Gouvernance de la sécurité : comment articuler les différentes normes et méthodes?

Publication des résultats par un wiki afin d'en assurer le suivi

Travail de Bachelor réalisé en vue de l'obtention du Bachelor HES

par :

Alexandre STEIGMEIER

Conseiller au travail de Bachelor :

(Rolf HAURI, chargé d'enseignement)

Carouge, le 6 novembre 2009

Haute École de Gestion de Genève (HEG-GE)

Filière Informatique de Gestion

Déclaration

Ce travail de Bachelor est réalisé dans le cadre de l'examen final de la Haute école de gestion de Genève, en vue de l'obtention du titre (…). L'étudiant accepte, le cas échéant, la clause de confidentialité. L'utilisation des conclusions et recommandations formulées dans le travail de Bachelor, sans préjuger de leur valeur, n'engage ni la responsabilité de l'auteur, ni celle du conseiller au travail de Bachelor, du juré et de la HEG.

« J'atteste avoir réalisé seul(e) le présent travail, sans avoir utilisé des sources autres que celles citées dans la bibliographie. »

Fait à Carouge, le 6 novembre 2009

Alexandre STEIGMEIER

……..

Remerciements

Je tiens tout d'abord à remercier M. Rolf HAURI pour son accompagnement tout au long de ce projet. C'est également lui qui m'a proposé ce sujet et je lui en suis reconnaissant.

Merci également aux relecteurs de ce travail d'avoir pris le temps de corriger les erreurs qu'il subsistait.

Je remercie aussi toutes les personnes qui ont participé de près ou de loin à la réalisation et au succès de ce travail.

Sommaire

Ce travail de Bachelor a pour but d'imaginer et de publier une représentation de l'articulation de normes et méthodes à propos de la sécurité des systèmes d'information. Il y est donc expliqué ce que sont la gouvernance d'entreprise, l'application de normes et de méthodes.

Il y est ensuite fait une description de la méthodologie de recherche, afin de définir le contexte, le cadre, et les outils employés dans le but de mener à bien ce mandat. Cette méthodologie explique également comment ce travail sera publié et suivi à l'avenir.

Puis vient le point clé de ce travail, l'articulation des normes, méthodes et même de quelques lois concernant la gestion de la sécurité de l'information. Un certain nombre de ces outils a été retenu, expliqué, puis ils ont été confrontés entre eux. Afin de garantir une vision la plus complète possible, deux schémas ont été imaginés. Le premier se basant sur le découpage de l'entreprise en trois systèmes : le système opérant, le système d'information, et tout en haut le système de pilotage. Grâce à l'analyse des normes et des méthodes, nous avons pu placer ces outils sur ledit schéma, afin de définir le type de destinataire au sein de l'entreprise. S'agit-il plutôt de directeurs ou de techniciens ? L'analyse suivante est-elle plutôt basée sur le niveau de maturité de l'entreprise ? En se basant sur le modèle de développement à cinq niveaux CMMI, ainsi que sur l'approche de M. C. MAURY du CLUSIS, nous avons établi notre propre échelle d'évaluation du niveau de maturité de l'entreprise. Nous avons donc pu à nouveau placer les divers outils retenus pour la gestion de la sécurité de l'information sur ce schéma afin d'en tirer des conclusions sur le type d'entreprise concernée par telle ou telle norme, ou méthode.

Afin de valoriser ce travail et de le rendre accessible au plus grand nombre, il a été décidé de le publier sur Internet au moyen d'un wiki. Cet outil de gestion de contenu a donc été mis en place après avoir comparé les diverses possibilités pour ce faire. Il sera finalement décidé de mettre en place le wiki « MediaWiki », connu pour être le support de la célèbre encyclopédie en ligne Wikipédia. Il a donc fallu tour à tour installer le système, le paramétrer, puis le remplir des articles concernant les normes, méthodes et lois de la gouvernance de la sécurité des systèmes d'information.

Table des matières

Liste des Tableaux

Liste des Figures

Introduction

Aujourd'hui, le monde de la sécurité de l'information joue un rôle capital dans la stratégie de l'entreprise. Depuis le début de la crise, beaucoup de choses ont changé, tant au niveau des mentalités que des ressources techniques et humaines engagées dans la sécurité par les entreprises, comme le démontre une étude CA[1].

Il est toutefois difficilement concevable à l'heure actuelle d'imaginer mettre en place des règles et des instruments destinés à assurer la sécurité de l'information sans se baser sur des outils spécifiquement conçus et imaginés à cet effet, tant les systèmes et leurs interactions sont devenus complexes. Il est aujourd'hui acquis qu'une entreprise se doit de considérer sa structure de manière systémique, et chaque secteur indépendamment. C'est là qu'interviennent les normes et les méthodes, véritables salvatrices des responsables de la sécurité des systèmes d'information.

Mais quelles sont-elles réellement ? Dans quel cadre et comment les utiliser ? Sont-elles toutes nécessaires ? Peut-on les classer ou les dissocier les unes des autres ? Il existe une multitude de solutions, d'origines diverses. Certaines sont publiées par des états, d'autres par des fournisseurs de services, d'autres encore sont directement issues de l'histoire et son évolution. Et c'est là un point important, car tous ces outils ne cessent d'évoluer, de s'adapter au contexte économique, social et politique du milieu auquel ils sont destinés. Comment s'orienter dans la jungle de solutions à disposition ? Et finalement, comment avoir une vue d'ensemble de ces règles ou recommandations, afin d'en faciliter l'appréhension et le choix ? Que sont-elles, à qui sont-elles destinées, et qu'est-ce qui les distingue ?

Il s'agira ensuite de les articuler entre elles, afin de répondre à ces deux questions : à qui sont-elles destinées, et à quel niveau de maturité l'entreprise qui tente de les mettre en place doit-elle se situer ?

Finalement, il sera question de publier ce rapport sur Internet, et trouver un système adéquat afin de garantir son suivi.

[1] Source : http://tinyurl.com/y87xmff - L'étude démontre que « 42% des entreprises prévoient d'augmenter leurs dépenses en sécurité informatique »

1. Normes, méthodes et gouvernance

Que sont les normes, les méthodes et la gouvernance ? Ces termes à la mode sont aujourd'hui dans la plupart des discussions de travail, mais que signifient-ils ? Voici un bref rappel de leur signification et en particulier dans le contexte de la sécurité de l'information.

1.1 Normes

L'ISO[2] et le CEI[3] donnent la définition suivante :

> *« Document établi par consensus et approuvé par un organisme reconnu, qui fournit, pour des usages communs et répétés, des règles, des lignes directrices ou des caractéristiques, pour des activités ou leurs résultats garantissant un niveau d'ordre optimal dans un contexte donné. »*
>
> *Il existe quatre types de normes :*
>
> 1. *Les normes fondamentales : elles donnent les règles en matière de terminologie, sigles, symboles, métrologie.*
> 2. *Les normes de spécifications : elles indiquent les caractéristiques, les seuils de performance d'un produit ou d'un service.*
> 3. *Les normes d'analyse et d'essais : elles indiquent les méthodes et moyens pour la réalisation d'un essai sur un produit.*
> 4. *Les normes d'organisation : elles décrivent les fonctions et les relations organisationnelles à l'intérieur d'une entité*
>
> Wikipédia - http://fr.wikipedia.org/wiki/Normes_et_standards_industriels

1.2 Méthodes

> *« Une méthode de travail est une marche à suivre pour réussir, ou, en abordant le travail sous un autre angle, elle est l'approche d'un problème.»*
>
> Wikipédia - http://fr.wikipedia.org/wiki/Méthode_de_travail

---

[2] ISO – *Organisation International de Normalisation*, a élaboré plus de 17'500 normes. Il publie également plus de 1100 normes chaque année. - http://www.iso.org/iso/fr/iso_catalogue

[3] CEI – *Commission électrotechnique internationale* est l'organisation internationale de normalisation chargée des domaines de l'électricité, de l'électronique et des techniques connexes. Elle est complémentaire de l'Organisation internationale de normalisation (ISO), qui est chargée des autres domaines. - Wikipédia

Les méthodes sont également des référentiels communs documentés. Ce sont des méthodes de travail, permettant de guider l'utilisateur de A à Z. Il s'agit de marches à suivre sur l'implantation d'un objectif défini, comme une politique de sécurité, par exemple.

1.3 Gouvernance

> ***« Etymologie** : de l'anglais, governance, gouvernement, venant du latin "gubernare", diriger un navire. »*

On peut donc facilement faire le rapprochement entre le navire et l'entreprise. Il s'agit en effet, tout comme le navire, de l'action de diriger, mais cette fois il est question d'une entreprise. Au niveau du système d'information, elle est définie par l'AFAI[4] de la façon suivante :

> *« Le terme IT Governance est devenu très "à la mode", mais rares sont les personnes, qui mettent le même contenu derrière ce label. Pour les uns, il s'agit principalement de conformité aux dispositions légales en matière de contrôle interne, notamment dans le contexte de lois, pour d'autres, il s'agit d'un ensemble de "bonnes pratiques" visant à mettre réellement l'informatique au service de la stratégie de l'entreprise et de ses objectifs de création de valeur.*
>
> *Pour répondre à cette question, l'IGSI[5] et l'IT Governance Institute proposent une définition équilibrant les aspects "compliance" et les aspects "performance", qui font tous les deux partie du concept de Gouvernance.»*

La gouvernance désigne donc à la fois la gestion et la politique à mettre en œuvre afin de parvenir à satisfaire les objectifs globaux d'une entreprise. Il s'agit là d'un terme générique, se déclinant parfois en « gouvernance politique » (dans un cadre plutôt étatique), et également connu sous la forme de « gouvernance d'entreprise ».

Une autre approche de la gouvernance est donnée pas le CIGREF[6] qui préfère, lui, donner une vision plus graphique en représentant la gouvernance par ses processus clés.

---

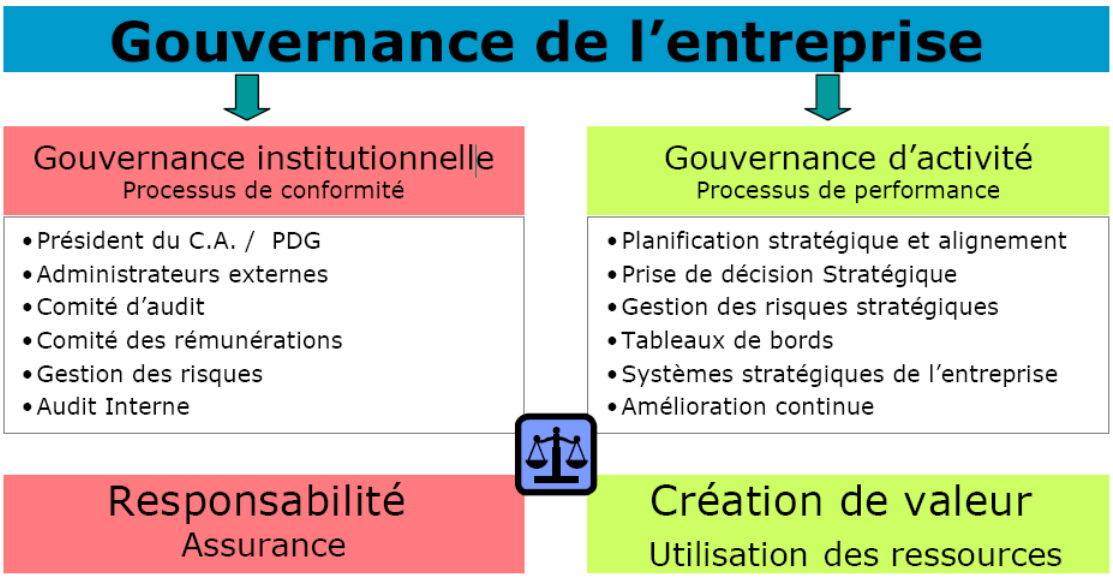
[4] L'AFAI - *Association Française de l'Audit et du Conseil Informatiques* - est le chapitre français de l'ISACA (cf. p. 12) et compte environ 600 membres.

[5] IGSI - La société IGSI est une société de services (S.S.I.I.) spécialisée dans l'infrastructure informatique, l'informatique de gestion et la communication. - http://www.igsi.fr/

[6] CIGREF - Le CIGREF, Club informatique des grandes entreprises françaises, a été créé en 1970. Il regroupe plus de cent très grandes entreprises et organismes français et européens de tous les secteurs d'activité (banque, assurance, énergie, distribution, industrie, services...).

