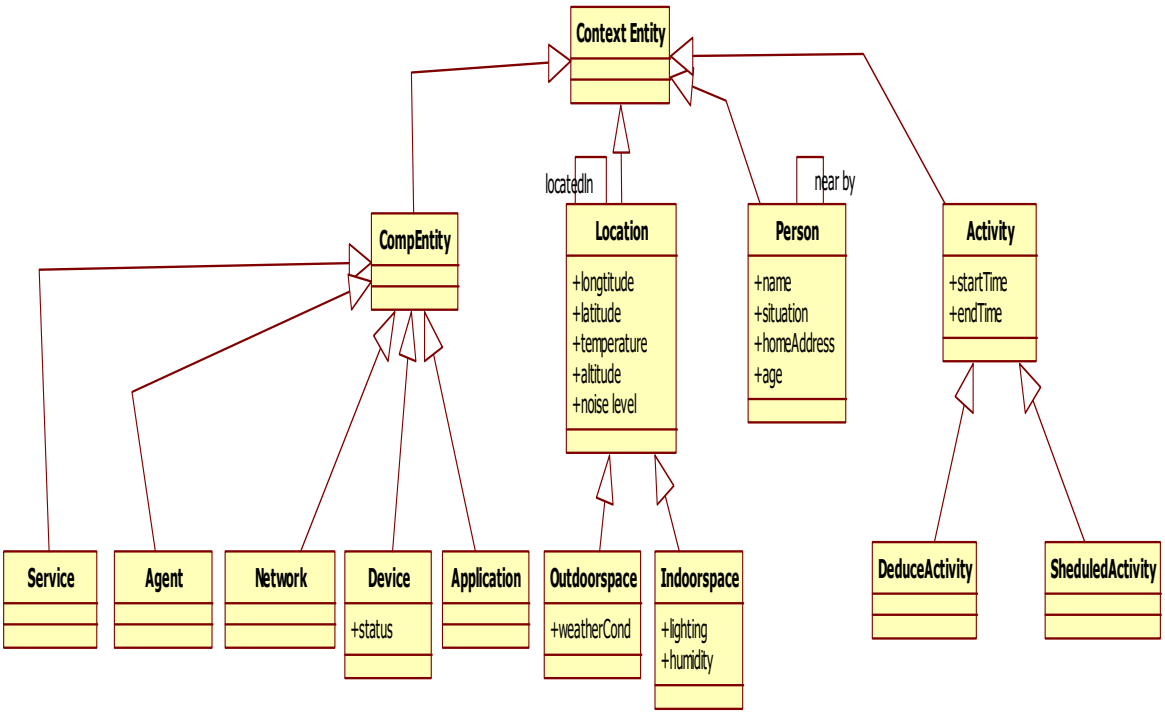


Figure 45 : Modèle du contexte CANON (Chen et al, 2003).

2. Le modèle d' Ejigu et al.

Le modèle du contexte d'Ejigu et al, classe le contexte en huit classes et propose des instances pour chacune des classes, comme suit:

- Utilisateur: l'identité, la préférence, l'activité, l'emplacement,
- Périphérique: la vitesse du processeur, taille de l'écran, l'emplacement,
- Software: la version, la disponibilité,
- Activité: domaine, l'heure de début, heure de fin, acteur, etc.
- Localisation: endroit,
- Réseau: vitesse minimale, vitesse maximale .
- Ressource: la disponibilité, taille, type, etc.
- Environnement physique: placement, l'éclairage, l'humidité ...

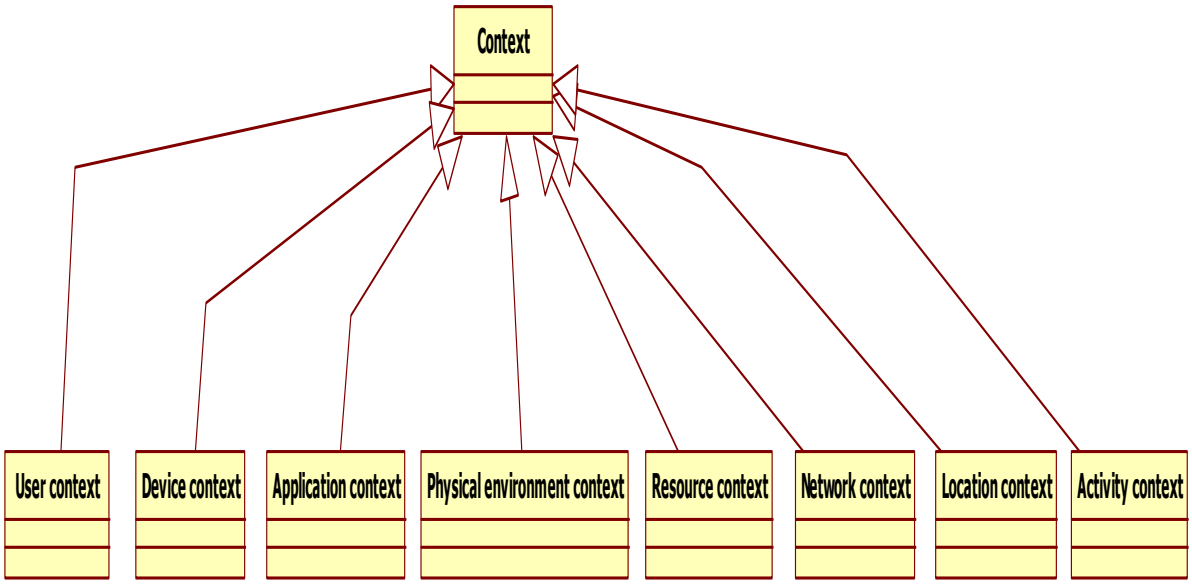


Figure 46 : Modèle du contexte (Ejigu et al, 2007).

3. **Le modèle du contexte de Cabrera et al**

Le modèle a été conçu pour des besoins spécifiques concernant l'approvisionnement de service, les auteurs ont utilié un glossaire de termes et des taxonomies conceptuelles existantes afin de construire leur modèle du contexte qu'est constitué des concepts suivant :

Temps, dans une situation particulière lorsqu'une activité se produit, c'est-à- dire le moment où une entité est impliquée dans le processus d'interaction d'approvisionnement et de la consommation de services.

Localisation, un lieu spatial physique où une entité Interagir avec un service.

Activité, déroulent avant, pendant ou après l'interaction avec un service**.**

Environnement, Paramètres de l'environnement tels que le niveau d'éclairage, la température ambiante Bruit, température, humidité, etc.,

Facteurs Humain, différents facteurs affectant l'humain avant, pendant ou après L'interaction avec un service. Par exemple, relation, social.

Ressource, exemple, smartphones, scanner, etc**.**

Politiques, sont un ensemble de règles spécifiées pour restreindre ou exécution des actions des entités avant, pendant ou après l'interaction avec un service.

Préférences, de l'entité avant, pendant ou après l'interaction avec un service.

Rôle, de l'entité avant, pendant ou après l'interaction avec un service.

Profils, de l'entité liés aux caractéristiques, capacités, l'éducation, etc., affectant la fourniture de services et consommation.

Infrastructures, prenant en charge la consommation de service.

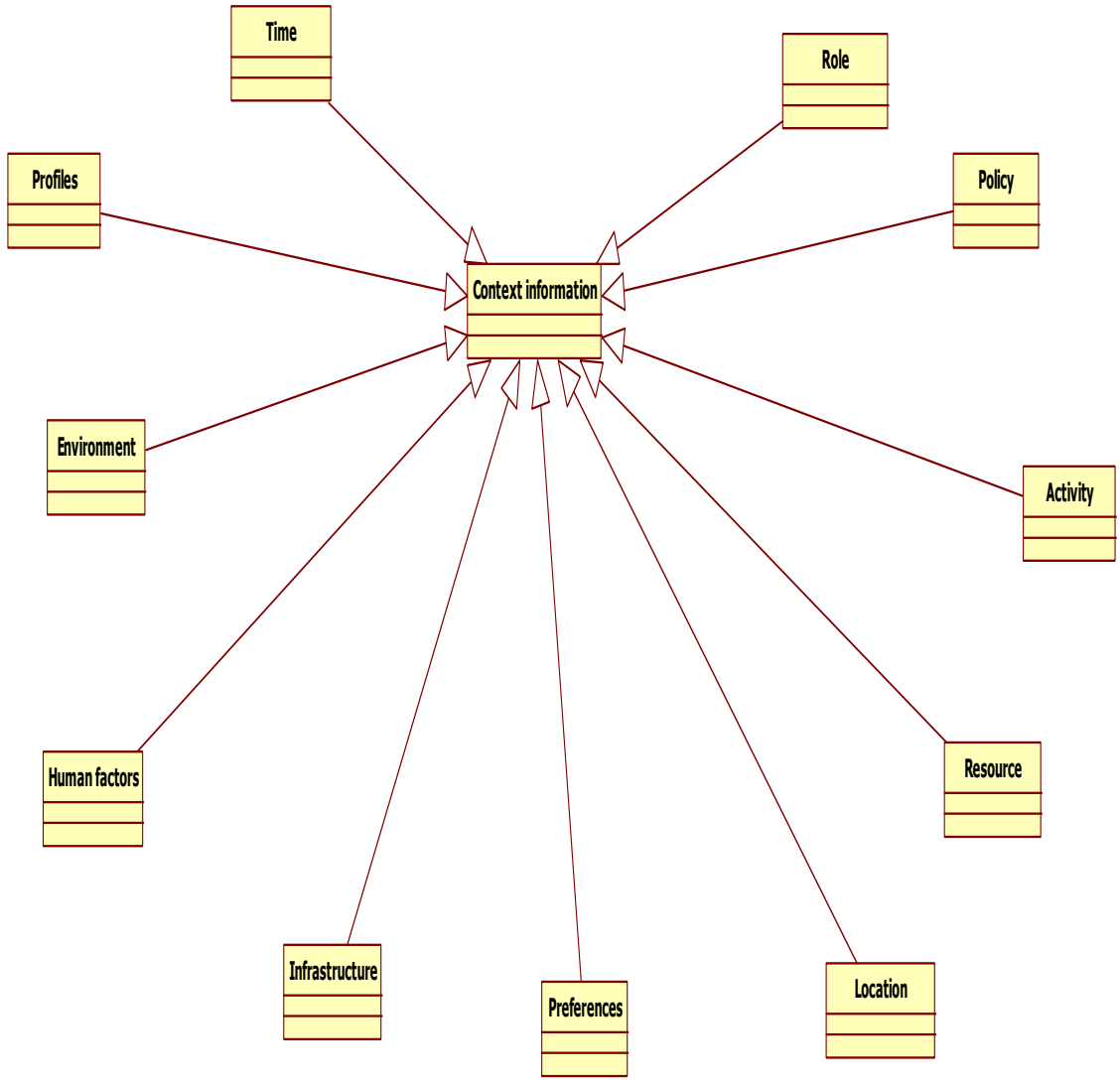


Figure 47 : Modèle du contexte (Cabrera et al, 2014).

4. Le modèle du contexte de Bulc˜ao Neto et al.

Ce modèle a été construit sur la base de réponses à cinq (05) questions qui sont :

- Qui : acteurs ;
- Où : localisation ;
- Quand : temps ;
- Quoi : activités ;
- Comment : moyens.

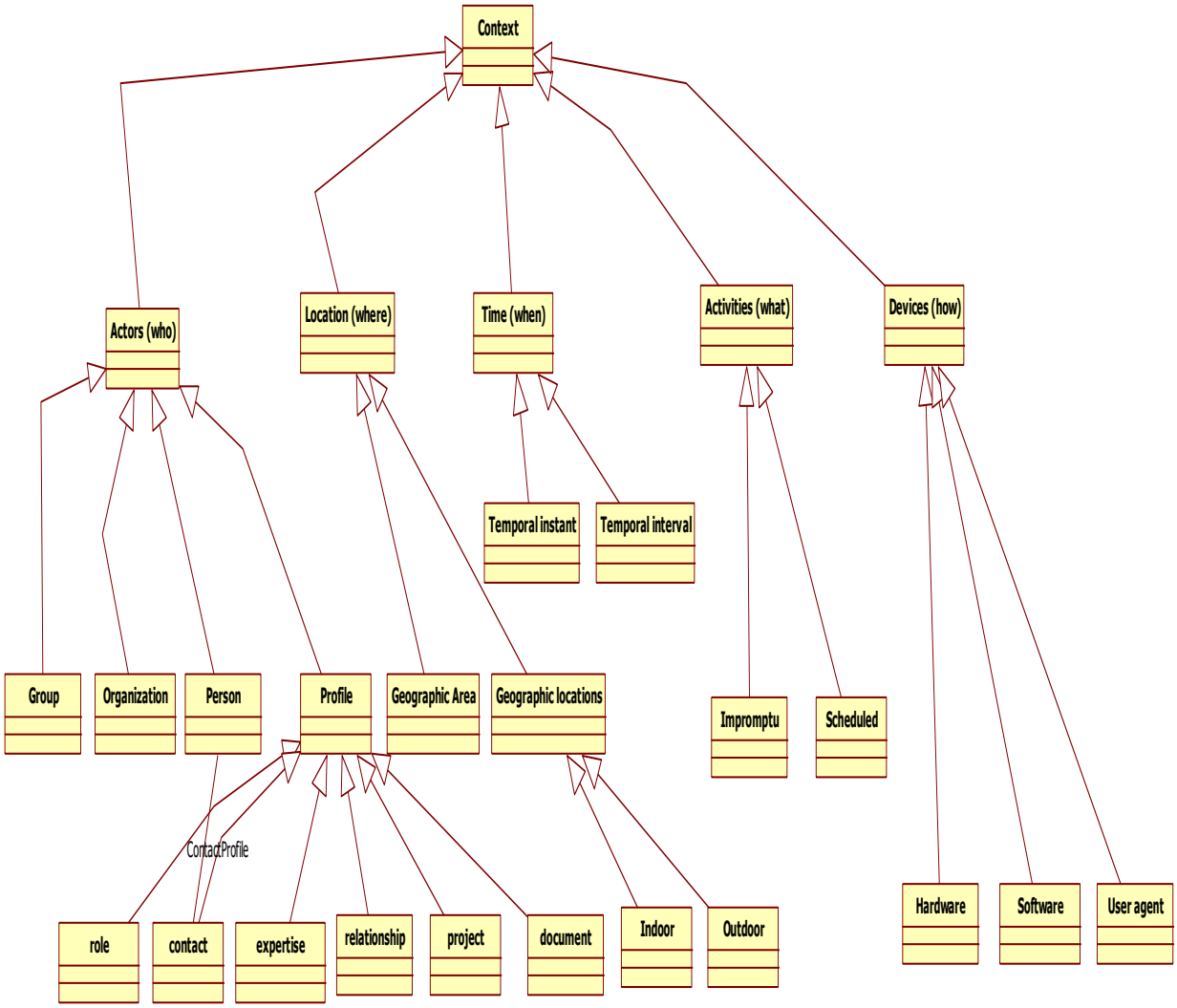


Figure 48 : Modèle du contexte d'après (Bulc˜ao Neto et al, 2005).

III.7.2 Construction de notre ontologie du contexte

Comme indiqué dans le sous chapitre **III.5.2**, nous utilisons la méthodologie **METHONTOLOGY** pour la construction de notre ontologie du contexte. Nous utilisons également les scénarios de construction d'ontologie proposés par la méthode NeOn.

III.7.2.1 Spécification

Domaine de connaissance : domaine sécurité des systèmes d'information.
Objectif : permet la caractérisation des éléments du contexte des organisations.
Utilisateurs : Praticiens et chercheurs du domaine.
Sources d'information : Norme ISO/CEI 27000 : 2016.

III.7.2.2 Acquisition des connaissances

Le but de cette phase est de fournir la liste des sources de connaissances dans le domaine de la construction de notre ontologie du contexte et de décrire le processus d'acquisition. Dans notre cas, nous avons présenté un état de l'art complet dans le sous chapitre **III.7.1**, que nous exploitons dans le cadre de nos recherches.

III.7 2.3 Construction

Nous avons choisi le modèle de la norme ISO/CEI 27000 : 2016 pour le contexte. Ce modèle répond à nos exigences, sachant que la réutilisation des ressources ontologiques sont permises dans les scénarios de construction des ontologies (voir scénarios 1 et 3 du chapitre **III.5.2**).

III.7.2.4 Intégration

Nous réutilisons les définitions proposées par la norme ISO/CEI 27000 : 2016.

III.7.2.5 Évaluation

Il existe plusieurs façons de valider les concepts et les relations d'une ontologie (Stumme et al, 2006). Dans le cas de cette ontologie, nous utilisons une classification existante d'une norme internationale de sécurité qui fait l'unanimité dans ce domaine, (ISO/CEI 27000).

NB : Dans le développement de la partie contexte externe, nous nous arrêtons au premier niveau d'abstraction dans l'ontologie, l'exploitation des éléments du contexte externe dans notre solution est envisageable dans nos perspectives.

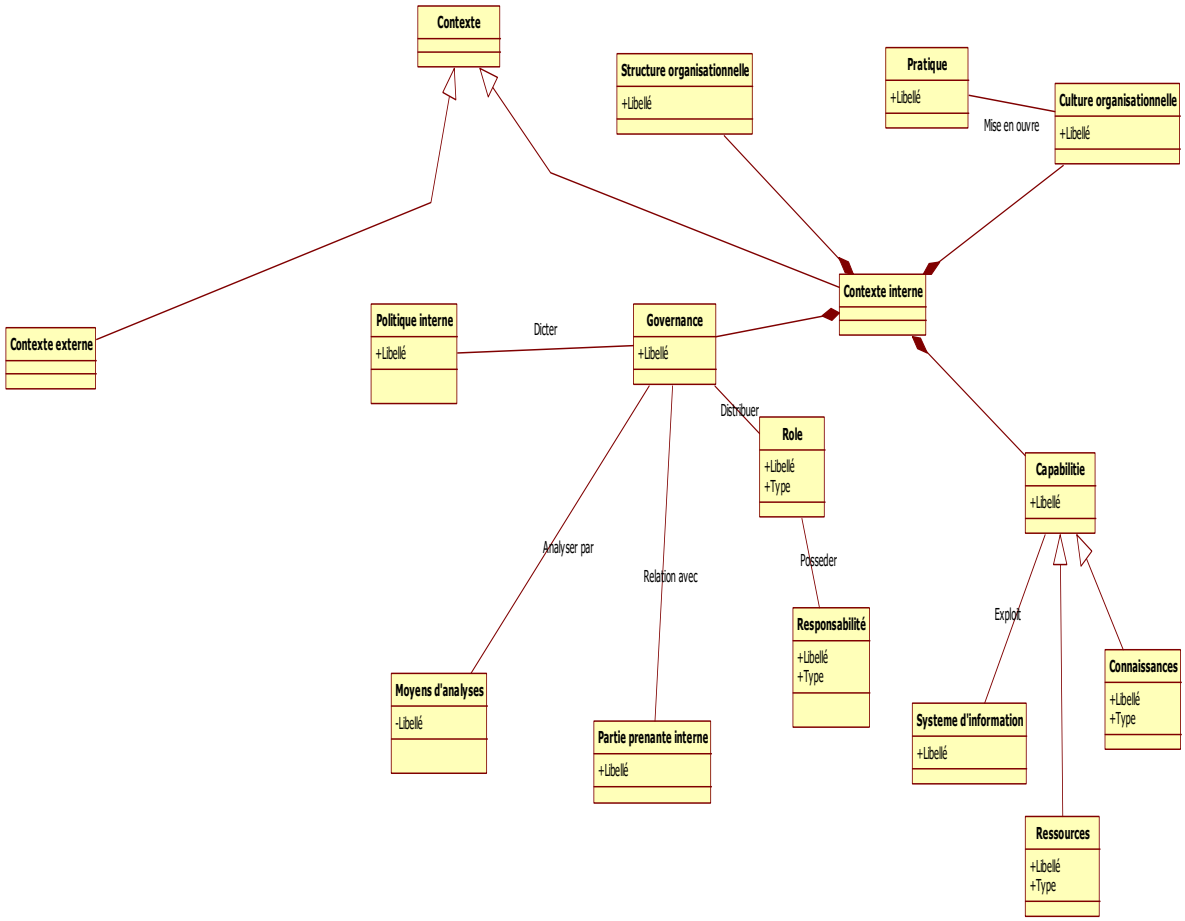


Figure 49 : Modèle de l'ontologie du contexte.

Le modèle de l'ontologie du contexte obtenus se base sur les concepts de la norme de sécurité ISO/CEI 27000 : 2016 qui engloble les principaux concepts du contexte cités dans l'état de l'art dédié (voir chapitre **III.7.1**)

Dans le section qui suit nous présentons la construction des ontologies des risques et des exigences de sécurité.

III.8 Ontologie des risques et des exigences de sécurité

Le but de cette section est de décrire le développement des deux ontologies. La première est liée aux risques tandis que la seconde est consacrée aux exigences de sécurité. Rappelons qu'une ontologie est une description explicite formelle d'un domaine, constituée de classes, qui sont les concepts trouvés dans le domaine (ISACA, 2012). Les ontologies permettent le partage des connaissances, fournissent la sémantique pour raisonner sur l'information, ce qui conduit à la logique d'inférence, et à faciliter la réutilisation des connaissances. Nous choisissons la méthodologie **MENTHONTOLOGY** (Fernandez-lopez et al, 1997) et nous appliquons les trois scénarios 1, 2 et 6 de la méthode de construction d'ontologie **NeOn**. Ces méthodes permettent de partir de l'existant et, à tout moment, de modifier, d'ajouter et ou de retirer des concepts dans l'ontologie. Ses phases sont liées à la spécification, l'acquisition de connaissances, l'intégration, la conceptualisation et l'évaluation.

III.8.1 Construction des ontologies

Dans notre processus de construction des ontologies, nous commençons par analyser les ontologies existantes, en particulier celles qui sont proposées par (Sonna Momo, 2009). Ensuite, nous complétons ces structures conceptuelles avec les termes utilisés dans les normes, les standards, les référentiels et les méthodes d'analyse de risques les plus récentes. Cela contribue à enrichir les ontologies avec des concepts structurels organisés en classes hiérarchiques. Les ontologies que nous développons sont composées de classes représentant les concepts des risques et des exigences de sécurité organisées en taxonomies hiérarchiques. Nous utilisons les termes du domaine considéré. Plus précisément, nous nous basons pour le développement de nos ontologies sur les phases suivantes proposées par **Methontology**.

III.8 1.1 Spécification

Au cours de cette phase, nous déterminons les domaines des ontologies. Des questions sont posées, telles que : quels sont les domaines que les ontologies couvriront ? Quelle est la raison de leur construction ? Plus précisément, nous caractérisons, à côté du domaine, le but, la limite et les sources de connaissance des ontologies. Dans notre cas, les domaines couverts par les ontologies sont respectivement les risques et les exigences de sécurité. Le but des ontologies est de fournir des connaissances de risques et d'exigences de sécurité génériques facilitant leur explicitation dans des contextes réels. Le champ contient des informations de risque et de sécurité ayant un impact sur les entités impliquées dans le domaine. Les sources de connaissance se composent principalement de publications académiques liées à l'ingénierie logicielle et au système d'information. Nous identifions les entités de base liées aux exigences en matière de risque et de sécurité, tels que les menaces, les accidents, les vulnérabilités, les erreurs, la sécurité des logiciels, des plans de récupération, les tests de validation, etc.

III.8 1.2 Acquisition des connaissances

Cette phase consiste à recenser les sources de connaissance traitant des ontologies des risques et exigences de sécurité et de décrire le processus d'acquisition. Dans notre cas, nous exploitons les toutes dernières connaissances émanant des ontologies, méthodes, standards et normes qui sont liées à la fois aux risques et aux exigences de sécurité. Nous nous intéressons à la classification qui a été proposée par (Souag et al, 2013). La classification fait état de l'existence de huit familles d'ontologies légère ou lourde, à savoir : les ontologies de sécurité de commencement, les taxonomies de sécurité, les ontologies générales de sécurité, les

ontologies de sécurité spécifiques, les ontologies de sécurité axées sur le Web, les ontologies de sécurité fondées sur les risques, les ontologies des exigences de sécurité et les ontologies de sécurité de modélisation.

Au cours de cette phase, après avoir analysé les risques et les méthodes d'exigence de sécurité, nous procédons à l'extraction des connaissances facilitant le choix des concepts et des entités concernées. Dans le domaine de la sécurité de l'information, les risques et les exigences de sécurité représentent les concepts les plus généraux comme c'est démontré dans les tableaux en annexes **B** et **C**.

III.8.1.3 Conceptualisation

L'objectif de cette phase est de structurer les connaissances du domaine dans un modèle conceptuel. Pour atteindre ce résultat, nous élaborons un glossaire des termes utilisés. Ensuite, on relie les termes ensemble à travers les relations taxonomiques, dont la catégorisation des mots en fonction de leurs valeurs sémantiques (reliant les concepts à ces termes) et la détermination des "questions de pertinence" potentiellement liées aux concepts candidats. Par exemple, dans le cadre de l'analyse des risques, le type de risque et son impact sur l'infrastructure physique ou sur les processus métiers sont considérés comme des concepts connexes. Chaque terme est un concept candidat et son critère de sélection nécessite une compréhension de son impact dans le cadre de la norme ISO/CEI 27000 :2016 et des méthodes associées. Si un concept est sélectionné, il constitue une classe dans l'ontologie. Dans cette phase, nous représentons dans l'ontologie chaque concept par une classe. Par exemple, les risques organisationnels sont considérés comme un type de risques liés à l'approche organisationnelle de l'entreprise. Ils représentent les risques associés aux décisions de l'organisation en raison de ses dysfonctionnements ou de l'absence de contrôle de prévention des conflits d'intérêts (pas de séparation des tâches).

Chaque classe peut avoir plusieurs sous-classes qui représentent des concepts plus spécifiques qui font partie de la même hiérarchie établie pour la classe "mère". L'approche utilisée pour développer les ontologies est fondée sur une organisation de concepts en commençant par des concepts plus généraux du domaine, puis poursuivant avec la définition de concepts plus spécifiques. En outre, la construction des ontologies prend en compte les relations menant à la cohérence de la structure taxinomique. La définition des relations hiérarchiques entre les concepts fournit une compréhension claire des relations entre les classes et sous-classes. Chaque classe doit avoir un sens unique, mais chaque sous-classe représente une spécificité de la classe correspondante.

III.8 1.4 Intégration

En raison des nombreux ouvrages sur le sujet, nous réutilisons les définitions existantes dans les autres ontologies. En particulier, cette étape permet la réconciliation des terminologies contradictoires et la détection puis l'élimination des conflits entre concepts.

III.8.1.5 Évaluation

Un procédé de validation de la pertinence des relations taxonomiques fondées sur les travaux de (Stumme et al, 2006), est appliqué. Il est décrit en détail dans le chapitre **IV**.

