UNIVERSITÉ CLAUDE BERNARD LYON 1

Livre Blanc

Maturité des outils de Gouvernance IT

Données relatives au rapport

Date du rapport	05/06/2009
Période couverte	du 25/11/08 au 05/06/2009
Version du rapport	1
Rédacteur	Benjamin Blanchin Emmanuel Dietrich Atisha Garin-Michaud Samuel Guillot Yann Valey

Données relatives au projet

Sujet	Maturité des outils de Gouvernance IT en France
Date de début du projet	25/11/2008
Date de fin du projet	05/06/2009
Tuteur communication	Stéphanie Pouchot
Tuteur technique	Yannick Prié

Données relatives au commanditaire

Nom du commanditaire	SOGETI
Personne contact	Madame Line Amour
E-mail	line.amour@sogeti.com

Table des matières

Table des figures

Propos du livre blanc

Ce rapport entre dans le cadre du projet de Veille Technologique en M1 MIAGe. Il s'agit d'étudier le domaine de la *Gouvernance IT* et particulièrement celui de la maturité des outils relatifs à celle-ci.

La première partie de ce rapport est donc consacrée aux fondamentaux de la gouvernance informatique. Vous y découvrirez les origines de ce concept et l'évolution du terme de gouvernance. Nous expliquerons pourquoi et comment la Gouvernance IT intervient dans les organisations.

La deuxième partie est consacrée à l'étude des "outils de gouvernance" développés pour appliquer la Gouvernance IT dans les entreprises. Il s'agit pour la plupart de référentiels de "bonnes pratiques" établis par des chercheurs et des professionnels du domaine. C'est à partir de ces ouvrages que les entreprises peuvent mettre en œuvre à leur tour une véritable Gouvernance IT. Les principaux outils de gouvernance seront décrits et confrontés au système de normalisation auquel le milieu économique et industriel est déjà familier.

La troisième section est dédiée à la mise en place d'une démarche de gouvernance. Elle doit être initiée par une réflexion sur le SI. À l'aide de référentiels et d'outils spécifiques comme des logiciels, les entreprises peuvent mettre en place des processus matures dans le fonctionnement.

1. La Gouvernance IT

Avant de présenter les outils de Gouvernance IT, il est important de savoir concrètement ce qu'est la Gouvernance IT. Il est vrai que ce terme est difficile à décrire précisément puisque celui-ci n'a pas de définition exacte. Pour vous présenter cette notion, nous allons vous présenter ses origines et son évolution pour la placer dans un contexte afin de décrire ce que cache cette notion.

1.1. Les origines de la Gouvernance IT

1.1.1. La place de l'informatique dans l'entreprise

L'informatique dans l'entreprise n'a pas toujours été ce qu'elle est aujourd'hui. Depuis son introduction dans le milieu économique dans les années 1960, l'informatique a occupé une place de plus en plus importante dans le fonctionnement des entreprises. En effet, l'informatique était considérée au début comme un moyen d'automatiser certaines tâches ou d'effectuer des calculs plus rapidement. On recherchait alors à maximiser la performance et la productivité des entreprises. Fort de ce succès, les dirigeants ont continué à implanter de nouveaux systèmes informatiques dans leurs entreprises.

Cependant ce rapport entre l'entreprise et l'informatique a évolué. Autrefois hôtes, on constate que les entreprises sont devenues complètement dépendantes de leurs moyens informatiques. Cette évolution a changé le fonctionnement des entreprises et donc par extension celui de l'économie qui doit intégrer les Technologies de l'Information comme une composante fondamentale de toute activité.

On remarque que les dirigeants ont changé leur façon de diriger leur Système d'Information : il n'est pas rare aujourd'hui de voir qu'ils aient adopté un mode de gestion essentiellement réactif. Le fait qu'ils aient perdu la maîtrise réelle ou supposée de processus qu'ils ont initialement engagé quelques années plus tôt, les amène à se poser la question suivante: "*Comment en est-on arrivé là ?*".

La réponse se trouve peut-être dans le fait que les services informatiques ont pendant de nombreuses années intégré différentes solutions logicielles dans leurs Systèmes d'Informations (SI) et ce afin d'augmenter la productivité de leurs processus métiers. Cependant les problèmes techniques et d'incompatibilités entres ces applications ont souvent mené les Directions de Système d'Information (DSI) à engloutir pendant des années un nombre croissant de ressources afin de répondre à ces besoins. A tel point que les DSI n'ont parfois été considérées que comme des centres de coûts et non pas comme des centres de créations de valeur.

Dans les années 70, le montant des investissements faits pour le développement de l'informatique continue de croître, alors que les bénéfices restent indéterminés et qu'il n'y a pas de réel management de ces ressources. Devant ce constat, de nombreuses organisations ont cherché à rationaliser la gestion des moyens informatiques.

En 1980, le gouvernement britannique commissionne l'agence des télécoms, la *Central Computer & Telecommunication Agency* (CCTA) de définir une librairie des meilleurs pratiques et référentiels afin de confronter leurs systèmes informatiques internes avec ceux disponibles sur le marché. Il s'agit du projet ITIL (*Information Technology Infrastructure Library*). Ce projet existe encore de nos jours, nous le décrirons plus tard avec l'ensemble des référentiels actuels.

Dans les années 90, de nombreux ouvrages décrivent différents dispositifs de management des Systèmes d'Information. En 1992, l'organisme COSO[1] publie un rapport appelé *Internal Control – Integrated Framework*. Puis en 1994, l'association américaine ISACA[2] publie à partir des travaux du COSO la première version de CobiT (*Control OBjectives for Information and Technology*). Ces deux rapports qui seront décrits plus en détails dans la seconde partie deviendront des références dans la maîtrise des risques, le contrôle des objectifs et la gestion des processus informatiques.

Les années 2000 sont marquées par de nombreux scandales dans le milieu financier. À cet égard, de nombreuses compagnies ordonnent des audits de leurs Systèmes d'Information financiers afin d'évaluer la fiabilité de leurs infrastructures informatiques. Il en ressort que le coût global de ces infrastructures peut représenter jusqu'à 40% des coûts de fonctionnement de l'entreprise. Ces dépenses exorbitantes montrent qu'il y a un réel problème de rentabilité des Systèmes d'Information et ce particulièrement à cause des coûts de maintenance. En outre, de nombreux audits révèlent des chiffres qui sont évocateurs de la sous-performance de ces Systèmes d'Information. Par exemple, il en ressort qu'un tiers des projets initiés n'ont jamais abouti et qu'un quart se terminent en dépassant le délai ou le budget. Beaucoup de problèmes sont mis en lumière, notamment à propos de la sécurité ou de la performance des Systèmes d'Information.

Face à ce constat alarmant, il fallait rapidement améliorer l'efficacité des services informatiques et mettre en place des dispositifs de supervision et de contrôle des SI : ce sont les débuts de l'***IT Management***.

[1] COSO : cf. Annexes – Les acteurs de la Gouvernance IT
[2] ISACA (*Information Systems Audit and Control Association):* cf. Annexes – Les acteurs de la Gouvernance IT

1.1.2. L'IT Management: les prémices d'une Gouvernance IT

On pourra définir l'IT Management comme la discipline visant à atteindre les objectifs suivants :

- Assurer une meilleure gestion décisionnelle au niveau du management ;
- Assurer le contrôle de l'activité informatique ;
- Identifier les rôles de chacun des intervenants autour de la DSI ;
- Responsabiliser les employés et prestataires ;
- Garantir la maîtrise des processus.

On note que cette transformation des méthodes de gestion des Technologies de l'Information doit se faire à partir d'une approche privilégiant l'utilisateur, les processus, la technologie et les services. De nombreuses méthodes existent et ont déjà fait leurs preuves. Par exemple, la librairie ITIL sert de base à partir des années 2000 pour les référentiels décrivant les démarches dites de "bonnes pratiques".

1.1.3. De la Gouvernance d'Entreprise à la Gouvernance IT

Les scandales financiers du début des années 2000, menant à la faillite les sociétés Enron et Worldcom ont créé une véritable crise de confiance dans le milieu économique. D'énormes fraudes ont été mises en place avec la complicité des cabinets d'audit qui étaient justement sensés assurer les contrôles financiers de ces entreprises.

Pour faire face à cette crise qui touche le milieu financier américain et afin de rétablir la confiance des investisseurs, les États-Unis ont décidé de renforcer les dispositifs assurant la sécurité financière des entreprises cotées en bourse grâce au *Sarbanes Oxley Act*.

La loi Sarbanes-Oxley (SOX) officialise alors sur le territoire américain l'application des règles de la *Corporate Governance* (gouvernance d'entreprise). Les premiers principes de ce concept ont en effet été définis en Angleterre en 1992 grâce au rapport de la commission Cadbury. Cette notion désigne l'ensemble des processus, réglementations, lois et institutions influant sur la manière dont l'entreprise est dirigée, administrée et contrôlée.

En imposant un tel dispositif, Sarbanes-Oxley redéfinit les règles de fonctionnement et de gestion des entreprises. Ces changements impactent indirectement les infrastructures IT sur lesquelles reposent ces organisations comme le montre la figure suivante.

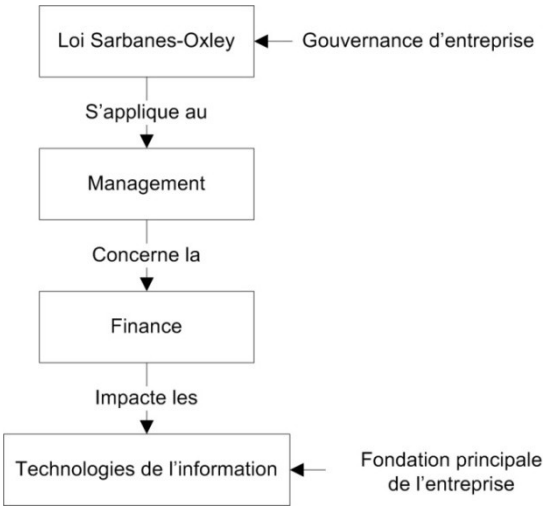

Figure 1 : Le dispositif de Gouvernance d'Entreprise impacte les ressources IT (source : IT Gouvernance, Frédéric Georgel, Éditions Dunod, 2ème édition, p.23)

C'est donc en référence à la gouvernance d'entreprise que les méthodes de l'IT Management ont progressivement vu changer leur nom pour s'appeler la "Gouvernance IT" ou "*IT Governance*".

1.1.4. Quelle législation pour la Gouvernance IT ?

Les scandales financiers de 2001 ont été à l'origine d'un renforcement de la législation en matière de gouvernance d'entreprise. Nous avons vu que celle-ci a eu un impact indirect sur les SI. Après, la crise bancaire et financière dite des *subprimes*, on aurait pu s'attendre à un renforcement de la réglementation pour prévenir une nouvelle crise de cette nature.