Voici la représentation de la gouvernance par le CIGREF :

Figure 1 - Représentation de la gouvernance par le CIGREF



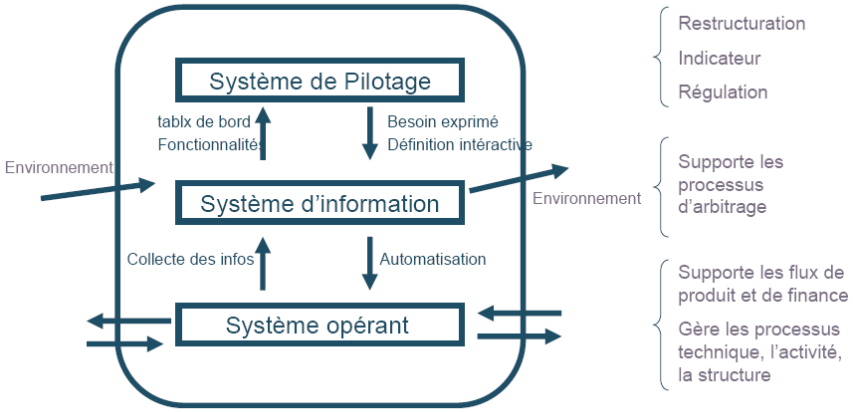
Source : adapté depuis CIMA

Trois dimensions peuvent alors être retenues des visions précédentes pour caractériser la gouvernance :

1. La **conformité** : L'entreprise doit suivre les règles et les lois en vigueur.
2. La **performance** : L'entreprise doit, dans son ensemble, être créatrice de valeur.
3. La **gestion des risques** : Une entreprise se doit de considérer les risques liés à son exploitation.

Afin de mieux situer la gouvernance au sein de l'entreprise, il peut être intéressant de la découper en trois systèmes de la manière suivante :

Figure 2 - Modèle O.I.D[7]



Au bas du modèle, se trouve le **système opérant**. C'est lui qui est chargé de créer ce que l'entreprise vend. C'est le secteur de production qui gère les processus techniques. Il est donc là pour mettre en place les solutions de sécurité, au niveau des procédés.

Au-dessus, se trouve le **système d'information**, qui est chargé de faire appliquer les décisions prises par le *système de pilotage*, afin que ces dernières soient prises en compte par le *système opérant*.

Et finalement, au sommet de l'architecture, se trouve le **système de pilotage**. Il est constitué de la direction générale. C'est lui qui est responsable de la prise de décision pour l'entreprise, et fixe les objectifs stratégiques.

C'est dans cette optique que la gouvernance des systèmes d'information s'articule. Il s'agit en effet d'assurer la conformité de l'entreprise avec les lois en vigueur dans sa création de valeur, tout en gérant les risques liés à cette exploitation. Ainsi, les décisions importantes sur l'orientation de la sécurité du système d'information peuvent se prendre en connaissance des objectifs globaux ainsi que de l'environnement et ses changements dans lequel l'entreprise évolue.

[7] Modèle OID – Le modèle *Opérant, Information, Décision* a été au tout début des années 80 adopté par la communauté des S.I. automatisés, et apparaissait dans les principes fondateurs des principales méthodes d'analyse développées alors.

2. Méthodologie de recherche

Comme tout travail de recherche, celui-ci nécessite un cadre, une structure afin d'en limiter l'étendue. Le monde de la sécurité de l'information, l'implantation de normes et le respect de méthodes de travail sont des univers très larges et il est donc primordial de déterminer clairement les sujets qui devront être traités, de ceux qui ne devront pas l'être. Ainsi, il a été logiquement décidé de traiter des normes et méthodes concernant la sécurité de l'information, et de ce contexte-ci uniquement. Il est facile, dans la jungle des normes notamment, de se laisser dériver vers d'autres sujets connexes, parfois à la frontière des deux mondes, tel que l'implantation et le suivi de processus qualité (par exemple la norme ISO 9001[8]). Ces sujets ne seront par conséquent pas traités ici, bien que leur rattachement à la gouvernance puisse bien sûr se justifier.

Une fois que le cadre de travail est fixé, il faut recueillir un panel le plus exhaustif possible, ou du moins le plus représentatif des outils de gestion de la sécurité de l'information. La première source d'information est bien évidemment Internet, avec ses milliers d'articles sur le sujet. Rien que Google, sur la requête « Sécurité de l'information », renvoie plus de 14'600'000 articles (le 30.10.2009). Il est donc clairement visible que le sujet concerne, passionne même, un grand nombre d'internautes. Afin de filtrer cette impressionnante quantité de données, et de mieux cadrer les recherches, une autre source importante vient se greffer à Google : le contenu des cours et des modules du MBA-ISSG[9]. Cette formation européenne de la gouvernance de la sécurité des systèmes d'information dispense en effet des cours dont le sujet est en relation directe avec la matière qui nous concerne ici. Il est donc logique que cette source soit également employée, par l'intermédiaire de M. Rolf HAURI, directeur adjoint du programme de ladite formation, et conseiller du présent travail.

[8] La norme ISO 9001 « spécifie les exigences relatives au système de management de la qualité », selon l'ISO – http://www.iso.org/

[9] MBA-ISSG : *Master of Business Administration-Information System Security Governance*

Suite aux recherches effectuées, un panel de normes et de méthodes a été défini. Il regroupe l'ensemble des solutions majeures utilisées pour les entreprises. Voici les éléments retenus (par ordre alphabétique) :

- Bâle II
- CobiT
- COSO
- EBIOS
- ISO 27000
- ISO 27001
- ISO 27002
- ISO 27005
- ISO 27006
- ITIL
- Mehari
- OCTAVE
- Risk IT
- SOX / C-SOX
- Val IT

Une fois ces données rassemblées, il convient de les confronter entre elles, comme le titre de ce travail le laisse entendre. Mais comment définir une articulation de normes et méthodes sur des sujets aussi complexes que variés que la gouvernance de la sécurité de l'information ? Il a fallu imaginer des outils capables de représenter les usages prévus par ces outils, des usagers auxquels ils s'adressent, et finalement quels sont leurs liens, leurs dépendances.

Il va de soi que ces outils ne cessent d'évoluer. Il est commun de dire que les systèmes d'information évoluent vite aujourd'hui, ce qui rend le contexte de ces outils extrêmement volatile. Afin de valoriser ce travail, et surtout de pouvoir l'adapter aux rapides changements auxquels il est sujet, il faut imaginer une solution dynamique pour sa publication, de manière à pouvoir le maintenir à jour au fil du temps et des évolutions.

3. Articulation des normes et méthodes

Afin de comprendre comment ces outils peuvent s'articuler entre eux, quels sont leurs liens, et à qui ils sont destinés, nous allons les présenter sur deux graphiques, représentant à tour de rôle l'entreprise et ses 3 systèmes (cf. page 5), puis leur implantation en fonction du niveau de maturité de l'entreprise.

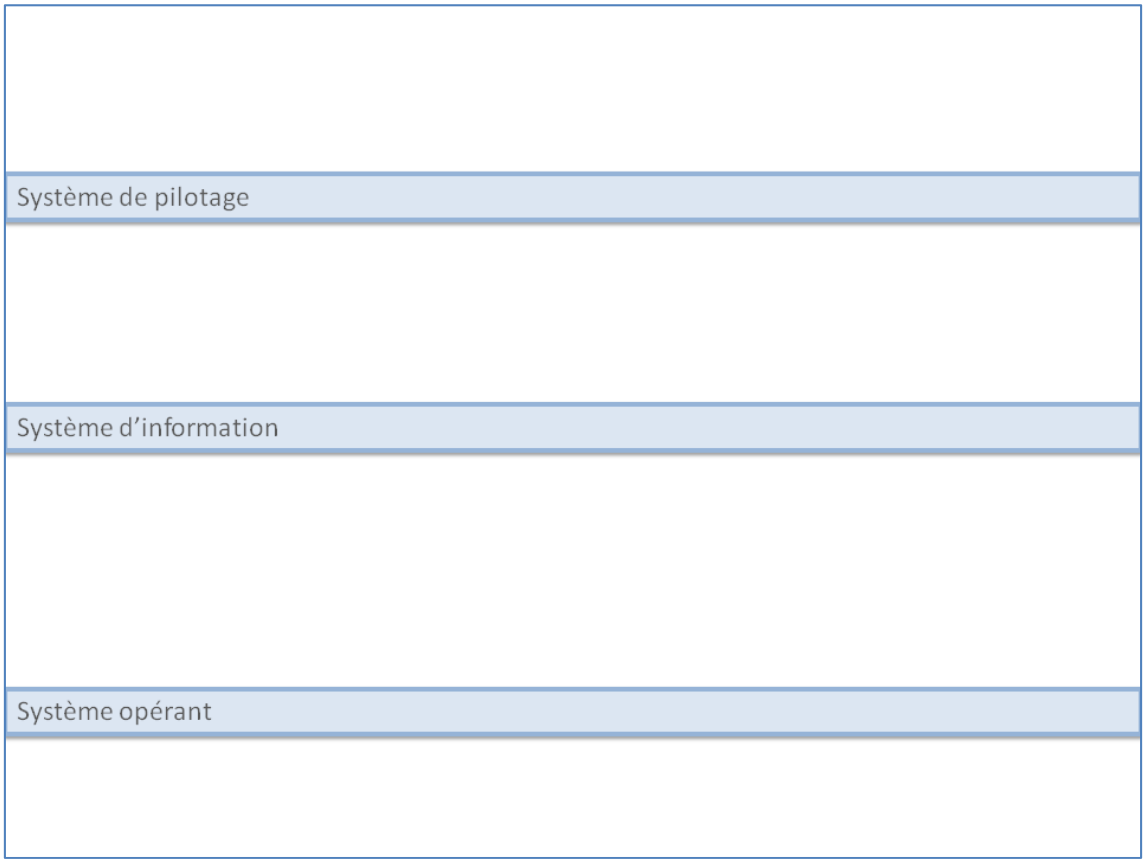
3.1 L'entreprise et ses 3 systèmes

Comme vu précédemment, l'entreprise peut être divisée en 3 grands systèmes :

1. Le système de pilotage
2. Le système d'information
3. Le système opérationnel

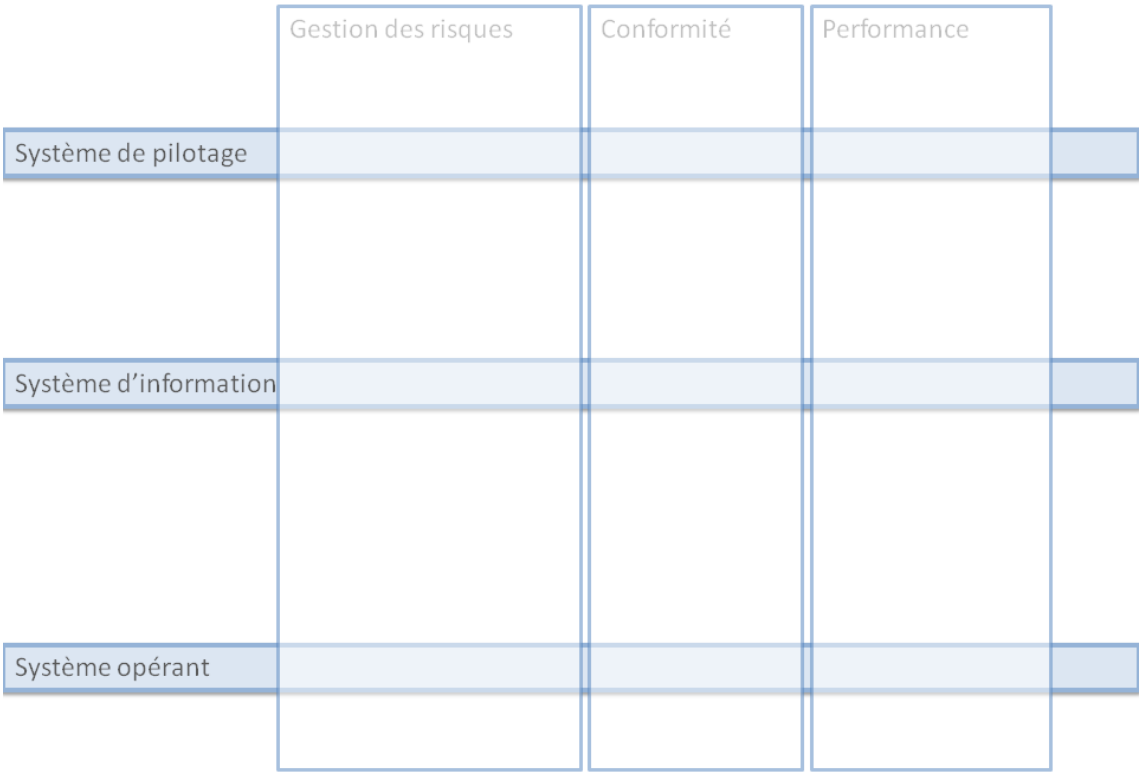
Ainsi, nous pouvons fixer le cadre de notre premier schéma de la manière suivante :