III.8.1 Ontologie des risques

En utilisant l'approche décrite dans les phases mentionnées ci-dessus, nous obtenons une ontologie composée des principaux concepts suivants (nous indiquons entre crochets les références correspondant à l'origine des concepts) :

• **Les risques organisationnels** : Ces risques sont associés aux décisions de l'organisation en raison de son mauvais fonctionnement ou de l'absence de contrôle de prévention des conflits d'intérêts (séparation des tâches).
Ils peuvent être divisés au deuxième niveau de l'ontologie en risques liés respectivement à un manque de contrôle et à un manque de processus d'escalade.
Au troisième niveau, les risques de contrôle, qui sont liés à un manque ou à l'absence de processus contrôlés consacrés à l'attribution des profils d'accès et d'utilisation, comprennent les risques de procédure, les risques de contrôle d'accès et les risques de contrôle d'utilisation. Les risques de procédure sont les risques qui peuvent être générés par un manque de contrôles de sécurité et / ou par un manque de processus de gestion. Les risques de contrôle d'accès sont associés à des risques résultant de l'affectation inappropriée des profils d'accès aux ressources. Enfin, les risques de contrôle d'utilisation sont liés à une mauvaise utilisation des ressources (Mayer, 2009).

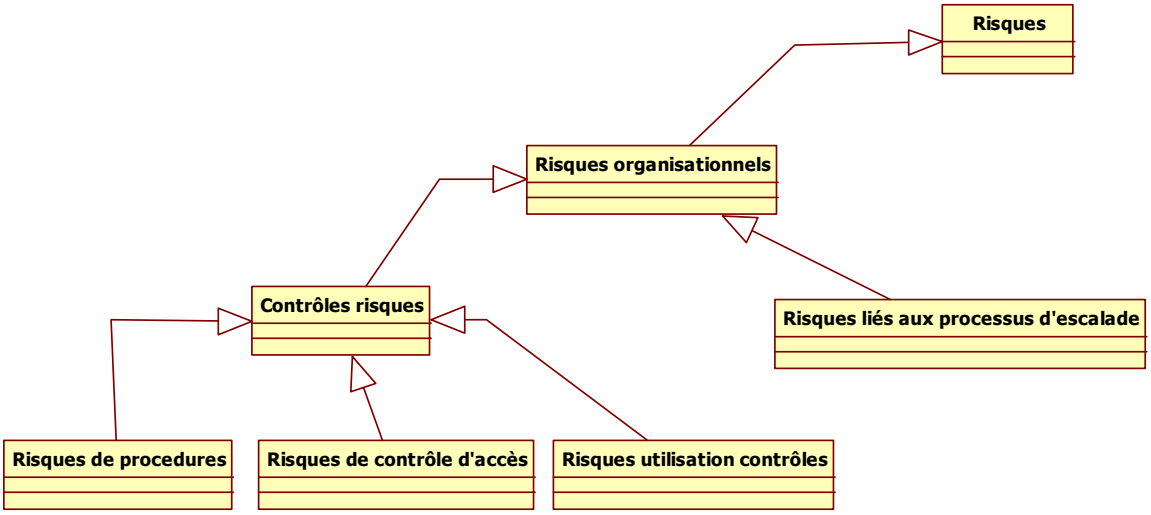


Figure 50 : Partie de l'ontologie des risques (Risques organisationnels).

• **Les risques résiduels** : Nous considérons les risques qui sont latents dans le système et découlent de l'application des mesures de sécurité visant à l'élimination, l'atténuation, le transfert ou l'acceptation des risques. (CRAMM, 2003)

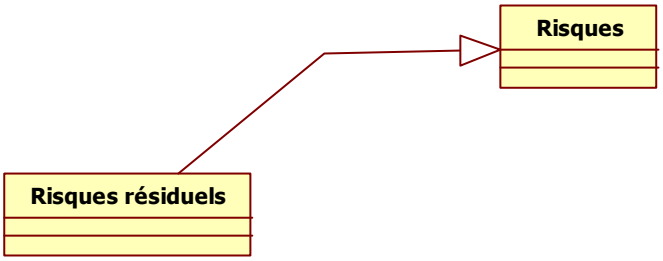


Figure 51 : Partie de l'ontologie des risques (Risques résiduels).

• **Accidents** : Ce sont des événements aléatoires, souvent imprévus, causés par des instabilités physiques ou techniques. Ils comprennent la destruction physique des actifs, la dégradation de la performance de l'actif, la destruction du logiciel et la modification de données considérées comme des actifs (EBIOS, 2010) (Mayer, 2009) (Sonna Momo, 2009).

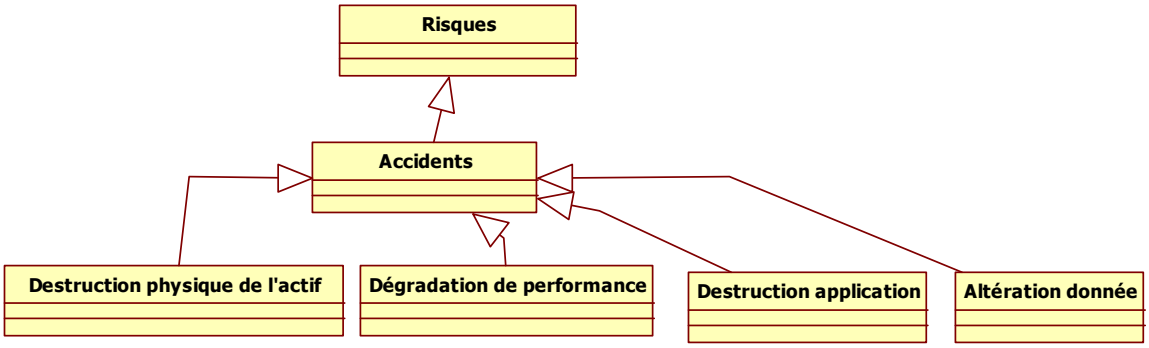


Figure 52 : Partie de l'ontologie des risques (Accidents).

• **Vulnérabilités** : Nous considérons les risques associés aux faiblesses physiques ou techniques des composants du système qui peuvent être exploités sur les actifs. Les vulnérabilités peuvent être définies comme des éléments faibles ou exploitables inhérents du SI et peuvent mettre en danger les actifs. Ils comprennent les vulnérabilités techniques résultant des éléments techniques entraînant des risques pour le système et les vulnérabilités physiques liées aux risques qui peuvent être générés par des éléments physiques (Mayer, 2009) (NIST, 2015) (Salini et al, 2008).

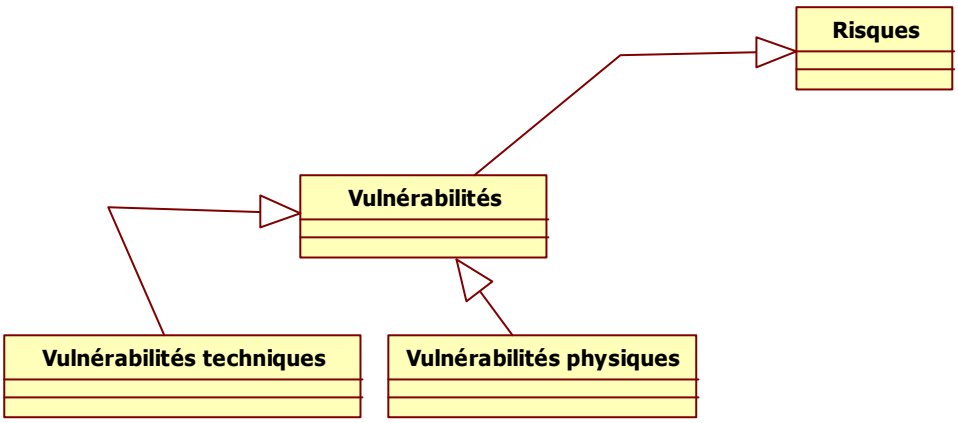


Figure 53 : Partie de l'ontologie des risques (Vulnérabilités).

• **Actions malveillantes** : Ce sont des faits, volontaires ou non, affectant la sécurité des actifs, les mettant en danger. Elles peuvent être décomposées en problèmes de sécurité liés à l'indisponibilité, la déviation, la manipulation et la disparition de l'information (Mayer, 2009) (Sonna Momo, 2009).

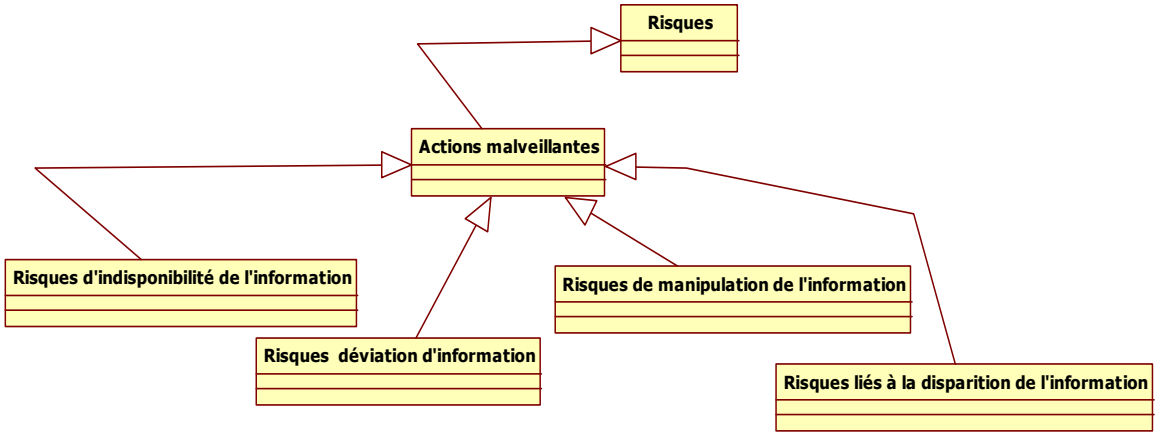


Figure 54 : Partie de l'ontologie des risques (Actions malveillantes).

• **Les risques de dommages des actifs** : Ils sont causés par des pannes imprévues et intempestives, connues ou accidentelles. Les raisons peuvent être des erreurs ou des actions malveillantes. Ils affectent les actifs. Ces risques concernent les actifs physiques, les échecs des opérations de logiciels et de matériel, l'utilisation non autorisée et la violation des critères de sécurité de l'information. Cette violation peut être décomposée respectivement en confidentialité, disponibilité, traçabilité, intégrité, efficacité, efficience et critères de qualité (FMECA, 1993).

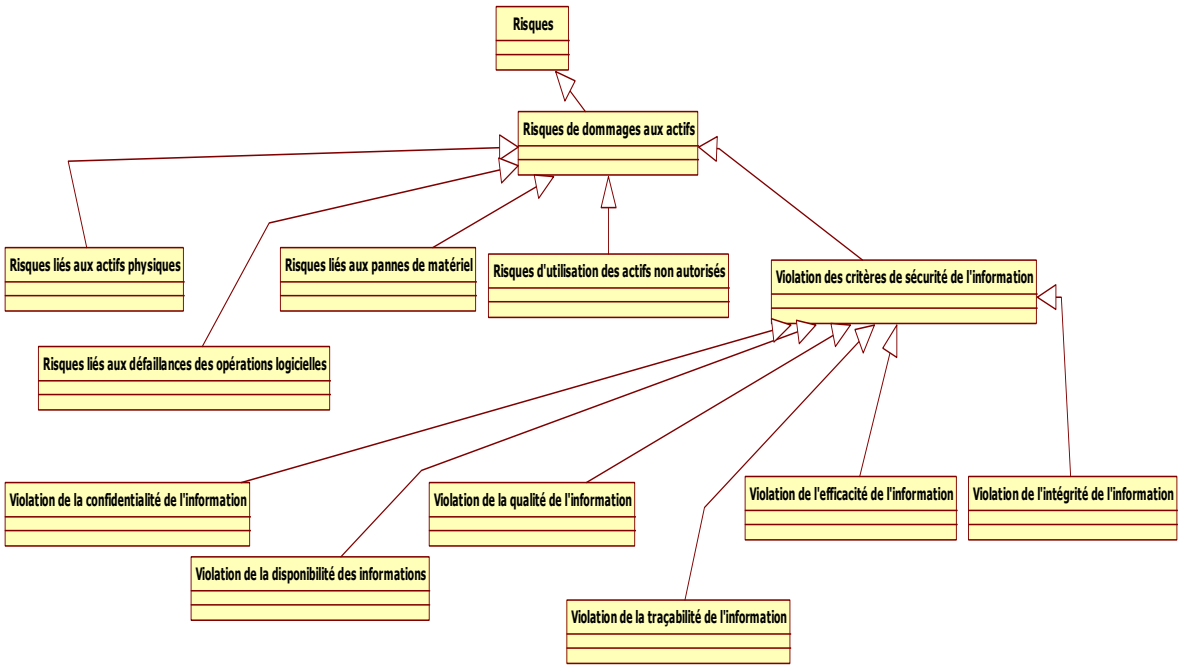


Figure 55 : Partie de l'ontologie des risques (Risques de dommages aux actifs).

• **Risques Business :** Ce type de risque est associé aux dynamiques internes et externes qui pourraient générer des risques pour l'entreprise. Il inclut les risques inattendus qui dépendent de facteurs de contingence tels que les virus, les risques de concurrence générés par le comportement et les stratégies des concurrents et les risques financiers conduisant à des pertes financières (ISACA, 2012).

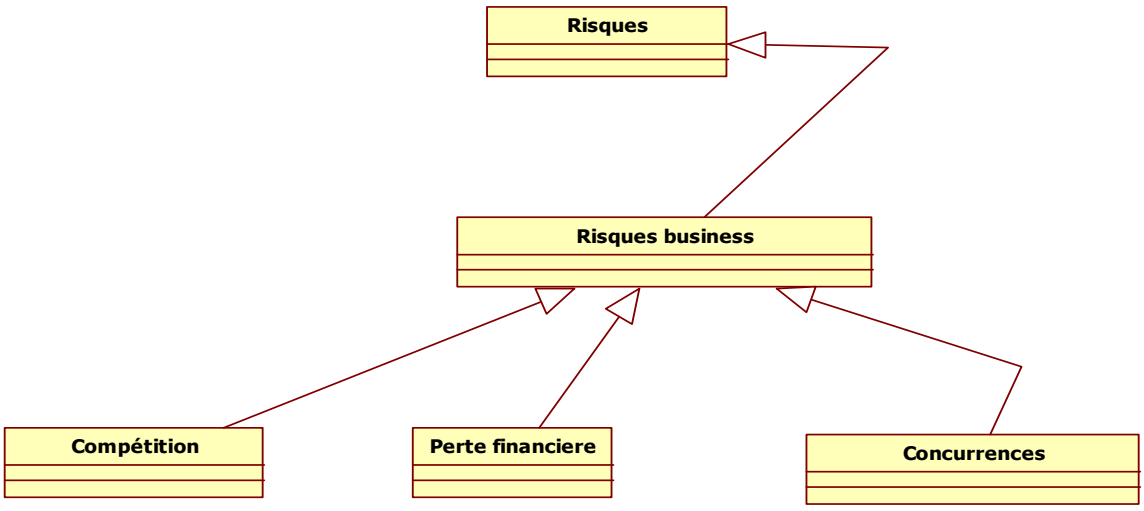


Figure 56 : Partie de l'ontologie des risques (Risques business).

Risques erreurs : Elles comprennent les risques d'utilisation, les risques d'exécution, les erreurs techniques et humaines. Les erreurs d'utilisation sont généralement associées à une utilisation inadéquate des ressources. Elles comprennent les erreurs de transmission, les erreurs de saisie de données et les erreurs de traitement conduisant à une perte d'information, à la destruction de cette dernière et à l'incohérence des données. Les erreurs d'exécution comprennent la conception, le développement et les erreurs de mise en œuvre (Mayer, 2009) (Sonna Momo, 2009).

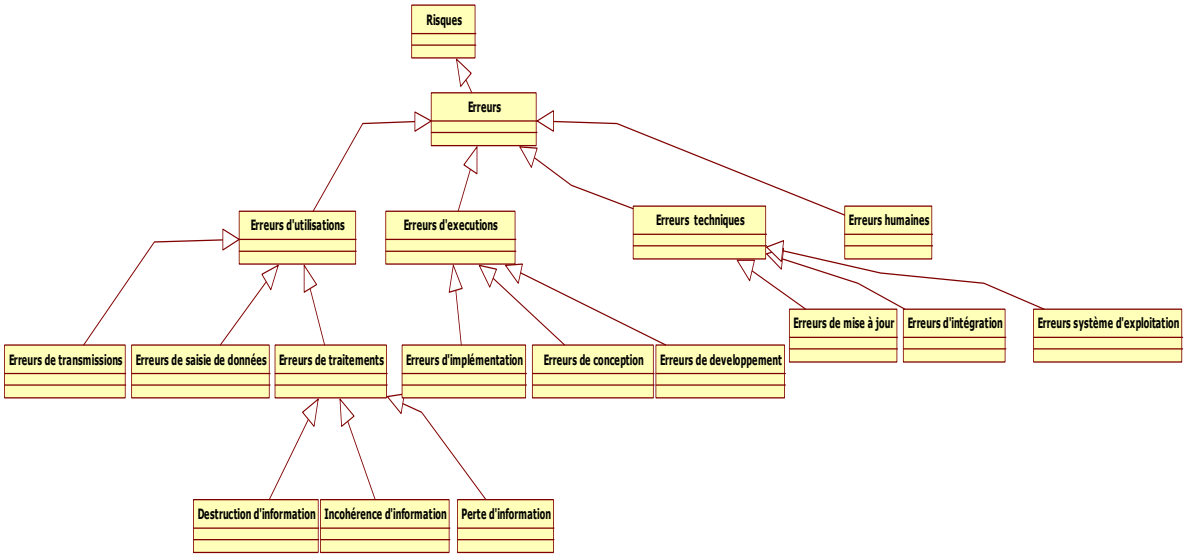


Figure 57 : Partie de l'ontologie des risques (Erreurs).

• **Les menaces** : Ce sont des événements qui se produisent dans le contexte d'un système d'information. Ils peuvent affecter ou déprécier les actifs. Ce sont des événements réels ou présumés qui peuvent affecter le SI. Ils sont composés d'attaques physiques conduisant à la destruction physique des actifs ainsi que les attaques techniques conduisant à la destruction logique des actifs (CRAMM, 2003).

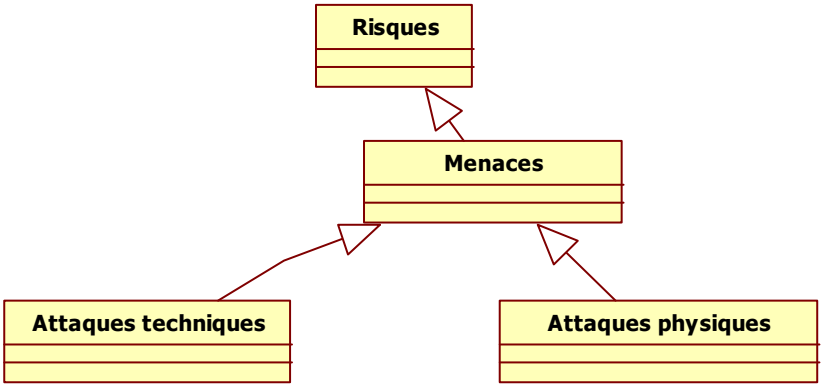


Figure 58 : Partie de l'ontologie des risques (Menaces).

• **Risques d'événements non planifiés** : Ce sont les risques liés aux changements imprévus dans les projets et les risques concernant les défaillances de fonctionnements imprévus (FMECA, 1993).

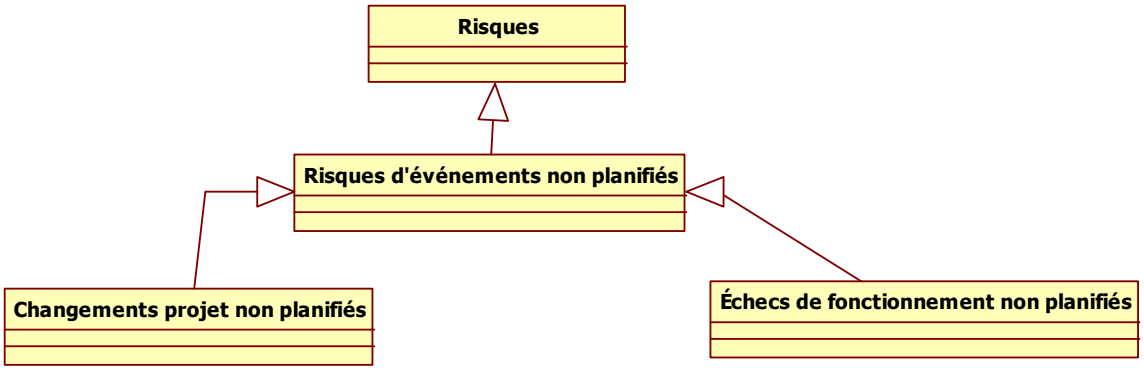


Figure 59 : Partie de l'ontologie des risques (Risques d'événements non planifiés).

L'ontologie complète des risques est présentée en annexe **A**. Mentionnons le fait que les concepts et leurs relations sont extraits des méthodologies décrites ci-dessus. Ils peuvent être communs à plusieurs méthodes. Nous choisissons d'utiliser les concepts trouvés dans les ontologies les plus explicites. Dans certains cas, nous complétons l'ontologie avec des concepts issus de notre propre expertise. L'origine des concepts représentés dans l'ontologie est présentée en annexe **B**.
Le modèle de l'ontologie des risques obtenu se base sur les concepts utilisés dans les normes, les standards, les référentiels et les méthodes d'analyse de risques les plus récents. Cela nous a permis d'obtenir une ontologie des risques riche avec des concepts structurels organisés en classes hiérarchiques. L'ontologie développée est composée de classes représentant les concepts des risques organisés en taxonomies hiérarchiques.

III.8.2 Ontologie des exigences de sécurité

De même que pour la construction des (03) trois ontologies précédentes, nous présentons ci-dessous, les termes les plus pertinents pour l'ontologie des exigences de sécurité.

1. Les tests de validation et de contrôle correspondent à plusieurs étapes du procédé, ce concept permet la validation et la quantification des caractéristiques du système et du logiciel associé. SIREN (Toval et al, 2001)

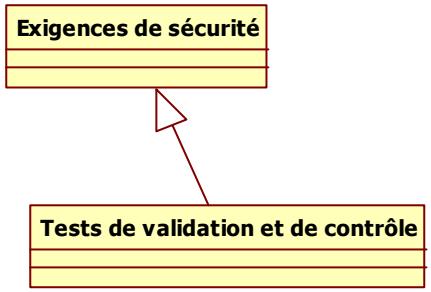


Figure 60 : Partie de l'ontologie des exigences de sécurité (Test validation et de contrôle).

2. **Objectifs de sécurité** : Ils consistent à définir les objectifs poursuivis par l'organisation en matière d'exigences de sécurité. Ils comprennent des objectifs liés à la maîtrise des vulnérabilités, au contrôle des menaces et aux objectifs de protection de l'information. Ces derniers peuvent être divisés en objectifs de disponibilité, d'intégrité, de confidentialité et de traçabilité. (MEHARI, 2010) (Matulevicius et al, 2008) (Shamal et al, 2010) (Toval et al, 2001).

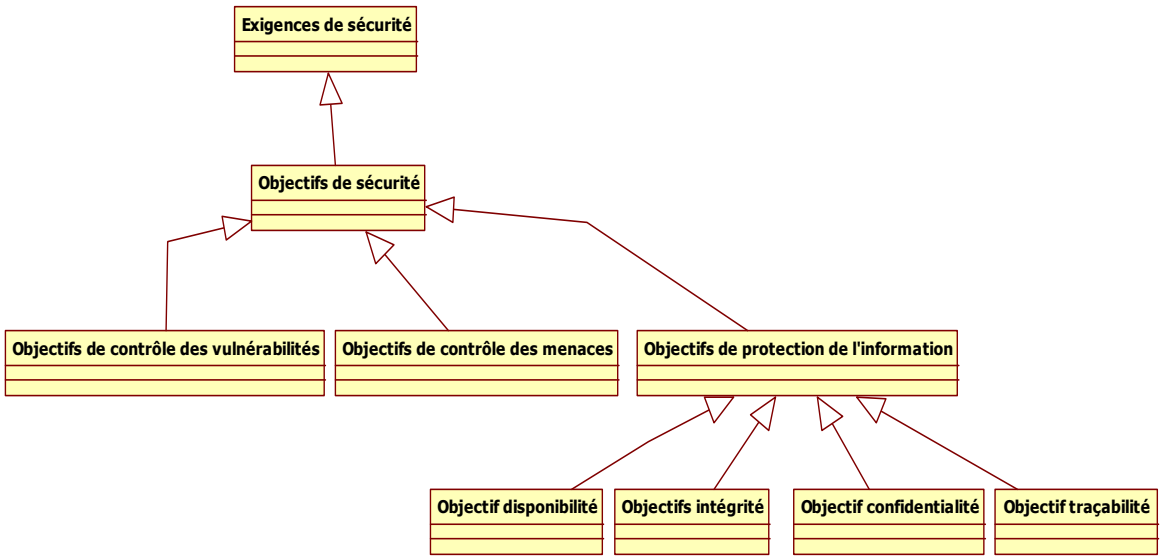


Figure 61 : Partie de l'ontologie des exigences de sécurité (Objectifs de sécurité).

3**. Exigences de sécurité du logiciel** : C'est le processus d'établissement d'objectifs de sécurité du logiciel en ce qui concerne le niveau de fonctionnalité et d'évolution nécessaire. Ce processus englobe les exigences de fonctionnement et les exigences d'interface externe. Les exigences de fonctionnement comprennent la mise en œuvre, la performance, la durabilité

et les exigences d'adaptabilité. Les exigences d'interface externe incluent le logiciel, l'utilisateur, l'infrastructure physique et les interfaces de communication (Toval et al, 2001).

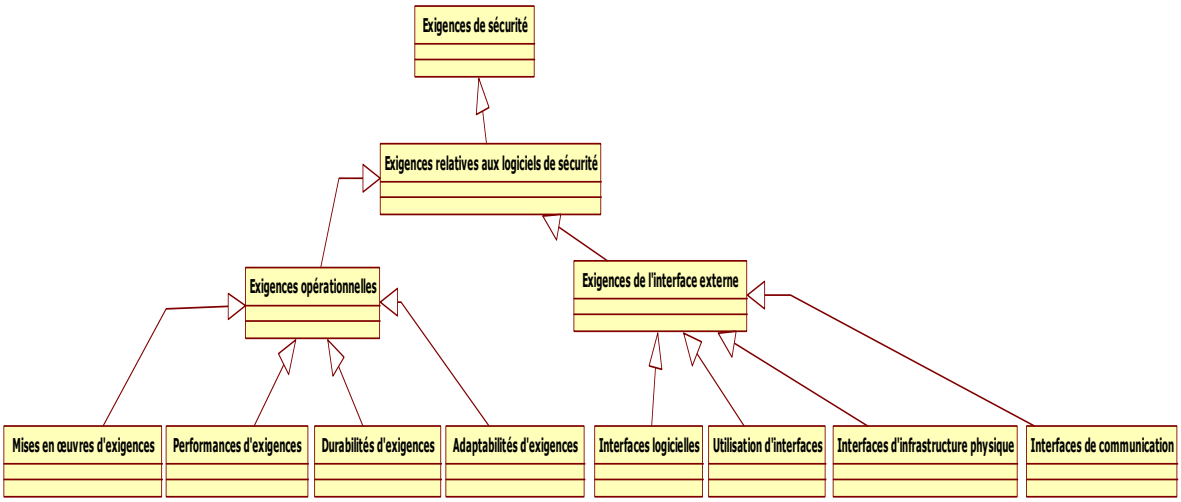


Figure 62 : Partie de l'ontologie des exigences de sécurité (Exigences de sécurité aux logiciels de sécurité).