Il n'existe pas de loi portant sur la gouvernance IT en tant que telle. C'est pourquoi dans notre démarche de description du cadre législatif, on s'intéresse aux réglementations sur le gouvernement d'entreprise. Nous allons donner un aperçu des textes incontournables qui impactent le SI.

1.1.4.1. Une première réponse : Sarbanes-Oxley

Intéressons nous d'abord à la loi phare, connue comme être à la naissance de la Gouvernance IT.

Les sénateurs Paul Sarbanes et Mike Oxley rédigent en 2002 une loi qui porte leurs noms : la loi Sarbanes-Oxley aussi communément appelée *SOX*. Votée à la quasi-unanimité par le congrès et le sénat américain le 25 Juillet 2002, elle est officiellement promulguée le 30 juillet 2002. Cette loi cherche à renforcer la qualité de la communication financière afin de rétablir la confiance du public, des épargnants et des investisseurs. Ce dispositif législatif concerne la régulation des investissements et s'articule autour de plusieurs objectifs :

- Responsabiliser davantage les dirigeants ;
- Garantir un meilleur accès à l'information et amélioration de la fiabilité ;

- Mettre en place des comités de vérification indépendants, chargés de superviser les processus de vérification ;
- Instaurer un organisme de réglementation et de surveillance : le PCAOB (*Public Company Accounting Oversight Board*). Il est en charge de contrôler les entreprises d'audit comptable.

Une des grandes spécificités de cette loi est son caractère extraterritorial. Les États-Unis exigent que toute entreprise cotée aux États-Unis respecte cette loi, qu'elle soit américaine ou non. Ainsi, plus de 300 entreprises françaises enregistrées auprès de la SEC (*Securities and Exchange Commission,* organisme fédéral américain de réglementation et de contrôle des marchés financiers) sont concernées.

La loi comporte soixante six articles qui portent globalement sur les dispositifs de contrôle et la régulation des instances des entreprises. Parmi ceux-ci, quatre concernent directement les départements IT, dont voici les grandes lignes :

- La gestion des documents traités dans le SIF[3] de l'ERP[4] doit fournir des protocoles d'audit afin d'avoir une visibilité claire des données financières ;
- Les sociétés doivent documenter et évaluer (annuellement) l'ensemble des dispositifs de contrôle interne impliqués dans les risques opérationnels. Ces dispositifs de contrôle s'appliquent donc à l'ensemble du SI ;
- Le SIF de l'ERP doit être en mesure de gérer les flux d'informations de façon immédiate afin d'offrir une visibilité et un contrôle en temps réel ;
- La gestion des documents dans le SI doit offrir des garanties d'intégrité, de complétude et de traçabilité des données.

1.1.4.2. Le volet français : la Loi de Sécurité Financière (LSF)

En France, un an après l'apparition du *Sarbanes-Oxley Act* et après la publication des travaux du groupe de travail présidé par Daniel Bouton (rapport Bouton), c'est au tour de la loi de Sécurité Financière d'être promulguée le 1er Aout 2003.

Tout comme *Sarbanes-Oxley*, LSF œuvre pour la transparence de l'activité de l'entreprise vis-à-vis de ses actionnaires. Pour cela, LSF entérine d'abord la création de l'Autorité des Marchés Financiers. Elle est le résultat de la fusion de trois anciens organismes français de contrôle des marchés financiers. Les deuxième et troisième volets portent sur la sécurité des épargnants et des assurés, et sur le contrôle légal des comptes.

Le président du conseil d'administration d'une entreprise devra présenter à l'assemblée annuelle des actionnaires, en plus du rapport habituel de gestion, un rapport concernant les procédés de contrôle interne mis en place par la société.

[3] Système d'Information Financier
[4] Enterprise Resource Planning : cf. Glossaire

Selon la Compagnie nationale des Commissaires aux Comptes, le contrôle interne est "l'ensemble des politiques et procédures mises en œuvre par la direction d'une entité en vue d'assurer, dans la mesure du possible, la gestion rigoureuse et efficace des activités. Ces procédures impliquent la respect des politiques de gestion, la sauvegarde des actifs, la prévention et la détection des fraudes et des erreurs, l'exhaustivité et l'exactitude des enregistrements comptables et l'établissement en temps voulu d'informations comptables et financières fiables".

L'étude de SOX et LSF montre que les seules contraintes au niveau du Système d'Information sont d'une part la mise en place ou le renforcement des contrôles financiers internes et d'autre part la mise en place d'un système de gestion des risques.

Le référentiel COSO est considéré par la SEC comme suffisant pour répondre aux exigences de contrôle interne de SOX. De même, les cabinets d'audit français considèrent COSO comme satisfaisant au vu de la réglementation française.

On peut retenir qu'une partie des entreprises choisissent d'implémenter les recommandations décrites dans le référentiel COSO et ce à cause du caractère extraterritorial de SOX. A l'instar de Sarbanes-Oxley, LSF impose aux entreprises françaises cotées en bourse de voir leurs applications informatiques financières être réglementées.

Utilisé avec COSO, le référentiel CobiT suffit à répondre aux exigences réglementaires. On retrouve fréquemment la configuration suivante :

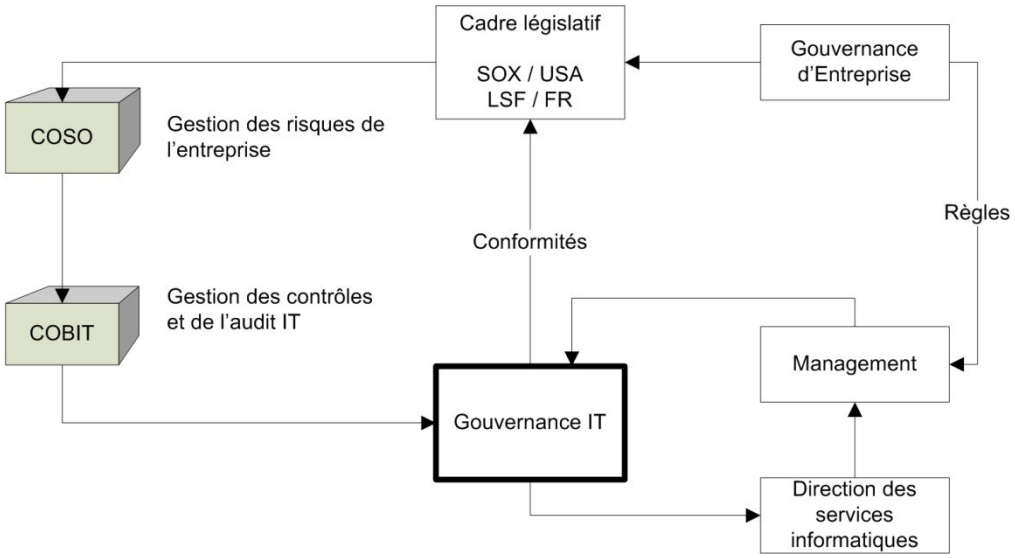

Figure 2 : Schéma de l'IT Gouvernance dans sa forme primitive
(source : IT Gouvernance, Frédéric Georgel, Éditions Dunod, 2ème édition, p.25)

Les scandales financiers et l'effet d'annonce de cette législation ont été un électrochoc qui a permis une prise de conscience de l'importance du SI pour l'activité de l'entreprise. Après les premières découvertes de fraudes financières, les actionnaires ont exigé des dirigeants des audits complets de leur entreprise. Dans de nombreuses entreprises, ces audits ont mis en lumière la "sous-performance" de leur SI et une rentabilité parfois limitée.

La législation a initié les entreprises à la gouvernance IT. C'est ensuite les entreprises elles-mêmes qui ont cherché à répondre à leurs problèmes en collaborant à la rédaction de référentiels de bonnes pratiques IT. On appelle ces derniers ouvrages les "outils de la gouvernance".

1.2. Les domaines stratégiques de la Gouvernance IT

Plusieurs études ont permis d'identifier des axes de travail principaux en matière de Gouvernance IT. Aujourd'hui, il n'existe toujours pas de consensus global quant à la question du nombre de ces domaines stratégiques. Deux courants dominent aujourd'hui dans le monde.

Celui de l'ITGI[5] qui identifie cinq domaines stratégiques qui ont été intégrés à CobiT V4.

L'autre, défini par des chercheurs indépendants et spécialistes de la gouvernance, issu de l'AIS (*Association for Information Systems*) propose une version étendue avec huit domaines stratégiques.

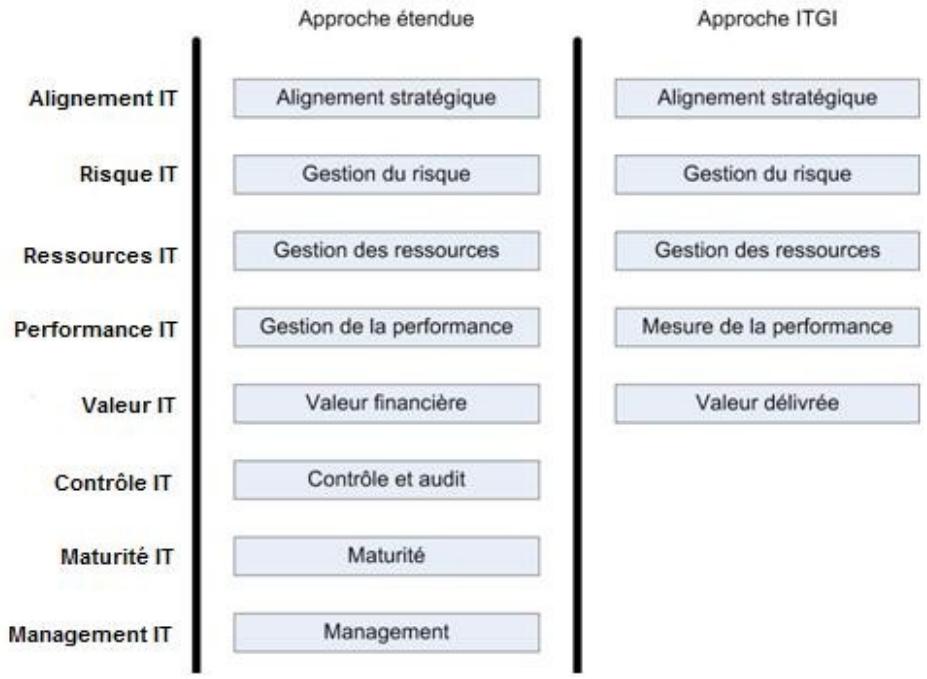

Figure 3: Domaines stratégiques de la Gouvernance IT
(source : IT Gouvernance, Frédéric Georgel, Éditions Dunod, 2ème édition, p.27)

[5] IT Governance Institute : cf. Annexes – Les acteurs de la Gouvernance IT

Nous choisirons de décrire ces différents domaines d'application selon l'approche étendue. En effet, celle-ci est plus complète et reste compatible avec celle de l'ITGI.