Figure 3 - Cadre de travail : les 3 systèmes de l'entreprise



Afin de placer judicieusement les outils d'aide à la gestion de la gouvernance de la sécurité de l'information, nous reprendrons ici les trois points de la gouvernance vus précédemment :

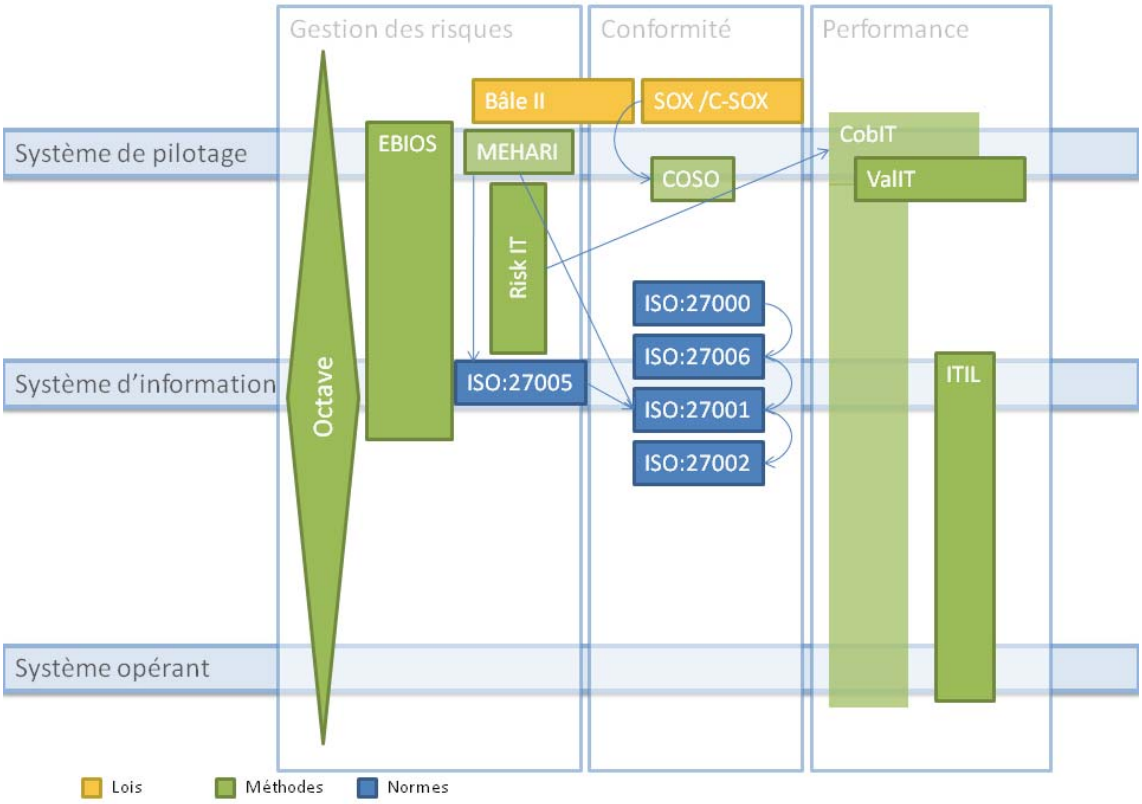
Figure 4 - Intégration des 3 dimensions de la gouvernance



On aperçoit de cette manière comment le panorama des normes et méthodes va être réparti, et à qui elles s'adressent. Nous aurons donc le choix entre les trois systèmes de l'entreprise, opérant, information et pilotage, puis entre les trois dimensions de la gouvernance, la gestion des risques, la conformité, et la performance. Il est possible que des outils se placent entre deux systèmes (voire même englobent les trois) ou entre deux dimensions.

Une fois le cadre de travail posé, il nous est maintenant possible de répartir les outils comme suit :

Figure 5 - Articulation des normes en méthodes au sein de l'entreprise



Bien sûr, un schéma tel que celui-ci (Figure 5) nécessite quelques explications.

Tout d'abord les couleurs. Chaque couleur fait référence à un type d'outil :

- En jaune : les lois
- En vert : les méthodes
- En bleu : les normes

Cela fournit une identification visuelle directe. Il est donc plus aisé de différencier les normes des méthodes.

3.1.1 Outils de gestion des risques

OCTAVE : Cette méthode concerne tous les secteurs de l'entreprise, de par son contenu même. En effet, elle fournit une approche tant **opérante** qu'**informationnelle**, en relation directe avec le *système de pilotage* et sa direction générale, selon Wikipédia :

« La méthodologie comprend trois phases principales :

- *Vue **organisationnelle** : création des profils de menaces sur les biens de l'entreprise ;*
- *Vue **technique** : Identification des vulnérabilités d'infrastructure ;*
- *Développement de la **stratégie** : analyse de risques, mise en place des mesures de sécurité. »*

Elle est basée sur la participation de tous les acteurs de l'entreprise afin de pouvoir identifier les actifs de l'entreprise, identifier les risques potentiels, et ainsi définir les stratégies à entreprendre afin d'en limiter les effets, ou leurs probabilités. Elle est néanmoins plus présente au niveau du *système d'information*, puisque c'est ce dernier qui sera chargé de rassembler les données relatives aux risques et à leur traitement.

EBIOS : Concernant EBIOS, les sources divergent en fonction du niveau auquel la méthode doit être implémentée. Pour la DCSSI[10], l'éditeur de la méthode, celle-ci est principalement orientée pour une utilisation au niveau du *système de pilotage*, dû au caractère générique de son contenu, alors que pour d'autres, comme la société Ysosecure[11], il s'agit clairement d'idées et de concepts définis, fournissant ainsi un cadre de travail correspondant au *système opérant*.

« Les concepts et les idées exposés sont clairement exprimés »

Ysosecure, à propos d'EBIOS

[10] DCSSI – *Direction Centrale de la Sécurité des Systèmes d'Information* jusqu'au 7 juillet 2009, puis ANSSI, *Agence Nationale de la SSI*. Défini par Wikipédia comme « l'organisme interministériel officiel définissant les normes de la sécurité des systèmes d'information » - http://fr.wikipedia.org/wiki/DCSSI

[11] Ysosecure est un cabinet de conseil spécialisée dans le domaine de la sécurité de l'information. - http://www.ysosecure.com/methode-securite/methode-ebios.asp

MEHARI : Le CLUSIF[12], l'éditeur de la méthode, définit cette dernière de la façon suivante :

« Mehari est développé […] pour aider les décideurs (responsables de la sécurité, gestionnaires de risques et dirigeants) à gérer la sécurité de l'information et à minimiser les risques associés. »

Il y est donc clairement fait mention du *système de pilotage*. Mehari respecte en outre certains principes de normes ISO tels que la norme ISO 27005 en gestion des risques, ou la norme ISO 27001 qui décrit les exigences pour la mise en place d'un SMSI[13].

Risk IT : La méthode Risk IT, élaborée tout comme CobiT et Val IT[14] par l'ISACA[15], repose sur le référentiel CobiT, dont il complète et précise la définition, en ce qui concerne les risques. Risk IT est composé de 9 processus, répartis en 3 phases. La première phase, nommée « Gouvernance des risques », s'adresse directement au *système de pilotage*, car il y est question de faire coïncider la gestion des risques à la vision stratégique de l'entreprise. La seconde phase, « Évaluation des risques », ainsi que la troisième, « Réponse aux risques » sont, quant à elles, plutôt orientées pour le *système d'information*, étant donné qu'il s'agit de prendre des décisions non pas pour l'ensemble des objectifs de la société, mais bien pour chaque secteur.

Bâle II : Il s'agit là d'une loi destinée à améliorer l'appréhension du risque bancaire et majoritairement le risque du crédit. Il est donc naturel de la placer à la fois dans la gestion des risques, et dans la gestion de la conformité, de par son statut de loi. Ce dernier la place également au niveau du *système de pilotage*, puisqu'il s'agit là de l'organe de décision de l'entreprise, qui doit notamment se référer aux lois en vigueurs.

---

[12] Le CLUSIF - *Club de la Sécurité de l'Information Français* - est un club professionnel, constitué en association indépendante, agissant pour la sécurité de l'information.

[13] SMSI – *Système de Management de la Sécurité de l'Information*

[14] Cf. page 14

[15] L' ISACA - *Information Systems Audit and Control Association* – est défini selon Wikipedia comme « une association internationale dont l'objectif est d'améliorer les processus et méthodologie des audits informatiques ».

3.1.2 Outils de gestion de la sécurité et de la conformité

COSO : Le référentiel COSO est un guide pour le management exécutif et donc pour le *système de pilotage*. Il fournit un cadre pour la mise en place de contrôles internes, généralement supervisés par le conseil d'administration. Il a essentiellement été promu grâce à l'entrée en vigueur de lois, telles que la loi Sarbanes-Oxley. Il est donc clairement défini que le *système de pilotage* est le principal utilisateur de COSO.

> *« Pour rappel, le COSO 1 propose un cadre de référence pour la gestion du contrôle interne. Le contrôle interne est un processus mis en œuvre par le* ***conseil d'administration****, les* ***dirigeants*** *[…] quant à la réalisation des objectifs » - Wikipédia*

ISO 27000 : La suite des normes ISO 27000 a été éditée afin de fournir un cadre regroupant les standards concernant la sécurité de l'information. Elles comprennent donc une vision globale et la définition du vocabulaire (ISO 27000), des exigences (ISO 27001, ISO 27006) pour la mise en place d'un SMSI, ainsi que la gestion d'une politique de sécurité, sa surveillance et son maintien (ISO 27002), mais également la gestion des risques liés à l'information (ISO 27005).

La sécurité de l'information passe par le *système d'information* dans le cadre de sa mise en place car il est nécessaire d'avoir un point de vue précis sur les activités de l'entreprise (*système d'information*), sans forcément posséder une vue d'ensemble générale de la stratégie d'entreprise (*système de pilotage*). En revanche, la prise de décision concernant l'implantation ou non d'une norme ou d'une autre au sein de l'entreprise nécessite d'en connaître les objectifs stratégiques, et donc de se situer au niveau du *système de pilotage*. Mais cela concerne la prise de décision, et non l'implantation, ce que nous avons tenté de représenter sur le présent schéma.

Loi SOX : La loi SOX est une loi américaine, sur la comptabilité des sociétés cotées en bourse ainsi que sur la protection des investisseurs. Elle concerne donc le *système de pilotage*, qui est chargé, entre autres, du respect des législations et règles, et la dimension « conformité » au sein de la

gouvernance. La plupart de ses mises en application s'appuient sur le référentiel COSO, comme le relève Wikipédia[16].

« En pratique le COSO *est le référentiel le plus utilisé. »*

3.1.3 Outils de performance

CobiT : CobiT fournit les outils afin de structurer les objectifs de la gouvernance de la sécurité de l'information.

*« COBIT's success as an increasingly internationally accepted set of **guidance materials for IT governance** has resulted in the creation of a growing family of publications and products designed to assist in the implementation of effective IT governance throughout an enterprise. »*

Le référentiel présente également les objectifs de contrôle et les bonnes pratiques, et les relie aux exigences métiers. Cela concerne donc principalement le *système de pilotage*. Mais CobiT précise aussi comment acquérir et mettre en place des technologies, afin de les aligner avec les objectifs métiers de l'entreprise. Cela se passe bien entendu au niveau du *système opérant*, alors que leur surveillance se situe, elle, au niveau du *système d'information*.

Val IT : Val IT fait partie, tout comme CobiT et Risk IT d'un cadre de travail fourni pour l'ISACA. Il est donc naturel de constater que Val IT s'appuie largement sur COBIT. Il donne un cadre à la gouvernance (*système de pilotage*) des investissements informatiques. Sur le schéma, il est représenté comme faisant partiellement partie de CobiT, tant son contenu est basé sur ce dernier. Sur le site de l'AFAI, il est même répertorié dans les produits CobiT[17], et peu d'articles concernant Val IT ne font pas mention de CobiT.

ITIL : ITIL fournit la méthodologie pour la mise en place de l'amélioration de la qualité du *système d'information*. Ces bonnes pratiques concernent donc également le *système opérant*, puisque c'est en définitive lui qui sera chargé d'implanter les nouvelles fonctionnalités au sein de l'entreprise.