4. **Stratégie de sécurité** : Nous considérons comme stratégie de sécurité les exigences imposées par l'entreprise et / où l'organisation du système d'information pour maintenir un cours normal des processus et activités. C'est le processus qui met les meilleures pratiques en alignement avec la stratégie de l'organisation. Il comprend l'existence d'un service de sécurité, d'un plan stratégique de sécurité, d'une politique de dotation de sécurité et d'un plan de sécurité de sensibilisation et de formation (Common Criteria, 2012).

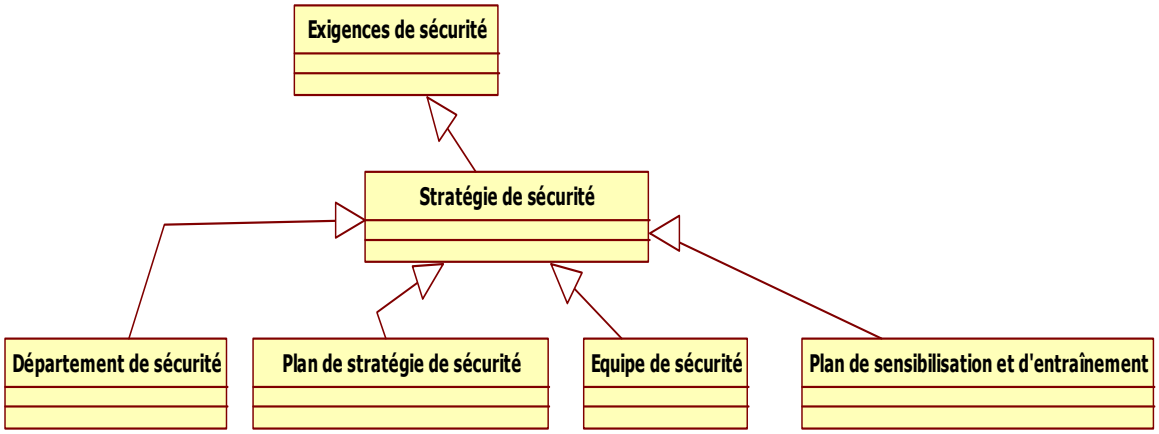


Figure 63 : Partie de l'ontologie des exigences de sécurité (Stratégie de sécurité).

5. **Plan de relance du système** : Il comprend un plan de reprise après un désastre, un plan de redressement de l'entreprise et le stockage des meilleures pratiques (Common Criteria, 2012).

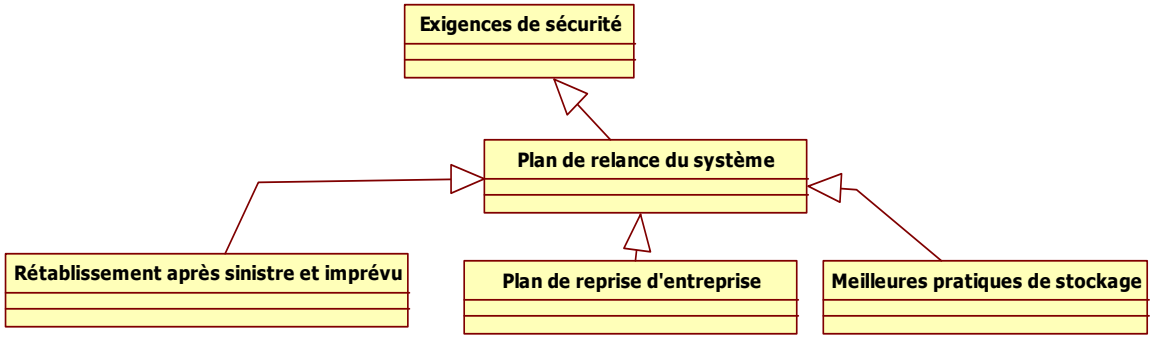
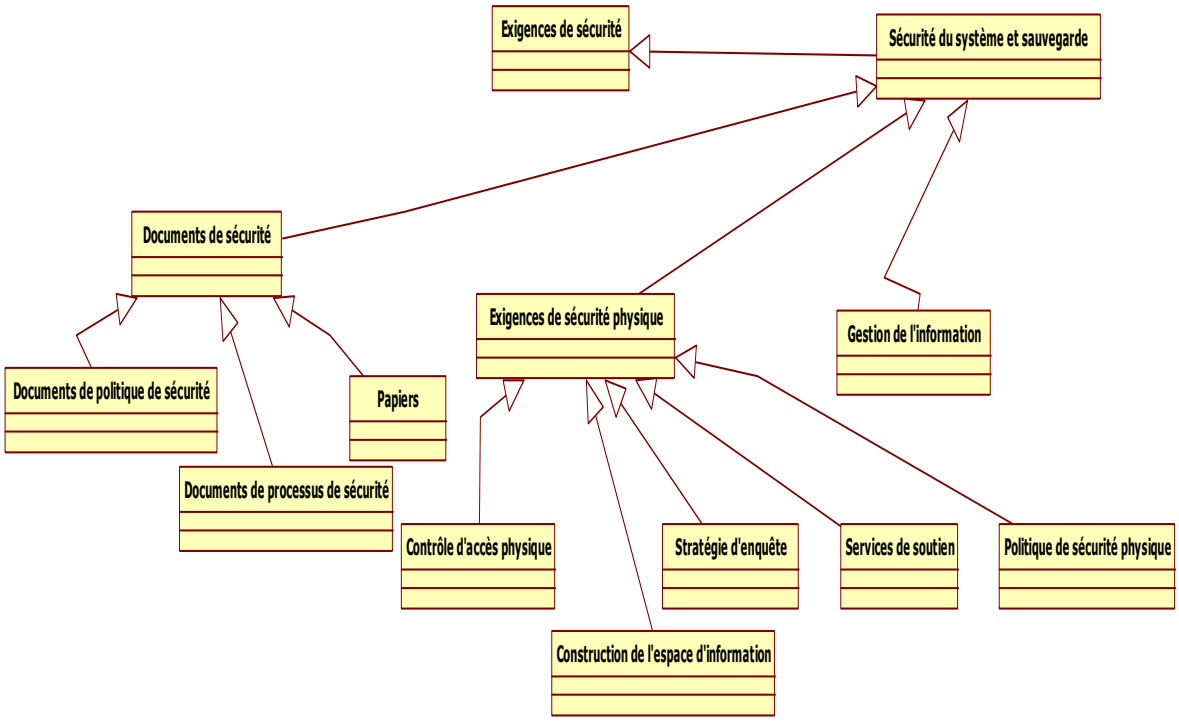
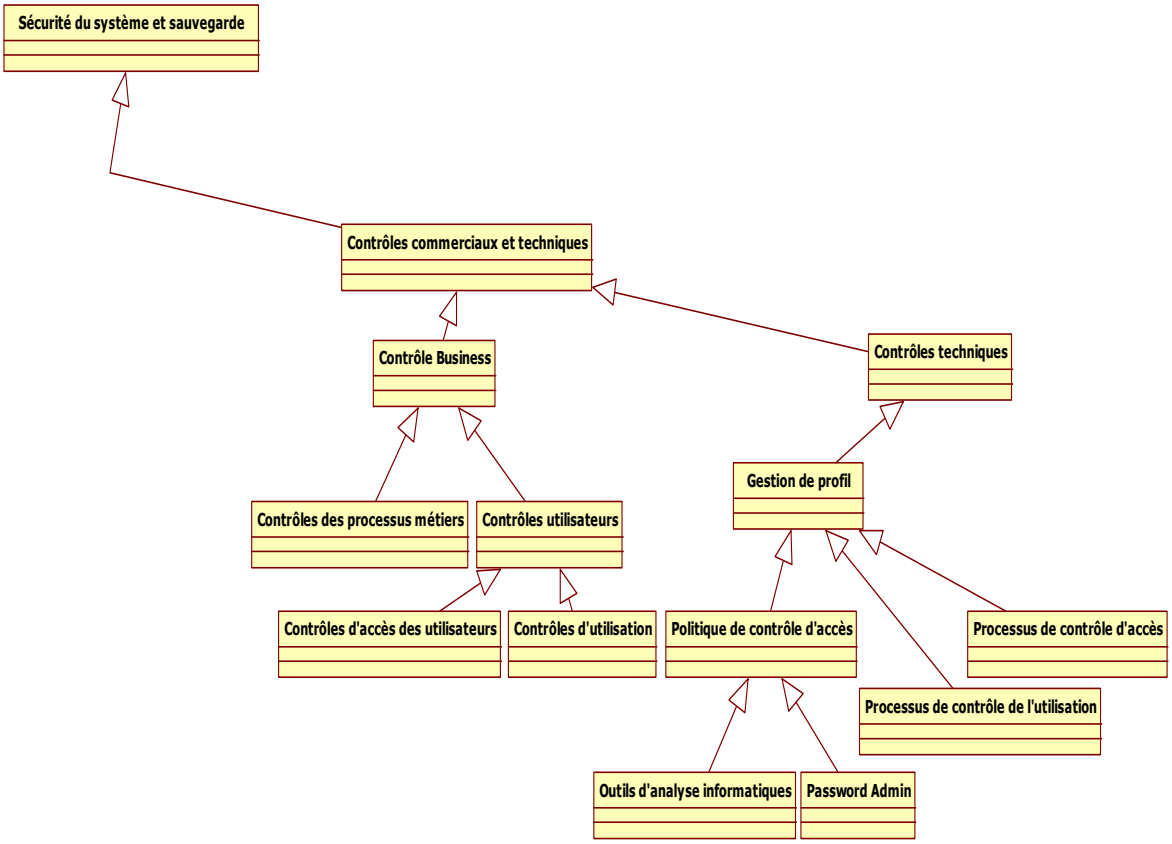


Figure 64 : Partie de l'ontologie des exigences de sécurité (Plan de relance du système).

6. **Sécurité du système et sauvegarde** : C'est le processus de définition des exigences afin d'être en mesure d'assurer un niveau de sécurité et de sûreté. Ce niveau est décomposé en quatre sous-niveaux : documents de sécurité, exigences de sécurité physique, gestion de l'information et exigences commerciales et techniques. Les documents de sécurité sont décomposés dans les politiques de sécurité en documents de traitement de sécurité et en documents de travail. Les exigences de sécurité physiques sont composées de contrôles d'accès physiques, y compris les dispositifs d'accès et les contrôles d'accès du personnel, la construction de l'espace des informations telles que les centres de données, la stratégie d'enquête telles que des pistes de vérification, les services de soutien, y compris les services d'énergie et les services des dispositifs physiques et la politique de sécurité physique. Les contrôles commerciaux et techniques sont divisés en deux composantes : les contrôles d'affaires et les contrôles techniques. Les contrôles d'affaires englobent les contrôles des processus d'affaires et les contrôles des utilisateurs. Ces derniers comprennent les contrôles d'accès de l'utilisateur et les contrôles d'usage. Les contrôles techniques sont divisés en gestion des profils, contrôles de sécurité de l'infrastructure physique, mécanismes de surveillance et en contrôle de gestion des incidents. La gestion des profils est divisée en politique de contrôle d'accès, y compris l'analyse informatique judiciaire et l'administration des mots de passe, les processus de contrôle d'utilisation et les processus de contrôle d'accès. Les contrôles de sécurité de l'infrastructure physique se composent des contrôles des virus et des contrôles de gestion de l'infrastructure de sécurité. La surveillance englobe les rapports de sécurité et les actions de prévention. Enfin, la gestion des incidents concerne le journal de stockage ainsi que l'analyse de l'enquête de l'incident.


Exigences de sécurité
Sécurité du système et sauvegarde
Documents de sécurité
Exigences de sécurité physique
Gestion de l'information
Documents de politique de sécurité
Papiers
Documents de processus de sécurité
Contrôle d'accès physique
Stratégie d'enquête
Services de soutien
Politique de sécurité physique
Construction de l'espace d'information


Sécurité du système et sauvegarde
Contrôles commerciaux et techniques
Contrôle Business
Contrôles techniques
Gestion de profil
Contrôles des processus métiers
Contrôles utilisateurs
Contrôles d'accès des utilisateurs
Contrôles d'utilisation
Politique de contrôle d'accès
Processus de contrôle d'accès
Processus de contrôle de l'utilisation
Outils d'analyse informatiques
Password Admin

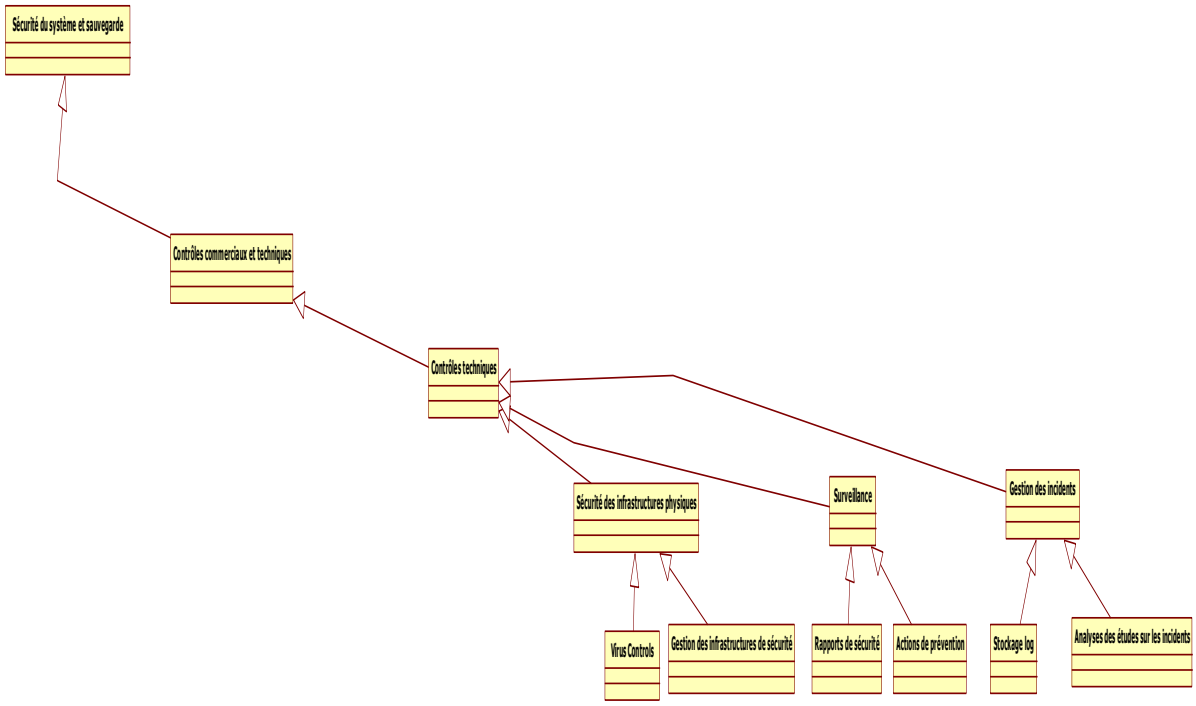


Figure 65 : Partie de l'ontologie des exigences de sécurité (Sécurité du système et sauvegarde).

L'ontologie des exigences de sécurité, ainsi que les origines des concepts représentés dans l'ontologie sont présentées respectivement dans les annexes **A** et **B**.

Le modèle de l'ontologie des exigences de sécurité obtenu se fonde sur les concepts utilisés dans les méthodes d'élicitation des exigences de sécurité les plus citées dans la littérature spécialisée. Cela nous a permis d'obtenir une ontologie des exigences de sécurité riche avec des concepts structurels organisés en classes hiérarchiques. L'ontologie développée est composée de classes représentant les concepts des exigences de sécurité organisées en taxonomies hiérarchiques.

Dans la partie qui suit, nous allons détailler notre processus de dérivation des exigences de sécurité.

III.9 Description détaillée des différentes étapes de l'approche

Rappelons que notre processus de dérivation des plans d'exigences de sécurité est composé de trois (03) phases :

1- Phase d'analyse du contexte ;
2- Phase d'analyse des risques
3- Phase de dérivation des exigences de sécurité

Phase 1 : Analyse du contexte

La première phase est composée de deux étapes :
- Identification et extraction des éléments du contexte et des actifs de l'entreprise,
- Détermination des critères de sécurité associés aux actifs de l'entreprise.

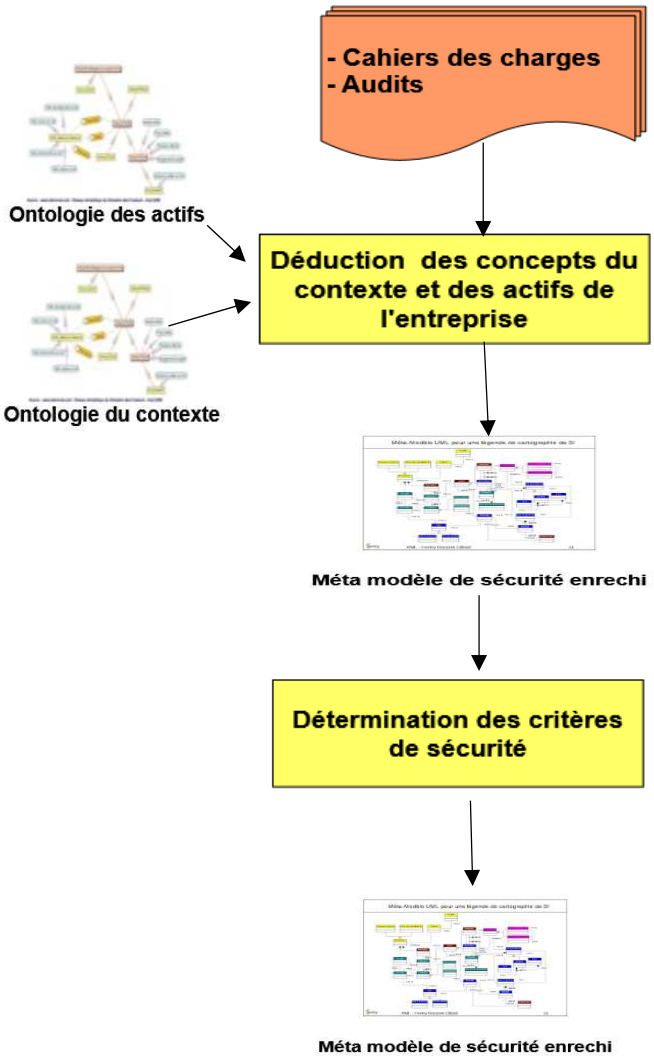


Figure 66: Première phase du processus de dérivation : Analyse du contexte.

a. Etape1 : Identification et extraction des éléments du contexte et des actifs de l'entreprise,

Cette phase requiert en entrée des informations concernant l'entreprise du champ d'étude (cahiers des charges pour la conception du SI ou des audits s'ils existent). Dans cette phase, on identifie les éléments du contexte et les actifs de l'entreprise. Pour cela, on fait appel aux ontologies du contexte et des actifs.

Nous faisons appel à une technique d'extraction d'information pour extraire, comparer et identifier les éléments du contexte et des actifs extraits des sources fournies par l'entreprise.
L'extraction d'information est un processus par lequel un système automatique est capable de traiter des documents par une approche linguistique (Turenne, 2010). Les domaines linguistiques les plus connus sont :

Morphologie : étude des types et de la formation des mots et de leurs variations. Mots simples et complexes, variables et invariables.
Syntaxe : étude de la combinaison des mots pour former des phrases ou des énoncés dans une langue;
Sémantique : étude du sens des mots, des phrases et des énoncés ;
Stylistique : étude du style d'un énoncé et la particularité d'écriture d'un texte.
Pragmatique : étude de l'utilisation des énoncés;
Cohérence : étude des facteurs de cohérence dans le traitement du langage naturel. Les informations recherchées sont généralement décrites en utilisant un langage naturel. À cette fin, nous avons fait un état de l'art sur les outils d'extraction d'informations utilisant les domaines linguistiques cités supra et qui nous donnent la possibilité de rajouter notre filtrage afin d'être en mesure d'extraire et de représenter le réseau sémantique sous-jacent. Le réseau sémantique ainsi que les résultats analytiques, qui proposent les outils de traitement de texte, nous permettent d'identifier la pertinence des concepts et de les positionner dans leurs ontologies respectives. Selon les critères retenus et cités supra, nous avons choisi les logiciels **AutoMap et ORA.**
Automap, est un outil dédié à l'exploration des textes. Il permet l'extraction d'informations à partir des textes en utilisant des méthodes d'analyse de texte. Il soutient l'extraction de plusieurs types de données, de documents non structurés. L'information qui peut être extraite comprend : le contenu des données analytiques (mots et fréquences), les données du réseau sémantique (réseau de concepts), les données méta réseau (la classification croisée des concepts dans leur catégorie ontologique comme les gens, les lieux et les choses et les liens entre ces concepts classés), et les données de sentiment (attitudes, croyances). L'extraction de chaque type de données suppose que le type précédemment énuméré de données a été extrait (Carley et al, 2013a).
En ce qui concerne le logiciel **ORA**, il sert surtout comme un outil pour la visualisation des données (Carley et al, 2013b).
Ces deux logiciels ont été développés par le groupe de recherche CASOS de la Carnegie Mellon University aux Etats Unis[10]. À noter que l'étape 1 s'exécute automatiquement en utilisant un logiciel d'exploration de texte utilisant la technique syntaxique. La mise en œuvre s'appuie pour son application sur un filtrage que nous avons conçu en utilisant les connaissances qui peuplent des ontologies du contexte et des actifs.
Le résultat de l'étape 1 est l' enrichissement du méta modèle de sécurité par les instances obtenues (contexte et actifs).

[10] Le site web du laboratoire CASOS : www.casos.cs.cmu.edu.

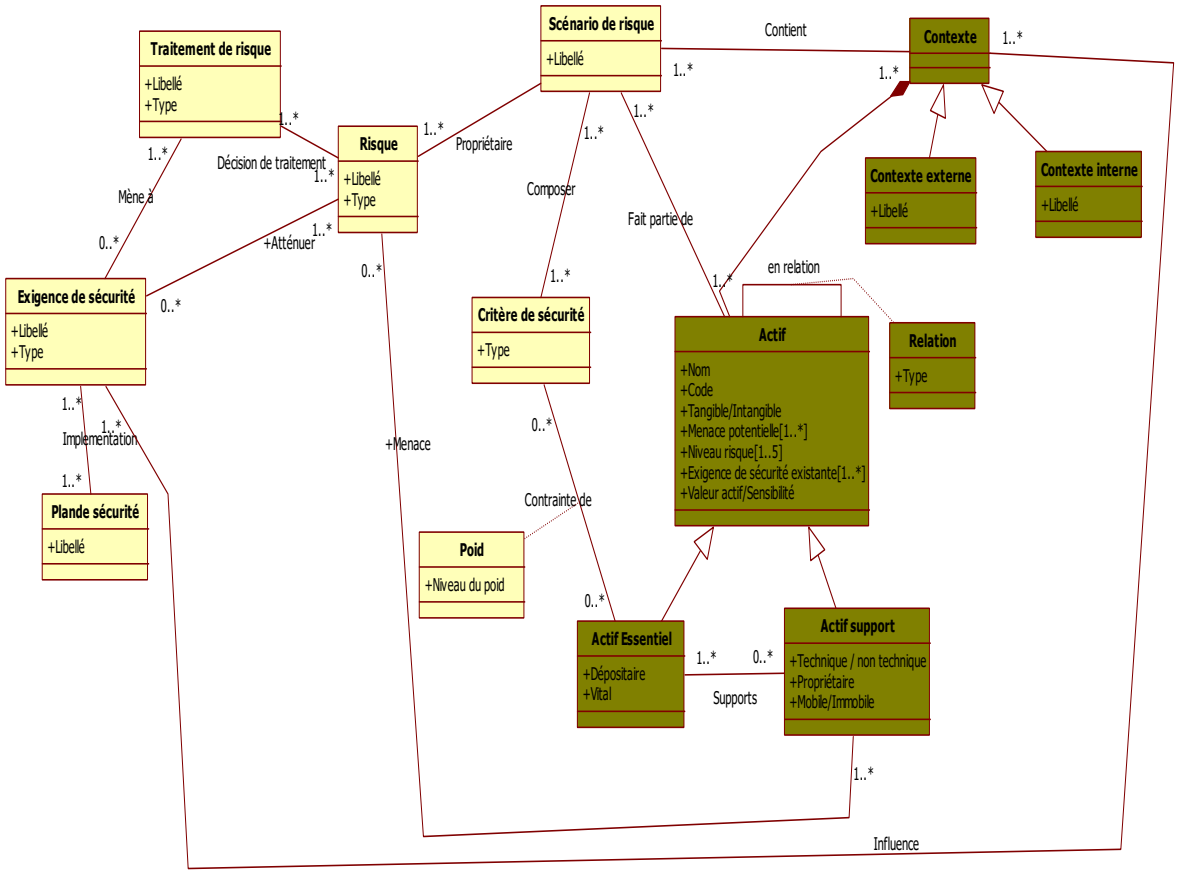


Figure 67 : Enrichissement du méta modèle de sécurité par les instances du contexte et les actifs.

L'instanciation des éléments du contexte s'effectuera grâce au résultat de l'étape 1 en les classant en tant qu'éléments du contexte externe ou interne de l'entreprise. L'enrichissement des actifs s'effectuera en les classant soit supports, soit essentiels et en rajoutant les relations et propriétés suivantes :

- Types de relation ϵ [Inclusion, interconnexions,...]
- Menaces Potentielles avec leurs classifications (EBIOS, 2010)
- Actif , soit sensitive soit il possède une valeur,
- Niveau de risque sur l'actif (Magerit, 2012)
- Très probable (fréquent)
- Probable (répétitif)
- Peu Probable (occasionnel).
- Improbable (rare).
- Très improbable (inexistant)
- Soit l'actif est tangible ou intangible

-Propriétaire pour les actifs supports et le dépositaire pour les actifs essentiels (EBIOS, 2010)

- Actif possède une localisation géographique si l'actif est intangible,
- Exigences de sécurité déjà mises en place, si elles existent,
- Actif support est technique ⇒ Actif ϵ [hardware, software, réseau] ;
- Actif support est non technique ⇒ Actif ϵ [personnel, site, organisation's structure]
- Actif support est mobile ⇒ Actif ϵ[hardware, software, réseau, personnel] ;
- Actif support est immobile ⇒ Actif ϵ [organisation's structure]

b. Etape 2 : Détermination des critères de sécurité associés aux actifs de l'entreprise

Le dernier point concernant la première phase d'analyse du contexte est la détermination des critères de sécurité des actifs de l'organisation.