Ces domaines stratégiques permettent d'évaluer le degré de mise en place de la Gouvernance IT au sein d'une organisation. Pour évaluer celle-ci, on attribue une note que l'on appelle communément "niveau de maturité" pouvant aller de 0 à 5 pour chacun de ces axes d'analyse.

Voici les niveaux de maturité correspondants:

- 0 : Inexistant ;
- 1 : Prise de conscience ;
- 2 : Début de mise en œuvre ;
- 3 : Formalisation ;
- 4 : Pilotage ;
- 5 : Optimisation.

On appelle "IT Scorecard", le schéma représentant la maturité de la gouvernance d'une entreprise. Nous allons maintenant présenter chacun des ces domaines stratégiques.

1.2.1. L'alignement stratégique : créateur de valeur

Il est nécessaire que le Système d'Information, la stratégie et la structure de l'entreprise soient cohérents. C'est à la DSI de mettre tout en œuvre afin que le SI s'adapte à ces deux dernières. Il existe deux niveaux d'alignement devant être réalisés de manière simultanée :

L'alignement des SI sur la stratégie de l'entreprise créé de la valeur. Pour se faire, les services informatiques doivent connaître les objectifs stratégiques de l'entreprise, notamment grâce aux plans de moyen et long terme de l'entreprise. Cet alignement stratégique ne provoquera aucun bénéfice si la politique stratégique de l'entreprise n'est pas cohérente.

D'autre part, on peut considérer un alignement stratégique sur les *Business Process*. Dans ce cas, il s'agit d'aligner les Systèmes d'Information sur les processus découlant des différentes activités de l'entreprise, on les appelle les *processus métiers*. Le service informatique devra ainsi posséder une cartographie de l'ensemble de ces processus métiers.

Dans les deux cas, la DSI devrait être informée de tout changement, que ce soit une modification de la stratégie de l'entreprise ou de la modification d'un des *Business Process*. Il est préférable que l'information soit communiquée à la DSI sans qu'elle n'en fasse la demande, afin que la DSI soit en mesure d'une réactivité complète.

1.2.2. La gestion des risques : une activité incontournable

Désormais, l'entreprise se base intégralement sur son Système d'Information pour atteindre ses objectifs. Se protéger contre les risques IT est une activité incontournable pour maintenir la capacité opérationnelle de l'entreprise.

Au sein de l'entreprise, la gestion des risques dépend du Comité du *Team Risk Management* (TRM), Ce comité s'intéresse à tous les risques de l'entreprise et n'est pas dédié au seul département informatique. Le TRM dépend généralement de la direction en charge de la stratégie. La gouvernance doit se baser sur les mêmes critères du TRM et adopter une gestion collaborative avec les directions clés de l'entreprise : finance, commerce, production, etc…

L'identification des risques

Les risques humains sont les plus importants et les plus dangereux. L'espionnage industriel et la criminalité informatique (destruction et vols d'informations, fraude, vol d'équipements,..) peuvent représenter à eux seules 75% des pertes et proviennent essentiellement de personnels internes aux entreprises. Le taux de criminalité informatique augmente d'un facteur de 3 à 9 en cas de crise sociale (plan de licenciement, liquidation judiciaire). L'erreur humaine est aussi une source de risque. Ces erreurs peuvent être des erreurs de compréhension, d'usage, de choix ou de conception.

Les risques technologiques qui comprennent les dysfonctionnements d'un composant de l'infrastructure IT peuvent perturber un ou plusieurs services. Les causes les plus fréquentes de dysfonctionnements sont des erreurs dans la phase d'intégration, des problèmes liés au fonctionnement d'un composant, des dysfonctionnements suite à des mises à jour, des pannes sur des équipements non sécurisés.

On peut aussi s'intéresser aux risques naturels. Il s'agit de s'assurer contre les risques climatiques. Les principaux risques sont l'inondation et la foudre, qui sont tout deux en augmentation et qui sont potentiellement dangereux pour les infrastructures. Le gel et la canicule sont liés aux systèmes de climatisation.

L'évaluation des risques

Elle permet de définir les priorités d'actions. Il est indispensable de connaître le niveau de tolérance et d'impact de chaque métier de l'entreprise face à chaque risque. L'évaluation peut ainsi prendre en compte le taux de probabilité et le degré d'impact du risque.

La réduction des risques

Un risque lié à un composant dépend de son cycle de vie. Les cycles de transition ont un coefficient de risque élevé par rapport aux cycles d'exploitation qui sont eux très faibles.

Pour chacune des menaces, il est possible d'envisager plusieurs scénarios de réponse. Le but est de faire la balance entre le coût de chacune des réponses et le coût des conséquences de la menace sur l'entreprise pour trouver une solution adaptée. En outre, un scénario de réponse comporte lui-même des risques résiduels, ceux-ci peuvent donc aussi faire l'objet de scénarios de réponse.

1.2.3. La gestion des ressources pour plus d'efficacité

Les ressources IT sont de toute évidence les composants technologiques (matériels et logiciels) qui constituent le Système d'Information, mais ce sont aussi les ressources humaines liées au service informatique.

Composants technologiques

La DSI devra assurer un management stratégique des ressources. Cela correspond à établir une architecture des ressources convenant à la structure et à l'activité de l'entreprise. Il existe plusieurs cadres (*Framework*) permettant d'organiser et de représenter une architecture des ressources informatiques d'un organisme. Le premier cadre d'architecture d'entreprise apparu est le *Zachman Framework for Entreprise Architecture.* Les modèles du DoDAF (*Department of Defense Architecture Framework*) ou du MODAF (*Ministry of Defense Architecture Framework*) originaires du milieu militaire dérivent de lui. Un autre cadre largement employé est le TOGAF (*The Open Group Architectural Framework*).

Le Management proactif des ressources consiste à anticiper les besoins en ressources. L'urbanisation de SI, appelée aussi « consolidation applicative » est une solution pour prévoir efficacement les futurs besoins de chaque service. Cette anticipation permet d'éviter de réaliser des investissements en ressources inutiles sans pour autant connaître des situations où les ressources seraient saturées. Ainsi, les investissements ne pourront pas avoir un caractère urgent et s'ouvrent des marges de négociations avec les différents fournisseurs de composants matériels. Le management proactif permet par conséquent de diminuer les coûts liés aux services informatiques.

Le Management actif des ressources est effectué grâce aux retours d'informations des consommateurs des services fournis. Le support technique ou *Help Desk* [6]permet d'obtenir ce *feedback*[7] utilisateur. Cela permet de mesurer la fiabilité de chaque service et même au niveau des composants de ces services. Ce management actif passe aussi par le management des sauvegardes. Le volume de données circulant dans l'entreprise a explosé et entraîne un accroissement massif des systèmes de stockages. Ces volumes peuvent atteindre des Téraoctets voire des Pétaoctets de données. Ce stockage coûte alors de plus en plus cher pour les organisations. Une solution serait de cibler les informations pertinentes à archiver et de se débarrasser des données relevant de la "pollution" (*Data Pollution Factor*, DPF). Ces données parasites peuvent être filtrées assez aisément.

Ressources humaines

Les hommes et les femmes impliqués dans le développement et la maintenance du Système d'Information sont de toute évidence encadrés et recrutés par le service des Ressources Humaines (RH). Ces derniers ne sont pas experts concernant le recrutement IT.

[6] Littéralement "bureau d'aide". Désigne le service d'assistance aux utilisateurs
[7] Retour d'expérience

Pour la DSI, il s'agit de collaborer avec la DRH[8] pour que ses besoins soient compris du mieux possible.

1.2.4. La gestion de la performance

Dans un premier temps, il est nécessaire d'établir un certain nombre d'indicateurs permettant d'évaluer la performance de chaque activité au sein même du service informatique et notamment la performance des services délivrés. Il est possible de mesurer le taux de fiabilité de chaque service et le taux de satisfaction des utilisateurs. Comme pour la gestion des ressources, le *Help Desk* est une source d'information potentielle.

1.2.5. La valeur financière : des indicateurs de rentabilité

L'informatique permet d'échanger et de traiter très rapidement un grand nombre d'informations sans erreur. Du point de vue des utilisateurs de ces applicatifs métiers, les bénéfices sont évidents. Un grand nombre de tâches peuvent être littéralement automatisées. Les tâches où une présence humaine est indispensable peuvent être grandement facilitées. L'informatique diminue par ailleurs les taux d'erreur. Ces gains de temps augmentent la productivité et la rentabilité des activités de l'entreprise. Mais en contrepartie, ces solutions métiers représentent de réels investissements. Il faut aussi incorporer les coûts de maintenance et coûts induits par l'infrastructure matérielle.

La valeur IT consiste à comparer les économies réalisées à l'aide du SI pour l'organisation par rapport aux coûts d'investissement et d'exploitation inhérents au Système d'Information.

Ce domaine spécifique de la gouvernance est primordial. C'est ce domaine qui justifie la place prédominante des technologies dans l'entreprise. Il faudra montrer aux dirigeants et actionnaires des entreprises que l'informatique n'est pas un *centre de coût* mais une véritable activité de *création de valeur*.

Les indicateurs T(x)O sont employés pour évaluer les systèmes existants. Ils prennent en compte les éléments clés constituant des ressources IT au sein d'une organisation. Chaque indicateur prend aussi en considération les niveaux directs et indirects. On peut les classer en fonction de leur importance, de la manière suivante :

- TCO : *Total Cost of Ownership* (coût total de possession) ;
- TBO : *Total Benefit of Ownership* (bénéfice total de possession) ;
- TRO : *Total Risk of Ownership* (risque total de possession) ;
- TVO : *Total Value of Ownership* (valeur totale de possession).

D'autres indicateurs existent notamment pour permettre de calculer la rentabilité d'investissements. Pour permettre de mieux mesurer et de maximiser le retour sur investissements portant sur les technologies de l'information, l'ISACA en 2006 a publié le référentiel *ValIT*.

[8] Direction des Ressources Humaines

1.2.6. Le contrôle et l'audit

L'audit et le contrôle ne sont pas réservés uniquement au domaine comptable. Les règles de gestion financière, SOX[9] et LSF[10] imposent à l'entreprise une mise en œuvre de plus en plus normative des dispositifs de surveillance dont le but est d'offrir un niveau de garantie maximum vis-à-vis des informations financières. COSO et COBIT sont les référentiels clés dans le management du contrôle et de l'audit. Leur application permet de respecter les règles issues de LSF.