« ITIL est une collection de livres qui recense […] les meilleures pratiques pour […] l'informatique au sein de l'entreprise […]. » - ITIL France

---

[16] Voir http://fr.wikipedia.org/wiki/Loi_Sarbanes-Oxley

[17] Voir http://www.afai.asso.fr/index.php?m=238 pour la présentation de Val IT comme un produit de CobiT.

3.2 Les niveaux de maturité de l'entreprise

Nous allons maintenant présenter l'articulation de nos normes et méthodes en les articulant autour du niveau de maturité de l'entreprise.

Afin de faciliter la compréhension du concept de maturité, nous nous baserons sur la structure d'un modèle de référence bien connu : le CMMI[18]. Celui-ci est en effet constitué de 5 niveaux :

1. Le **niveau initial** est un niveau ou rien n'est géré. Tout est indépendant et il n'y a pas d'effort à la gestion et à la cohésion d'un tout. Le résultat final en devient imprévisible.

2. Le **niveau discipliné**, un léger contrôle a lieu. Les rôles sont répartis, certains processus sont documentés et vérifiés et les activités sont planifiées.

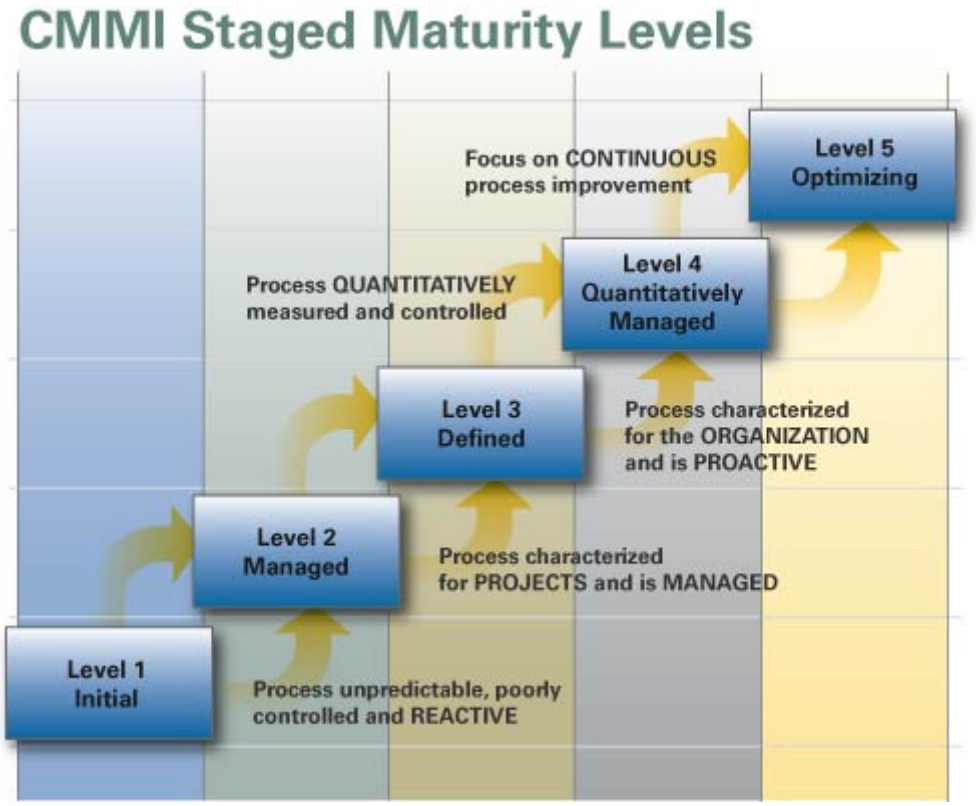
3. Le troisième niveau, le **niveau ajusté**, comprend des règles d'entreprise. Chaque projet possède un ensemble de processus standards et ajustés sur les objectifs de l'entreprise. Les projets sont documentés, et l'entreprise tire profit des projets passés, en améliorant sans cesse ses propres processus.

4. Le niveau quatre, **géré quantitativement**, possède des statistiques sur ses processus clés. Cela permet d'optimiser la productivité en améliorant les pratiques. Cela permet également d'identifier les activités n'ayant pas atteint les objectifs fixés, et d'agir en conséquence.

5. Le cinquième et dernier niveau, **en optimisation**, établit des processus en constante évolution, grâce notamment aux analyses coût/bénéfice. Grâce aux statistiques, l'analyse causale permettra d'effectuer une optimisation des processus.

[18] Le CMMI - *Capability Maturity Model Integration* – « est un modèle de référence, un ensemble structuré de bonnes pratiques, destiné à appréhender, évaluer et améliorer les activités des entreprises d'ingénierie », selon Wikipédia.

Figure 6 - Les 5 niveaux de maturité du CMMI



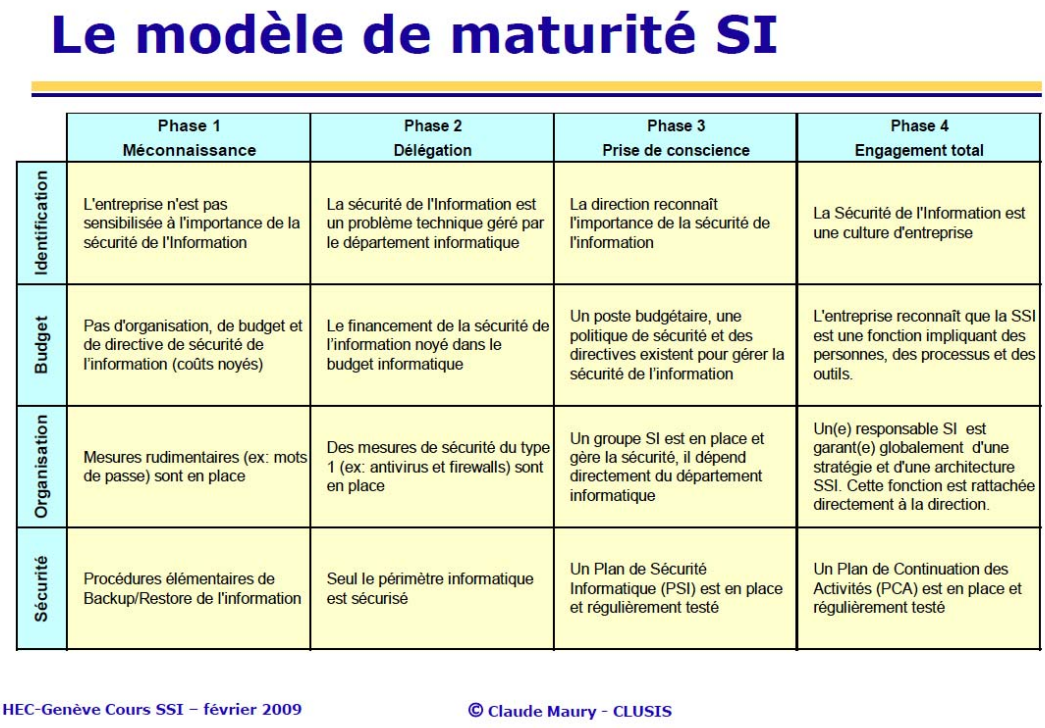
Source : http://www.mustang-technologies.com/Quality/SWCMMI.aspx

Dans le cadre de CMMI, ces niveaux sont complémentaires. En effet, on ne peut atteindre le niveau 3 sans avoir atteint le 2, le 4 sans le 3, etc… Dans le cadre qui nous intéresse ici, ces niveaux doivent être indépendants. En effet, il serait bien moins judicieux pour nous de conserver cette dépendance, car nous risquerions de nous retrouver dans le cas où de grandes colonnes viendraient remplir notre schéma, et l'on perdrait ainsi le niveau précis auquel la norme ou la méthode doit être placée.

Une autre approche de la maturité de l'entreprise est avancée par Claude MAURY, du CLUSIS[19]. Il s'agit d'un modèle à 4 niveaux, basé sur l'engagement des ressources de l'entreprise pour la gestion des systèmes d'information :

[19] Le CLUSIS – *Club de la Sécurité de l'Information Suisse* – Branche Suisse du CLUSIF

Figure 7 - Modèle de maturité des SI par le CLUSIS



Le modèle de maturité SI

	Phase 1 Méconnaissance	Phase 2 Délégation	Phase 3 Prise de conscience	Phase 4 Engagement total
Identification	L'entreprise n'est pas sensibilisée à l'importance de la sécurité de l'Information	La sécurité de l'Information est un problème technique géré par le département informatique	La direction reconnaît l'importance de la sécurité de l'information	La Sécurité de l'Information est une culture d'entreprise
Budget	Pas d'organisation, de budget et de directive de sécurité de l'information (coûts noyés)	Le financement de la sécurité de l'information noyé dans le budget informatique	Un poste budgétaire, une politique de sécurité et des directives existent pour gérer la sécurité de l'information	L'entreprise reconnaît que la SSI est une fonction impliquant des personnes, des processus et des outils.
Organisation	Mesures rudimentaires (ex: mots de passe) sont en place	Des mesures de sécurité du type 1 (ex: antivirus et firewalls) sont en place	Un groupe SI est en place et gère la sécurité, il dépend directement du département informatique	Un(e) responsable SI est garant(e) globalement d'une stratégie et d'une architecture SSI. Cette fonction est rattachée directement à la direction.
Sécurité	Procédures élémentaires de Backup/Restore de l'information	Seul le périmètre informatique est sécurisé	Un Plan de Sécurité Informatique (PSI) est en place et régulièrement testé	Un Plan de Continuation des Activités (PCA) est en place et régulièrement testé

HEC-Genève Cours SSI – février 2009 © Claude Maury - CLUSIS 9

En tirant profit des deux schémas présentés ici, nous pouvons établir notre propre base de référence. Nous retiendrons une architecture à 5 niveaux, pour des raisons de commodité, en gardant à l'esprit que la part d'engagement de l'entreprise au niveau de ses investissements et engagements est un facteur favorisant l'accession au niveau suivant.

Le **niveau 1** n'adopte aucune stratégie. L'entreprise ne fixe pas d'objectifs à atteindre au niveau de la sécurité de l'information. Les procédés sont basique, et indépendants les uns des autres.

Le **niveau 2** possède un contrôle de base des processus de sécurité. Un département informatique gère les problèmes techniques, un budget pour la sécurité est prévu et des rôles commencent à apparaître au niveau de la sécurité de l'information. La sécurité de l'information ne concerne que l'informatique.

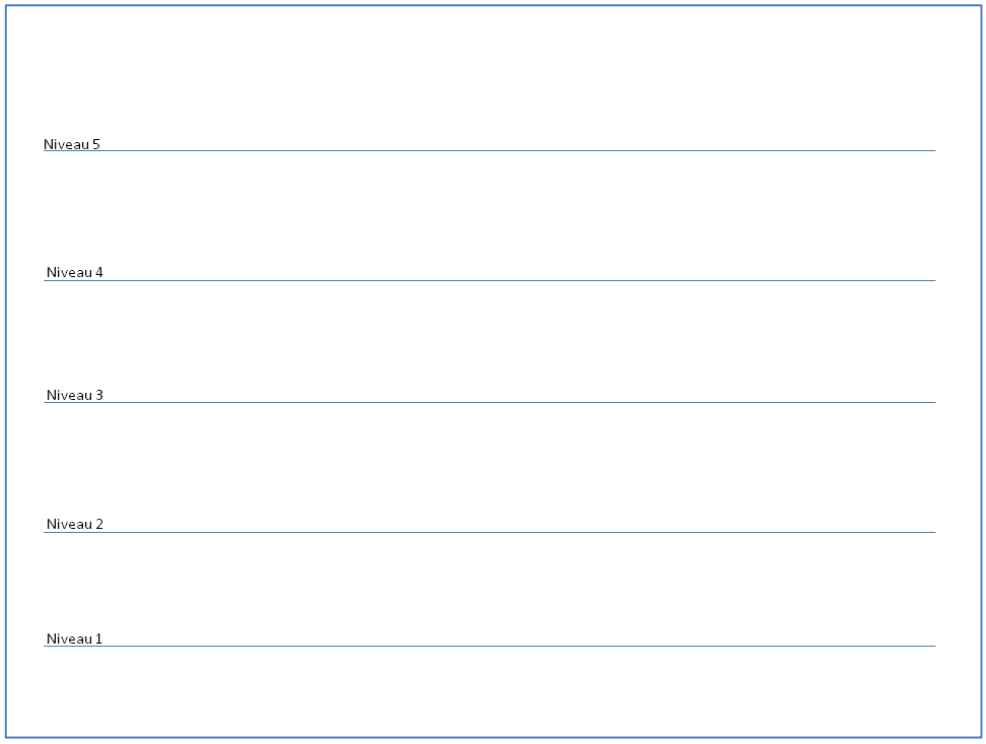
Le **niveau 3** suit des règles d'entreprise. Une amélioration des processus a lieu, en se basant sur l'expérience de projets déjà vécus. Les projets sont donc documentés. La sécurité de l'information reste cantonnée à l'informatique, mais un groupe de professionnels y est dédié.