Les critères de sécurité des actifs sont là pour garantir que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prevu. Chaque actif peut avoir un ou plusieurs critères de sécurité selon le contexte d'utilisation et un niveau de gravité selon le scénario de risque. Pour cela, nous avons rajouté comme guidage à l'utilisateur un concept (Poids) dans le méta modèle de sécurité qui possède comme attribut le niveau de gravité d'utilisation d'un des critères de sécurité qui sont :

Confidentialité : seules les personnes autorisées ont accès aux informations qui leur sont destinées ;
Disponibilité : le système doit fonctionner sans failles et garantir l'accès aux services et ressources ;
Intégrité : les données doivent être celles que l'on attend, et ne doivent pas être altérées de façon fortuite, illicite ou malveillante ;
Traçabilité (ou « Preuve ») : garantie que les accès et tentatives d'accès aux éléments considérés sont tracés et que ces traces sont conservées et exploitables.

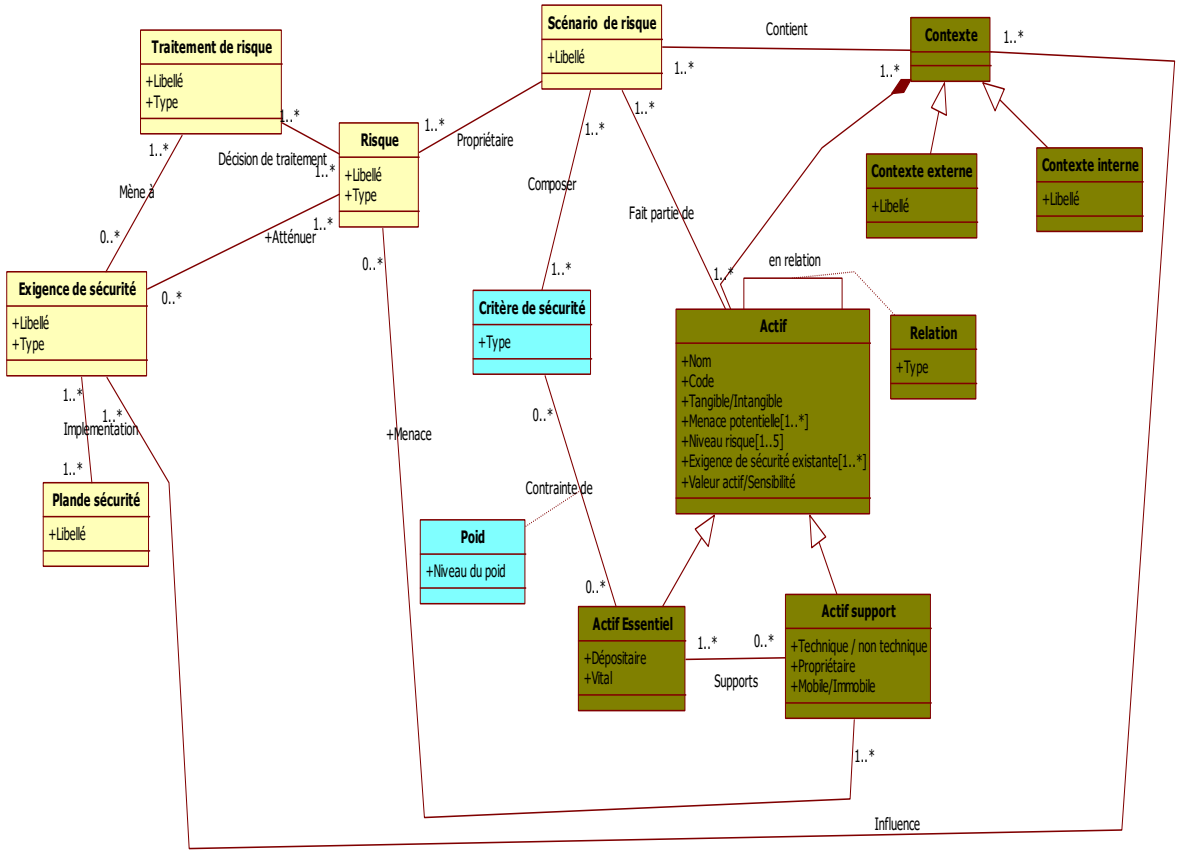


Figure 68: Enrichissement du méta modèle de sécurité par les instances de la phase du contexte.

Le résultat de cette étape est l'enrichissement du méta modèle de sécurité avec les critères de sécurité des actifs de l'entreprise en précisant le poids de réalisation de chacun.

Après avoir caractérisé l'organisation, nous passons à la phase d'analyse des risques.

Phase 2 : Analyse des risques

Cette phase est composée de trois étapes:

- Identification des scénarios de risques,
- Identification des risques,
- Caractérisation des risques.

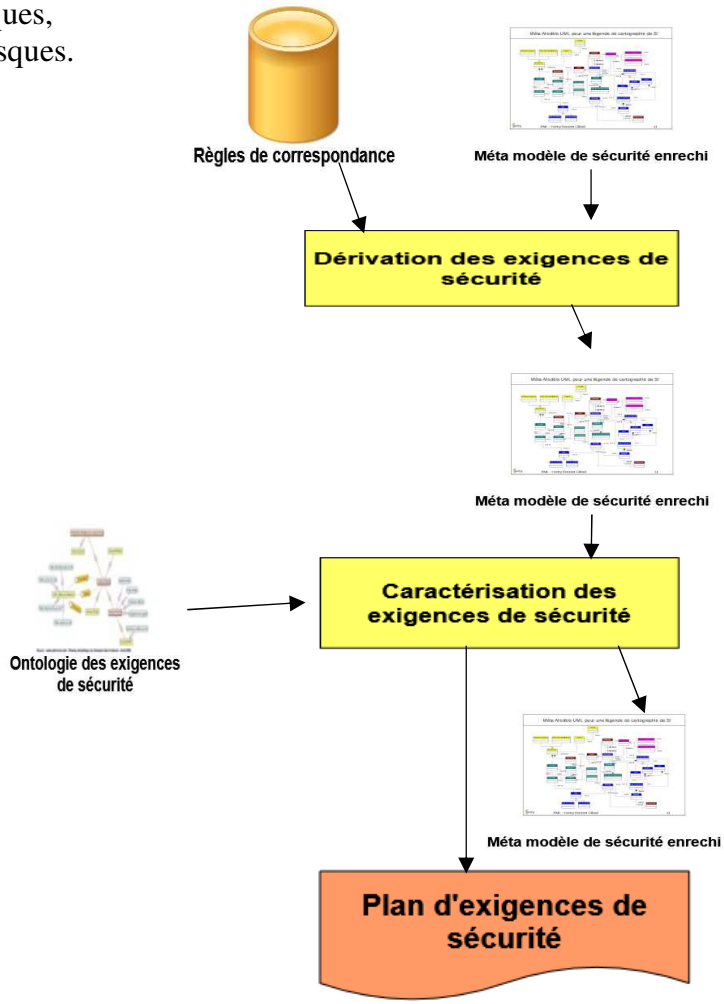


Figure 69: Deuxième phase du processus de derivation: Analyse des risques.

En entrée, nous utilisons les éléments suivants : les instances du méta modèle de la phase de contexte, la liste des scénarios de risques obtenue à partir de notre état de l'art et l'ontologie des risques. En sortie, nous obtenons un méta modèle d'instanciation qui regroupe la phase du contexte et la phase d'analyse des risques.

a. Identification des scénarios de risques

En général, les organisations ont tendance à raisonner en matière de scénarios de risques de façon globale, sans prendre en considération les risques particuliers. C'est la raison pour laquelle les méthodes présentent plusieurs scénarios de risques. Ceux-ci sont composés d'une liste de risques génériques qui peuvent être appliqués selon la situation de l'organisation.

Nous avons extrait l'ensemble des scénarios de risques proposés par les approches citées dans notre état de l'art principal (voir chapitre **II**), ce qui nous permet de constituer une base de connaissances composée de 28 scénarios de risques qui englobent toutes les possibilités auxquelles un SI pourrait être exposé. Ci-dessous nous présentons un extrait de ces scénarios.

N°	Scénarios	Méthodes d'extraction
1	Panne d'un matériel du système, entraînant la dégradation de service ou l'indisponibilité du système.	EBIOS-MEHARI
2	Implantation de fonctionnalités illicites dans un équipement ou une plate-forme du système, en vue de provoquer des dysfonctionnements ou des détournements d'information.	EBIOS-MEHARI
3	Usurpation de l'identité ou des droits d'accès d'une personne autorisée, par une personne malintentionnée.	EBIOS
4	Destruction ou altération de ressources techniques, de supports de stockage, de documents ou de locaux du système, par un phénomène naturel majeur.	EBIOS

Tableau 15 : Extrait de la base de connaissances des scénarios de risques.

Nous avons peu formalisé ces scénarios des risques pour mieux les exploiter dans l'étape d'identification des risques.

Un scénario de risque est composé de la:

- Liste des éléments du contexte de l'entreprise,
- Liste d'actifs de l'entreprise,
- Liste de risques encourus par l'entreprise,
- Liste de critères de sécurité.

Mentionnons, à titre d'exemple, un scénario de risque tiré de notre base de connaissances :

- Destruction ou altération de ressources techniques, de supports de stockage, de documents ou de locaux du système, par un phénomène naturel majeur.

Contexte	Actifs	Risques	Critères de sécurité
Contexte externe	Matériel Application Site	Dégradation Altération Destruction Violation des critères de sécurité	Intégrité Disponibilité Confidentialité

Tableau 16: Extraction d'informations d'un scénario de risque.

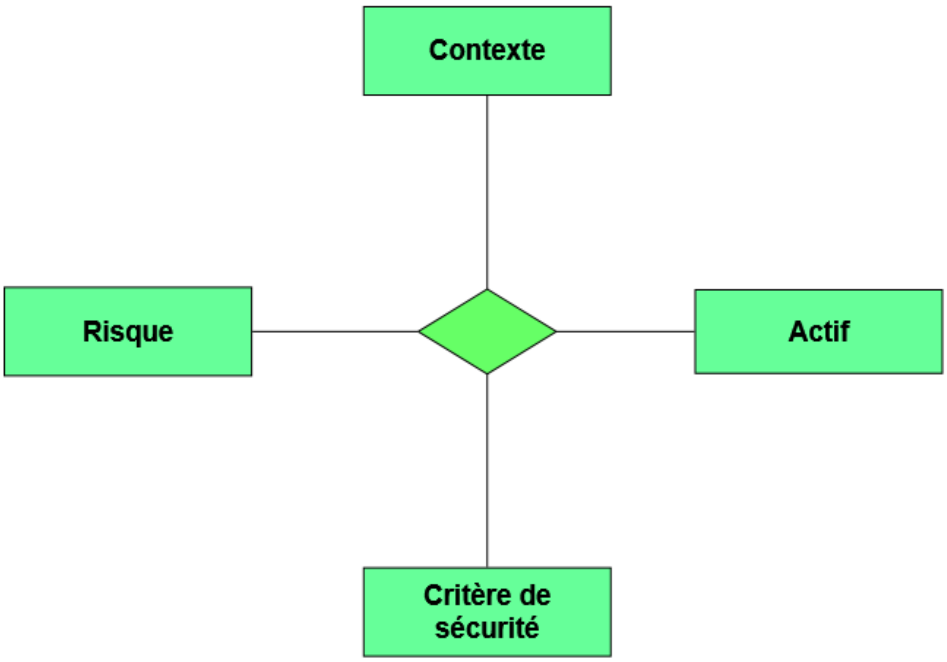


Figure 70 : Modèle de construction d'un scénario de risque.

b. Identification des risques

L'exploitation de l'étape précédente nous permet d'extraire les risques encourus par l'entreprise à partir des scénarios des risques identifiés.
A titre d'exemple, considérons le scénario suivant extrait des méthodes EBIOS et MEHARI : *Panne d'un matériel du système, entraînant la dégradation de service ou l'indisponibilité du système.*
A l'aide du méta modèle d'instanciation de la phase du contexte et du modèle de construction des scénarios des risques, nous sommes en mesure d'extraire ce qui suit :

- Panne, indisponibilité (critère de sécurité: disponibilité),
- Service (contexte : contexte interne),
- Matériel, système (actif: actif support),
- Dégradation (risque).

L'exploitation de notre ontologie des risques et des domaines linguistiques (voir sous chapitre **III.9**) donne la possibilité de rajouter d'autres concepts de risques.
Dans l'exemple précédent, nous obtenons les risques suivants :*Performance Degradation, Financial Lost, Information Loss, physical Asset Risks.*

c. Caractérisation des risques

Après avoir identifié les risques, nous caractérisons chaque risque avec les propriétés suivantes :

- **Propriétés statiques** : identifiant, libellé, classe de risque, résumé, les causes, les conséquences et sa répétabilité,
- **Propriétés dynamiques :** pour chaque risque, nous prenons en compte son impact en matière de coûts, délais, performances, détectabilité, probabilité et évolution,
- **Actions**: type de traitement.

Nous présentons ci-dessous un exemple lié à la caractérisation d'un risque : *Access Control Risks*.

Access Control Risks		
Propriétés Statiques	Identifiant dans l'ontologie	1.1.2
	Libellé	Access Control Risks
	Classe du risque	Organization Risks
	Résumé	Ces risques sont liés à l'absence de restrictions à l'accès des ressources de l'organisation ou avec une mauvaise mise en œuvre de ces restrictions visant à éviter tout accès non autorisé qui peut conduire à une récupération, modification ou suppression des informations.
	Causes	Absence de mise en œuvre des processus contrôlés visant à une affectation appropriée des profils, l'attribution inadéquate des profils d'accès aux ressources, erreur de mise en œuvre, l'ignorance des besoins des utilisateurs et des profils utilisateurs.
	Conséquence	Accès aux ressources non autorisées.
	Répétable	Oui
Propriétés Dynamiques	Incidence des coûts	Catastrophique
	L'impact de retard	Majeur
	Impact Performances	Majeur
	Détectabilité	Détectable
	Probabilité	Haut
	Évolution	En augmentant
Actions	Type de traitement	Prévention

Tableau 17 : Fiche de caractérisation des risques

Un type de traitement de risque est associé à chaque risque (voir sous chapitre **II.1.1**). Cette opération a été automatisée grâce aux fiches de caractérisation des concepts de l'ontologie des risques.

Le résultat de la deuxième phase de notre processus de dérivation des exigences de sécurité est l'enrichissement du méta modèle de sécurité par les nouvelles instances obtenues.

-Scénarios de risques de l'entreprise,
-Risques encourus par l'entreprise,
-Type de traitement des risques.

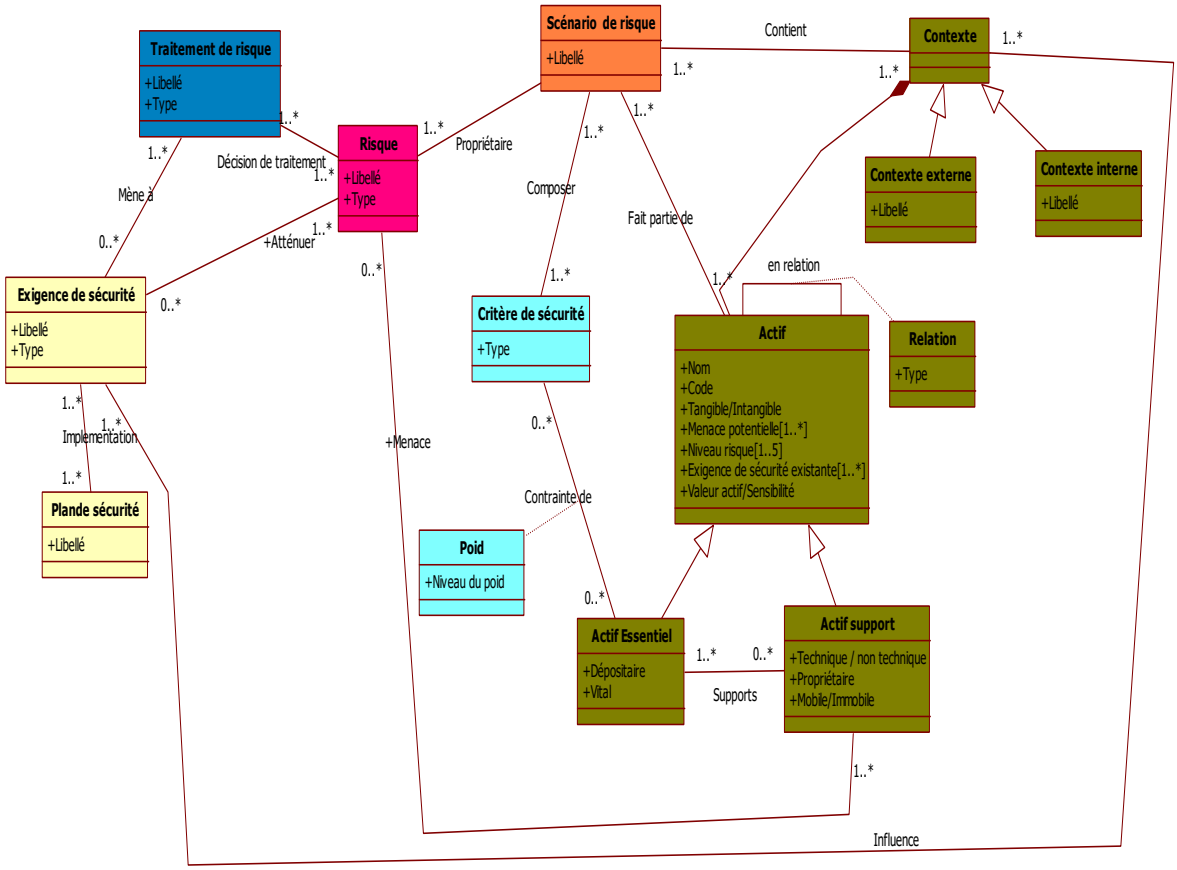


Figure 71 : Enrichissement du méta modèle de sécurité par les instances de la phase d'analyse des risques.

Phase 3 : Dérivation des exigences de sécurité

La troisième phase est composée de deux étapes:
- Dérivation des exigences de sécurité,
- Caractérisation des exigences de sécurité.

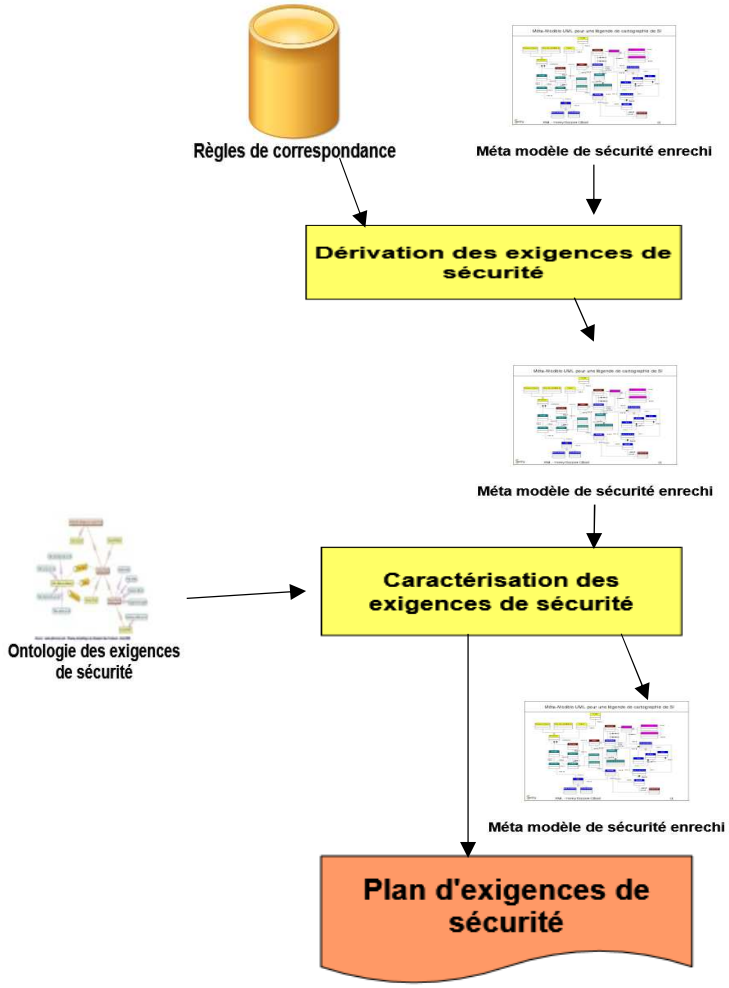


Figure 72 : Troisième phase du processus de derivation: Dérivation des exigences de sécurité.

Cette phase requiert en entrée les instances du méta modèle de la phase du contexte et de la phase d'analyse des risques, les règles de correspondance et l'ontologie des exigences de sécurité. En sortie, nous obtenons un méta modèle de sécurité dédié à l'entreprise du champ d'études.

a. Dérivation des exigences de sécurité

Le processus de dérivation est fondé sur l'alignement des ontologies des risques et des exigences de sécurité. La littérature traitant du domaine ne fournit pas une approche permettant l'alignement entre les ontologies des risques et d'exigences de sécurité.

(Shvaiko et al, 2013) présente un état de l'art sur l'alignement des ontologies. Il présente les bases de l'alignement et fournit des applications correspondantes. Il aborde également certains défis liés à cette question. Il ne mentionne pas l'application des exigences de sécurité.
(Mayer, 2009) décrit un procédé permettant d'aligner les concepts utilisés dans les méthodes de gestion des risques des systèmes d'information avec les méthodes qui prennent en charge le concept d'exigence de sécurité. Il ne traite pas le problème lié à l'alignement des ontologies.
(Ionita et al, 2013) identifie trois types de relations entre l'analyse des risques et l'élicitation des exigences de sécurité. La première relation est liée au fait qu'un résultat d'une évaluation du risque peut être utilisée comme base pour déduire les besoins de sécurité. La seconde tient au fait que, s'il existe des exigences de sécurité, l'évaluation du risque doit les respecter. La dernière relation peut être rencontrée lorsqu'un écart existe entre un système mis en place et l'ensemble des exigences de sécurité préexistantes. Dans ce cas, le but est d'identifier l'écart et de préciser les risques générés.

Bien qu'ils puissent exister, ce genre de relation entre l'analyse des risques et les exigences de sécurité, ces concepts ne fournissent pas un moyen pour calculer ou dériver les exigences de sécurité à partir d'une analyse des risques.
Dans notre solution, nous créons un alignement de concepts entre les deux ontologies en utilisant un ensemble de règles, ce qui nous permet d'évaluer leur utilité sémantique. Il est nécessaire de comparer, d'exploiter et de connecter les concepts des deux ontologies afin d'être en mesure de passer de l'une à l'autre ou de partager les ressources et les instances entre eux.

Afin d'effectuer l'alignement des deux ontologies, nous développons une liste de règles de correspondance exprimées en SWRL (Semantic Web Rule Language) en fonction de la connaissance générée à partir des méthodologies et des approches décrites dans le chapitre **II**. Le but est de réduire la participation directe des utilisateurs dans le processus de dérivation. De plus, nous fournissons toutes les étapes de construction des ontologies ainsi que les phases de dérivation des exigences de sécurité afin que la solution soit exploitée par l'ensemble des utilisateurs et d'assurer les mises à jour futures des bases de connaissances existantes. Rappelons que notre objectif est de ne pas fusionner deux ontologies représentant partiellement le même domaine, mais de relier l'ensemble des deux représentations de sujets connexes à savoir les risques et les exigences de sécurité. Par conséquent, l'alignement ne consiste pas à fusionner des nœuds et / ou la création de liens de subsomption.

Il faut noter que nous ne représentons pas les règles en utilisant la syntaxe abstraite SWRL, car elles sont verbeuses. Nous avons choisi de les représenter en utilisant une syntaxe lisible, comme **antécédent ⇒ conséquente** (Annexe **E**).
A titre d'exemple : considérons que l'organisation fait face à un scénario de risque composé d'un seul risque lié à la vulnérabilité physique (*Physical Vulnerabilities*) avec un type de traitement de risque qui est la (*Prevention*). Ce risque est d'abord identifié et caractérisé grâce à l'ontologie des risques. L'étape suivante consiste en l'exploitation des fiches de caractérisation des exigences de sécurité (voir tableau **19**) ainsi que des bases de connaissances. Ainsi nous obtenons la correspondance exacte. Dans notre exemple, nous obtenons les exigences de sécurité suivantes : *Control Validation Tests* et *Vulnerabilities Control Goals*.

La règle de correspondance est donc :

Risk=*'Physical Vulnerabilities*' ∧ **Type of treatment**=*'Prevention'*
⇒ **SR**=*'Control Validation Tests*' ∧ **SR**=*'Vulnerabilities Control Goals*'

Cette règle de correspondance peut être généralisée à un scénario.

Nous présentons ci-dessous un second exemple de correspondance.

Le scénario extrait de la méthode MEHARI, correspond à : *la perte de données ou à la non-disponibilité ou la perte de données publiées dans les sites publics ou privés ou en cas de dépassement des limites d'utilisation d'un matériel.*

Les risques associés à ce scénario sont présentés dans la première colonne du tableau **18** ci-dessous. La deuxième colonne présente le type de traitement de risque que l'on peut associer à un risque (voir chapitre **II**, partie terminologie). La troisième colonne présente l'identifiant du risque dans l'ontologie. Enfin, la dernière colonne contient les exigences de sécurité liées à chaque risque et obtenues en utilisant les règles de correspondance .

Risque	**Type de traitement**	**Risque position**	**Exigences de sécurité**
Unplanned Projet Changes	*Mitigate*	10.1	*Control Validation Tests*
Information Loss	*Mitigate*	8.1.3.3	*DisasterRecovery&Contingency/BusinessRecoveryPlan/StorageBestPractices/SecurityPoliciesDocuments/WorkingPapers/ComputerForensicAnalysis*
Information Destruction	*Avoid*	8.1.3.1	*DisasterRecovery&Contingency/BusinessRecoveryPlan/ StorageBestPractices/ SecurityPoliciesDocuments/Working Papers/ComputerForensicAnalysis*
Unauthorized Assets Usage Risks	*Mitigate*	6.4	*PhysicalSecurityPolicy/AccessControlPolicy/VirusControl*
Financial Loss	*Avoid*	7.2	*SecurityStrategyPlan/ComputerForensicAnalysis*
Transmission Errors	*Mitigate*	8.1.1	*SecurityProcessDocuments/Working Papers/ SecurityPoliciesDocuments*
Conceptual Design Errors	*Prevention*	8.2.2	*ControlValidationTests/AdaptavilityRequirements/ImplementationRequirements/PerformanceRequirements/ DurabilityRequirements/SecurityPoliciesDocuments*

Tableau 18 : Relation d'alignement des risques et les exigences de sécurité.