1.2.7. La maturité des processus

La maturité est la capacité d'une organisation, qu'elle soit à caractère public ou privé, d'engager des politiques de changement afin de s'adapter aux variations qui lui sont imposées par son environnement.

	Entreprise immature	Entreprise mature
Processus	Improvisés en fonction des demandes	Définis, contrôlés, documentés, supportés, exploités
Personnel	Stress permanent	Qualité de vie plus importante
Coût, Délais, Qualité	Imprévisible	Prévisible
Réussite	Individuelle et hors processus	Collective dans le cadre de processus
Technologie	Mal maîtrisée, mal adaptée	Alignée sur les besoins et les objectifs
Changement	En dernière extrémité	En continu
Management	Par crise, au fil de l'eau	Par anticipation

Figure 4 : Caractéristiques clés de la maturité d'une organisation,
(source : IT Gouvernance, Frédéric Georgel, Éditions Dunod, 2ème édition, p.146)

Une entreprise mature fonctionne donc à l'aide d'un ensemble de processus qu'elle maîtrise. On parle alors de maturité des processus.

Nous détaillerons un modèle de maturité dans la partie consacrée au référentiel CMMi.

1.2.8. Le management de l'entreprise impliqué

Il est indispensable pour la DSI d'identifier les rôles de chacun des intervenants autour du Système d'Information. Dans toutes les entreprises, des solutions informatiques sont présentes pour chaque activité métier, mais très peu d'entre elles pensent à évaluer la performance des managers. Il est notamment possible de comparer leurs résultats à leurs objectifs initiaux. De nombreuses entreprises mettent en place certains comités et groupes de travail afin d'assurer une gouvernance de leur service IT.

Dans une entreprise, les membres du *Conseil de la Gouvernance* sont nommés en Conseil d'Administration par les actionnaires ou par les administrateurs. Il est composé au minimum de trois membres dont au moins un tiers ne fait pas partie des structures dirigeantes de l'entreprise. Le Conseil décide des règles à appliquer et rend des comptes au Conseil d'Administration. Il choisit les membres du *Comité de la Gouvernance*.

[9] Loi Sarbanes-Oxley : cf. Glossaire
[10] Loi de Sécurité Financière: cf. Glossaire

Le Conseil est responsable de la conformité des ressources technologiques vis-à-vis des dispositifs réglementaires (SOX, LSF,…). Il doit aussi rendre compte de la gestion des Technologies et de l'Information aux actionnaires.

Le *Comité de la Gouvernance* doit prendre en charge :

- L'organisation et la gestion des audits ;
- La rédaction des rapports d'activités pour le Conseil ;
- Le contrôle de gestion ;
- La gestion des domaines stratégiques ;
- La gestion des capacités organisationnelles ;
- La coordination des groupes de travail ;
- La mise en œuvre et l'évaluation des dispositifs de conformité ;
- Le management des projets grâce à l'arbitrage par portefeuille.

Le *Comité de la Gouvernance* (CGIT) met en place des groupes de travail pour répondre à ses missions. Ces groupes peuvent être permanents ou exister de manière temporaire pour des missions spécifiques.

Le *Comité de la Gouvernance* tient à jour un catalogue de services IT disponibles. Il centralise les différents besoins des acteurs de l'entreprise qui ne sont pas satisfaits et les intègre dans le portefeuille de projets avec une priorité spécifique.

Cette priorité est attribuée en fonction d'un certain nombre de critères. Le choix est fait en fonction du gain en performance potentiel, des risques liés au projet, du coût total du projet, de l'urgence du besoin, etc. Un projet sera retenu si son intérêt est démontré pour le groupe et pas seulement pour le seul bénéfice d'une *Business Unit* ou d'un service.

2. Les outils de gouvernance IT

Nous allons maintenant nous intéresser à ce que l'on appelle les outils de la gouvernance IT. Il s'agit de l'ensemble des outils au sens des instruments à notre disposition pour mettre en place une bonne gouvernance IT. Il s'agit dans un premier temps des référentiels de bonnes pratiques. Ces ouvrages recensent des témoignages de DSI et des thèses de professionnels afin de capitaliser ces expériences en valeur pour la DSI. Notre étude porte sur les référentiels considérés comme les plus importants. On commencera par parler bien évidemment du référentiel ITIL, considéré comme le référentiel à adopter, puis de son adaptation aux petites organisations. On continuera avec CobiT, la référence pour l'audit et le contrôle des systèmes d'informations. La suite concernera le modèle pour le développement des logiciels CMMi. Le référentiel eSCM, modèle pour la gestion de la relation client-fournisseur, sera aussi abordé avant de parler de Six Sigma qui lui apporte une approche statistique pour la gouvernance. Ce dernier met en avant sa complémentarité avec le référentiel ITIL. Enfin, nous verrons le projet FUSING pour finir en s'interrogeant sur l'avenir des référentiels.

2.1.Les principaux référentiels de Gouvernance

2.1.1. ITIL, la référence incontestée

ITIL (*Information Technology Infrastructure Library* pour "Bibliothèque pour l'infrastructure des technologies de l'information") est un ensemble d'ouvrages recensant des bonnes pratiques pour la gestion des services informatiques, édictées par l'Office public britannique du Commerce (OGC). Concrètement ITIL se présente sous la forme de livres décrivant des processus qui, si une entreprise les adopte, permettent une bonne gestion de son système d'information.

Au départ, vers la fin des années 1980, ITIL dans sa première version était un ensemble de 40 à 50 livres qui recensait les bonnes pratiques en matière de gouvernance d'un système d'information.
Au début des années 2000, ITIL a été restructuré sous forme de 7 à 8 livres fondamentaux. Dans cette deuxième version, le cœur d'ITIL (2 livres) correspond aux processus de fourniture et de soutien des services informatique.
En 2004, le projet *ITIL Refresh* est lancé et celui va aboutir à la publication en 2007 de la version 3 du référentiel. Cette fois-ci les différents acteurs de part le monde utilisant ITIL ont réfléchi ensemble et proposé des améliorations à la version précédente. Ceci permet une meilleure compréhension et une mise en place du référentiel facilitée dans les entreprises de différents métiers.

La DSI, une SSII interne

Pour ITIL, une DSI est assimilable à une Société de Service en Ingénierie Informatique (SSII) qui fournit des services tant aux différentes composantes de l'entreprise, qu'aux clients et autres partenaires de l'entreprise. Le référentiel est composé d'un ensemble de processus à mettre en place pour permettre le bon déroulement de chacun des phases du cycle de vie d'un processus.

Ces phases sont :

- Spécification ;
- Fabrication ;
- Déploiement ;
- Exploitation.

ITIL V2

La version 2 d'ITIL est actuellement la version la plus utilisée dans les entreprises. Dans cette version d'ITIL le découpage est organisé par rapport aux processus. Les processus de gouvernance sont regroupés par domaine. A chaque domaine correspond un livre décrivant les processus. Les domaines couverts par ITIL V2 sont :

- Fourniture de services : il s'agit de structurer, séquencer le service tout au long du cycle de vie ;
- Le Soutien des services : processus pour maîtriser la mise en place et le support des services ;
- La perspective "métier" : il s'agit de la stratégie globale des services vis à vis de l'entreprise et donc de son métier ;
- La gestion des TIC : processus permettant de mettre en place une structure d'accueil la plus flexible possible pour les services ;
- La gestion des applications : processus pour le bon déroulement du cycle de vie du développement d'un logiciel ;
- La planification de la mise en place de la gestion des services ;
- La gestion de la sécurité.

Le cœur d'ITIL correspond aux deux ouvrages décrivant les processus de gestion des services c'est à dire :

- La Fourniture des services avec les processus :
  - La gestion du niveau de service ;
  - La gestion de la disponibilité ;
  - La gestion de la capacité ;
  - La gestion de la continuité du service ;
  - La gestion du financement des services.
- Le Soutien des services avec les processus :
  - Le centre de services ;
  - La gestion des incidents ;
  - La gestion des problèmes ;

- La gestion des configurations ;
- La gestion des changements ;
- La gestion des mises en production.

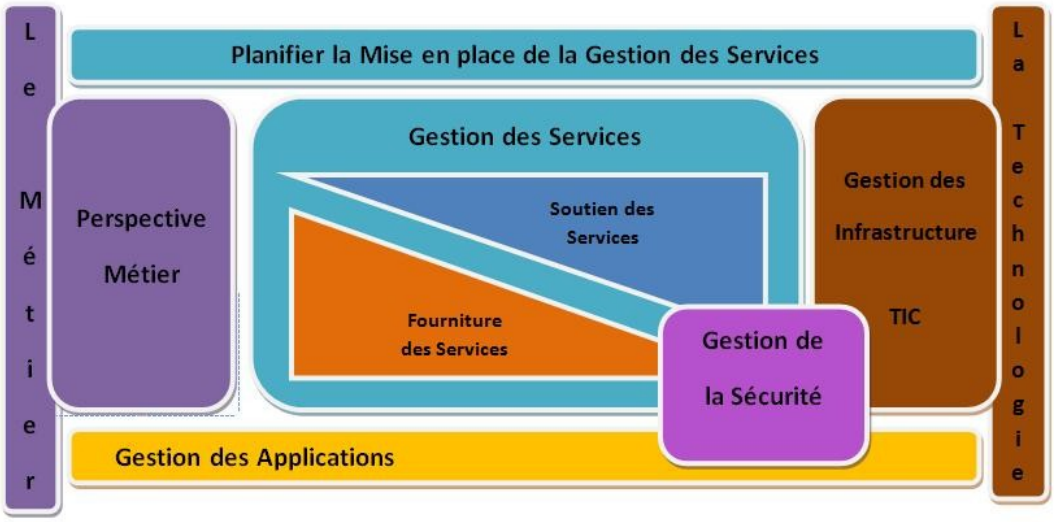

Figure 5: ITIL V2
(source : Podcast vidéo ITILV3, Vincent Douhairie, SupInfo)

ITIL V3 : une vision plus complète

ITIL, dans sa deuxième version, a été un vrai succès et a très vite été adopté par une multitude d'entreprises dans de nombreux pays. Avec le temps les entreprises ayant mis en place ITIL ont commencé à chercher à l'améliorer. C'est pourquoi en 2004 est lancé le projet *ITIL Refresh* dans le but de faire évoluer ce référentiel. De nombreuses entreprises et industries de part le monde vont alors participer à ce projet sous forme de forum et donner leur avis sur ITIL. Les buts recherchés à travers ce projet sont :

- Apporter plus de facilité à la mise en place d'ITIL ;
- Permettre une meilleure adaptation des processus au métier de l'entreprise ;
- Améliorer la structure des processus en incluant des exemples pour chacun d'eux ;
- Faire des liens avec les autres référentiels notamment CobiT.