Le **niveau 4** comprend des statistiques sur les processus clés de l'entreprise. La production et la sécurité sont optimisées grâce à ces statistiques. Un plan de sécurité est imaginé et testé. La sécurité de l'information s'étend au reste de l'entreprise.

Le **niveau 5** exige que la sécurité de l'information fasse partie intégrante de la stratégie d'entreprise. Un RSSI est nommé à la direction, possède un budget et son équipe. La stratégie de l'entreprise et les objectifs de la sécurité de l'information sont régulièrement mis à jour pour être le plus cohérent possible avec le contexte de la société.

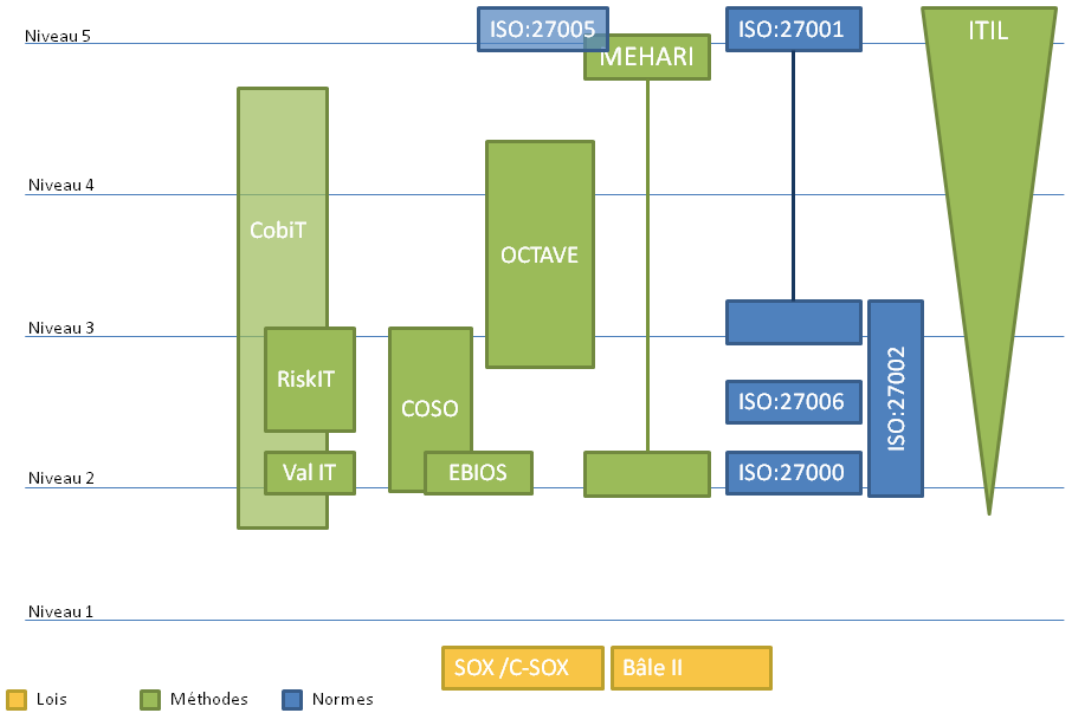
Enfin, le schéma suivant pose les bases pour la suite de notre travail. Comment les normes, méthodes et lois s'articulent-elles autour de ces niveaux ?

Figure 8 - Maturité de l'entreprise - cadre de travail



Une fois ces niveaux établis, il nous est possible de placer les outils de sécurité de la manière suivante :

Figure 9 – Maturité de l'entreprise – intégration des outils de sécurité



A nouveau, ce schéma requiert quelques explications. Les codes de couleurs sont conservés, à savoir que les lois sont en jaune, les méthodes en vert, et les normes en bleu.

Premier élément marquant de ce graphique, **les lois**. Elles ne sont rattachées à aucun niveau. Cela est logique, puisque cette représentation modélise le niveau de maturité d'une entreprise et que les lois en sont par conséquent indépendantes. Elles sont également placées au dessous du 1er niveau car les lois doivent être respectées, indépendamment du niveau de maturité de l'entreprise, par l'ensemble des sociétés.

Viennent ensuite les méthodes du cadre de travail de l'ISACA. Il s'agit des méthodes CobiT, Val IT et Risk IT. Le CobiT est l'outil de fond du framework[20]. Il décompose la gouvernance de la sécurité des systèmes d'information en processus, permettant une gestion simplifiée et à la fois plus fine des systèmes. C'est notamment dans ce cadre que Risk IT et Val IT seront développés. Ils reposent en effet, tel que le schéma le montre, sur CobiT, et s'en inspirent largement, reprenant ainsi sa méthodologie, et en l'appliquant plus précisément à leur sujet, à savoir respectivement la gestion des risques et la gestion des investissements.

Leur situation sur ce graphique s'explique de la manière suivante :

CobiT : Il interagit au **niveau 2** par la gestion des ressources humaines et la définition des rôles du personnel de l'entreprise au niveau de la gestion de la politique de sécurité. Il est également présent aux **niveaux 3 et 4** pour le contenu de ses 4 domaines internes. Ceux-ci présentent successivement la gestion du planning et de l'organisation, de même que la gestion des acquisitions et leur mise en place pour le **niveau 3**, puis viennent au **niveau 4** tout l'aspect de la surveillance de la solution mise en place.

Risk IT : Risk IT s'insère entre les **niveaux 2 et 3** par l'identification des bonnes pratiques (**niveau 2**), et l'intégration des risques à la stratégie de l'entreprise (**niveau 3**).

Val IT : Val IT se positionne plutôt au **niveau 2**, car il ne contient que des lignes directrices pour la gestion et le suivi des investissements. Il permet de fait de ne conserver que ce qui est vraiment nécessaire au niveau des projets de l'entreprise, ainsi que de rationnaliser les investissements futurs.

[20] Framework – anglicisme signifiant « cadre de travail ».

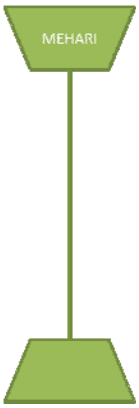
Son ensuite présentées les méthodes de gestion de contrôles internes, COSO et EBIOS.

COSO est représenté au **niveau 2** par la définition des rôles[21] (ceci est en partie une nouveauté de la version 2 du référentiel), ainsi qu'au **niveau 3** en intégrant une relation entre la stratégie de l'entreprise et la mise en place du contrôle interne.

En ce qui concerne **EBIOS**, il fournit une méthode de référence en matière d'analyse des risques[22] concernant le **niveau 2** car il n'instaure qu'une documentation des processus de contrôle interne. Il ne préconise pas de statistiques, comme les niveaux suivants le requièrent.

Passons maintenant à **OCTAVE** et à la norme **ISO 27005**, toutes deux axées sur la gestion des risques. Comme l'indique le graphique, la méthode OCTAVE s'oriente plutôt vers des entreprises matures, puisqu'elle concerne les **niveaux 3 et 4**. Elle comprend en effet une gestion complète de profils de menaces sur les biens de l'entreprise, ainsi qu'une vue plus technique, basée sur l'évaluation des composants et leur optimisation. Il en résulte un développement de la stratégie d'entreprise, basé sur ces nouvelles considérations.

La norme **ISO 27005** collabore, quant à elle, avec d'autres références sur laquelle elle s'appuie (telle que la norme ISO 27001) et est également utilisée par des méthodes telles que Mehari. La norme ISO 27005 est dédiée à l'amélioration de la gestion des risques grâce à une démarche PDCA[23], entraînant de fait une amélioration constante des processus, la plaçant au **5ème niveau** de maturité de notre schéma.



Dans cette optique, la méthode **MEHARI** constitue une deuxième solution pour la gestion des risques, complémentaire à la norme ISO 27005. Elle comprend aussi une approche PDCA pour la gestion et le suivi de l'amélioration des processus (**niveau 5** de notre graphique), mais fournit

---

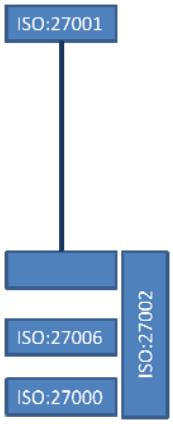
[21] Par exemple le rôle de « Risk Officer », apparu dans COSO 2.

[22] Selon la DCSSI - http://www.ssi.gouv.fr/IMG/pdf/ebiosv2-memento-2004-02-04.pdf

[23] La méthode PDCA – *Plan Do Check Act* – « comporte quatre étapes, chacune entraînant l'autre, et vise à établir un cercle vertueux. Sa mise en place doit permettre d'améliorer sans cesse la qualité d'un produit, d'une œuvre, d'un service », selon Wikipédia.

également une analyse et une évaluation des risques qui la placent donc au **niveau 2** de notre schéma.

Puis vient la suite des normes 27000, dont le sujet est la mise en place d'une politique de gestion de la sécurité de l'information, composée à l'heure actuelle des normes suivantes :



ISO 27000 : Première norme de la suite, précisant le vocabulaire et proposant une vue globale sur le chapitre de la sécurité de l'information. Elle se place donc à un niveau relativement peu élevé de notre schéma (**niveau 2**) car elle ne fait que préciser le contenu et le cadre des processus.

ISO 27001 : Elle fournit les outils de contrôle à mettre en place pour une gestion efficace de la sécurité de l'information (**niveau 2**) et préconise également la mise en place d'une boucle d'amélioration de type PDCA (**niveau 5**).

ISO 27002 : Elle précise les rôles des acteurs de la sécurité de l'information (contrôles d'accès, sécurité des ressources humaines) qui relèvent du **niveau 2**, ainsi qu'un léger processus d'amélioration axé sur les objectifs de l'entreprise, équivalent au **niveau 3** de notre schéma.

ISO 27006 : A demi-niveau, la norme 27006 précise les exigences et les lignes directrices d'audit et de certification pour les entités souhaitant intégrer un SMSI. Le niveau de maturité est donc un peu supérieur au **niveau 2**, puisque celui-ci ne demande qu'une légère planification des activités, mais légèrement en deçà du **niveau 3** qui lui, intègre clairement les règles d'entreprise dans la mise en place des processus.

Finalement, **ITIL**, fournit des lignes directrices pour l'implantation de services répondant à des normes de qualité, basé sur une évolution constante des processus. Il peut donc être implanté au sein d'entreprises dont le niveau de maturité est faible, puisque plus celui-ci augmente et plus l'implantation d'ITIL sera forte.

Un dernier point reste cependant à soulever. Il s'agit de l'absence d'outils au **niveau 1** de maturité. Mais cela est logique. Lorsque l'on y repense, tous ces éléments sont fournis à des entreprises soucieuses de la qualité de leurs processus. Il s'agit par conséquent d'entreprises possédant un certain niveau de maturité, dont les processus offrent une certaine cohérence.

4. Publication des résultats

L'analyse et l'articulation étant faites, il nous faut maintenant trouver un moyen de publier les résultats obtenus de manière simple et dynamique afin de pouvoir en assurer le suivi. Il est clair qu'une publication pour le plus grand nombre passe aujourd'hui par Internet.

Le contenu de cette publication est en effet destiné dans un premier temps à être repris et amélioré par les professionnels du monde de la sécurité de l'information, tels que ceux intervenants dans les cours de la formation du MBA-ISSG, par exemple. Ils apporteront alors au contenu de ces pages leur expérience et expertise dans le domaine.

Dans l'optique de ces modifications, et en imaginant une publication sur Internet, il paraît naturel aujourd'hui de les insérer dans un système de gestion de contenu dynamique, autogéré, et où chacun peut librement laisser parler son expérience pour en enrichir le contenu. Il s'agit ici de la définition même du wiki. C'est donc un outil de ce type qui sera utilisé pour ladite publication. Mais comment mettre ce wiki en place ?

4.1 Wiki ? Rappel

Le chapitre de la mise en place du wiki sera d'abord constitué d'un rappel de ce qu'est un wiki. Viendra ensuite la comparaison des différents outils disponibles, selon les critères établis. Puis, finalement, la mise en place de la plateforme choisie, de même que sa prise en main seront l'objet de notre attention.