En utilisant SWRL, on obtient les expressions des règles suivantes :

Risk=' *Unplanned Projet Changes'* ∧ **Type of treatment**=*'Mitigate'*
⇒ **SR** =*'Control Validation Tests* '

Risk=' *Information Loss'* ∧ **Type of treatment** = *'Mitigate'*
⇒**SR**=*'Disaster Recovery Plan*' ∧ **SR**=*'Business Recovery Plan*' ∧ **SR**=*'Storage Best Practices*' ∧ **SR**=*'Security Policies Documents*' ∧ **SR**=*'Working Papers*' ∧ **SR**=*'Computer Forensic Analysis*'

Risk=' *Information Destruction*' ∧ **Type of treatment**=*'Avoid'*
⇒**SR**=*'Disaster Recovery Plan'*∧ **SR**=*'Business Recovery Plan*' ∧ **SR**=*'Storage Best Practices*' ∧ **SR**=*'Security Policies Documents*'∧ **SR**=*'Working Papers*' ∧ **SR**=*'Computer Forensic Analysis*'

Risk=*'Unauthorized Assets Usage Risks*' ∧ **Type of treatment**=*'Mitigate'*
⇒ **SR**=*'Physical Security Policy'* ∧ **SR**=*'Access Control Policy*' ∧ **SR**=*'Virus Control*'

Risk=' *Financial Loss*' ∧ **Type of treatment**=*'Avoid'*
⇒ **SR**=*'Security Strategy Plan*'∧ **SR**=*'Computer Forensic Analysis*'

Risk=*'Transmission Errors*' ∧ **Type of treatment** =' *Mitigate'*
⇒ **SR**=*'Security Process Documents*' ∧ **SR**=*'Security Policies Documents*'
∧ **SR**=*'Working Papers'*

Risk=' *Conceptual Design Errors'* ∧ **Type of treatment**=*'Prevention'*
⇒ **SR**=*'Control Validation Tests*' ∧ **SR**=*'Adaptavility Requirements'* ∧ **SR**=*'Implementation Requirements'* ∧ **SR**=*'Performance Requirements'* ∧ **SR**='Durability Requirements' ∧ **SR**= *'Security Policies Documents'*

b. Caractérisation des exigences de sécurité

Notre objectif dans cette partie est de caractériser le concept d'exigence de sécurité par des propriétés claires, efficaces et qui rajoutent un plus à notre démarche. Pour cela, nous mettons en avant les propriétés suivantes :

- **Risques qui sont couverts** : cette propriété est extraite du déroulement des méthodes citées dans l'état de l'art principal (chapitre **II**). Grâce à elles, on peut vérifier la pertinence des règles de correspondance .
- Les propriétés **ressources** et **connaissances** qui font le lien avec le contexte de l'organisation.

La caractérisation des exigences de sécurité est comme suit :

Propriétés statiques : identification, libellé, classe d'exigence de sécurité, résumé, risques qui sont couverts, l'exhaustivité et la date de mise en œuvre.

Propriétés dynamiques : niveau de performance, la flexibilité, la stabilité, la difficulté, la priorité, les ressources et les connaissances.

Nous présentons ci-dessous un exemple lié à une exigence de sécurité caractérisée : *Log Storage.*

Log Storage		
Propriétés statiques	Identifiant dans l'ontologie des exigences de sécurité	6.4.2.4.1
	Libellé	*Log Storage*
	Classe	*System Security&Backup*
	Résumé	Solution de stockage visant à maintenir trace des informations. Elle permet de nous conformer à la réglementation relative à la conservation des données électronique. Log Storage stock les identifiants, les adresses MAC des utilisateurs, les adresses IP des sites Web visités ainsi que leur date d'activation et l'heure…
	Risques qui sont couverts	*Information Security Criteria Violation,* *Information Deviation Risks,* *Information Manipulation Risks,* *Use Control Risks,* *Information Unavailability Risks,* *Information Disappearance Risks,* *Information Confidentiality Violation,* *Information Availability Violation,* *Information Quality Violation,* *Information Traceability Violation,* *Information Effectiveness Violation,* *Information Efficiency Violation,* *Information Integrity Violation,* *Technical Attacks.*
	Complétude	Sauvegarde de stockage des journaux avec une étude statistique éventuelle des entrées et sorties, les associant à leur adresse IP ou MAC afin de mieux configurer les pare-feu et l'IDS. Il nous permet d'avoir une idée sur les profils des utilisateurs
	Date de mise en œuvre	24/07/2016
Propriétés dynamiques	Performance	Haute
	La flexibilité	Non
	La stabilité	Stable
	Difficulté	Moyenne
	Priorité	Haute
	Ressources	Logiciel d'analyse, IDS
	Connaissances	Programmation, langues

Tableau 19 : Fiche de caractérisation des exigences de sécurité.

Le résultat de la troisième phase de notre processus de dérivation des exigences de sécurité est l'enrichissement du méta modèle de sécurité par les exigences de sécurité caractérisées applicables à l'entreprise de notre champ d'études.

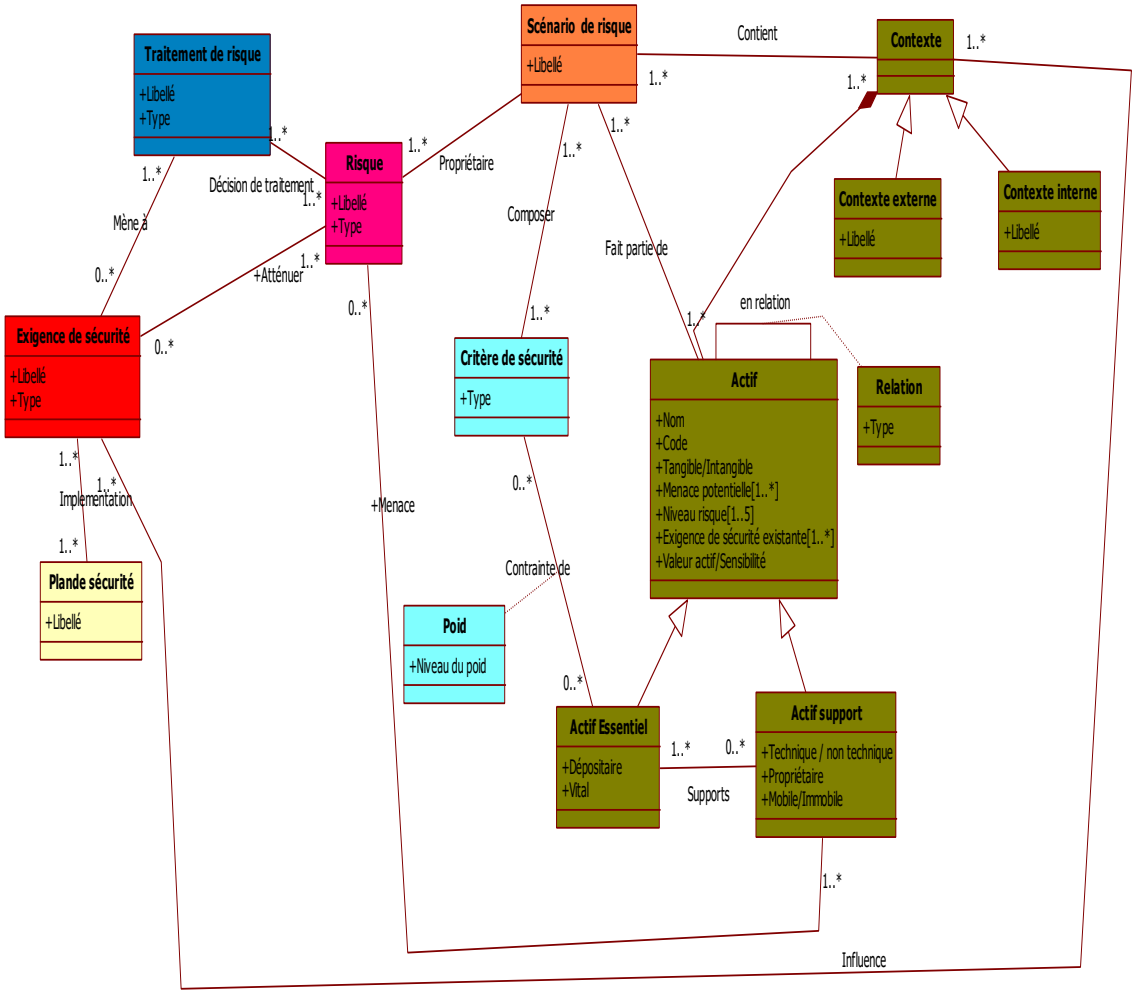


Figure 73: Enrichissement du méta modèle de sécurité par les instances de la phase de dérivation des exigences de sécurité.

En guise de conclusion de ce chapitre, nous résumons nos contributions comme suit :

- Construction de quatre (04) ontologies (actifs, contexte, risques et exigences de sécurité)
- Processus de dérivation des exigences de sécurité qui propose un guidage total à l'utilisateur;
- Modèle de construction des scénarios de risques;
- Fiches de caractérisation des concepts ontologiques;
- Règles de correspondance (risques, exigences de sécurité);
- Enrichissement du méta modèle de sécurité.

Le chapitre suivant traite de la validation des ontologies et la mise en œuvre de l'approche par une étude académique et un cas réel (confidentiel).

Chapitre IV

Mise en œuvre et validation de l'approche

IV. Mise en œuvre et validation de l'approche

IV.1 Introduction

La validation des ontologies des risques et des exigences de sécurité consiste en une vérification des mesures pertinentes des relations taxonomiques. Cette vérification est fondée sur le nombre de coïncidences (Hits) existant entre les concepts trouvés en utilisant un moteur de recherche classique (Google). L'approche de validation est décrite dans le sous chapitre **IV.2**.

Nous développons et nous mettons en œuvre un prototype fondé sur nos ontologies et les règles de correspondance décrites dans le chapitre **V**. À cet effet, nous modélisons les ontologies avec le logiciel Protegé [11]. Protégé permet d'utiliser le langage OWL, qui est le langage informatique utilisé pour modéliser des ontologies. Les fonctionnalités de Protegé peuvent être étendues grâce à une architecture en plugin et à l'aide de l'API Java fournie, ce qui permet, en outre, de générer automatiquement du code Java. Ce code généré, nous l'exploitons dans notre prototype développé sous la plateforme Java NetBeans version 8.1, plateforme de développement choisie est open source. Elle possède une communauté mondiale d'utilisateurs et de développeurs.

Le code généré inclus tous les concepts et instances qui peuplent les quatre ontologies de notre solution. Nous avons programmé les règles de correspondance (chapitre **III.9** phase 3) et la liste des scénarios de risque obtenue de notre état de l'art, comme le montre la figure ci-dessous.

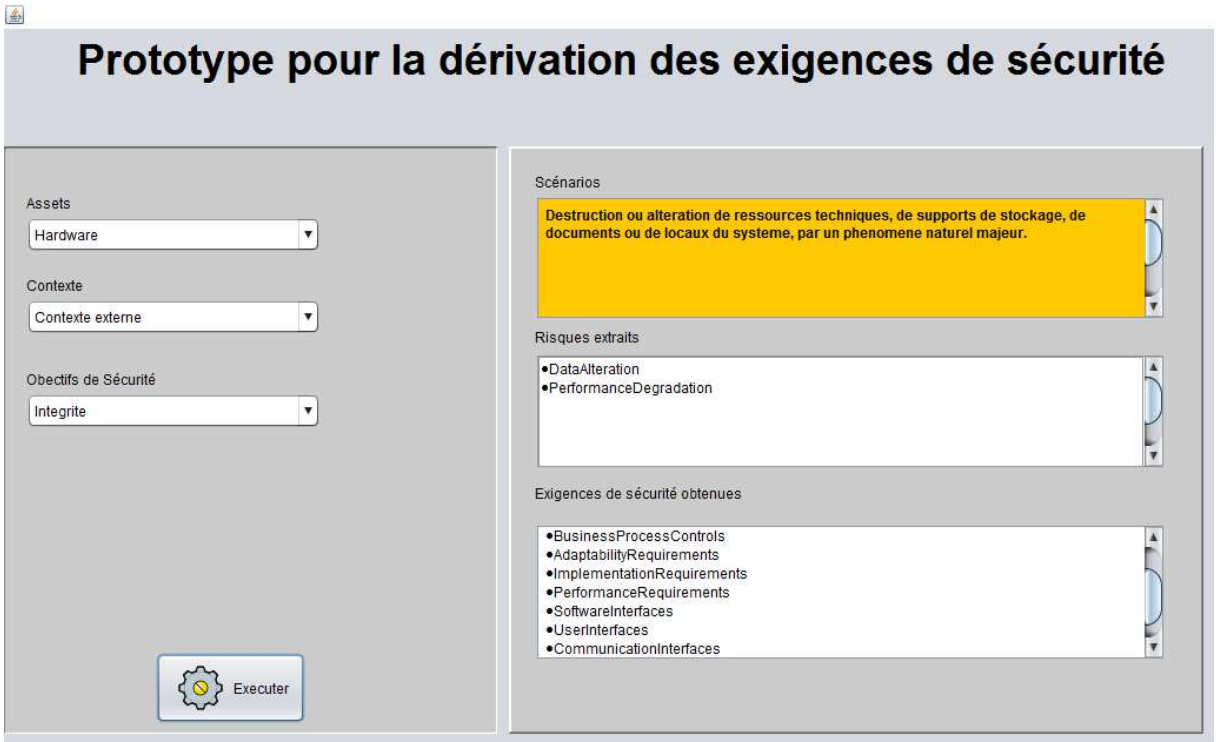


Figure 74 : Prototype pour la derivation des exigences de sécurité.

[11] Protégé, est un éditeur d'ontologies, et un framework de base de connaissances très conviviales, basé sur Java.

Dans notre démarche de guidage, nous exploitons les données extraites du traitement effectué sur le contexte général de l'entreprise grâce à la fonctionnalité de filtrage que nous incorporons dans le logiciel Automap. Aussi, nous rajoutons dans le prototype développé une aide de décision dans l'étape du choix de scénario de risque. A cette fin, nous classifions chaque combinaison de probabilité des éléments de construction d'un scénario de risque (voir figure **70**), en niveau fort ou moyen. Ceci est rendu possible grâce aux attributs du méta modèle de sécurité enrichi par la phase du contexte de notre processus de dérivation.

N°	Scénarios	Actifs	Éléments du Contexte	Critères de sécurité	Niveau de la réalisation du scénario
1	Destruction ou altération de ressources techniques, de supports de stockage, de documents ou de locaux du système, par un phénomène naturel majeur.	Matériel	Contexte externe	Intégrité	Moyenne
				Disponibilité	Forte
		Application	Contexte externe	Intégrité	Forte
				Disponibilité	Moyenne
				Confidentialité	Moyenne
		Site	Contexte externe	Disponibilité	Forte

Tableau 20 : Exemple de niveau de probabilité de la réalisation d'un scénario de risque.

IV.2 Validation des relations taxonomiques

Rappelons qu'une ontologie est définie comme un ensemble formel de concepts et de relations partagées par les membres d'une communauté. De cette définition, nous pouvons identifier des critères simples et détaillés pour la phase de validation. (Stumme et al, 2006) propose quelques définitions utiles à partir desquelles, nous déduisons les critères de validation.

Soit O une ontologie, C_i le concept « enfant » et α le concept « parent ».
α <c désigne la structure hiérarchique des concepts

Notre approche est fondée sur le nombre de coïncidences (Hits) existant entre les concepts trouvés en utilisant un moteur de recherche classique (Google).

Un autre concept utile pour enrichir l'ontologie est le voisinage. Ce concept nous permet d'établir des relations d'ordre entre les concepts taxonomiques et associatifs dans l'ontologie O.
Ce concept permet également de comprendre la structure des relations entre les concepts et de valider l'association des concepts existants dans les ontologies.

La mesure proposée, appelée « proximité », est notée Prox (Ci, α). Elle est définie comme suit :

$$\Pr ox.(C_i, \alpha) = \frac{(Hits\ (C_i, \alpha))}{HitsC_i} = Score_{Ci,\alpha}$$

où Hits (C_i, α) représente le nombre de hits ramenés par Google pour la co-citation des concepts C_i et α et où Hits(C_i) représente le nombre de hits renvoyés par le moteur de recherche Google pour le concept Ci.

Cette mesure a été appliquée pour l'ensemble des concepts des ontologies des risques et exigences de sécurité.
Prenant en exemple un concept de l'ontologie du risque « Risks » et pour l'ontologie des exigences de sécurité « Security Requirements ». Les tables **21** et **22** fournissent quelques mesures de proximités pour un sous-ensemble de concepts contenus dans chacune des deux ontologies.

C_i	**Concepts**	**No. Hits**	**Hits (C_i, Risks)**	**Score (C_i, Risks)**
C_1	OrganizationalRisks	53,9	20,4	0,378478664
C_2	ResidualRisks	5,31	1,45	0,27306968
C_3	Accidents	30,8	7,68	0,249350649
C_4	Vulnerabilities	14,4	7,82	0,543055556
C_5	Malicious Actions	11,4	3,77	0,330701754
C_6	AssetsDamageRisks	74,1	11,6	0,156545209
C_7	BusinessRisks	161	49,9	0,309937888
C_8	Errors	134	14	0,104477612
C_9	Threats	130	13,8	0,106153846
C_{10}	UnplannedeventsRisks	10,2	2,46	0,241176471

Tableau 21 : Mesures de proximité des niveaux 1 et 2 de l'ontologie des risques.

C_i	**Concepts**	**No. Hits**	**Hits (C_i, Sec.Req)**	**Score (C_i, Sec.Req)**
C_1	ControlValidationTests	45,6	42,2	0,925438596
C_2	SecurityGoals	41,4	40,3	0,973429952
C_3	SecuritySoftwareRequirements	15,7	12,8	0,815286624
C_4	Strategy Practices	283	178	0,628975265
C_5	Security RecoveryPlan	137	135	0,98540146
C_6	SystemSecurity&Backup	43	40,5	0,941860465

Tableau 22 : Mesures de proximité des niveaux 1 et 2 de l'ontologie des exigences de sécurité.

Si l'on considère le concept « Errors » qui a le score minimum, mais qui est extrait par la méthode MEHARI, on peut constater que les autres valeurs ont le même ordre de magnitude et, dans tous les cas, une meilleure valeur de proximité.

De manière équivalente, dans le cas des exigences de sécurité, toutes les valeurs sont équivalentes. Une exception d'interprétation de la valeur du concept « ControlValidationTests » (validé dans SIREN par (Lambert, 2011)) nous conduit à supposer que les autres valeurs ont un meilleur niveau de pertinence.

IV.3 Validation du processus de guidage

IV.3.1 Cas d'étude académique

Un des cas sur lequel repose notre validation du processus de guidage a été extrait d'une étude sur la sécurité effectuée par l'institut d'ingénierie de logiciel de Carnegie Mellon, en association avec le CERT et les services secrets des Etats Unis (Keeney et al, 2005). Rappelons qu'une partie de cette étude a déjà été publiée par notre équipe (Vasquez et al, 2012).

Ce cas d'étude académique a été constitué pour traiter les incidents de sécurité perpétrés par les utilisateurs internes qui, intentionnellement, ont contourné ou mal utilisé les profils d'accès, affectant par-là la sécurité de l'organisation, des données, des systèmes, ou le déroulement des processus métiers.

Les incidents incluent les risques suivants :

1) Manipulation de l'information (falsification, suppression, changement ou modification),
2) Accès non autorisé à l'information et divulgation,
3) Violation des critères de classification de l'information.

L'analyse de l'information distingue cinq catégories d'analyse :

- L'analyse du comportement de l'attaquant (sa motivation et ses intentions liées à sa rationalité et sa relation avec l'entreprise et/ou ses collègues),
- L'analyse de l'évolution de l'attaque (exploitation des vulnérabilités dans les applicatifs, réseaux, processus, etc). Fréquemment, l'attaquant utilise son nom d'utilisateur et son profil d'administrateur pour créer des utilisateurs non autorisés ou utilise les noms d'utilisateurs partagés,
- L'analyse de la détection de l'attaque. La détection peut être effectuée a priori ou, a posteriori. Dans cette phase, les systèmes détectent l'origine de la menace, les causes et les activités d'identification et de description de l'attaque (enregistrement des événements et des corrélations entre événements),
- L'analyse de la prévention. Dans cette phase, l'analyse s'appuie sur les éléments suivants :
    - La gestion des ressources humaines liée aux technologies de l'information ;
    - La gestion des exigences de protection de l'information : destruction, disponibilité, intégrité, confidentialité, traçabilité, partage et stockage de l'information ;
    - La gestion documentaire de la sécurité : processus d'administration des accès et des usages ;
    - L'utilisation de techniques de détection proactive : enregistrement des événements et surveillance ;

- La gestion des exigences « métiers » et organisationnelles (plan de formation et sensibilisation, plan de reprise d'activité, besoins liés aux actifs critiques, besoins de récupération après sinistre et/ou contingences, besoins liés à la gouvernance de l´entreprise, besoins de conformation aux réglementations et besoins de séparation de responsabilité),
- L'analyse des associations entre risques : dans cette phase, l'emphase est mise sur les relations entre besoins pour renforcer les mécanismes de sécurité. Dans ce cas, l'attention est portée sur :
  - La culture organisationnelle : contrôle des changements et besoins des processus métier en termes de sécurité,
  - les processus et la technologie pour la mise en œuvre de mécanismes de protection de l'information partagée,
  - La mise en place de mécanismes d'activation, suppression, changement des utilisateurs au niveau des accès logiques et physiques (selon le type d'activité, la durée de l'activité, etc.),
  - L'analyse fonctionnelle pour assurer la mise en œuvre du processus de séparation de responsabilité,
  - L'audit procédural et technique des activités des administrateurs,
  - La surveillance pour la détection des outils ou méthodes d'accès aux ressources informatiques,
  - L'attention portée aux sabotages physiques, à la prestation de services (électricité, climatisation, etc.) et à la manipulation psychologique (ingénierie sociale : coercition, intimidation, etc.),
  - Le contrôle, la protection et le stockage d'informations liées à l'enregistrement des activités.

Nous résumons dans la table suivant les principaux résultats de l'application des deux premières phases de notre approche de guidage en les confrontant aux résultats obtenus par l'institut d'ingénierie de logiciel de Carnegie Mellon.

Liste des risques mentionnés par (Keeney, 2005)	**Liste des risques obtenus grâce à notre approche de guidage**	**Liste des exigences de sécurité mentionnées par (Keeney, 2005)**	**Listes des exigences de sécurité obtenues grâce à notre approche de guidage**
Information manipulation	Information Manipulation Risks	Requirements business Requirement of Awareness Requirement of Monitoring Security Requirement protection of information	Computer Forensic Analysis Storage Best Practices ; Log Storage

		Requirement of management documentary Requirement of access control Logic	
Unauthorized access Information	Unauthorized AssetsUsage Risks	Requirements business Requirement of access control logic	Physical Security; Access Control Policy; Virus Controls
Criteria Violation of classification of Information	Information Security Criteria Violation	Requirement of management Information	Security Policies Documents; Working Papers; Computer Forensic Analysis Information Management; Prevention Actions; LogStorage; Traceability Goal; Confidentiality Goal ; Access Control Process ; Physical Security Policy Availability Goal ; Integrity Goal

Tableau 23 : Résultat de l'application du processus de guidage au cas d'étude.

Le tableau montre que notre processus offre une précision dans la caractérisation des risques mentionnés dans le cas d'étude que nous avons présenté supra. A titre d'exemple, la liste obtenue via le processus correspond aux différents sous-types du risque « information manipulation » obtenue par l'institut d'ingénierie de logiciel de Carnegie Mellon. Cette précision est dûe au fait, que via les liens d'héritage, on peut atteindre tous les sous-types de risque.

Aussi, nous pouvons noter que cette précision dans la caractérisation des risques nous permet une identification précise des exigences de sécurité.

Il est important de noter que ces constatations dans la précision d'obtention des risques encourus par les organisations et leurs couvertures par des exigences de sécurité issues des l'ontologies associées a fait l'objet d'une vérification et de confirmation à l'aide d'une étude de cas réel (voir sous chapitre **IV.3.2- confidentiel**) et de deux autres études académiques qui sont :

- Etude de cas de vol des données personnelles des clients dans près de 2000 magasins Target aux États-Unis d'Amérique en décembre 2013 (Radichel, 2014),

- Etude sur la cyber attaque de la société américaine Sony Pictures en novembre 2014 où cette filiale du groupe Sony a été victime d'un piratage massif de ses données.

Notons que ces deux cas d'études sont en phase de finalisation et vont faire l'objet d'une publication dans un journal spécialisé.
Le cas réel étudié est confidentiel.

Chapitre V

Conclusion et perspectives

V. Conclusion et perspectives

V.1 Conclusion

Au cours de ces dernières années, les technologies de l'information ont complètement révolutionné notre société et ont même envahi notre vie privée. C'est une raison suffisante pour affirmer que la sécurité du système d'information est devenu le défi du siècle pour le monde.

Les innombrables motifs d'inquiétude et la faculté de faire face par avance à ce qui est pressenti comme menace, sont particulièrement importants pour toute conception d'un système d'information viable et pérenne. Notre objectif, avec la présente thèse, est de lancer une dynamique permettant de pallier l'absence de guidage qui semble caractériser les approches passées. Notre démarche consiste à dériver les exigences de sécurité à partir de l'analyse des risques en prenant en compte les critères de sécurité dès la phase de spécification des besoins. Les principales contributions de cette thèse peuvent être énumérées comme suit :

La création de quatre ontologies à partir de la sélection, l'uniformisation, l'intégration et la mise en conformité des sources d´informations hétérogènes, qui ont été créées ou adaptées pour le traitement de la sécurité des systèmes d´information. Une des difficultés résulte du fait que ces méthodologies définissent des concepts avec une syntaxe et/ou une sémantique différente. Pour faire face à cette situation, nous procédons à l'extraction de toutes les définitions disponibles dans notre état de l'art principal en utilisant leurs noyaux de sens permettant l'uniformisation du vocabulaire avec l'ambition modeste d'une forte homogénéité dans les usages des termes.

Dans notre démarche, nous créons quatre ontologies :

- Une ontologie du contexte construite sur la base de la norme de sécurité ISO/CEI 27000 : 2016,

- Une ontologie des actifs issue d'un état de l'art dédié et de l'application des scénarios de construction des ontologies,

- Les ontologies des risques et des exigences de sécurité construites respectivement à partir des méthodologies d'analyse des risques et des approches d'élicitation des exigences de sécurité.

Nous fournissons pour chaque concept des quatre ontologies une fiche de caractérisation. Le but de cette fiche est d'identifier avec exactitude chaque concept, soit pour un enrichissement de connaissance des ontologies (synonyme, ..), soit pour détecter des conflits entre concepts. Les fiches de caractérisation des éléments du contexte ainsi que ceux des actifs sont établis en fonction des attributs des concepts des ontologies (voir annexe **A**).

Nous proposons pour chaque concept de l'ontologie des risques d'associer un type de traitement de risque dans sa fiche de caractérisation. Quant aux concepts d'exigences de sécurité, nous proposons les risques qui sont couverts par cette exigence dans sa fiche de caractérisation ainsi que les ressources et connaissances extraites du contexte.

Nous développons un processus de guidage composé de trois phases. La première phase consiste à caractériser une organisation grâce aux deux ontologies (actifs et contexte) associées à cette phase. Les informations relatives aux actifs, aux contextes et aux critères de

sécurité sont extraites automatiquement en appliquant un filtrage intégré dans le logiciel de traitement de texte (Automap).

Nous formalisons un modèle de construction d'un scénario de risque à partir des éléments du contexte, des actifs, des critères de sécurité et des risques.

Nous avons défini une liste de scénario de risques générique composée de vingt huit (28) scénarios. Cette liste est extraite des bases de connaissance. Nous avons établi une aide à l'utilisateur dans ce choix en classant les combinaisons possibles des concepts selon la probabilité de réalisation (forte ou moyenne). Cette classification est réalisée grâce aux attributs des instances du méta modèle de sécurité enrichi lors de la phase du contexte de notre processus de dérivation.