Le projet *ITIL Refresh* a abouti à la publication en 2007 d'ITIL version 3. Cette nouvelle version d'ITIL comprenant 5 livres de base est organisée autour des services informatiques et non plus autour des processus. Chaque livre correspond désormais à une étape du cycle de vie d'un service informatique.
Au centre de la roue formée par ITIL V3 (figure 13), on retrouve le premier livre sur la stratégie des services c'est à dire la stratégie permettant de fournir des services créateurs de valeur.

Autour, nous avons ensuite les trois livres correspondant aux grandes phases de la vie d'un service : la conception du service, la transition, et les opérations sur le service. Enfin nous trouvons autour de ceci la partie Amélioration continue du service informatique.

Le dernier cercle correspond à des compléments au référentiel qui vont permettre d'adapter celui-ci au métier de l'entreprise pour une mise en place personnalisée d'ITIL.

Figure 6: ITIL V3
(source : Podcast vidéo ITILV3, Vincent Douhairie, SupInfo)

ITIL encore plus adoptée grâce à V3

En termes de tendances d'adoption on peut observer deux groupes. Le premier tend à déployer les processus ITIL touchant directement les équipes opérationnelles, notamment ceux concernant la gestion des incidents et des problèmes. Le second opte pour un déploiement global d'ITIL.

Pour la 3ème version, l'année 2008 compte 14% des entreprises européennes (source : IDC) qui auraient démarré la mise en place de cette mouture, contre 26% au États-Unis. Selon l'ensemble des sociétés de conseil et des SSII du marché, aujourd'hui quasiment 100 % des grands comptes sont engagés dans une démarche ITIL (avec évidemment des degrés d'avancement divers). Il faut rappeler ici que le référentiel ITIL engage les entreprises dans une démarche de longue haleine. En effet, il faut compter environ cinq ans pour parvenir à un rythme de croisière.

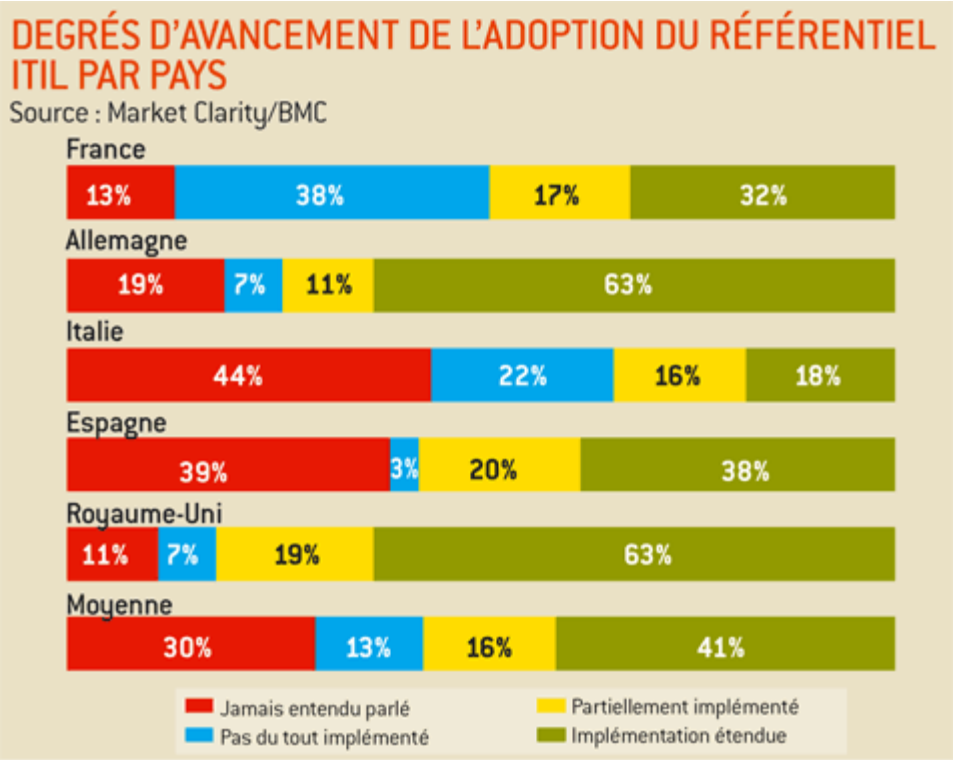

Figure 7 : Degrés d'avancement de l'adoption du référentiel ITIL par pays (source : www.bonneaud.net) - Janvier 2007

En France, on remarque que 38% des DSI n'ont pas du tout implémenté ITIL, les DSI n'étant pas convaincus par son apport en matière de qualité ou étant réticents face à sa complexité. On peut prévoir qu'une grande partie de ces DSI vont adopter ITIL car la version 3 est améliorée et plus simple à mettre en œuvre.

40% des DSI italiens et espagnols n'ont pas connaissance d'ITIL. L'effet d'annonce suite à la publication de la V3 va permettre de mieux faire connaître le référentiel auprès de ces publics.

ITIL et les PME

Nous allons voir dans quelles mesures ITIL est adapté aux petites structures. ITIL traite de deux axes principaux qui sont l'orientation "client" par la gestion des services ainsi que la démarche d'amélioration de la qualité avec la mise en place de processus. L'objectif final est la réduction des coûts. ITIL permet de s'appuyer sur des expériences partagées afin d'éviter les erreurs fréquentes et permet ainsi de ne pas tout repenser. Toute entreprise y trouve donc son intérêt et ceci peu importe sa taille. On en déduit qu'ITIL peut donc être un outil intéressant pour les PME/PMI.

De plus, les PME possèdent des avantages par rapport aux grandes organisations qui leur permettent une intégration plus facile et plus rapide du référentiel ITIL. Du fait de leur taille réduite, les PME sont capables de s'adapter plus facilement au changement en mobilisant des ressources impliquées. De plus, leurs faisceaux de communication raccourcis permettent une meilleure perception des résultats de l'utilisation des meilleurs pratiques dans de très courts délais.

A l'inverse, il convient de nuancer cette réponse du fait qu'ITIL est une boîte à outils contenant les meilleurs pratiques qui peut s'avérer trop lourde pour ces petites organisations. Des compromis doivent être réalisés car leurs ressources sont plus limitées. Ainsi, la mise en œuvre d'ITIL nécessite la plupart du temps de s'adapter à l'environnement cible, en simplifiant énormément certains processus. C'est pourquoi, les responsables dans les petites organisations excluent souvent ITIL car ils le considèrent trop complexe et consommateur de ressources. C'est d'ailleurs une des raisons du lancement de FUSING, cadre de référence adapté au PME/PMI (cf. FUSING).

2.1.2. CobiT, la référence pour l'audit

Le référentiel CobiT [11]est un modèle développé, mis au point et fourni par l'ISACA[12] qui permet de contrôler les objectifs et de manager les processus de l'IT. Il s'inscrit ainsi dans une logique de contrôle et d'audit.

Créée en 1967, l'ISACA est une association dont le rôle est de définir des processus d'audit et de contrôle dans les systèmes d'informations. Elle est représentée en France depuis 1982 par l'AFAI[13].

Depuis sa première version publiée en 1994, le CobiT connait de nombreuses mises à jour grâce aux retours d'expériences quasi-systématiques de la part des adhérents de l'ISACA :

- 1994 : publication de la première version du CobiT ;
- 1998 : établissement de l'*IT Governance Institute* (ITGI). CobiT passe en version 2 ;
- 2001 : publication de la version 3 du CobiT ;
- 2003 : publication de "*IT Control Objectives for Sarbanes-Oxley*" ;
- 2005 : mise à jour du CobiT en version 4.

A ce jour CobiT est disponible en version 4.1.

Le principal objectif du référentiel CobiT est de répondre aux besoins de l'entreprise. Pour cela, CobiT va fournir un ensemble de moyens pour gérer les niveaux de contrôle qui doivent être exercés sur les ressources IT. Par le contrôle, CobiT organise l'alignement entre les objectifs, les besoins des différents corps de métier, ainsi que les moyens techniques mis en œuvre.
CobiT est donc considéré comme le socle de la gouvernance des SI et est devenu l'intégrateur des meilleures pratiques en technologies de l'information qui aide à comprendre et à gérer les risques.

Le référentiel CobiT s'adresse aux 3 acteurs principaux de l'entreprise à savoir le management, les utilisateurs et les auditeurs.

[11] Control Objectives for Information and related Technology
[12] Information Systems Audit and Control Association : cf. Annexes – Les acteurs de la Gouvernance IT
[13] Association Française de l'Audit et du conseil Informatique : cf. Annexes – Les acteurs de la Gouvernance IT

CobiT est utilisé pour le management comme moyen d'aide à la décision en estimant précisément le niveau de risque que l'entreprise peut supporter pour aligner les ressources IT sur le plan financier, organisationnel et technologique.
Les utilisateurs peuvent avoir grâce à CobiT une garantie sur la sécurité et les contrôles des SI. Enfin, les auditeurs l'utilisent car il leur permet une analyse plus facile mais aussi plus efficace étant donné que CobiT leur proposent des moyens d'interventions reconnus.

Le référentiel CobiT est structuré autour de 8 thèmes. Chacun est présenté sous forme de guide ayant pour but d'apporter des réponses aux différents enjeux induits par la gestion de l'alignement des ressources IT sur les objectifs fondamentaux de l'entreprise :

- Synthèse (*Executive Overview*) ;
- Cadre de référence (*Framework*) ;
- Objectifs de contrôle (*Control Objectives*) ;
- Pratiques de contrôle (*Control Practices*) ;
- Guide management (*Management Guidelines*) ;
- Guide de l'assurance IT (*IT Assurance Guide*) ;
- Guide de l'implémentation de la Gouvernance IT (*IT Governance Implementation Guide*) ;
- Objectifs de contrôle IT pour SOX (*IT Control Objectives for Sarbanes-Oxley*).