4.1.1 Qu'est-ce qu'un wiki ?

> *« Un **wiki** est un logiciel de la famille des systèmes de gestion de contenu de site web rendant les pages web modifiables par tous les visiteurs y étant autorisés. Il facilite l'écriture collaborative de documents avec un minimum de contraintes. »*
> *(Wikipedia [http://fr.wikipedia.org/wiki/Wiki], le 21 septembre 2009)*

C'est donc un système qui fournit les outils nécessaires à la collaboration de tous les visiteurs, afin d'optimiser son contenu. Il permet à chacun d'apporter des précisions sur un sujet de manière aisée et intuitive.

4.1.2 Pourquoi avoir créé un wiki ?

Comme énoncé dans sa définition, un wiki permet à toute personne désireuse de le faire d'apporter des précisions à un article sur un sujet pour lequel elle est compétente. De ce fait, la qualité des articles s'améliore au fil du temps et des retouches. Chacun est libre, dans la mesure de ses droits, d'apporter ses connaissances et expériences afin de faire progresser le contenu du wiki.

Il ne faut pas non plus perdre de vue qu'un wiki est avant tout un site web, donc consultable gratuitement et en tout temps par la majorité des gens. Ce site web a donc une vocation de référence, sur laquelle il sera possible de s'appuyer, grâce notamment à l'expertise de ses collaborateurs.

4.2 Comparaison des outils

4.2.1 Critères

Afin de comparer les outils de mise en place et de gestion de wiki, et pour garantir une évaluation univoque, des critères de choix ont été mis en place, puis les plateformes évaluées. Voici une liste des critères retenus :

- **Prix** – N'ayant pas de budget à consacrer à ce travail, il semblerait superflu qu'un logiciel payant soit testé. Néanmoins, dans le cas où un logiciel viendrait à répondre parfaitement aux besoins du mandat, et qu'aucun équivalent gratuit ne puisse être trouvé, il serait peut-être envisageable de décrocher les fonds nécessaires à son acquisition.

- **Technologies utilisées** – Nous disposons d'un serveur de type LAMP (Linux[24], Apache[25], MySQL[26], PHP[27]). Il faut donc que la plateforme candidate utilise ces technologies. Il est évident que toutes les technologies présentes sur le serveur ne doivent pas obligatoirement être utilisées. En revanche une bonne utilisation des ressources mises à disposition permettrait d'optimiser le fonctionnement du système final.

[24] Linux est un système d'exploitation, tel que Microsoft® Windows®, ou Mac OS.

[25] Apache est le logiciel de serveur le plus populaire du Web. C'est un logiciel libre, possédant sa propre licence, la licence Apache.

[26] MySQL est un Système de Gestion de Base de Données (SGBD), sous licence libre ou propriétaire.

[27] PHP est un langage de programmation libre utilisé pour le Web.

- **Facilité de mise en place** – Il est plus efficace de travailler avec des systèmes aboutis qu'avec des systèmes dont certaines fonctionnalités, telles que l'installation, ne sont pas totalement, voire pas du tout, développées.

- **Présentation des articles** – La présentation des articles a une large part dans la note finale puisque c'est ce que nous allons présenter aux visiteurs. Il faut que l'interface de présentation soit claire, aisée à prendre en main, si possible connue ou proche d'une interface déjà existante, afin que tous les utilisateurs puissent rapidement trouver leurs marques au sein du système.

- **Facilité de modification des articles** – Les articles seront modifiés régulièrement par des personnes probablement différentes. Il est donc normal que ce point retienne notre attention.

- **Gestion des utilisateurs** – Afin de définir une politique de gestion des droits de modification, il doit être possible de gérer les utilisateurs et leurs droits sur le système.

Une fois ces critères arrêtés, il faut encore leur attribuer une pondération car ils n'ont pas forcément tous la même valeur pour le système recherché. Pour ce faire, tous les critères ont été numérotés de 1 à 6, du moins important au plus indispensable. Chaque critère a été choisi en fonction d'un besoin du système final, une fois en tant qu'administrateur du système, une autre en tant qu'utilisateur, afin de prendre en compte les différents points de vues de la plateforme.

Finalement, les critères d'évaluation ont été notés de 1 à 3, selon l'échelle suivante :

a. Prix :
   1. Payant
   2. Gratuit – utilisation limitée
   3. Gratuit – utilisation illimitée

b. Technologies utilisées :
   1. HTML[28]/Javascript[29] simple
   2. PHP, sans base de données

[28] L'HTML – *HyperText Markup Language* – est un langage balisé permettant de définir la structure des pages Web.

[29] Javascript est défini selon Wikipédia comme « un langage de programmation de scripts principalement utilisé dans les pages Web interactives »

3. PHP/MySQL (ou autre SGBD)

c. Installation :

1. Aucune installation fournie
2. Fichier de configuration à modifier manuellement
3. Assistant d'installation des fichiers, de la configuration, et de la BDD[30]

d. Facilité de navigation :

1. Difficile – Une seule page, sans structure, sans menu, navigation peu claire
2. Moyen – Plusieurs pages, structure déroutante, système peu clair
3. Facile – Plusieurs pages, présentation intuitive/connue, menus

e. Modification des articles :

1. Modification du code[31] HTML
2. Formulaire de modification de l'article, sans WYSIWYG[32]
3. Formulaire de modification de l'article, avec WYSIWYG

f. Gestion des utilisateurs :

1. Pas de gestion des utilisateurs
2. Deux niveaux d'identification, visiteur et administrateur
3. Gestion complète des utilisateurs, plusieurs comptes

Nous pouvons maintenant rassembler divers outils de gestion de wiki, afin de les confronter entre eux.

4.2.2 Les outils comparés

Pour trouver des plateformes de wiki, nous avons effectué quelques recherches sur internet. Il en ressort quelques noms bien connus, d'autres un peu moins. Voici les différents outils qui seront comparés entre eux :

- **MediaWiki** – le moteur de Wikipedia, l'encyclopédie libre mondialement connue. Il fonctionne grâce à un serveur PHP et une base de données MySQL.
- **TiddlyWiki** – Un wiki ultrasimple, constitué d'une seule page html, qui se modifie en ligne, essentiellement gérée en javascript.

---

[30] BDD – *Base De Données*

[31] Le code source informatique est « un ensemble d'instructions écrites dans un langage de programmation informatique de haut niveau, compréhensible par un être humain entraîné, permettant d'obtenir un programme pour un ordinateur. », selon Wikipédia.

[32] Éditeur WYSIWYG – *What You See Is What You Get* – Littéralement « Vous obtenez ce que vous voyez ». Ce sont des éditeurs permettant de définir une mise en page voulue sans se soucier du code source à mettre en place pour y parvenir, l'éditeur s'en chargeant.

- **WikiNi** – Un des nombreux systèmes de gestion de wiki en PHP/MySQL
- **DokuWiki** – Plateforme de gestion de wiki, écrite en php. A la différence de beaucoup d'autres systèmes, il ne se connecte à aucune base de données, mais gère son contenu en fichiers plats, stockés sur le serveur.

On remarque que les quelques outils retenus couvrent divers types de solutions, de technologies. Cet éventail de solutions permet de tester l'ensemble des possibilités de gestion d'un wiki.

4.2.3 Comparaison des outils

Grâce aux critères et à leurs règles, on peut maintenant effectuer une comparaison des outils candidats :

Outil Critère Commentaire Points obtenus

MediaWiki :

a. Licence GNU/GPL[33] 3
b. 3
c. 3
d. Interface connue, largement répandue 3
e. Formulaire d'édition, WYSIWYG « partiel », aperçu avant publication..... 3
f. 3

TiddlyWiki :

a. Licence BSD[34] 3
b. 1
c. Installation manuelle 1
d. Navigation difficile, va-et-vient dans une même page 1
e. 1
f. 1

[33] Licence GNU/GPL – *GNU General Public License* – Licence Publique Générale est un type de licence « qui fixe les conditions légales de distribution des logiciels libres du projet GNU » (Wikipédia).

[34] Licence BSD – *Berkley Software Distribution License* – est un type de licence, libre, utilisée pour la distribution de certains logiciels.

WikiNi :

a. Licence GPL 3
b. 3
c. Installation automatique 3
d. Présentation des liens internes étrange 2
e. Le système d'édition n'est pas complet, manque des boutons d'accès aux fonctionnalités de l'édition 2
f. Gestion complète des utilisateurs 3

DokuWiki :

a. Licence CreativCommon –by-nc-sa[35] 3
b. Absence de base de données 2
c. La configuration est automatique 3
d. Navigation peu intuitive, menu en petit fil d'Ariane peu visible 2
e. 3
f. Gestion des utilisateurs absente en version de base (plugin nécessaire) 2

Le tableau ci-dessous récapitule l'ensemble de ces résultats, ainsi que les totaux obtenus pour chaque outil.

Tableau 1 – Synthèse de la comparaison des outils

Critère	a	b.	c	d.	e.	f	**Total**
Pondération	2	6	1	5	4	3	
MediaWiki	**3**	**3**	**3**	**3**	**3**	**3**	63
TiddlyWiki	**3**	**1**	**1**	**1**	**1**	**1**	25
WikiNi	**3**	**3**	**3**	**2**	**2**	**2**	54
DokuWiki	**3**	**2**	**3**	**2**	**3**	**2**	49

[35] Les licences Creative Commons, « proposent des contrats-type pour la mise à disposition d'œuvres en ligne » (Source : http://fr.creativecommons.org). Les cigles –by-nc-sa précisent la portée des licences. Voir : http://fr.creativecommons.org/contrats.htm

Le total pour chaque outil est obtenu en multipliant les notes et les pondérations de chaque critère, puis en les additionnant par outil.

4.2.4 Interprétation des résultats

Le tableau de comparaison des outils nous donne les résultats suivants :

- MediaWiki : 63 – 33% de la note finale
- TiddlyWiki : 25 – 13% de la note finale
- WikiNi : 54 – 28% de la note finale
- DokuWiki : 49 – 26% de la note finale

On voit clairement que deux outils prédominent les autres, il s'agit de MediaWiki, et de WikiNi. Il s'agit d'un résultat plus ou moins logique lorsqu'on regarde avec attention ces deux systèmes, puisqu'ils ont énormément de points communs.

En ce qui concerne les deux plateformes marginales, on constate sans trop de surprise que TiddlyWiki, qui part d'une bonne intention à la base (faciliter au maximum l'installation et la publication), se retrouve bien vite limité. DokuWiki, dont la présentation est quelque peu déroutante, répond à la plupart des critères, sauf celui de la gestion des utilisateurs. En effet, celle-ci n'est pas comprise à l'installation du logiciel et nécessitera l'installation d'un plugin après coup.

Il nous reste donc les deux ténors de ce comparatif, à savoir MediaWiki et WikiNi, qui répondent tous deux aux critères fixés, à quelques différences près.

Premièrement, MediaWiki est le moteur de la célèbre encyclopédie Wikipedia. Il parait donc logique qu'une structure telle que celle de la célèbre encyclopédie possède toutes les caractéristiques d'une référence.

Ensuite, WikiNi possède à quelques détails près toutes les caractéristiques de MediaWiki. La grande différence entre ces deux systèmes vient surtout de la présentation des informations. WikiNi est certes bien pensée, mais MediaWiki possède l'énorme avantage d'être bien connue du public et de profiter d'une grande communauté d'utilisateurs soucieux d'améliorer sans cesse leur produit.