Nous avons aussi construit des règles de correspondance formelles et vérifiables via les méthodes de notre état de l'art principal. Ces règles permettent de passer d'un risque à sa couverture par une ou plusieurs exigences de sécurité.

L'alignement entre les deux ontologies (risque et exigences de sécurité) est fondé les règles de correspondance extrait des bases de connaissances étudiées dans notre état de l'art principal. L'approche produit des alignements sémantiques qui ont été extraits à partir des recommandations contenues dans les méthodologies étudiées dans notre état de l'art principal.

D'un point de vue opérationnel, nous avons conçu et mis en œuvre un prototype fondé sur les informations modélisées avec le logiciel Protegé. Ce dernier nous permet de travailler avec une structure composée de classes et sous-classes constituant l'ontologie des risques et des exigences de sécurité. En outre, nous avons développé un prototype avec java Net Beans exploitant le code java généré grâce au logiciel Protégé. Ce prototype exploite les informations qui peuplent les ontologies, liste des scénarios de risques, ainsi que les règles de correspondance.

Nous avons procédé à la validation des ontologies et à la mise en œuvre de l'approche de guidage sur des études issues du monde académique ainsi que sur une étude de cas réel.

V.2 Perspectives

Plusieurs axes de recherche future sont possibles. Citons notamment :

- L'enrichissement des ontologies et des règles de correspondance associées.
- L'intégration de l'expérience d'experts dans les bases de connaissances.
- Une validation plus large des concepts et des relations ontologiques.
- L'application de la démarche à plus d'exemples.
- L'exploitation de l'aspect « contexte externe » ainsi que des scénarios de risques associés.

- L’ajout d’autres critères de sécurité.

- L’ajout d’autres niveaux d’abstractions dans les ontologies.
- La détection de nouveaux conflits potentiels entre les risques et/ou les exigences de sécurité.
- L’étude des scénarios multiples et évolutifs du contexte externe.

- Le développement d’un module dédié à l'extraction d'informations à partir des textes et la visualisation des données sous forme de réseau sémantique.

- La construction d’une ontologie modulaire en se basant sur nos quatre ontologies et les liens déja détectés entre elles.

Publications et bibliographie

Publications :

Conférences internationales:

- J. Akoka, I. Comyn-Wattiau, N. Laoufi. "Research on Big Data - Characterizing the Field and its Dimensions", Advances in Conceptual Modeling, MOBID Workshop, Proceedings of ER2015 Workshops., October 2015, Vol. 9382, pp.173-183, Series Lecture Notes in Computer Science (LNCS), Stockholm, Suède, (DOI: 10.1007/978-3-319-25747-1_18)

- Nabil Laoufi. "Risk Analysis to the Expression of Security Requirements for Systems Information".Fourth International Conference on Cyber Security, Cyber Warfare, and Digital Forensic, Cybersec 2015, DOI: 10,1109 / CyberSec.2015.25, Jakarta, Indonisia.

- J. Akoka, I. Comyn-Wattiau, N. Laoufi. "Characterizing Research on Big Data and Security based on a Bibliometric Study", Software Engineering, Cyber Security, Big Data and Conceptual Modeling (SCBC Workshop) in Conjunction with International Conference on Conceptual Modeling (ER2015), October 2015, pp.1, Stockholm, Suède.

Papier journal :

- J. Akoka, I. Comyn-Wattiau, N. Laoufi. "Research on Big Data - A systematic mapping study", Computer Standards & Interfaces, DOI: 10.1016/j.csi.2017.01.004, 2017.

Bibliographie

Allen, J., Alberts, C., Stoddard, R., 2012. «Deriving Software Security Measures from Information Security Standards of Practice», SEI/Carnegie Mellon.

Anton, A.I., Earp, J.B.,2000. «Strategies for developing policies and requirements for secure electronic commerce systems». In: Proceedings of the 1st ACM workshop on security and privacy in e-commerce, Athens, Greece.

Asnar, Y., Giorgini P., Massacci F., Zannone N. 2007. « From Trust to Dependability through Risk Analysis ». In The Second International Conference on Availability, Reliability and Security, 2007. ARES 2007, 19-26.

Asnar, Y., Giorgini P., 2006. «Modelling Risk and Identifying Countermeasure in Organizations». CRITIS 2006: 55-66.

Aussenac-Gilles, N., Biébow, B., Szulman S, 2000. «Modélisation du domaine par une méthode fondée sur l'analyse», de corpus, actes de la conférence IC'2000, Journées Francophones d'Ingénierie des connaissances, pages 93-103.

Behnia, A., Abd Rashid, R., Chaudhry, J.A, 2012. «A Survey of Information Security Risk Analysis Methods», Smart Computing Review, 2(1), DOI: 10.6029/smartcr.2012.01.007.

Bhattacharjee, J., Sengupta, A, Mazumdar, C., 2013. «A formal methodology for enterprise information security risk assessment». In: Proc. 8th International Conference on Risks and Security of Internet and Systems (CRiSIS), pp. 1–9. IEEE Press, New York.

Brézillon, P., Abu-Hakima, S., 1995. «Using knowledge in its context», Report on the IJCAI-93 Workshop. The AI Magazine, 16(1) pp. 87-91.

BS 7799, 2002. «British Standards Institution., Information security management systems», specification with guidance for use, London.

Bulc˜ao Neto, R. F., Pimentel, M. G. C., 2005. «Toward adomain-independent semantic model for context-awarecomputing». In Proceedings of the 3rd Latin American Web Congress (LA-WEB'05), pages 61–70, Buenos Aires, Argentina, 2005. Available in the IEEE CS DL athttp://dx.doi.org/10.1109/LAWEB.2005.43.

Bucuret, O., Beaune, P., Boissier, O., 2005. « Définition et Représentation du Contexte pour des Agents Sensibles au Contexte », Actes de la 2ème Conférence Francophone Mobilité et Ubiquité, vol. 120 de ACM International Conference Proceeding Series, Grenoble (France), juin 2005, p. 13–16.

Cabrera, O. Franch, X., Marco, J., 2014. «A Context Ontology for Service Provisioning and Consumption». IEEE RCIS 2014.

Carley, Kathleen, M., 2013a. Dave Columbus and Peter Landwehr, "AutoMap User's Guide 2013," Carnegie Mellon University, School of Computer Science, Institute for Software Research, Technical Report, CMU-ISR-13-105.

Carley, Kathleen, M., 2013b. ORA: Quick Start Guide, Unpublished Manuscript.

CASOS, Center for Computational Analysis of Social and Organizational Systems: [Online]: http://www.casos.cs.cmu.edu/

Chen, H., Finin, T., Joshi, A., 2003. «Using OWL in a Pervasive Computing Broker». In Proceedings of Workshop on Ontologies in Open Agent Systems (AAMAS 2003).

Chowdhury, M., 2012. «Towards Security Risk-oriented Mal Activity Diagram». International Journal of Computer applications 56(10):47-52, Published by Foundation of Computer Science, New York, USA.

Chowdhury, M., 2014. «Security Risk Modelling Using SecureUML».16th int'l Conf .

Christopher, A.J., Dorofee, A.J., 2010. «RMF Risk Management Framework».

Clifton, A., 1999. «Fault Tree Analysis, A History». The Boeing Company; Seattle Washington.

CLUSIF. 2004. «Méthode Harmonisée d'Analyse de Risques (MEHARI), Principes et mécanismes». [Online] http://www.clusif.asso.fr/.

Common criteria, 2012. «Common criteria for information technology security evaluation», version 3.1 revision 4.

CRAMM, 2003. «CCTA Risk Analysis and Management Method», User Guide version 5.0, Insight Consulting – SIEMENS.

Dey, A., Abowd, G., 1999. «Towards a better understanding of Context and Context-Awareness», GVU Technical Report GIT-GVU-00-18.

EBIOS, Secrétariat Général De la Défense Nationale, 2010. « EBIOS-Expression des Besoins et Identification des Objectifs de Sécurité ». http://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/

European Network and Information Security Agency, February 2013. Inventory of risk management/risk assessment methods, [Online]: http://rm-inv.enisa.europa.eu/methods.

Ejigu, D., Scuturici, M., Brunie, L., 2007. «An Ontology-Based Approach to Context Modeling and Reasoning in Pervasive Computing», Proceedings of CoMoReaWorkshop of the IEEE International Conference (PerCom'07), New York, USA.

Fabian, B, Gürses, S, Heisel, M., Santen, T., Schmidt, H., 2010. «A comparison of security requirements engineering methods». Requirements Engineering Journal, 15(1), pp. 7-40, DOI 10.1007/s00766-009-0092-x.

FAIR, Jones, J. A., 2005. «An Introduction to Factor Analysis of Information Risk (FAIR) », 2005.

Fernández-Lopez, M., Gómez-Pérez, A., x Juristo, A., 1997. «METHONTOLOGY: from ontological art towards ontological engineering», Actes de AAAI.

FMECA, 1993. « Failure Mode, Effects and Criticality Analysis», Reliability Analysis Center and Rome Laboratory.

Firesmith, D.G., 2003a. «Security Use Cases». Journal of Object, Technology. Vol. 2, No. 3, 53-64.

Firesmith, D.G., 2003b. «Engineering Security Requirements». Journal of Object, Technology. Vol 2, No 1, 53-64.

Gandotra, V., Singha, A., Bedi, P., 2009. «Identifying Security Requirements Hybrid Technique». In Proceedings of the 4th International Conference on Software Engineering Advances, Porto, Portugal, IEEE Computer Society, 407- 412. DOI: 10.1109/ICSEA.2009.65.

GERAM, 1999. «Generalized Enterprise Reference Architecture and Methodology», Version 1.6.3, IFAC-IFIP Task Force on Architecture for Enterprise Integration, IFAC-IFIP Task Force.

Glinz, M., 2005. «Rethinking the Notion of Non-Functional Requirements». Proceedings of the Third World Congress for Software Quality, Munich, Germany,

Glossary of Security Terms, 2012. «Definitions, And Acronyms», [Online] www.cdse.edu/documents/cdse/Glossary_Handbook.pdf.

Graa, M., Cuppens-Boulahia, N., Autrel, F., Azkia, Hanieh., Cuppens , F., Coatrieux, G., Ana, R., Mammar, A. «Using Requirements Engineering in an Automatic Security Policy Derivation», DPM/SETOP 2011.

G¨urses, S.F., Berendt, B., Santen, T.H., 2006. «Multilateral security requirements analysis for preserving privacy in ubiquitous environments». In Proceedings of the Workshop on Ubiquitous Knowledge Discovery for Users at ECML/PKDD 2006, pages 51–64, Berlin.

Haley, C.B., Moffet, J.D., Laney, R., Nuseibeh, B., 2006. «A framework for Security Requirements Engineering», SESS ’06.

Haley, C.B., Laney R., Moffett J.D., and Nuseibeh B., 2008. «Security Requirements Engineering: A Framework for Representation and Analysis ». IEEE Transactions on Software Engineering 34 (1): 133-53.

Hatebur, D., Heisel, M., Schmidt, H., 2007. «A pattern system for security requirements engineering». In: Proceedings of the international conference on availability, reliability and security (AReS). IEEE Computer Society, (2007) pp 356–365. DOI: 10.1109/ARES.2007.12.

Hernandez-Ardieta, J.L., Blanco, P., Vara, D., 2012. «A methodology to construct Common Criteria security targets through formal risk analysis».

Héon, M., Paquette, G., Basque J., 2008. «Transformation of Semi-Formal Models into Ontologies According to a Model Driven Architecture», JFO 2008, Lyon, France.

Hochstein, Rudiger, Z., Walter, B., 2005. «ITIL as Common Practice Reference Model for IT Service Management», Formal Assessment and Implications for Practice", 2005 IEEE International Conference on e-Technology, eCommerceand e-Service (EEE'05), March 2005.

Ionita, D., Current, E., 2013. «Risk Assesment Methodologies and Tools», Master Thesis, Univesiteit Twente, July 2013.

ISACA, 2012. «Framework and related products that help professionals attain value from information systems», [Online] HYPERLINK http://www.isaca.org/Knowledge-Center/cobit/Documents/CobiT-Products.pdf.

ISACA, 2009. «The risk IT framework», ISBN 978-1-60420-111-6, 2009.

ISAMM, 2002. «Information Security Assessment and Monitoring Method», Belgacom's methodology towards integrated security management.

ISO/CEI 17799, 2005. «Information technology - Security techniques - Code of Practice for Information Security Management», International Organisation for Standardisation, Genève.

ISO/CEI 20000, 2011. «Technologies de l'information - Gestion des services - Partie 1: Exigences du système de management des services», International Organisation for Standardisation, Genève.

ISO/CEI 27000, 2016. «Technologies de l'information - Techniques de sécurité - Systèmes de gestion de sécurité de l'information Vue d'ensemble et vocabulaire», International Organisation for Standardisation, Genève.

ISO/CEI 27001, 2013. «Technologies de l'information - Techniques de sécurité - Systèmes de management de la sécurité de l'information - Exigences», International Organisation for Standardisation, Genève.

ISO/CEI 27002, 2013. «Technologies de l'information - Techniques de sécurité - Code de bonne pratique pour le management de la sécurité de l'information», International Organisation for Standardisation, Genève.

ISO/CEI 27003, 2010 «Technologies de l'information - Techniques de sécurité - Lignes directrices pour la mise en oeuvre du système de management de la sécurité de l'information», International Organisation for Standardisation, Genève.

ISO/CEI 27004, 2009. «Technologies de l'information - Techniques de sécurité - Management de la sécurité de l'information - Mesurage», International Organisation for Standardisation, Genève.

ISO/CEI 27005, 2011. «Technologies de l'information - Techniques de sécurité - Gestion des risques liés à la sécurité de l'information, International Organisation for Standardisation, Genève.

ISO/CEI 27006, 2015. «Technologies de l'information - Techniques de sécurité - Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information», International Organisation for Standardisation, Genève.

ISO/CEI 27007, 2011. «Technologies de l'information - Techniques de sécurité - Lignes directrices pour l'audit des systèmes de management de la sécurité de l'information», International Organisation for Standardisation, Genève.

ISO/CEI 27011, 2008. «Technologies de l'information - Techniques de sécurité - Lignes directrices du management de la sécurité de l'information pour les organismes de télécommunications sur la base de l'ISO/CEI 27002», International Organisation for Standardisation, Genève.

ISO/CEI TR 27008, 2011. «Technologies de l'information - Techniques de sécurité - Lignes directrices pour les auditeurs des contrôles de sécurité de l'information», International Organisation for Standardisation, Genève.

ISO/CEI 27010, 2015. «Technologies de l'information - Techniques de sécurité - Gestion de la sécurité de l'information des communications intersectorielles et inter organisationnelles», International Organisation for Standardisation, Genève.

ISO / CEI 27011, 2008. «Technologies de l'information - Techniques de sécurité - Lignes directrices du management de la sécurité de l'information pour les organismes de télécommunications sur la base de l'ISO/CEI 27002», International Organisation for Standardisation, Genève.

ISO/ CEI 27013, 2013. «Technologies de l'information - Techniques de sécurité - Guide sur la mise en œuvre intégrée d'ISO/CEI 27001 et ISO/CEI 20000-1», International Organisation for Standardisation, Genève.

ISO/ CEI 27014, 2013. «Technologies de l'information - Techniques de sécurité - Gouvernance de la sécurité de l'information, International Organisation for Standardisation, Genève.

ISO / CEI TR 27015, 2012. «Technologies de l'information - Techniques de sécurité - Lignes directrices de gestion de la sécurité de l'information pour les services financiers», International Organisation for Standardisation, Genève.

ISO/ CEI TR 27016, 2014. «Technologies de l'information - Techniques de sécurité - Management de la sécurité de l'information - Économie organisationnelle», International Organisation for Standardisation, Genève.

ISO / CEI TR 27019, 2013. «Technologies de l'information - Techniques de sécurité - Lignes directrices de gestion de la sécurité de l'information fondé sur la norme ISO / CEI 27002 pour les systèmes de contrôle de processus spécifiques à l'industrie des services publics d'énergie», International Organisation for Standardisation, Genève.

ISO / CEI 27031, 2011. «Technologies de l'information - Techniques de sécurité - Lignes directrices pour l'information et la technologie des communications de préparation pour la continuité des activités», International Organisation for Standardisation, Genève.

ISO / CEI 27035, 2011. «Technologies de l'information - Techniques de sécurité - Gestion de l'information des incidents de sécurité», International Organisation for Standardisation, Genève.

ISO/CEI 27799, 2016. « Informatique de santé - Management de la sécurité de l'information relative à la santé en utilisant l'ISO/CEI 27002», International Organisation for Standardisation, Genève.

ISO/CEI 31000, 2005. «Management du risque - Principes et lignes directrices», International Organisation for Standardisation, Genève.

Jureta, I., Mylopoulos, J., Faulkner, S., 2008. «Revisiting the core ontology and problem in requirements engineering». In: Proceedings of 16th IEEE international requirements engineering conference (RE '08), pp 71–80. DOI:10.1109/RE.2008.13.

Jurjens, J., 2002. «UMLSec: Extending UML for secure systems development, software and systems engineering», department of informatics, Munich University of Technologies, Germany.

KACTUS, 1996. The KACTUS Booklet version 1.0. Esprit Project 8145 KACTUS.

Kassou, M., Kjiri, L., 2012. « Ingénierie des exigences de la sécurité informatique: Revue de travaux de recherche de l'élicitation à la spécification », Revue e-Ti, No 6, 22pages.

Keeney, M., Kowalski, E., 2005. «Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors in May 2005». Report study case. University Carnegie Mellon, [Online]: http://www.cert.org/insider_threat/insidercross.html.

Khelifa, L.N., 2014. «Construction, Évolution et Visualisation de Topic Maps contextualisées», Doctoral Thesis in Computer sciences.

Kotonya, G., Sommerville, I., 1998. «Requirements Engineering: Processes and Techniques», New York: John Wiley & Sons.

Lammari, N., Bucumi, J. S., Akoka, J., Comyn Wattiau, I., 2011. «A conceptual Meta, Model for Secured Information Systems», ICSE´11. 2011. DOI :10.1145/1988630.1988635.

Leech, G., 1981. «Semantics: The Study of Meaning». Harmondsworth, UK: Penguin, (1981)

Lin, L., Nuseibeh, B., Ince, D., Moffett, J., Jackson, M., 2003. «Using Abuse Frames to Analyse Security Requirements», Proc. Of 11th IEEE International Requirements Engineering Conference (RE'03), USA.

Lodderstedt, T., Basin, D., Doser, J., 2002. «SecureUML: A UML-Based Modelling Language for Model-Driven Security», in the Proceedings of the 5th International Conference on the Unified Modeling Language.

Maedche, A., Staab, S., 2001. «Ontology Learning for the Semantic Web». IEEE Intelligent Systems, Special Issue on the Semantic Web, 16(2), 2001.

Magerit V3, 2012. «Methodology for Information Systems Risk Analysis and Management», The Method, Ministry of Public Administration, Madrid,.

Matoussi, A., Laleau, R., 2008. «A Survey of Non-Functional Requirements in Software Development Process». Rapport Technique TR–LACL–2008–7. Paris: Laboratoire d'Algorithmique, Complexité et Logique (LACL), Université Paris 12.

Matulevicius, R., Mouratidis, H., Mayer, N., Dubois, E., Heymans, P., 2012. «Syntactic and Semantic Extensions to Secure Tropos to Support Security Risk Management», Journal of Universal Computer Science (J.UCS), March 2012, Vol. 18, N°6, pp.816-844.

Matulevicˇius, R., Mayer, N., Mouratidis, H., Dubois, E., Heymans, P., Genon, N., 2008. «Adapting secure tropos for security risk management in the early phases of information systems development». In: CAiSE '08: proceedings of the 20th international conference on advanced information systems engineering. Springer, Berlin, pp 541–555.

Matulevičius, R., Heymans, P., Opdahl, A.L., 2007. «Comparing GRL and KAOS using the UEML Approach», Accepted at the 3rd International Conference on Interoperability for Enterprise Software and Applications (I, ESA 2007), Madeira, Portugal. DOI: 10.1007/978-1-84628-858-6_7.

Mayer, N., 2009. «Model based Management of Information System Security Risk», Doctoral Thesis in Computer sciences.

Mayer, N., Dubois, E., Heymans, P., Matulevicius, R., 2008. «Défis de la sécurité de l'information. Support à la gestion des risques de sécurité par les modèles», in : C. Rolland, O. Pastor, J.-L. Cavarero (eds.), "Nouveaux challenges dans les systèmes d'information", Ingénierie des Systèmes d'Information (Networking and Information Systems), Volume 13/1, March 2008.

McDermott, J., Fox, C., 1999. « Using abuse case models for security requirements analysis ». in the Proceedings of the 15th annual Computer Security Applications Conference, 1999. (ACSAC'99).55-64.

McEvoy, N., Whitcombe, A., 2002. «Structured risk analysis», InfraSec 2002. LNCS 2437; p. 88e103.

Mellado, D., Fernández, E., Medina Piattini, M., 2006. « SREP: A Proposal for Establishing Security Requirements for the Development of Secure Information Systems». WOSIS 2006: 135-145.

Moffett, J.D., Haley, C.B., Nuseibeh, B., 2004. «Core Security Requirements Artefacts», Technical report, Open University, 2004, UK.

Morana, S., Schacht, S., Scherp, A., and Maedche, A. 2014. "Conceptualization and Typology of Guidance in Information Systems," Working Paper Series in Information Systems No. 007, Mannheim.

Naved, A., 2014. «Deriving Security Requirements from Business Process Models», ISBN 978-9949-32-716, 4.

NIST, 2015. «National Institute of Standards and Technology, Special Publication 800-53», Security and Privacy Controls for Federal Information Systems and Organizations, April 2013, includes updates as of 01-22-2015.

Nuseibeh, B., Easterbrook, S., 2000. «Requirements Engineering: A Roadmap». In Proceedings of International Conference on Software Engineering, ACM Press. Limerick, Ireland.

OCTAVE. 1999. «Operationally Critical Threat, Asset and Vulnerability Evaluation», Carnegie Mellon, Software Engineering Institute.

Özacar, T., Öztürk, O., Ünalir, M.O., 2011. «ANEMONE: An environment for modular ontology development». Data & Knowledge Engineering, vol. 70, n 6, p. 504-526.

Peltier, T.R., 2005. «Information Security Risk Analysis (2nd ed.) », Boca Raton, FL: CRC Press.

Pyka, M., Januszkiewicz, P.,2013. «The OCTAVE methodology as a risk analysis tool for business resources», Proceedings of the International Multiconference on Computer Science and Information Technology, pp. 485 – 497.

Radichel, T., 2014. «Case study: critical controls that could have prevented target breach», Sans Information security reading room infosec, 2014.

Ramanauskaite, S., Olifer, D., Goranin, N., Čenys, A., 2013. «Security Ontology for Adaptive Correspondance of Security Standard», International Journal of Computers, Communications & Control (IJCCC), Vol 8, No 6 (2013).

Risk Management, 2004. Australian/New Zealand Standard 4360, ISBN 0733759041-2004.

Robbins, B., 2007. «The Case for Functional Security Requirements: Deriving a Framework for Functional Security Requirements Engineering», International Conference on Software Engineering Research & Practice, SERP 2007, Volume I, June 25, 28, 2007, Las Vegas Nevada, USA.

Roussey, C., Chanet, J.P., 2013. «Le premier module d'une ontologie agricole sur la protection des cultures: Agronomic Taxon». Atelier INtegration de sources/masses de données hétérogénes et Ontologies, dans le domaine des sciences du VIVant et de l'Environnement, IN-OVIV 2013 associ´e `a la Plate-forme IA 2013 (PFIA 2013) et aux 24`eme journ´ees d'Ing´eni´erie des Connaissances (IC 2013), Jul 2013, Lille, France. p. 5 - p. 16.

Rune, W., Ole Arnt, J., Bjørn, A.G.,2007. «Security Assessments of Safety Critical Systems Using HAZOPs», Faculty of Computer Sciences, Østfold University College and Institute for Energy Technology, Norway. DOI: 10.1007/3-540-45416-0_2.

Salini, P., Kanmani, S., 2011. «A Survey on Security Requirements Engineering», International Journal of Reviews in Computing, 8(1), pp. 1-10, DOI:10.1016/ j. compeleceng.2012.08.008.

SANS Institute, 2002. «A quality Risk Analysis and Management Tool-CRAMM», Infosec Reading Room.

SANS Institute, 2003. «Using a Capability Maturity Model to Derive Security Requirements».

Schmidt, H., 2009. «Pattern-based confidentiality, preserving refinement». In: Engineering secure software and systems—first international symposium (ESSoS), ser. LNCS, vol 5429.Springer, Berlin, pp 43–59, 2009. DOI: 10.6029/smartcr.2012.01.007.

Shamal, F., Fléchais, I., 2010. «Meta-Model for Usable Secure Requirements Engineering». SESS '10, May 2010, Cape Town, South Africa. DOI:10.1145/1809100.1809105.

Shameli-Sendi, A., Aghababaei-Barzegar, R., Cheriet, M., 2016. «Taxonomy of information security risk assessment (ISRA) ». Computers & Security, 57:14 – 30.

Shvaiko, P., Euzenat, J., 2013. «Ontology matching: state of the art and future challenges», IEEE Transactions on Knowledge and Data Engineering, Institute of Electrical and Electronics Engineers (IEEE), 2013, 25 (1), pp.158-176.

Silver, M. S., 1991. «Decisional Guidance for Computer-Based Decision Support», MIS Quarterly (15:1), pp. 105-122.

Sindre G., Opdahl A.L. 2005. « Eliciting Security Requirements with Misuse Cases ». Requirements engineering 10, no. 1 (2005): 34-44.

Soler, E., 2008. «Towards Comprehensive Requirement Analysis for Data Warehouses: Considering Security Requirements». Thèse de doctorat. Vienna University of Technology.

Sonna Momo, L., 2009. «Development of Dynamic Dashboards SSI: An approach based on ontologies». PhD in Information Systems.

Soomro, I., Ahmed, N., 2012. «Towards Security Risk-oriented Misuse Cases». In Proceedings of the of Business Management Workshops, BPM 2012 workshops, LNBIP, vol 132, (pp. 673-684).

Souag, A., Salinesi, C., Comyn-Wattiau, I., 2013. « Using security and domain ontologies for security requirements analysis». In: Computer Software and Applications Conference Workshops (COMPSACW), 2013 IEEE 37th Annual. DOI:10.1109/COMPSACW.2013.124.

Srivatanakul, T., Clark, J.A., Polack, F., 2004. «Effective Security Requirements Analysis: HAZOP and Use Cases», K. Zhang and Y. Zheng (Eds.): ISC 2004, LNCS 3225, pp. 416–427, 2004. c© Springer, Verlag Berlin Heidelberg.

Staab, S., Schurr, H., Studer, P., Sure, Y., 2001. « Knowledge processes and ontologies » IEEE Intelligent Systems 16(1):26-34.

Stoneburner, G., Goguen, A., Feringa, A., 2007. «NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems», United States National Institute of Standards and Technology, Washington, DC, (2007).

Stumme, G., Hotho, A., Berendt, B., 2006. «Semantic web mining: State of the art and future directions». Web Semantics: Science, Services and Agents on the World Wide Web, 4(2), pp.124–143.