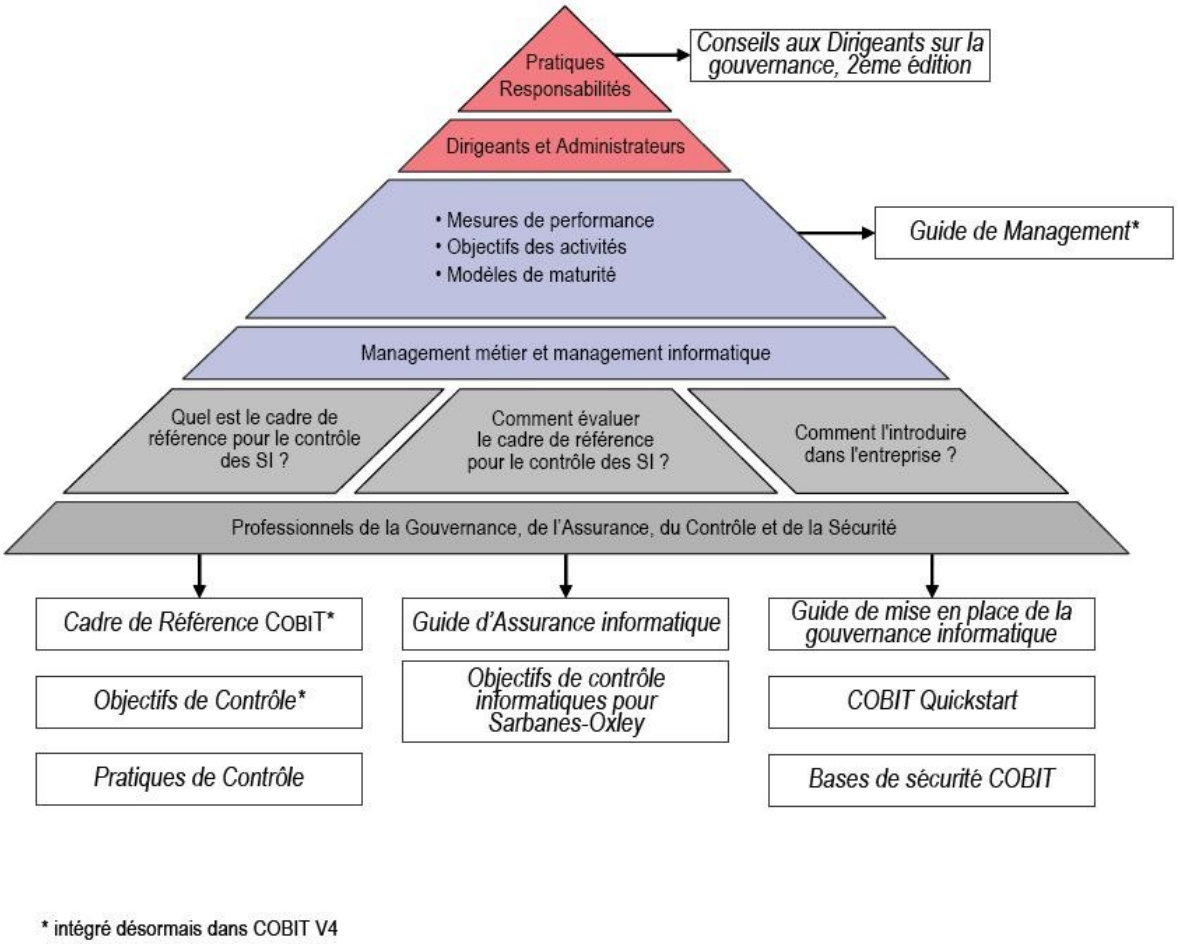

Figure 8 : Produits CobiT (source : www.afai.fr)

Tous ces thèmes sont reliés entre eux et visent à répondre aux besoins de gouvernance, de gestion, de contrôle et d'audit de différents acteurs, comme on le voit sur la figure 6.

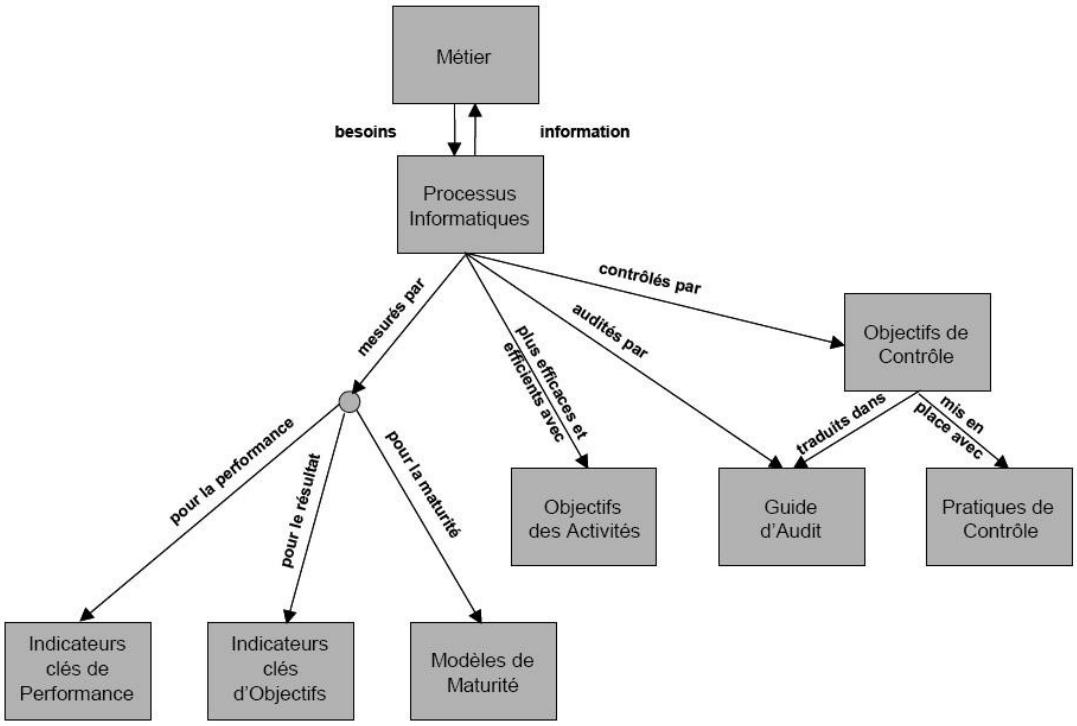

Figure 9 : Relations entre les composants CobiT (source : www.afai.fr)

Synthèse

La synthèse (ou *Executive Overview*) présente les grands principes du management tels que les objectifs, indicateurs, mesures, etc. ainsi que ceux de la gouvernance des technologies de l'information. Elle constitue une vue d'ensemble de la méthodologie CobiT et doit être utilisée en préalable à toute autre action.

Cadre de référence

Le cadre de référence se fonde sur les besoins d'information de l'entreprise, les ressources informatiques dont elle dispose et enfin les domaines dans lesquels peuvent être définis des objectifs de contrôle. Le cadre de référence est donc axé sur les besoins de l'entreprise, ses ressources ainsi que ses processus.

1. Enjeux pour l'entreprise

Afin d'atteindre ses objectifs, l'entreprise se doit de disposer d'informations pertinentes. La qualité de ces informations est essentielle pour sa compétitivité. Aussi, le volume d'information croit continuellement avec la croissance d'une entreprise, ce qui généralement entraîne une détérioration de la qualité de ces informations. La pertinence de

l'information est donc ici primordiale et devient un enjeu majeur pour le développement d'une organisation.

Le CobiT utilise 7 critères pour déterminer cette pertinence (cf. figure 7).

CRITERES	DESCRIPTION
Efficacité	Qualité et pertinence de l'information, distribution cohérente
Efficience	Rapidité et délivrance
Confidentialité	Protection conte la divulgation
Intégrité	Exactitude de l'information
Disponibilité	Accessibilité à la demande et protection (sauvegarde)
Conformité	Respect des règles et lois
Fiabilité	Exactitude des informations transmises par le management

Figure 10 : Critères permettant de déterminer la pertinence de l'Information

2. Ressources IT

Concernant les ressources IT, le CobiT établit quatre catégories à prendre en compte dans le cadre du management des Systèmes d'Information :

- Informations : données relatives à l'activité insérées ou fournies par le SI ;
- Applications : systèmes automatisés de traitement des informations ;
- Infrastructures : technologies et équipements (serveurs, SGBD, réseau, etc.) ;
- Personnels : techniciens et ingénieurs en charge du management du SI.

Une ressource IT entraîne la mise en œuvre d'un ou plusieurs processus IT.

3. Processus IT

Un processus se définit comme un ensemble de tâches ou d'activités. Il doit être managé, contrôlé et possède un niveau de maturité. L'orientation processus de CobiT est illustrée par un modèle qui subdivise l'informatique en 34 processus répartis entre les quatre domaines de responsabilités que sont: *planifier et organiser*, *acquérir et implémenter*, *délivrer et supporter* et *surveiller et évaluer*. Ces domaines représentés dans la figure 8 donnent ainsi une vision complète de l'activité informatique.

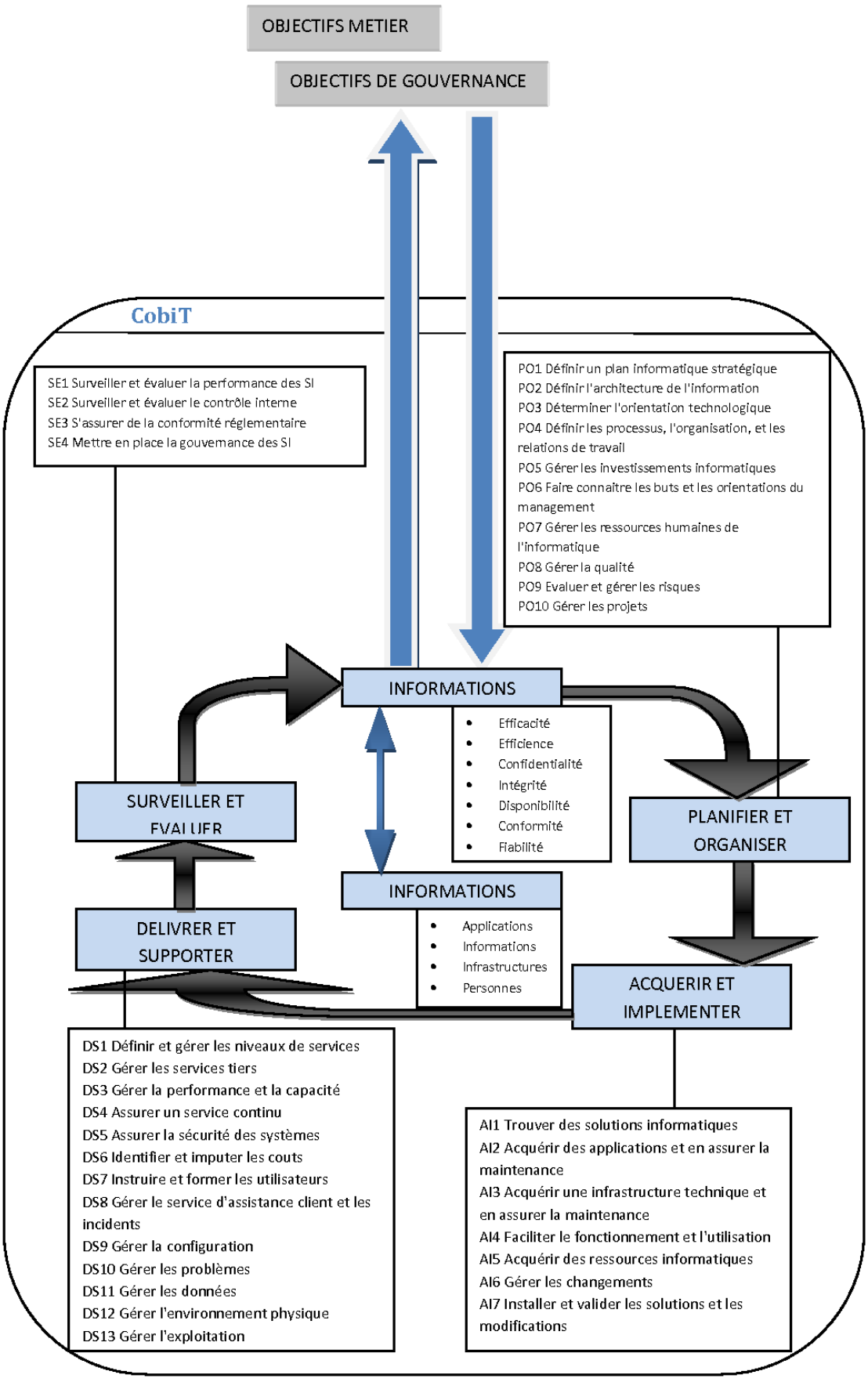

Figure 11 : Les processus IT au sein de CobiT
(source : www.afai.fr)