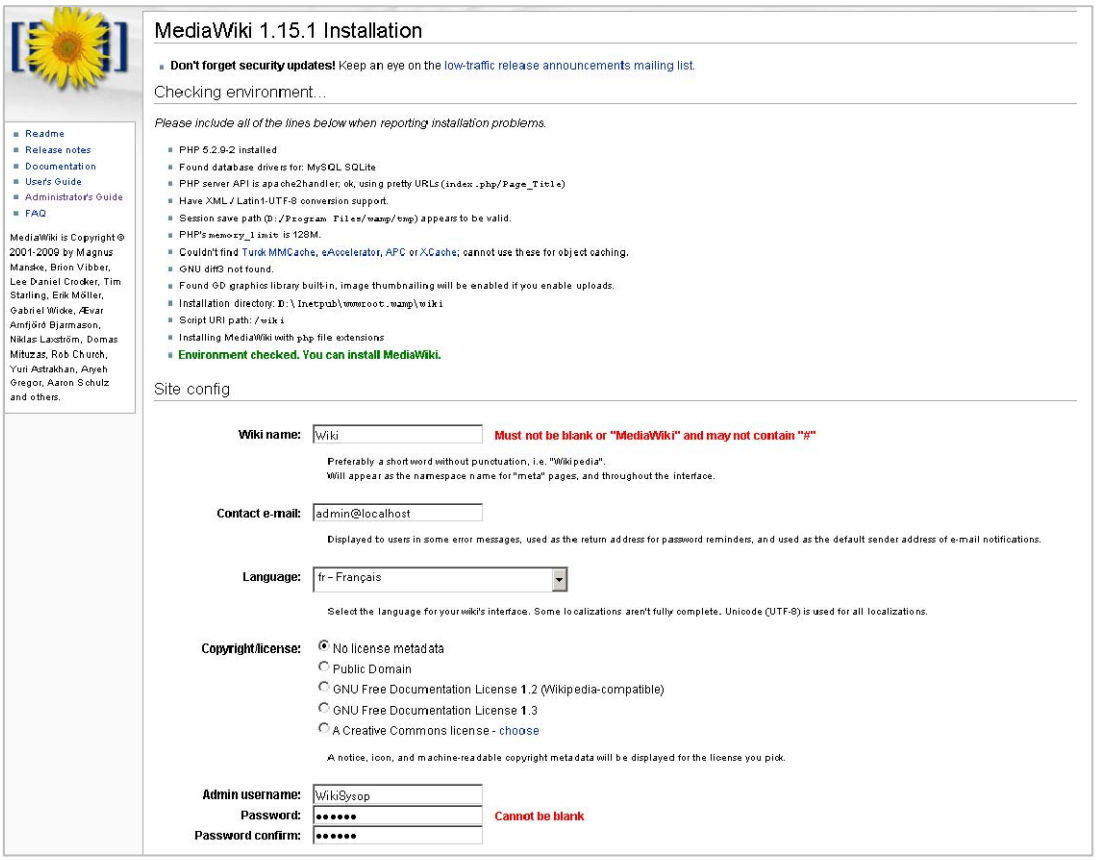
Au vu de ce qui précède, notre choix s'est donc porté sur MediaWiki.

4.3 Mise en place du wiki « Mediawiki »

La mise en place de MediaWiki est relativement aisée. Le système est pourvu d'un assistant d'installation qui permet de faciliter sa mise en place. Ce dernier commencera par vérifier que l'environnement sur lequel la plateforme sera installée est conforme aux nécessités de cette dernière. Si cette opération échoue, il faudra corriger les éventuelles erreurs avant de poursuivre.

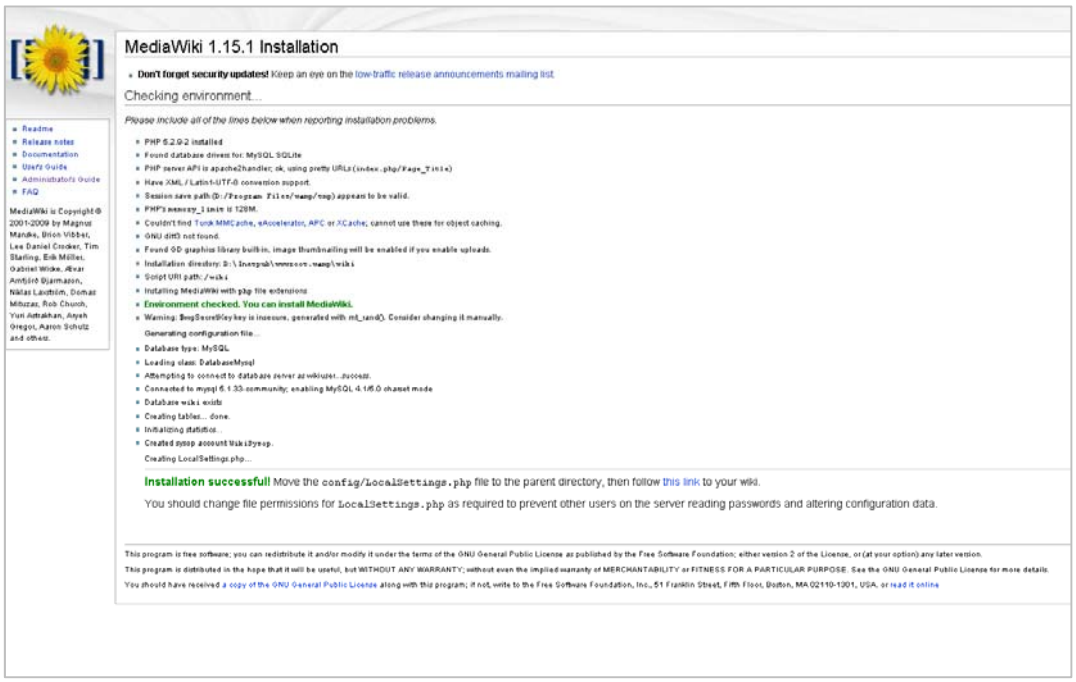
Une fois cela fait et le test de l'environnement passé, le programme d'installation demande (Figure 10) à l'utilisateur toutes les informations concernant le wiki, comme la langue, le nom d'utilisateur et mot de passe de l'administrateur, les données de connexion à la base de données, quelques options de configuration du futur wiki, etc.

Figure 10 - Installation de MediaWiki



Une fois tous les champs remplis et l'installation lancée, il ne reste plus qu'à attendre le message de confirmation suivant :

Figure 11 - Confirmation de l'installation



MediaWiki est maintenant installé, il ne reste « plus qu'à » le prendre en main, et le remplir !

4.4 Prise en main de la plateforme « Mediawiki »

4.4.1 Trouver de la documentation

Un des gros avantages lors de l'utilisation de systèmes bien connus tels que MediaWiki, est qu'ils possèdent pour la plupart d'entres eux une communauté très active permettant de prendre aisément ses repères sur le système, fournissant une quantité non négligeable d'aides et de supports divers.

Il existe aussi un suivi officiel de la prise en main de la plateforme qui fournit à lui seul une solide base pour qui désire se lancer dans la compréhension du système.

La prise en main de MediaWiki n'est donc pas difficile. Il suffit pour cela de faire quelques recherches sur internet pour avoir rapidement une bonne quantité de documentation.

Le site principal de références concernant le wiki MediaWiki est http://meta.wikimedia.org/. Il concerne, en fait, tous les projets de la fondation

Wikimedia qui est, entre autre, chargée du maintien de Wikipedia. Il présente les fonctions de base du système et de l'aide de premier niveau pour tout ce qui concerne la prise en main pour les nouveaux utilisateurs. Vous trouverez en annexe (Annexe 4 et Annexe 5) deux feuillets tirés de ce site illustrant parfaitement la qualité de l'aide fournie, bien qu'il ne s'agisse que d'exemples. Ils présentent respectivement la syntaxe de base pour l'écriture d'articles dans le wiki, et une aide concernant l'importation d'images et de fichiers sur le système.

4.4.2 Structure et mise en place des pages

Une fois que le système a été pris en main, il faut encore définir la structure des articles afin d'uniformiser le contenu du wiki. Pour 'identifier au premier coup d'œil quel type d'article il s'agit (explication d'une méthode, d'une norme, d'un terme en général, etc…), un code couleur a été mis en place. Il s'agit des mêmes couleurs que celles rencontrées précédemment dans les schémas d'articulation des normes et méthodes. De cette manière, l'utilisateur sait instinctivement de quoi l'article parle et dans quel contexte il doit être interprété.

Conclusions

Il y a plusieurs conclusions à tirer de ce rapport. Premièrement, les normes et les méthodes sont deux choses distinctes mais complémentaires. En effet, il n'est pas rare de voir des méthodes de travail s'appuyer sur des normes, afin de standardiser encore un peu plus les processus mis en œuvre. Ceci est notamment le cas entre la méthode Mehari et la norme ISO 27005.

Au niveau de leur utilisation respective, on se rend bien compte que ces outils sont très largement destinés à un public de grandes sociétés, avec de grosses structures. Les processus à mettre en œuvre pour une certification sont longs et complexes et nécessitent beaucoup de ressources humaines et financières. Il est donc normal de constater, au regard du graphique sur la maturité des entreprises (Annexe 3), qu'aucune société de niveau 1 ne peut implémenter de pareilles solutions. En revanche, ces procédés sont destinés à toute la chaîne de l'entreprise, aussi bien au système opérant qu'au système de pilotage, tant les champs couverts par les recommandations et standards sont variés. Ainsi, moyennant une grosse structure d'entreprise, tout le monde est susceptible de trouver l'outil qui correspond à ses besoins.

Il va de soi que les outils mis en avant dans ce document sont presque tous orientés vers la gouvernance d'entreprise qui est elle-même positionnée dans le système de pilotage. D'autres outils sont, bien sûr, adaptés aux systèmes inférieurs, mais ils n'ont pas été traités ici.

On remarque également que certaines normes ou méthodes sont plus dépendantes les unes des autres, comme Val IT qui n'a que très peu de chance d'être employée sans CobiT, alors que d'autres sont très indépendantes, comme ITIL par exemple.

Pour en finir avec ce qui concerne les normes et les méthodes, on pourra retenir qu'il n'y a pas de bon ou de mauvais choix quant à l'implantation de telle ou telle norme, de telle ou telle méthode au sein de son entreprise. Au regard des investissements nécessaires à leur implémentation, c'est une décision qui doit être mûrement réfléchie mais qui apporte une plus-value certaine à l'entreprise qui décide d'en faire usage. Il est même possible, dans certains cas de figure, qu'une certification ou le suivi de référentiels soit obligatoire afin de pouvoir décrocher des contrats avec des entreprises exigeant un niveau de confiance et de traçabilité des processus.

En ce qui concerne la mise en place du wiki, on constatera sans surprise que l'outil choisi pour sa mise en place, à savoir MediaWiki, est un des acteurs principal du marché du wiki. Son interface graphique est immédiatement identifiée par les visiteurs qui savent donc instinctivement utiliser le système. Sa facilité de mise en place, la quantité énorme de documentation librement accessible, ainsi que l'énorme publicité que constitue Wikipédia en ont assurément fait l'outil phare de la gestion de wiki.

Sa prise en main est aussi aisée que son installation, et, à l'heure de terminer ce travail, le wiki est déjà fort de plus de 25 articles, attendant tous l'expertise de ses futurs utilisateurs. Qui sait, il deviendra peut-être un jour la référence européenne de la gouvernance de la sécurité et de l'articulation de ses normes et méthodes !

Bibliographie

Sites

Wikipédia. Wikipédia, l'encyclopédie libre [en ligne].
http://fr.wikipedia.org/wiki/Accueil
(consulté régulièrement)

Organisme international de normalisation. ISO [en ligne]
http://www.iso.org/iso/fr/home.htm
(consulté régulièrement)

Ysosecure. Accueil [en ligne]
http://www.ysosecure.com/
(consulté régulièrement)

AFAI. Présentation de la famille COBIT [en ligne]
http://www.afai.asso.fr/index.php?m=238
(consulté le 25.08.2009)

ISACA. COBIT Products [en ligne]
http://www.isaca.org/Content/NavigationMenu/Members_and_Leaders1/COBIT6/COBIT_Publications/COBIT_Products.htm
(consulté le 25.08.2009)

CLUSIF. Présentation de MEHARI [en ligne]
https://www.clusif.asso.fr/fr/production/mehari/
(consulté le 25.08.2009)

Développez.com.Les méthodes d'analyse de risque [en ligne]
http://cyberzoide.developpez.com/securite/methodes-analyse-risques/
(consulté le 28.09.2009)

Ernst & Young. Communiqués de presse [en ligne]
http://www.ey.com/CH/fr/Newsroom/News-releases
(consulté le 05.10.2009)

ISF. The Standard of Good Practice [en ligne]
https://www.isfsecuritystandard.com/SOGP07/index.htm
(consulté le 14.10.2009)

Études et enquêtes

Étude comparée de référentiels et méthodes utilisées en sécurité informatique
http://www.cases.public.lu/fr/publications/recherche/r2sic/wp11_2.pdf
M.POGGI Sébastien, 2005

Enquête sur la sécurité de l'information
https://www.cefrio.qc.ca/upload/1602_1378DepEnqueteSec2004F.pdf
CEFRIO, 2004

Cours

HAURI, Rolf. Politique de sécurité. Genève, 2008-2009

MAURY, Claude. Le modèle de maturité SI. Cours SSI. Genève, 2009

MBA-ISSG. Cours de la formation. Gouvernance de la sécurité des systèmes d'information. Genève – Aix-en-Provence 2008-2009

Annexe 1
Glossaire[36]

Ce glossaire englobe toutes les définitions données en pied de page de ce dossier. Pour plus d'informations sur les termes spécifiques à la gouvernance des systèmes d'information, n'hésitez pas à vous référer au wiki de ce travail, disponible à l'adresse : http://www.mba-issg.com/wiki/

A

- AFAI : L'Association Française de l'Audit et du Conseil Informatiques - est le chapitre français de l'ISACA et compte environ 600 membres.

- **Apache** : Apache est le logiciel de serveur le plus populaire du Web. C'est un logiciel libre, possédant sa propre licence, la licence Apache.