Suárez-Figueroa, M.C., Gómez-Pérez, A., Fernández-López, M., 2012. «The NeOn Methodology for Ontology Engineering», Book Chapter in Ontology Engineering in a Networked World, 2012, Publisher: Springer Berlin Heidelberg, pp. 9-34.

TARA. 2011. «Methodology Description, Threat Assessment / Remediation Analysis», [Online] http://www.mitre.org/sites/default/files/pdf/11_4982.pdf.

Tomhave, B., Heidt, E., Robins, A., 2014. «Comparing Methodologies for IT Risk Assessment and Analysis». Gartner, 30 January 2014.

Tondel, I.A., Jaatun, M.G., Meland, P.H., 2008. «Security Requirements for the Rest of Us: A Survey». IEEE Software. 2008. DOI: 10.1109/MS.2008.19.

Toval A., Nicolás J., Moros B., García O. 2001. « Requirements Reuse for Improving Information Systems Security: A Practitioner's Approach ». Requirements Engineering Journal 6: 205-19.

Travis, C., Mead, N., 2010. «Security Requirements Reusability and the SQUARE Methodology», Technical note, CMU/SEI,2010, TN,027 CERT® Program. September 2010.

Turenne, N., 2010. «Apprentissage statique pour l'extraction de concepts à partir de textes», Doctoral Thesis in Computer sciences.

Van Lamsweerde A. 2004. « Elaborating security requirements by construction of intentional antimodels ». In the proceedings of the 26th International Conference on Software Engineering, 2004. ICSE 2004., 148-57.

Vasquez, M., Lammari, N., Comyn Wattiau, I., Akoka, J., 2012. « De l´analyse des risques à l´expression des exigences de sécurité des systèmes d'information», Inforsid 2012.

Vorster, A., Labuschagne, L., 2005. «A framework for comparing different information security risk analysis methodologies». In Proceedings of the South African Institute for Computer Scientists and Information Technologists, (2005), pp. 95-103.

Vraalsen F., den Braber F., Lund M.S., Stølen K. 2005. « The CORAS Tool for Security Risk Analysis ». In Trust Management, edited by Peter Herrmann, Valérie Issarny, Simon Shiu, 402-5. Lecture Notes in Computer Science 3477. Springer Berlin Heidelberg.

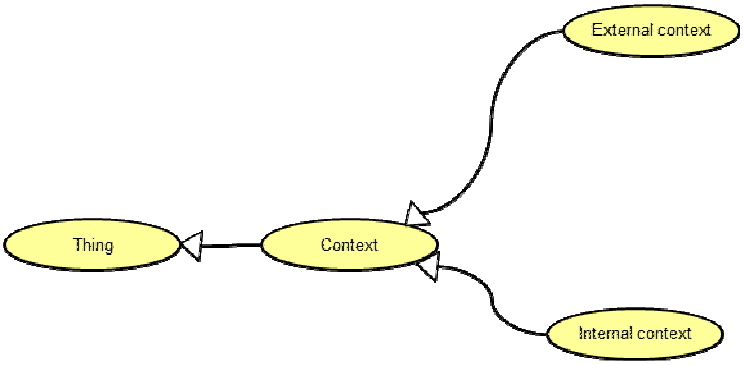
Wagner, S., Méndez-Fernández, D., Islam, S., Lochmann, K., 2009. « A security requirements approach for web systems», in: Proc. Quality Assessment in Web (QAW 2009), CEUR.

Yu, E., Liu, L., 2006. «Mylopoulos A social ontology for integrating security and software engineering», in integrating security and software engineering: advances and future visions, Idea Group Publishing, pp. 743-772.

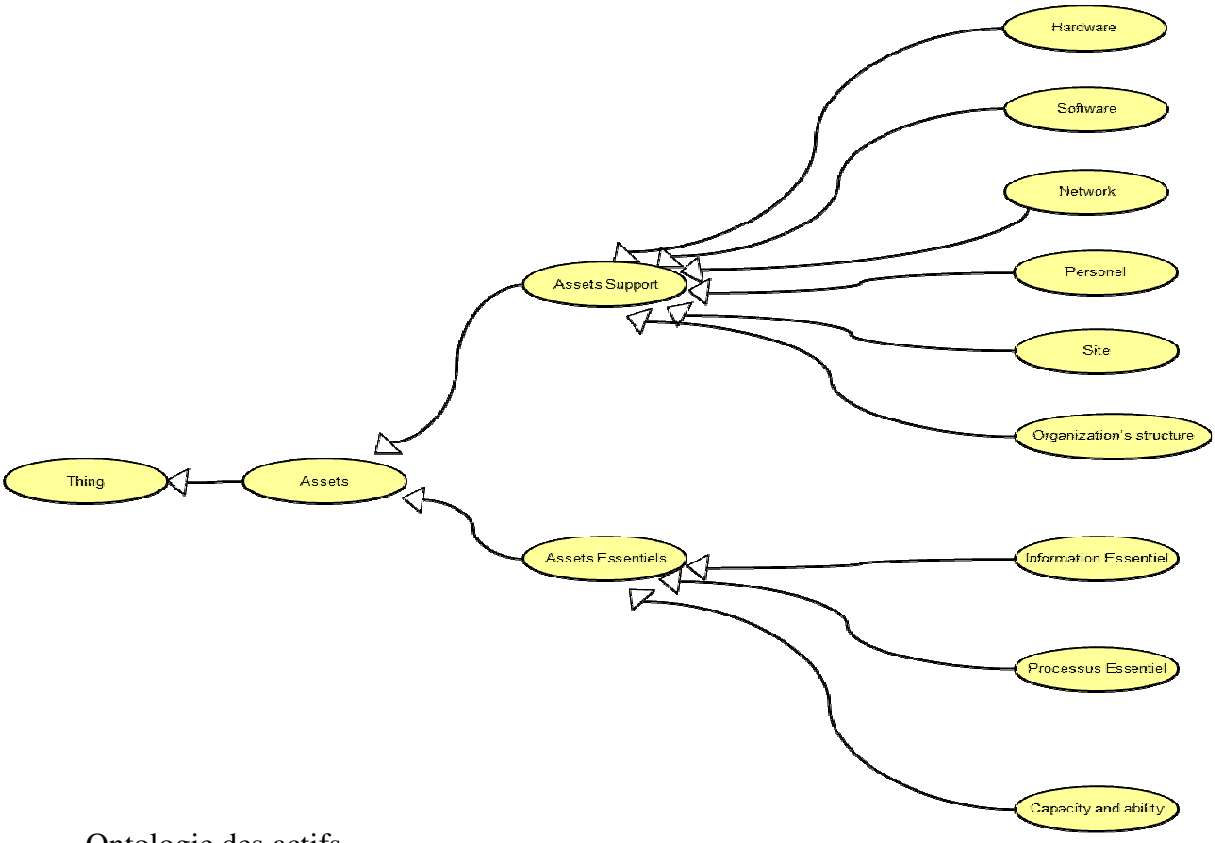
Zambon, E., Etalle, S., Wienringa, R.J., Hartel, P., 2011. «Model, based qualitative risk assessment for availability of IT infrastructures», Software System Model, 10(4): 553-580. DOI 10.1007/s10270-010-0166-8.

Annexes

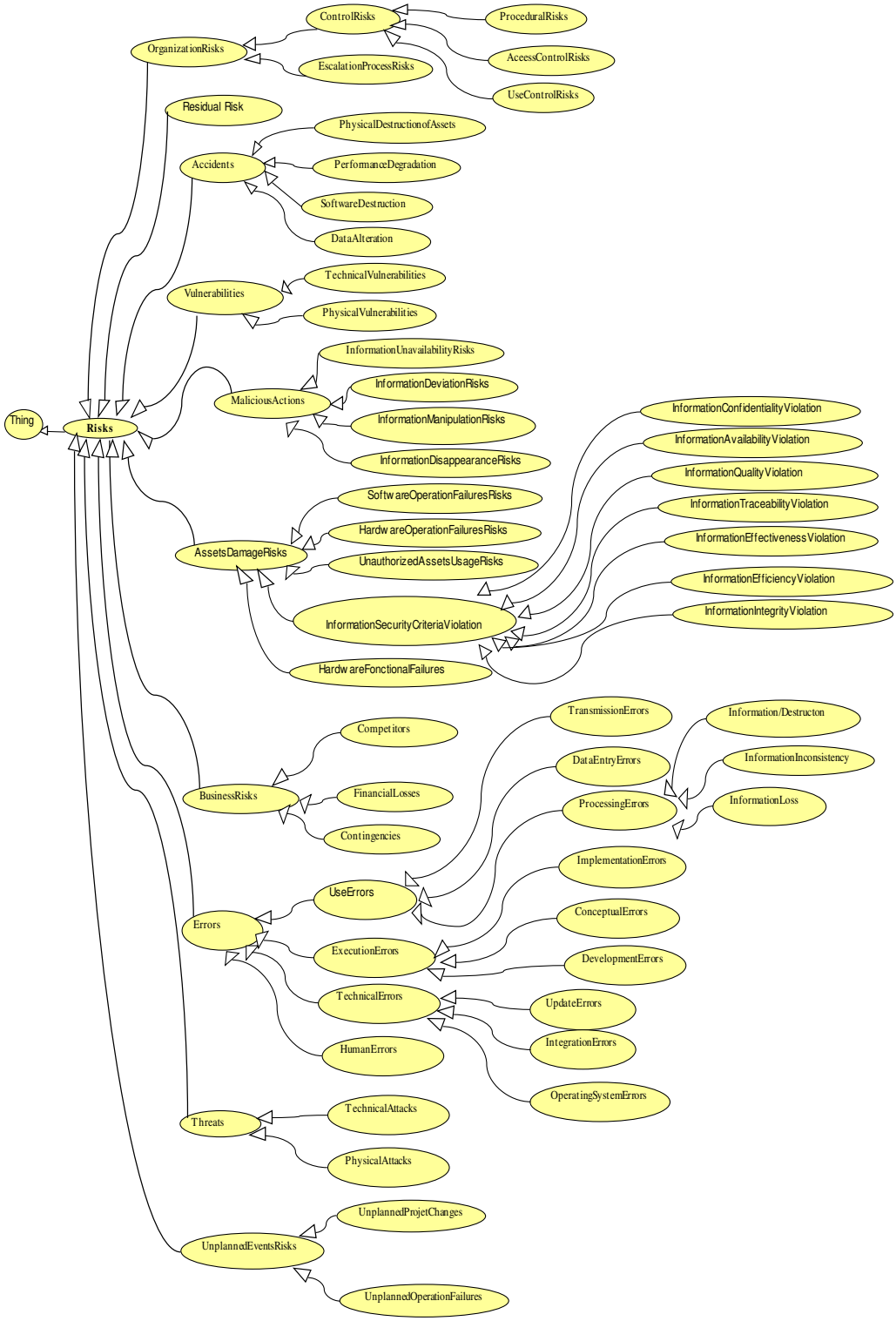
- **Annexe A** : Les ontologies :



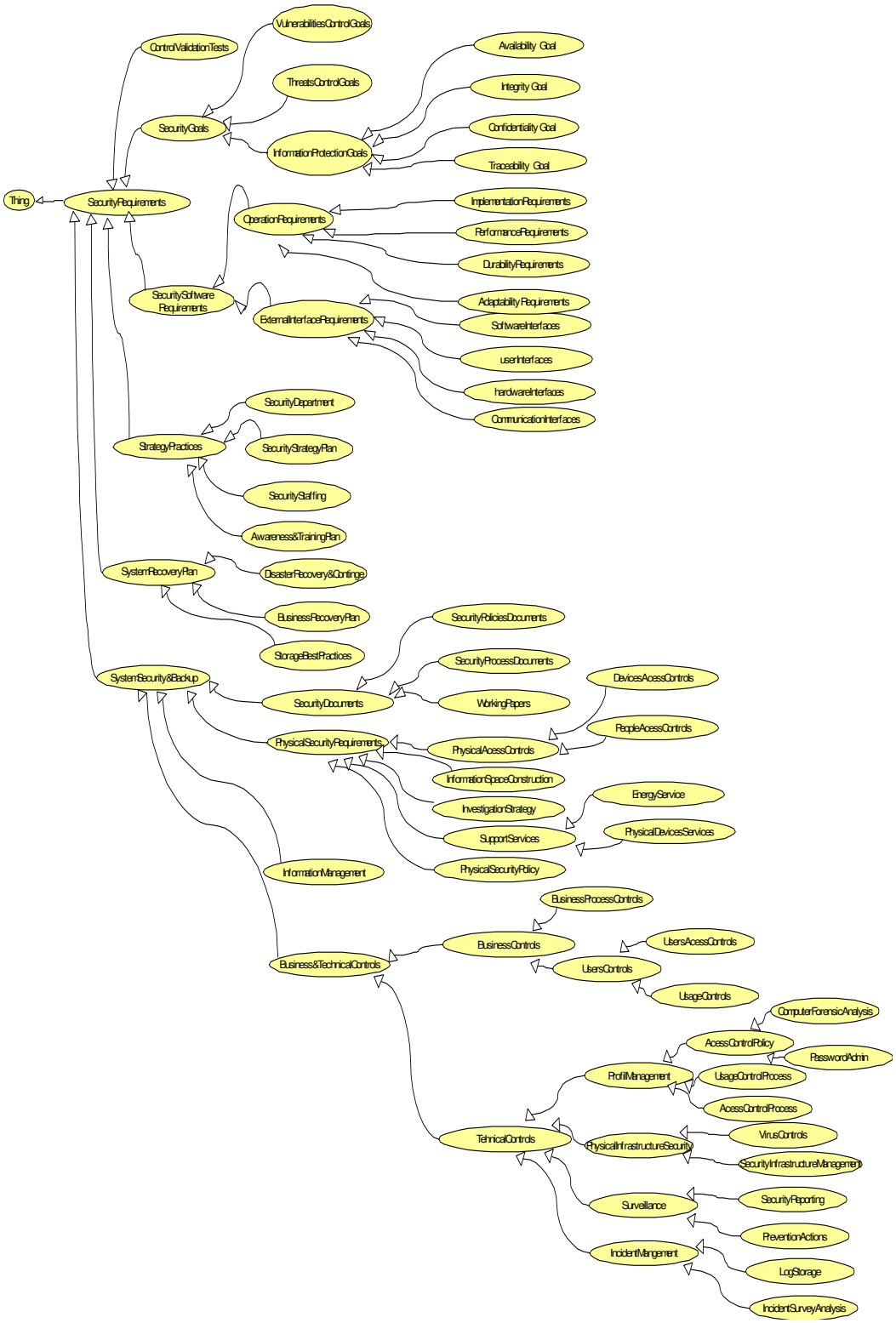
Ontologie du contexte



Ontologie des actifs



Ontologie des risques



Ontologie des exigences de sécurité

Annexe B: Origine des concepts utilisés dans l'ontologie des risques

Niveau 1	Niveau 2	Niveau 3	Niveau 4	Méthodologies
1.Organization Risks	1.1 ControlRisks	1.1.1 Procedural Risks		FAIR-OCTAVE
		1.1.2 Access Control Risks		FAIR-OCTAVE
		1.1.3 Use Control Risks		FAIR-OCTAVE
	1.2 Escalation Process Risks			OCTAVE
2. Residual Risks				EBIOS-CRAMM
3. Accidents	3.1Physical Destruction Of Assets			MEHARI
	3.2Performance Degradation			MEHARI
	3.3 Software Destruction			MEHARI
	3.4 Data Alteration			EBIOS-MEHARI
4. Vulnerabilities	4.1Technical Vulnerabilities			EBIOS-CRAMM
	4.2 Physical Vulnerabilities			EBIOS-CRAMM
5. Malicious Actions	5.1Information Unavailability Risks			EBIOS-MEHARI
	5.2 Information Deviation Risks			EBIOS-MEHARI
	5.3 Information Manipulation Risks			CRAMM-OCTAVE
	5.4 Information Disappearance Risks			CRAMM-OCTAVE
6. Assets Damage Risks	6.1 Physical Assets Risks			OCTAVE-CRAMM
	6.2 Software Operation Failures Risks			OCTAVE-CRAMM
	6.3Hardware Operation Failures Risks			OCTAVE-CRAMM
	6.4 Unauthorized Assets Usage Risks			OCTAVE-CRAMM
	6.5Information Security Criteria Violation	6.5.1 Information Confidentiality Violation		OCTAVE-CRAMM
		6.5.2 Information Availability Violation		OCTAVE-CRAMM
		6.5.3 Information Quality Violation		OCTAVE-CRAMM
		6.5.4 Information Traceability Violation		OCTAVE-CRAMM
		6.5.5 Information Effectiveness Violation		OCTAVE-CRAMM
		6.5.6 Information Efficiency Violation		OCTAVE-CRAMM
		6.5.7 Information Integrity Violation		OCTAVE-CRAMM
7. Business	7.1 Competition			FAIR-COBIT-ITIL--RMF-

Risks	7.2 FinancialLoss			FAIR-COBIT-ITIL
	7.3 Contingencies			FAIR- COBIT-ITIL
8. Errors	8.1 Use Errors	8.1.1Transmission Errors		MEHARI
		8.1.2 Data Entry Errors		MEHARI
		8.1.3 Processing Errors	8..1.3.1 Information Destruction	MEHARI
			8.1.3.2 Information Inconsistency	MEHARI
			8.1.3.3 Information Loss	MEHARI-EBIOS
	8.2 Execution Errors	8.2.1 Implementation Errors		HAZOP
		8.2.2 Conceptual Design Errors		HAZOP
		8.2.3 Development Errors		HAZOP
	8.3 Technical Errors	8.3.1 Update Errors		MEHARI
		8.3.2 Integration Errors		MEHARI
		8.3.3 Operating System Errors		MEHARI
	8.4 Human Errors			HAZOP
9. Threats	9.1 TechnicalAttacks			EBIOS-CRAMM-
	9.2 Physical Attacks			EBIOS - CRAMM
10. Unplanned Events Risks	10.1Unplanned Projet Changes			FMECA
	10.2 Unplanned Operation Failures			FMECA

Annexe C: Origine des concepts utilisés dans l'ontologie des exigences de sécurité

Niveau 1	Niveau 2	Niveau 3	Niveau4	Niveau 5	Niveau 6	Méthodologies
1.Control Validation Tests						SIREN
2. Security Goals	2.1Vulnerabilities Control Goals					MEHARI-SECURETROPOS-SIREN
	2.2 Threats Control Goals					SIREN-SECURE TROPOS
	2.3 Information Protection Goals	2.3.1 Availability Goal				MEHARI-SECURE TROPOS-SIREN
		2.3.2 Integrity Goal				MEHARI-SECURE TROPOS-SIREN
		2.3.3 Confidentiality Goal				MEHARI-SECURE TROPOS-SIREN
		2.3.4 Traceability Goal				MEHARI-SECURE TROPOS-SIREN
3. Security Software Requirements	3.1 Operation Requirements					CC-SIREN-
		3.1.1 Implementation Requirements				SIREN
		3.1.2 Performance Requirements				SIREN
		3.1.3 Durability Requirements				SIREN
		3.1.4 Adaptavility Requirements				SIREN
	3.2 External Interface Requirements					CC
		3.2.1 Software Interfaces				CC- SIREN
		3.2.2 User Interfaces				CC
		3.2.3 Physical Infrastructure Interfaces				CC
		3.2.4 Communication Interface				CC
4. Strategy Practices	4.1 Security Department					CC
		4.1.1 Information Management				CC
		4.1.2 Prevention Actions				CC
	4.2 Security Strategy Plan					CC
	4.3 Security Staffing					CC
	4.4 Awareness &TrainingPlan					CC
5. System Recovery Plan	5.1DisasterRecovery& Contingency					CC
	5.2 Business Recovery Plan					CC
	5.3 Storage Best Practices					CC- SIREN
	6.1 Security Documents					CC
		6.1.1 Security Policies Documets				CC

6. SystemSecurity &Backup		6.1.2 Security Process Documents				CC
		6.1.3 Working Papers				CC- SIREN
	6.2 Physical Security Requirements					CC- SIREN
		6.2.1 Physical Access Controls				CC
			6.2.1.1 Devices Access Controls			CC
			6.2.1.2 People Access Controls			CC
		6.2.2 Information Space Construction				CC
		6.2.3 Investigation Strategy				CC
		6.2.4 Support Services				CC
			6.2.4.1 Energy Services			SIREN
			6.2.4.2 Physical Devices Services			CC
		6.2.5 Physical Security Policy				CC
	6.3. Information Management					CC
	6.4 Business&Technical Controls					CC
		6.4.1 Business Controls				CC
			6.4.1.1 Business Process Controls			SIREN
			6.4.1.2 Users Controls			SIREN
				6.4.1.2.1Users Access Controls		SIREN- CC
				6.4.1.2.2 Usage Controls		CC
		6.4.2 Technical Controls				CC
			6.4.2.1 Profil Management			CC
				6.4.2.1.1 Access Control Policy		SIREN
					6.4.2.1.1.1 Computer Forensic Analysis	SIREN
					6.4.2.1.1.2 Pasword Admin	SIREN- CC MEHARI
				6.4.2.1.2 Usage ControlProcess		SIREN
				6.4.2.1.3 Access Control Process		SIREN-CC
			6.4.2.2 Physical Infrastructure Security			CC
				6.4.2.2.1 VirusControls		CC
				6.4.2.2.2 Security Infrastructure Management		MEHARI-CC-SIREN
			6.4.2.3 Surveillance			CC-MEHARI

				6.4.2.3.1 Security Reporting		SIREN
				6.4.2.3.2 Prevention Actions		SIREN
			6.4.2.4 Incident Mangement			CC
				6.4.2.4.1 LogStorage		CC
				6.4.2.4.2 Incidents SurveyAnalysis		CC

Annexe D : Liste des scénarios des risques

N°	Scénarios
1	Destruction ou altération de ressources techniques, de supports de stockages, de documents ou de locaux du système, par un phénomène naturel majeur.
2	Destruction ou altération d'un équipement ou d'un support de stockage d'une plate-forme du système, due à un accident ou une négligence ou encore à un acte délibéré, par une personne ayant accès à ces éléments.
3	Arrêt ou dysfonctionnement de la climatisation dans les locaux d'une plate-forme, de ceux de stockage de supports, de documents ou d'équipements, suite à une panne ou un acte volontaire
4	Surtensions, perturbations ou arrêt de l'alimentation électrique d'une plate-forme du système.
5	Incident rendant indisponible les moyens de télécommunications nécessaires au fonctionnement du système ou à son utilisation
6	Observation des activités d'exploitation ou d'administration du système par des personnes non autorisées (visiteurs, caméras cachées, observateurs par des fenêtres).
7	Au niveau des réseaux ou des supports de communication utilisés, interception des échanges entre un utilisateur et le système, entre deux plates-formes du système, entre deux équipements d'une même plate-forme.
8	Vol de documents du système, vol ou substitution d'un support de stockage d'informations dans un site du système, dans un site de stockage.
9	Vol ou substitution d'équipements dans les locaux d'une plate-forme, ou dans ceux de stockage ou à la faveur de la maintenance interne ou le transport interne de ces équipements, avec capture éventuelle de données résiduelles.
10	Exploitation de données résiduelles sur les supports de stockage ou les équipements retirés du système avant réemploi par ailleurs ou mise au rebut.
11	Personne interne a l'organisme qui, par négligence, diffuse de l'information à d'autres personnes de l'organisme n'ayant pas le besoin d'en connaître, ou à l'extérieur. Personne diffusant consciemment de l'information à d'autres personnes de l'organisme n'ayant pas le besoin d'en connaître, ou à l'extérieur.
12	Personne transmettant des informations fausses, destinées à être intégrées au système d'information, pour désinformer le destinataire et porter atteinte à la fiabilité du système ou la validité des informations.
13	Implantation de fonctionnalités illicites dans un équipement ou une plate-forme du système, en vue de provoquer des dysfonctionnements ou des détournements d'information.
14	Implantation et activation de fonctions illicites (cheval de troie, bombe logique, virus, keylogger...) dans les logiciels du système ou propagation de telles fonctions à partir des dispositifs d'accès des utilisateurs ou des postes de travail des autres accédants.
15	Panne ou dysfonctionnement d'un matériel du système, entraînant la dégradation de service ou l'indisponibilité du système.

16	Saturation des équipements du système lié à un défaut de capacité ou de conception ou à une sollicitation anormale du système (attaque de type déni de service par exemple).
17	Fonctionnement non conforme du logiciel du système, résultant d'un défaut de réalisation, d'installation, de maintenance ou d'exploitation.
18	Impossibilité ou difficulté à assurer le maintien en condition opérationnelle du système, du fait de défauts de conception du système, d'insuffisances du dispositif de soutien, de défaillances de fournisseurs, d'obsolescence de ressources techniques.
19	Accès à un équipement système par une personne non autorisée et utilisation de cet équipement pour accéder aux fonctions ou aux données du système.
20	Copie frauduleuse de logiciels du système en vue de leur utilisation par ailleurs.
21	Mise en œuvre dans le système de logiciels dont les droits d'utilisation ou d'exploitation sont insuffisants (contrefaits ou copiés).
22	Modification/altération des données échangées entre les équipements ou les plates-formes du système ou entre le système et les dispositifs d'accès des utilisateurs (menace de type Man in the middle), ou modification/altération des données sur les supports de stockage (voire substitution de support) ou dans les équipements du système.
23	Traitement illicite des données personnelles, utilisation des données personnelles à d'autres fins que celles autorisées par la législation ou un règlement.
24	Erreur d'exploitation ou d'intervention, erreur d'utilisation.
25	Utilisation ou exploitation du système par une personne autorisée, dans le but malintentionné, abus de droit.
26	Usurpation de l'identité ou des droits d'accès d'une personne autorisée, par une personne malintentionnée.
27	Contestation, par une personne autorisée, des actions effectuées sur le système ou ses informations.
28	Indisponibilité du personnel d'exploitation ou d'administration ou impossibilité pour celui-ci d'accéder au système effectuer les actions nécessaires (exemples : pandémie, évacuation d'un site, mouvement social).