Le schéma ci-dessus nous montre les relations des composants au sein de CobiT, où l'on retrouve les domaines principaux de CobiT qui sont au nombre de 4, chacun reliés à un certain nombre de processus correspondants au domaine. Tout cela tourne autour d'une information rendue pertinente grâce aux différents critères vus plus tôt, liée aux objectifs de la gouvernance.

La notion de domaine est ici très importante car elle définit une répartition logique dans le management des SI. Ces domaines sont les suivants :

- Planifier et Organiser (10 processus) : domaine permettant de savoir comment utiliser les technologies afin que l'entreprise atteigne ses objectifs. Ce domaine s'inscrit donc dans une démarche stratégique.
- Acquérir et Implémenter (7 processus) : CobiT cherche ici à définir, acquérir et mettre en œuvre des technologies en les alignant avec les processus métiers de l'entreprise. L'objectif est de déployer la stratégie informatique définie lors de l'étape "Planification et Organisation".
- Délivrer et Supporter (13 processus) : l'objectif est ici de garantir l'efficacité et l'efficience des systèmes technologiques en action.
- Surveiller et Évaluer (4 processus) : ce domaine permet de s'assurer que la solution mise en place soit en adéquation avec les besoins de l'entreprise dans une vision stratégique. Il convient donc d'effectuer une évaluation de la qualité et de la performance selon des objectifs de contrôle déterminés préalablement.

Guide de management

Considéré par l'AFAI comme l'un des grands thèmes du CobiT, le *Guide de Management* concerne l'exploitation des ressources IT et va permettre de disposer d'indicateurs clés pour estimer la performance des processus, d'identifier et de mettre en place des contrôles, et enfin de sensibiliser aux risques et d'avoir des moyens de comparaison.

Tout d'abord les directives de gestion, ou *management guidelines*, vont permettre d'avoir une dépendance amont et aval pour chaque processus, exprimée en termes d'entrées/sorties. Elles permettent également d'identifier pour chaque activité du processus les acteurs responsables, garants, consultés ou informés, mais aussi de prendre en compte les objectifs et mesures (*metrics*).

Le guide de management propose aussi un modèle de maturité qui correspond globalement à une évaluation du processus sur une échelle de maturité de six positions (de inexistant à optimisé), permettant ainsi de se fixer des objectifs de progrès. Cette maturité peut se définir comme l'alignement des systèmes informatiques sur les objectifs de l'entreprise. Chaque niveau de celle-ci est décrit dans le tableau ci-dessous.

NIVEAU	DESCRIPTION
0 - Inexistant	Absence totale de processus
1 - Initial	Processus spécifiques et approche non structurée
2 - Reproductible	Réutilisation de processus pour les mêmes tâches
3 - Défini	Processus standardisés, documentés, communiqués
4 - Géré	Mesure et supervision de la conformité des processus
5 - Optimisé	Processus ayant le niveau de pratiques référentes

Figure 12 : Description des différents niveaux du modèle de maturité

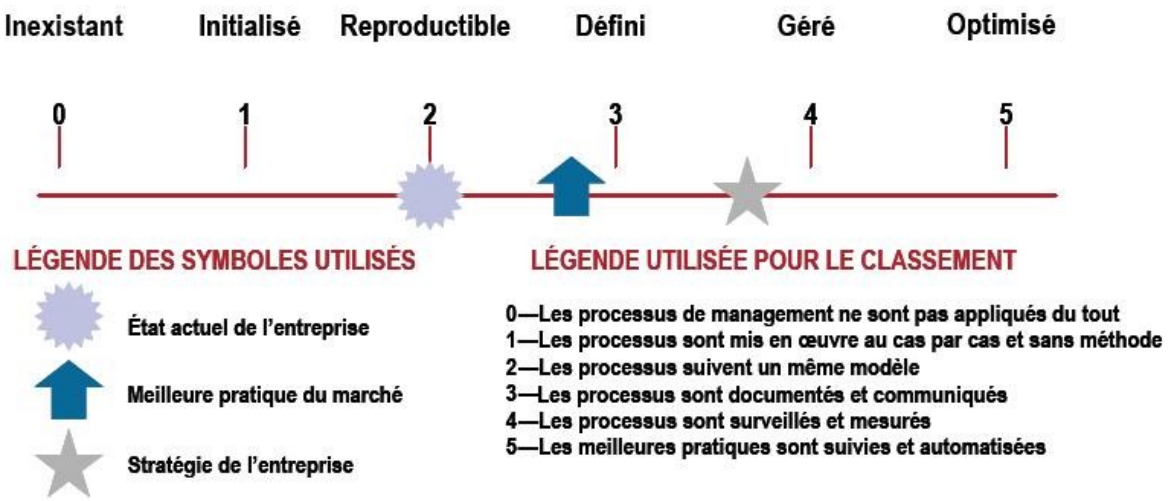

Figure 13 : Présentation graphique des modèles de maturité
(source : www.afai.fr)

La mesure de la performance est essentielle à la gouvernance des SI. Elle est un élément de CobiT et consiste entre autres à fixer et à surveiller des objectifs mesurables pour ce que les processus informatiques sont censés fournir (résultat du processus) et pour la façon dont ils le fournissent (capacité et performance du processus). CobiT fait référence aux indicateurs d'objectifs (KGI) et aux indicateurs clés de performance (KPI). Un KGI permet d'évaluer le niveau de la réponse à atteindre par le processus IT vis-à-vis des objectifs définis par l'entreprise. Un KPI permet de mesurer l'activité d'un processus en déterminant la probabilité d'échec et/ou de réussite d'un processus en regard des objectifs préalablement déterminés par l'entreprise.

Ces deux indicateurs sont étroitement liés dans la mesure où un KGI renvoie systématiquement à un KPI si on se place sur le plan des objectifs et inversement si on se place sur le plan de la performance.

Objectifs de contrôle

Objectifs de contrôle (ou *Control Objectives*) est le deuxième grand thème de CobiT qui est orienté vers les équipes en charge des services informatiques et vers le management. Les objectifs de contrôle de CobiT sont les exigences minimales d'un contrôle efficace de chaque processus informatiques. Ils sont définis en fonction de trois paramètres : le domaine IT, les besoins de l'entreprise, et enfin les ressources informatiques. Dans ce guide, on retrouve une description point par point de chaque objectif de contrôle en fonction du domaine auquel il appartient.

Afin de définir les objectifs de contrôle, CobiT se base sur 4 étapes de contrôle (Processus IT, Besoins de l'organisation, Étapes de contrôle, Pratiques de contrôles) comme l'indique le schéma ci-dessous :

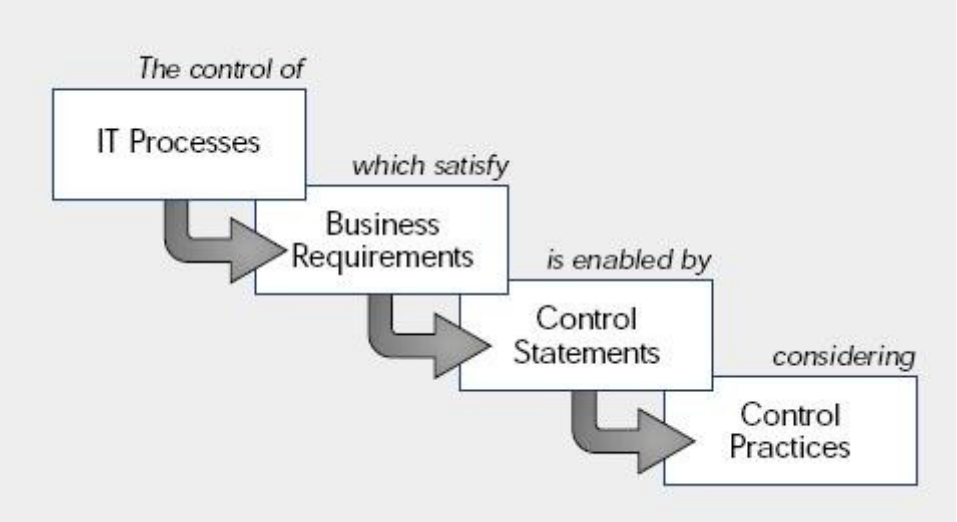

Figure 14 : Étapes de contrôle (source : www.bwise.com)

Guide de l'audit

Ce guide va permettre de déceler, d'analyser, et d'expliquer les failles d'un système et les risques qui en découlent afin de leur apporter des solutions. Il offre donc une méthodologie complète aux auditeurs dans le cadre d'une évaluation d'un SI et/ou d'une démarche de conformité.

CobiT propose pour cela une approche sur plusieurs niveaux :

1. Acquérir une bonne compréhension de la situation (identifier les activités de l'organisation afin de mettre en place des objectifs de contrôle et des indicateurs pertinents)
2. Évaluer les étapes de contrôle
3. Évaluer la conformité (s'assurer que les procédures de contrôle définies s'exercent correctement)
4. Justifier le risque (permet au management d'anticiper et d'agir en conséquence)

Ces niveaux constituent la structure générale du guide de l'audit.

2.1.3. CMMi, un modèle de maturité du SI

CMMi est un référentiel de bonnes pratiques conçu en 1987 à partir des meilleures pratiques de conception des logiciels par le SEI[14] de l'Université Carnegie Mellon.