B

- **BDD** : Base De Données

- **BSD** : Licence BSD – Berkley Software Distribution License – est un type de licence, libre, utilisée pour la distribution de certains logiciels.

C

- **CEI** : La *commission électrotechnique internationale* « est l'organisation internationale de normalisation chargée des domaines de l'électricité, de l'électronique et des techniques connexes. Elle est complémentaire de l'Organisation internationale de normalisation (ISO), qui est chargée des autres domaines. »

- **CIGREF** : Le *Club Informatique des Grandes Entreprises Françaises*, a été créé en 1970. Il regroupe plus de cent très grandes entreprises et organismes français et européens de tous les secteurs d'activité (banque, assurance, énergie, distribution, industrie, services...).

- **Code Source** : Le code source informatique est « un ensemble d'instructions écrites dans un langage de programmation informatique de haut niveau, compréhensible par un être humain entraîné, permettant d'obtenir un programme pour un ordinateur. ».

[36] Les définitions dont tout ou une partie sont contenus entre « » sont tirées de l'encyclopédie en ligne Wikipédia.

- **CLUSIF** : Le CLUSIF - Club de la Sécurité de l'Information Français - est un club professionnel, constitué en association indépendante, agissant pour la sécurité de l'information.

- **CLUSIS** : Le CLUSIS – Club de la Sécurité de l'Information Suisse – est la branche suisse du CLUSIF.

- **CMMI** : Le CMMI - Capability Maturity Model Integration – « est un modèle de référence, un ensemble structuré de bonnes pratiques, destiné à appréhender, évaluer et améliorer les activités des entreprises d'ingénierie ».

- **Creative Commons** : Les licences Creative Commons, « proposent des contrats-type pour la mise à disposition d'œuvres en ligne » (Source : http://fr.creativecommons.org). Les cigles –by-nc-sa précisent la portée des licences. Voir : http://fr.creativecommons.org/contrats.htm

D

- **DCSSI** : Direction Centrale de la Sécurité des Systèmes d'Information jusqu'au 7 juillet 2009, puis ANSSI, Agence Nationale de la SSI. Défini par Wikipédia comme « l'organisme interministériel officiel définissant les normes de la sécurité des systèmes d'information ».

F

- **Framework** : anglicisme signifiant « cadre de travail ».

G

- **GNU/GPL** : Licence GNU/GPL – GNU General Public License – Licence Publique Générale est un type de licence « qui fixe les conditions légales de distribution des logiciels libres du projet GNU ».

H

- **HTML** : L'HTML – HyperText Markup Language – est un langage balisé permettant de définir la structure des pages Web.

I

- IGSI : La société IGSI est une société de services (S.S.I.I.) spécialisée dans l'infrastructure informatique, l'informatique de gestion et la communication. - http://www.igsi.fr/

- **ISACA** : L'ISACA - Information Systems Audit and Control Association – est « une association internationale dont l'objectif est d'améliorer les processus et méthodologie des audits informatiques ».

- **ISO** : Organisation International de Normalisation, a élaboré plus de 17'500 normes. Il publie également plus de 1100 normes chaque année. http://www.iso.org/iso/fr/iso_catalogue

- **ISO 9001** : La norme ISO 9001 « spécifie les exigences relatives au système de management de la qualité », selon l'ISO.

J

- **Javascript** : Javascript est « un langage de programmation de scripts principalement utilisé dans les pages Web interactives ».

L

- **Linux** : Linux est un système d'exploitation, tel que Microsoft® Windows®, ou Mac OS.

M

- **MySQL** : MySQL est un Système de Gestion de Base de Données (SGBD), sous licence libre ou propriétaire.

- **MBA-ISSG** : MBA-ISSG : Master of Business Administration - Information System Security Governance. Première formation européenne de la gouvernance de la sécurité.

O

- **Modèle OID** : Le modèle *Opérant, Information, Décision* a été au tout début des années 80 adopté par la communauté des S.I. automatisés, et apparaissait dans les principes fondateurs des principales méthodes d'analyse développées alors.

P

- **PDCA** : La méthode PDCA – Plan Do Check Act – « comporte quatre étapes, chacune entraînant l'autre, et vise à établir un cercle vertueux. Sa mise en place doit permettre d'améliorer sans cesse la qualité d'un produit, d'une œuvre, d'un service ».

- **PHP** : PHP est un langage de programmation libre utilisé pour le Web.

S

- **SMSI** : Système de Management de la Sécurité de l'Information

W

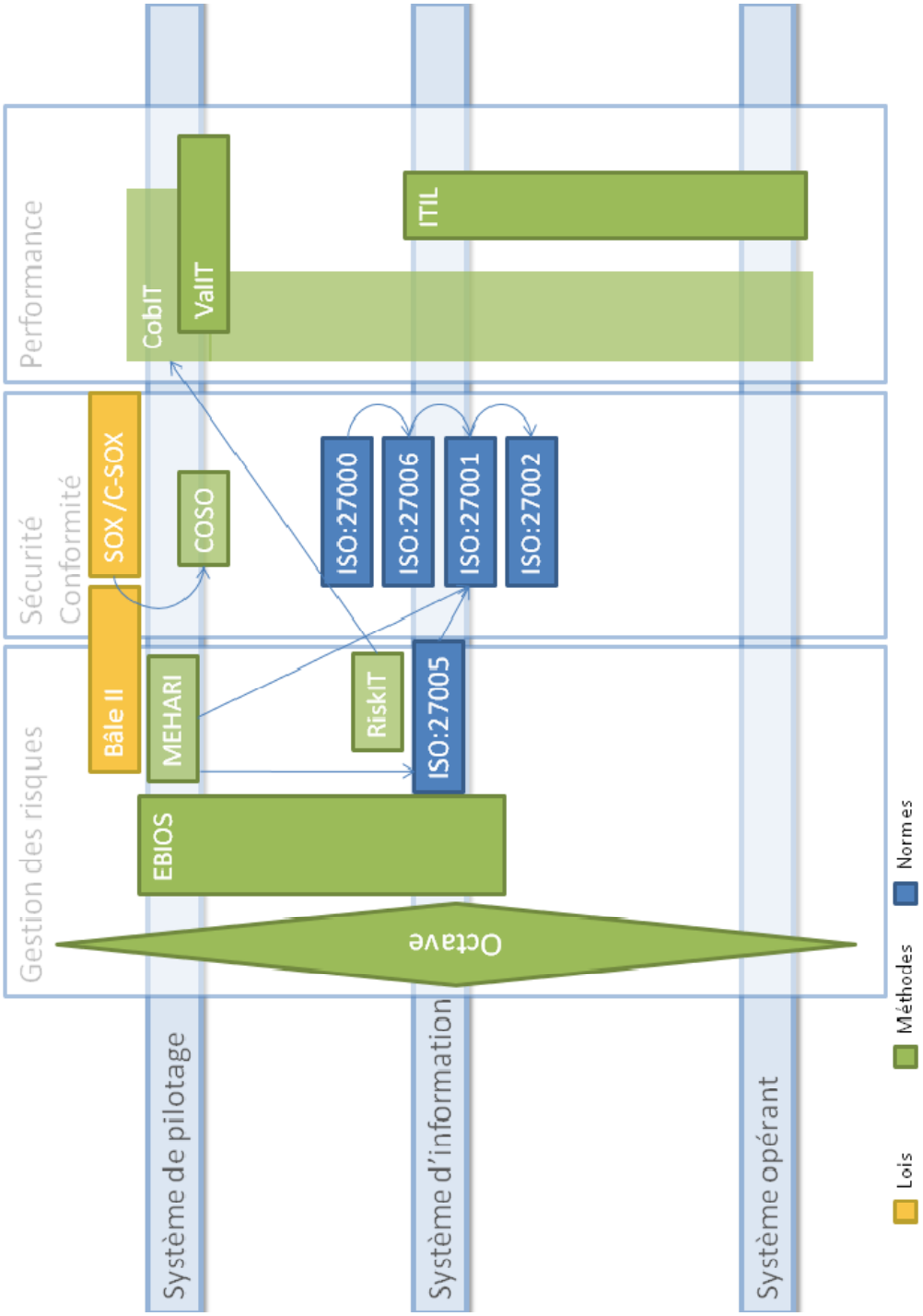
- **WYSIWYG** : What You See Is What You Get – Littéralement « Obtenez ce que vous voyez ». Ce sont des éditeurs permettant de définir une mise en page voulue sans se soucier du code source à mettre en place pour y parvenir, l'éditeur s'en chargeant.

Y

- **Ysosecure** : Cabinet de conseil spécialisé dans le domaine de la sécurité de l'information.

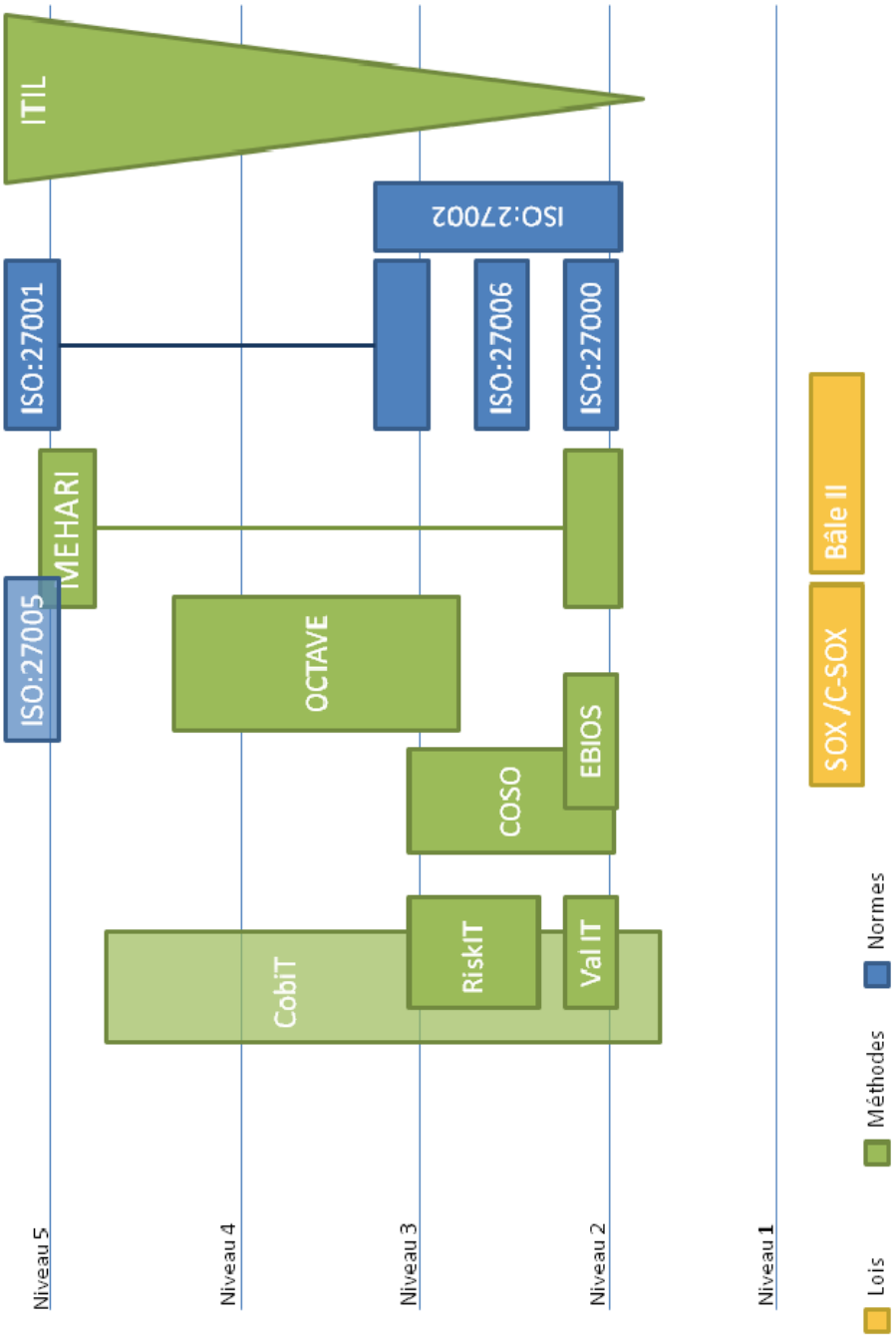
Annexe 2

Articulation des normes sur les systèmes de l'entreprise



Annexe 3

Intégration des outils de sécurité à la maturité de l'entreprise



Annexe 4

Référence pour la prise en main de la syntaxe wiki

Annexe 5

Référence pour l’ajout d’images et de fichiers au wiki