Annexe E: Les règles de correspondance

1. *Risk='ProceduralRisks' ∧ Type of treatment='Prevention'* ⇒ *SR='BusinessProcessControls' ∧ SR='SecurityProcessDocuments'*
2. *Risk='AccessControlRisks' ∧ Type of treatment='Prevention '* ⇒ *SR=' ControlValidationTests' ∧ SR='BusinessProcessControls' ∧ SR='PasswordAdmin' ∧ SR=' AccessControlPolicy' ∧ SR='UsageControlProcess''∧ SR=' AccessControlProcess'*
3. *Risk='UseControlRisks' ∧ Type of treatment='Prevention'* ⇒ *SR='BusinessProcessControls' ∧ SR='PasswordAdmin'∧ SR='UsersControls' ∧ SR='LogStorage' ∧ SR='UsageControlProcess' ∧ SR='ComputerForensicAnalysis'∧ SR='AccessControlPolicy'*
4. *Risk='EscalationProcessRisks' ∧ Type of treatment='Mitigate'* ⇒ *SR='UsageControlProcess' ∧ SR='AccessControlProcess'*
5. *Risk='ResidualRisks' ∧ Type of treatment='Prevention'* ⇒ *SR='SecurityDocuments' ∧ SR='SecurityStrategyPlan'*
6. *Risk=' PhysicalDestructionofAssets' ∧ Type of treatment='Tolivewith'* ⇒ *SR=' InformationSpaceConstruction'∧ SR=' InvestigationStrategy'∧ SR=' EnergyServices'∧ SR=' PhysicalDevicesServices' ∧ SR=' PhysicalSecurityPolicy' ∧ SR='SecurityInrastructureManagement'*
7. *Risk='PerformanceDegradation' ∧ Type of treatment='Mitigate'* ⇒ *SR='AdaptabilityRequirements'∧ SR='ImplementationRequirements'∧ SR='PerformanceRequirements'∧ SR='DurabilityRequirements'∧ SR='SoftwareInterfaces'∧ SR='UserInterfaces'∧SR='CommunicationInterfaces'*
8. *Risk='SoftwareDestruction' ∧ Type of treatment='Prevention'* ⇒ *SR='AdaptabilityRequirements'∧ SR='ImplementationRequirements'∧ SR='PerformanceRequirements'∧ SR='DurabilityRequirements'*
9. *Risk=' DataAlteration' ∧ Type of treatment='Avoid'* ⇒ *SR=' BusinessRecoveryPlan' ∧ SR=' StorageBestPractices'∧ SR=' BusinessProcessControls'*
10. *Risk='TechnicalVulnerabilities' ∧ Type of treatment='Prevention'* ⇒ *SR='ControlValidationTests' ∧ SR='VulnerabilitiesControlGoals'*
11. *Risk='PhysicalVulnerabilities' ∧ Type of treatment='Prevention'* ⇒ *SR='ControlValidationTests' ∧ SR='VulnerabilitiesControlGoals'*
12. *Risk='InformationUnavailabilityRisks' ∧ Type of treatment='Mitigate'* ⇒ *SR=' StorageBestPractices' ∧ SR='LogStorage' ∧ SR='ComputerForensicAnalysis'*
13. *Risk='InformationDeviationRisks' ∧ Type of treatment='Avoid'* ⇒ *SR=' StorageBestPractices' ∧ SR='LogStorage' ∧ SR=' ComputerForensicAnalysis'*
14. *Risk='InformationManipulationRisks' ∧ Type of treatment=Prevention*

⇒ *SR='StorageBestPractices' ∧ SR='LogStorage' ∧ SR='ComputerForensicAnalysis'*
15. Risk='InformationDisappearanceRisks' ∧ Type of treatment='Mitigate' ⇒ *SR='StorageBestPractices'∧ SR=LogStorage' ∧ SR='ComputerForensicAnalysis'*
16. Risk='PhysicalAssetsRisks' ∧ Type of treatment='Mitigate' ⇒ *SR='InformationSpaceConstruction' ∧ SR='InvestigationStrategies' ∧ SR='EnergyServices' ∧ SR='PhysicalDevicesServices' ∧ SR='PhysicalSecurityPolicy'*
17. Risk='SoftwareOperationFailuresRisks' ∧ Type of treatment='Mitigate' ⇒ *SR='InformationSpaceConstruction' ∧ SR='InvestigationStrategies' ∧ SR='EnergyServices' ∧ SR='PhysicalDevicesServices' ∧ SR='PhysicalSecurityPolicy'*
18. Risk='HardwareOperationFailuresRisks' ∧ Type of treatment='Mitigate' ⇒ *SR='DisasterRecoveryPlan' ∧ SR='BusinessRecoveryPlan'∧ SR='StorageBestPractices'*
19. Risk='UnauthorizedAssetsUsageRisks' ∧ Type of treatment='Mitigate' ⇒ *SR='PhysicalSecurityPolicy' ∧ SR='AccessControlPolicy' ∧ SR='VirusControls'*
20. Risk='InformationConfidentialityViolation' ∧ Type of treatment='Detection' ⇒ *SR='ConfidentialityGoal' ∧ SR='SecurityPoliciesDocuments' ∧ SR='PhysicalSecurityPolicy' ∧ SR='InformationManagement' ∧ SR='AccessControlPolicy' ∧ SR='AccessControlProcess'∧ SR='PreventionActions' ∧ SR='LogStorage'∧ SR='ComputerForensicAnalysis'*
21. Risk='InformationAvailabilityViolation' ∧ Type of treatment='Avoid' ⇒ *SR='AvailabilityGoal' ∧ SR='PhysicalSecurityPolicy' ∧ SR='InformationManagement '∧ SR='PreventionActions' ∧ SR='LogStorage'∧ SR='ComputerForensicAnalysis'*
22. Risk='InformationQualityViolation' ∧ Type of treatment='Prevention' ⇒ *SR='InformationManagement'∧ SR='PreventionActions' ∧ SR='LogStorage'∧ SR='ComputerForensicAnalysis'*
23. Risk='InformationTraceabilityViolation' ∧ Type of treatment='Detection' ⇒ *SR='TraceabilityGoal'∧SR='InformationManagement'∧ SR='PreventionActions' ∧ SR='LogStorage'∧ SR='ComputerForensicAnalysis'*
24. Risk='InformationEffectivenessViolation' ∧ Type of treatment='Avoid' ⇒ *SR='PerformanceRequirements'∧SR='InformationManagement '∧ SR='PreventionActions' ∧ SR='LogStorage'∧ SR='ComputerForensicAnalysis'*
25. Risk='InformationEfficiencyViolation' ∧ Type of treatment='Avoid' ⇒ *SR='PerformanceRequirements'∧SR='InformationManagement' ∧ SR='PreventionActions' ∧ SR='LogStorage'∧ SR='ComputerForensicAnalysis'*
26. Risk='InformationIntegrityViolation ∧ Type of treatment='Prevention' ⇒ *SR='IntegrityGoal'∧ SR='PhysicalSecurityPolicy'∧ SR='InformationManagement' ∧ SR='PreventionActions' ∧ SR='LogStorage'∧ SR='ComputerForensicAnalysis'*
27. Risk='Competition' ∧ Type of treatment='Avoid' ⇒ *SR='SecurityStrategyPlan'*

28. Risk='FinancialLoss' ∧ Type of treatment='Avoid'   *⇒ SR='SecurityStrategyPlan'∧ SR='ComputerForensicAnalysis'*
29. Risk='Contingencies' ∧ Type of treatment='Avoid'   *⇒ SR='SecurityStrategyPlan'∧ SR='DisasterRecoveryPlan'∧ SR='BusinessRecoveryPlan'*
30. Risk='TransmissionErrors' ∧ Type of treatment='Mitigate'   *⇒ SR='SecurityProcessDocuments' ∧ SR='SecurityPoliciesDocuments' ∧ SR='WorkingPapers'*
31. Risk='DataEntryErrors' ∧ Type of treatment='Mitigate'   *⇒ SR='UsersControls' ∧ SR='UsageControlProcess' ∧ SR=' AccessControlProcess'*
32. Risk='InformationDestruction' ∧ Type of treatment='Avoid'   *⇒ SR='DisasterRecoveryPlan' ∧ SR='BusinessRecoveryPlan'∧ SR='StorageBestPractices'∧SR='SecurityPoliciesDocuments' ∧ SR='WorkingPapers' ∧ SR='ComputerForensicAnalysis*
33. Risk='InformationInconsistency' ∧ Type of treatment='Avoid'   *⇒SR='SecurityPoliciesDocuments' ∧ SR='WorkingPapers' ∧ SR='ComputerForensicAnalysis'*
34. Risk='InformationLoss' ∧ Type of treatment='Mtigate'   *⇒SR='DisasterRecoveryPlan' ∧ SR='BusinessRecoveryPlan'∧ SR='StorageBestPractices'SR='SecurityPoliciesDocuments' ∧ SR='WorkingPapers' ∧ SR='ComputerForensicAnalysis*
35. Risk='Implementation Errors' ∧ Type of treatment='Prevention'   *⇒ SR ='ControlValidationTests' ∧ SR='AdaptavilityRequirements' ∧ SR='ImplementationRequirements' ∧ SR='PerformanceRequirements'*   *∧ SR='DurabilityRequirements' ∧ SR='SoftwareInterfaces'∧ SR ='UserInterfaces'∧ SR='CommunicationInterfaces'*
36. Risk='ConceptualDesignErrors' ∧ Type of treatment='Prevention'   *⇒ SR ='ControlValidationTests' ∧ SR='AdaptavilityRequirements' ∧ SR='ImplementationRequirements' ∧ SR='PerformanceRequirements'*   *∧ SR='DurabilityRequirements' ∧ SR='SecurityPoliciesDocuments'*
37. Risk='DevelopmentErrors' ∧ Type of treatment='Prevention'   *⇒ SR ='ControlValidationTests '∧ SR='SecurityPoliciesDocuments' ∧ SR='SecurityProcessDocuments'*
38. Risk='UpdateErrors' ∧ Type of treatment='Prevention'   *⇒ SR='AdaptabilityRequirements'∧ SR='ImplementationRequirements'∧ SR='DurabilityRequirements'∧ SR='SoftwareInterfaces'*
39. Risk='IntegrationErrors' ∧ Type of treatment='Prevention'   *⇒ SR='SoftwareInterfaces'∧ SR='UserInterfaces'∧ SR='CommunicationInterfaces '*
40. Risk=' OperatingSystemErrors ' ∧ Type of treatment='Prevention'   *⇒ SR ='AdaptavilityRequirements'∧ SR=' ImplementationRequirements'*
41. Risk=' HumanErrors ' ∧ Type of treatment='Prevention'   *⇒ SR =' SecurityStaffing'∧ SR=' AwarenessTrainningPlan'∧ SR=' SecurityPoliciesDocuments'∧ SR='WorkingPapers'∧ SR=' ProcessControls'∧ SR=' UsersControls'∧ SR='LogStorage'∧ SR='ComputerForensicAnalysis'*

42. Risk='PhysicalAttacks' ∧ Type of treatment='Mitigate'   *⇒ SR='ThreatsControlGoals' ∧ SR='InformationSpaceConstruction' ∧ SR='InvestigationStrategy ' ∧ SR='PhysicalSecurityPolicy'*
43. Risk='TechnicalAttacks' ∧ Type of treatment='Mitigate'   *⇒ SR='ThreatsControlGoals' ∧ SR='SecurityStaffing' ∧ SR='AwarenessTrainingPlan' ∧ SR='LogStorage' ∧ SR='ComputerForensicAnalysis'*
44. Risk='UnplannedProjetChanges' ∧ Type of treatment='Mitigate'   *⇒ SR ='ControlValidationTests '*
45. Risk='UnplannedOperationFailures' ∧ Type of treatment='Mitigate'   *⇒ SR ='ControlValidationTests'∧ SR='BusinessRecoveryPlan'∧ SR=' StorageBestPractices' ∧ SR='WorkingPapers'∧ SR='VirusControls'∧ SR='PreventionActions'∧ SR='LogStorage' ∧ SR='ComputerForensicAnalysis'*

Annexe F: Déroulement de l'approche

Liste scénario (AnnexeD)	Actifs	Éléments du contexte	Objectifs de sécurité	Échelle de réalisation du scénario	Positionnement dans l'ontologie des risques	Positionnement dans l'ontologie des exigences de sécurité
1	Matériel	Contexte externe	Intégrité	Moyenne	**3.4** **3.2**	**5.2** **5.3** **6.4.1.1** **3.1.4** **3.1.1** **3.1.2** **3.2.1** **3.2.2** **3.2.4**
			Disponibilité	Forte	**3.1** **6.3**	**5.2** **5.3** **6.4.1.1** **6.2.2** **6.2.3** **6.2.4.1** **6.2.4.2** **6.2.5** **6.4.2.2.2** **5.1** **3.1.3**
	Application	Contexte externe	Intégrité	Forte	**3.4** **3.2**	**5.2** **5.3** **3.1.4** **3.1.1** **3.1.2** **3.2.1** **3.2.2** **3.2.4**
			Disponibilité	Moyenne	**3.2** **3.3**	**3.1.4** **3.1.1** **3.1.2** **6.2.2** **6.2.4.1** **6.2.4.2** **6.2.5**
			Confidentialité	Moyenne	**6.5**	**3.1.4** **3.1.1** **6.2.5** **6.4.2.4.1** **6.4.2.3.2** **6.4.2.1.1.1** **2.3.1** **2.3.2** **2.3.3** **2.3.4** **4.1.1** **6.1.1** **6.3** **6.4.2.1.1**

	Site	Contexte externe	Disponibilité	Forte	**3.1**	**3.1.1** **3.1.2** **3.2.1** **3.2.2** **3.2.4** **6.2.2** **6.2.3** **6.2.4.1** **6.2.4.2** **6.2.5** **6.4.2.2.2**
2	Matériel	Gouvernance	Intégrité	Moyenne	**3.4** **3.2**	**5.2** **5.3** **6.4.1.1** **3.1.4** **3.1.1** **3.1.2** **3.2.1** **3.2.2**
			Disponibilité	Forte	**3.1** **6.3**	**5.2** **5.3** **6.2.2** **6.2.3** **6.2.4.1** **6.2.4.2** **6.2.5** **6.4.2.2.2** **5.1**
			Confidentialité	Moyenne	**6.5**	**6.2.5** **6.4.2.4.1** **6.4.2.3.2** **6.4.2.1.1.1** **2.3.1** **2.3.2** **2.3.3** **2.3.4** **4.1.1** **6.1.1** **6.3** **6.4.2.1.1**
3	Matériel	Ressources	Disponibilité	Moyenne	**3.2**	**3.1.4** **3.1.1** **3.1.2** **3.2.1** **3.2.2** **3.2.4**
4	Matériel	Ressources	Disponibilité	Moyenne	**3.2**	**3.1.4** **3.1.1** **3.1.2** **3.2.1** **3.2.2** **3.2.4**
5	Matériel	Ressources	Disponibilité	Moyenne	**3.2**	**3.1.4** **3.1.1** **3.1.2** **3.2.1** **3.2.2** **3.2.4**

6	Structure Organisation nelle	Contexte externe	Confidentialité	Forte	**1.1.2** **9.1** **9.2**	**6.4.1.1** **6.2.2** **6.2.3** **6.2.5** **6.4.2.4.1** **6.4.2.1.1.1** **1** **4.3** **6.4.1.2.2** **4.4** **2.2** **6.4.2.1.1** **6.4.2.1.2**
7	Réseau	Ressources	Confidentialité	Forte	**6.5.1**	**6.2.5** **6.4.2.4.1** **6.4.2.3.2** **6.4.2.1.1.1** **2.3.3** **4.1.1** **6.1.1** **6.3** **6.4.2.1.1**
	Réseau	Ressources	Intégrité	Forte	**6.5.7**	**6.2.5** **6.4.2.4.1** **6.4.2.3.2** **6.4.2.1.1.1** **2.3.2** **4.1.1** **6.1.1** **6.3** **6.4.2.1.1**
	Réseau	Ressources	Disponibilité	Forte	**6.5.2**	**6.2.5** **6.4.2.4.1** **6.4.2.3.2** **6.4.2.1.1.1** **2.3.1** **4.1.1** **6.1.1** **6.3** **6.4.2.1.1**
8	Software	Site	Confidentialité	Forte	**6.5** **1.1.2** **8.1.3.3**	**5.2** **5.3** **6.4.1.1** **6.2.5** **5.1** **6.4.2.4.1** **6.4.2.3.2** **6.4.2.1.1.1** **1** **6.1.3** **2.3.1** **2.3.2** **2.3.3** **2.3.4**

						4.1.1 **6.4.1.2.2** **6.1.1** **6.3** **6.4.2.1.1** **6.4.2.1.2**
9	Matériel	Site	Confidentialité	Forte	**6.5** **1.1.2**	**6.4.1.1** **6.2.5** **6.4.2.4.1** **6.4.2.3.2** **6.4.2.1.1.1** **1** **2.3.1** **2.3.2** **2.3.3** **2.3.4** **4.1.1** **6.4.1.2.2** **6.1.1** **6.3** **6.4.2.1.1** **6.4.2.1.2**
10	Application	Ressources	Confidentialité	Moyenne	**6.5.1** **5.3**	**5.3** **6.2.5** **6.4.2.4.1** **6.4.2.1.1.1** **2.3.3** **4.1.1** **6.1.1** **6.3** **6.4.2.1.1**
11	Application	Gouvernance	Confidentialité	Forte	**6.5.1** **8.1** **8.4**	**5.3** **6.2.5** **6.4.2.4.1** **6.4.2.3.2** **6.4.2.1.1.1** **6.1.3** **2.3.3** **4.3** **4.1.1** **6.4.1.2.2** **6.1.1** **6.1.2** **6.3** **6.4.2.1.2**
12	Personnel	Système d'information	Intégrité	Moyenne	**5.2** **8.1.2** **5.4**	**5.3** **6.4.2.4.1** **6.4.2.1.1.1** **6.4.1.2.2** **6.4.2.1.1** **6.4.2.1.2**
13	Actif support (Technique)	Ressources	Intégrité	Forte	**9.2** **6.5.7** **5.3** **7** **4.2**	**5.3** **6.4.1.1** **6.2.5** **6.4.2.4.1** **6.4.2.3.2** **6.4.2.1.1.1** **1** **2.3.2**

						4.1.1 **6.4.1.2.2** **6.1.1** **6.3** **6.4.2.1.1** **6.4.2.1.2**
	Actif support (Technique)	Ressources	Disponibilité	Forte	**9.2** **5.1** **4.2**	**6.4.1.1** **6.2.5** **6.4.2.4.1** **6.4.2.3.2** **6.4.2.1.1.1** **1** **2.3.1** **4.1.1** **6.4.1.2.2** **6.1.1** **6.3** **6.4.2.1.1** **6.4.2.1.2**
	Actif support (Technique)	Ressources	Confidentialité	Forte	**9.2** **6.5.1** **4.2**	**6.4.1.1** **6.2.5** **6.4.2.4.1** **6.4.2.3.2** **6.4.2.1.1.1** **1** **2.3.3** **4.1.1** **6.4.1.2.2** **6.1.1** **6.3** **6.4.2.1.1** **6.4.2.1.2**
14	Application	Ressources	Intégrité	Forte	**9.1** **6.5.7** **5.3** **4.1**	**5.3** **6.4.1.1** **6.2.5** **6.4.2.4.1** **6.4.2.3.2** **6.4.2.1.1.1** **1** **2.3.2** **4.3** **4.1.1** **6.4.1.2.2** **4.4** **2.1** **2.2** **6.1.1** **6.3** **6.4.2.1.1** **6.4.2.1.2**
	Application	Ressources	Disponibilité	Forte	**9.1** **4.1**	**5.3** **6.4.1.1** **6.2.5** **6.4.2.4.1** **6.4.2.3.2** **6.4.2.1.1.1** **1** **2.3.1**

						4.3 **4.1.1** **6.4.1.2.2** **4.4** **2.1** **2.2** **6.1.1** **6.3** **6.4.2.1.1** **6.4.2.1.2**
	Application	Ressources	Confidentialité	Forte	**9.1** **6.5.1** **4.1**	**6.4.1.1** **6.2.5** **6.4.2.4.1** **6.4.2.3.2** **6.4.2.1.1.1** **1** **2.3.3** **4.1.1** **6.4.1.2.2** **2.1** **6.1.1** **6.3** **6.4.2.1.1** **6.4.2.1.2**
15	Matériel	Système d'information	Disponibilité	Forte	**6.3** **10.2**	**5.2** **5.3** **6.2.5** **5.1** **6.4.2.4.1** **6.4.2.3.2** **6.4.2.1.1.1** **1** **6.1.3** **2.3.1** **4.1.1** **6.4.2.2.1** **6.1.1** **6.3** **6.4.2.1.1**
16	Actif support (Technique)	Capabilité	Disponibilité	Forte	**9.1** **7** **10.2** **8.2.2**	**5.2** **5.1** **6.4.2.4.1** **6.4.2.1.1.1** **4.3** **4.4** **2.2** **6.4.2.1.1**
17	Application	Pratique	Disponibilité	Forte	**8.2.3** **8.2.1** **2**	**3.1.1** **3.1.2** **1** **3.1.3** **6.1.1** **6.1.2**
18	Application	Gouvernance	Disponibilité	Moyenne	**8.2.2** **10**	**5.2** **5.3** **3.1.1** **3.1.2** **6.4.2.4.1** **6.4.2.3.2**

						6.4.2.1.1.1 **1** **6.4.2.2.1** **3.1.3** **6.1.1** **6.1.2** **6.4.2.1.1**
19	Matériel	Politique interne	Confidentialité	Forte	**9.1** **6.5.1** **1.1** **7.2**	**6.4.1.1** **6.2.5** **6.4.2.4.1** **6.4.2.1.1.1** **1** **2.3.3** **4.3** **4.1.1** **6.4.1.2.2** **4.4** **2.2** **6.1.1** **6.3** **6.4.2.1.1** **6.4.2.1.2**
	Réseau	Politique interne	Confidentialité	Forte	**9.1** **6.5.1** **1.1** **7.2**	**6.4.1.1** **6.2.5** **6.4.2.4.1** **6.4.2.1.1.1** **1** **2.3.3** **4.3** **4.1.1** **6.4.1.2.2** **4.4** **2.2** **6.1.1** **6.3** **6.4.2.1.1** **6.4.2.1.2**
20	Application	Capabilité	Confidentialité	Moyenne	**3.4** **6.5.1** **5.3** **7**	**5.2** **5.3** **6.2.5** **6.4.1.1** **5.1** **6.4.2.4.1** **6.4.2.1.1.1** **2.3.3** **4.1.1** **4.2** **6.1.1** **6.3** **6.4.2.1.1**
21	Application	Politique interne	Traçabilité	Moyenne	**6.5.4** **7**	**5.2** **6.2.5** **5.1** **6.4.2.4.1** **6.4.2.3.2** **6.4.2.1.1.1** **2.3.4** **4.1.1** **4.2** **6.1.1**

						6.3 **6.4.2.1.1**
22	Actif support (Technique)	Ressources	Intégrité	Forte	**6.5.7** **5.3** **7** **4.2**	**5.2** **5.3** **6.2.5** **5.1** **6.4.2.4.1** **6.4.2.3.2** **6.4.2.1.1.1** **2.3.2** **4.1.1** **4.2** **6.1.1** **6.3** **6.4.2.1.1**
23	Application	Contexte externe	Confidentialité	Forte	**6.5.1** **5.3** **7**	**5.2** **5.3** **6.2.5** **6.2.5** **5.1** **6.4.2.4.1** **6.4.2.3.2** **6.4.2.1.1.1** **2.3.3** **4.1.1** **4.2** **6.1.1** **6.3** **6.4.2.1.1**
		Politique interne	Confidentialité	Forte	**6.5.1** **5.3** **7**	**5.2** **5.3** **6.2.5** **6.4.2.4.1** **6.4.2.3.2** **6.4.2.1.1.1** **2.3.3** **4.1.1** **4.2** **6.1.1** **6.3**
24	Actif support (Technique)	Contexte interne	Intégrité	Moyenne	**8.1** **8.4** **8.2** **8.3**	**5.3** **6.4.2.1.1.1** **6.1.3** **4.3** **6.4.1.2.2** **6.1.2** **6.4.2.1.1** **6.4.2.1.2**
	Actif support (Technique)	Contexte interne	Disponibilité	Moyenne	**8.1** **8.4** **8.2** **8.3**	**5.3** **6.4.2.1.1.1** **6.1.3** **4.3** **6.4.1.2.2** **6.1.2** **6.4.2.1.2**
25	Actif support (Technique)	Politique interne	Confidentialité	Forte	**6.5.1** **7** **5**	**5.2** **6.2.5** **6.4.2.4.1** **6.4.2.3.2**

						6.4.2.1.1.1 **2.3.3** **4.1.1** **4.2** **6.1.1** **6.3** **6.4.2.1.1**
26	Actif support	Capabilité	Confidentialité	Forte	**9.1** **6.5.1** **7** **10.2**	**5.2** **6.2.5** **6.4.2.4.1** **6.4.2.1.1.1** **2.3.3** **4.3** **4.1.1** **4.4** **2.2** **4.2** **6.1.1** **6.3** **6.4.2.1.1**
27	Application	Ressources	Confidentialité	Moyenne	**6.5.1** **5.3** **7** **4.1**	**5.2** **5.3** **6.2.5** **6.4.2.4.1** **6.4.2.3.2** **6.4.2.1.1.1** **1** **2.3.3** **4.1.1** **2.1** **4.2** **6.1.1** **6.3** **6.4.2.1.1**
28	Personnel	Gouvernance	Disponibilité	Moyenne	**6.5.2** **7.2**	**6.2.5** **6.4.2.4.1** **6.4.2.3.2** **6.4.2.1.1.1** **2.3.1** **4.1.1** **6.1.1** **6.3** **6.4.2.1.1**

le cnam

Nabil LAOUFI

Processus guidé pour l'identification des exigences de sécurité à partir de l'analyse des risques

Résumé : Toute organisation est activée par un flux physique continu et un flux décisionnel qui opèrent de symbiose pour atteindre des objectifs déterminés. Ce qui engendre l'implantation d'un système d'information fiable, opérant avec un contrôle continu et une sécurité maximale, prenant en compte le contexte interne et externe pour garder son rôle opérationnel et stratégique. Compte tenu du niveau d'exposition aux risques et de la dépendance vitale des entreprises vis-à-vis de leurs systèmes d'information, il est crucial de prêter attention aux exigences de sécurité. La réalisation d'un équilibre entre la sécurité et l'efficacité du système d'information est une tâche complexe qui exige au préalable une analyse approfondie du contexte organisationnel. Elle nécessite également l'identification, l'analyse, et la gestion des risques encourus par l'entreprise. Elle nécessite aussi la détermination des exigences de sécurité. Peu d'approches offrent un guidage permettant de dériver les exigences de sécurité à partir des risques encourus. Le but de cette thèse est de concevoir un mécanisme de guidage suggestif qui permet de dériver les exigences de sécurité à partir de l'analyse des risques. Nous proposons, pour cela, une approche fondée sur les ontologies et un ensemble de règles de correspondance. A cette fin, nous proposons le développement de quatre ontologies et un processus d'alignement entre celles-ci en utilisant des relations sémantiques cohérentes. Le processus de validation se fonde sur une étude de cas et un prototype.

Mots clés : Actifs, Contexte, Risques, Menaces, Vulnérabilités, Traitements de risques, Exigences de sécurité, Analyse des risques, Règles de correspondance, Ontologies.

Résumé en anglais : Any organization is enabled by continuous physical flow and decision flow from operating symbiosis to achieve specific objectives. Which generates the implementation of a reliable information system, operating with a continuous control and maximum security, taking in to account the internal and external environment to maintain its operational and strategic role. Given the level of risk exposure and the vital dependence of companies on their information systems, it is crucial to pay attention to security requirements. Achieving a balance between the security and effectiveness of the information system is a complex task requiring an in-depth analysis of the organizational context. It also requires the identification, analysis, and management of the risks incurred by the company. It also requires the determination of security requirements. Few approaches offer guidance to derive security requirements from the risks involved. The aim of this thesis is to design a suggestive guiding mechanism that allows to derive the security requirements from the risk analysis. We propose an approach based on ontologies and a set of correspondence rules. To achieve, we propose the development of four ontologies and an alignment process between then using consistent semantic relationships. The validation process is based on a case study and a prototype.

Keywords : Assets, Contexts, Risks, Threats, Vulnerabilities, Risks treatments, Security requirements, Risks analysis, Correspondance rules, Ontologies.