Ce référentiel représente donc un ensemble de bonnes pratiques pour le développement de logiciels. L'organisation utilisant CMMi va voir sa qualité de prestation augmenter, qualité qui sera mesurable étant donné la présence d'indicateurs pour chacun des processus et domaines de processus. Les domaines de processus correspondent ici à un ensemble de processus regroupés par domaines (au nombre de 22 dans la version 1.2 de CMMi), ils seront présentés un peu plus loin.

Les 3 modèles de CMMi sont CMMI-DEV, axé sur le développement de système, CMMI-ACQ pour la maîtrise des activités d'achat et enfin CMMI-SVC, centré sur la fourniture de services. Ces modèles tournent autour d'une partie commune représentant environ 60% des pratiques.
Il faut savoir que le modèle CMMi possède deux approches conceptuelles. La première dite *étagée* consiste à aborder la mise en œuvre de tous les processus (par domaines) et de définir la maturité de l'ensemble (niveau 1, niveau2, etc.). Dans cette approche l'organisation tout entière doit évoluer au regard des 5 niveaux définis dans CMMI, on parle alors de *maturité*.
La deuxième dite *continue* aborde quand à elle la maturité des processus mais individuellement, c'est donc le niveau de chaque processus qui est important, on parle alors d'aptitude. Il faut préciser que le niveau 0 n'existe pas en représentation étagée contrairement à l'approche continue.
Le choix entre l'une ou l'autre dépend ici de son utilisation. Dans le cas par exemple d'une certification de toute une organisation vers CMMi, l'approche étagée est conseillée. En revanche, si l'on souhaite intervenir sur des processus inexistants ou insuffisamment matures, on préfère privilégier l'approche continue.

Au niveau de sa structure le modèle CMMi est constitué de :

- Niveaux de maturité des processus ;
- Pratiques génériques spécifiques à un niveau de maturité ;
- Objectifs génériques qui sous tendent les pratiques génériques ;
- Pratiques spécifiques qui complètent les pratiques et objectifs génériques ;
- Objectifs spécifiques qui soutiennent les pratiques spécifiques ;
- Sous pratiques qui complètent ou détaillent les pratiques spécifiques.

Le modèle de maturité

CMMi définit une échelle de mesure de la maturité comportant 5 niveaux (de 1 à 5), correspondant respectivement aux états "initial", "reproductible", "défini", "maitrisé" et enfin "optimisé". Les indicateurs permettant l'évaluation des activités sont également définis par CMMi.

[14] Software Engineering Institute - cf. Annexes – Les acteurs de la Gouvernance IT

Le schéma ci-dessous présente le détail des 5 niveaux de maturité de CMMi avec une description pour chaque niveau.

Les niveaux de maturité CMMi

Niveaux	Explication
Niveau 1	C'est l'état **initial** : L'organisation est « artisanale », les processus n'existent pas. Les contraintes de délai, sécurité et qualité ne sont pas contrôlables
Niveau 2	C'est l'état **reproductible** : L'organisme sait reproduire des plans de projet déjà expérimentés. Des jalons sont mis en œuvre, et les contraintes sont vérifiées
Niveau 3	C'est l'état **défini** : La gestion de projet et l'Organisme suivent des règles prédéterminées.
Niveau 4	C'est l'état **Maitrisé** : Les processus sont éprouvés et mesurés. La gestion du projet devient proactive.
Niveau 5	C'est l'état **Optimisé** : L'organisme, les processus et les projets sont améliorés de manière continue.

Figure 15 : Les niveaux de maturité selon CMMi (source : itil.fr)

Les contraintes de coût, de qualité et de délais de la gestion de projet ont aidé à l'émergence de ce référentiel qui est par conséquent devenu un modèle de développement et de maintenance des systèmes et applications informatiques.

Chacun des niveaux de CMMi possède des objectifs génériques (GG pour *Generic Goals*). De ce fait, lorsque l'organisation vise un niveau supérieur de maturité, elle doit dans un premier temps intégrer les nouveaux objectifs génériques et pratiques associées et dans un second temps continuer à mettre en œuvre les GG du niveau inférieur.

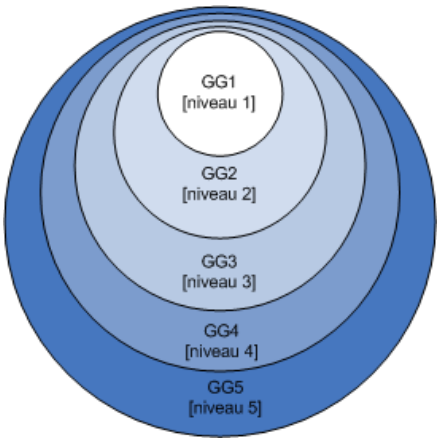

Figure 16 : Imbrication des niveaux et des objectifs génériques (source : itil.fr)

CMMi prône la mise en œuvre de 24 processus, regroupés sur la gestion des processus, la gestion de projet, l'ingénierie et enfin le support. Le schéma suivant représente la répartition des processus par niveaux. On y retrouve les niveaux CMMi, les domaines de processus par niveaux et les activités et domaines de processus constituants.

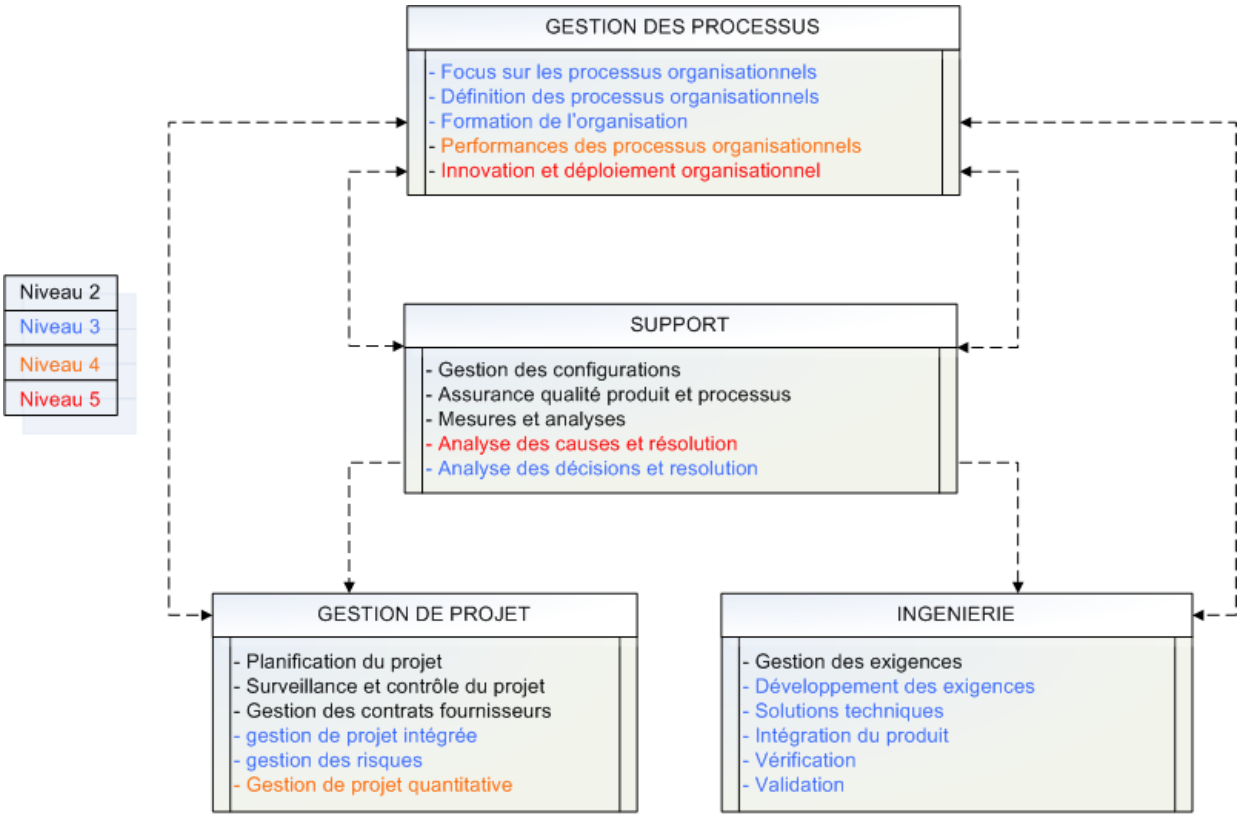

Figure 17 : Répartition des processus par niveaux de CMMi (source : itil.fr)

CMMi va donc trouver sa place dans toute organisation IT en permettant :

- D'assurer l'équilibre entre les coûts, les délais et la sécurité ;
- De mettre en œuvre les conditions d'une amélioration continue ;
- De garantir que les coûts sont maitrisés ;
- D'assurer un niveau optimal de Qualité de la conception des logiciels ;
- D'évaluer le coût d'un projet ;
- De mettre en œuvre les conditions de partenariats avec des tiers (infogérance, offshore,…).

2.1.4. eSCM, un référentiel pour la relation client/fournisseur

eSCM est un référentiel élaboré depuis 2001 par l'Université Carnegie Mellon/ItSQC afin d'améliorer la relation entre clients et fournisseurs dans le cadre de la fourniture de services utilisant les technologies de l'information. Contrairement à ITIL qui s'occupe de la production et CMMi du développement, eSCM va quand à lui viser la relation client dans le eSourcing en tentant de régir les opérations d'externalisation (informatique et processus métier). L'*externalisation* a pour vocation de confier la gestion de tout ou d'une partie de son informatique et des processus de gestion IT associés. Il devient donc nécessaire pour le client et le fournisseur de s'entendre sur des pratiques et un langage commun.

Pour ce faire, ce modèle de bonnes pratiques possède deux volets. Le premier est orienté client, c'est eSCM-CL (*eSourcing Capability Model for Client Organizations*) volet ayant vu le jour en 2001, avec une seconde version plus aboutie en 2004. Il permet aux organisations clientes d'évaluer et d'améliorer leur aptitude à gérer leurs fournisseurs de services récurrents, dans la mesure où les relations développées seront plus efficaces et mieux gérées, ce qui permettra ainsi de diminuer les échecs lors des relations client/fournisseurs.

Le deuxième, eSCM-SP (*eSourcing Capability Model for Service Providers*), a été conçu en 2005 avec une seconde version disponible depuis 2006. C'est le volet prestataire du référentiel eSCM, qui a pour objectifs de :

- Fournir aux prestataires des directives pour les aider à améliorer leur aptitude tout au long du cycle de vie du sourcing ;
- Fournir aux organisations clientes un outil objectif d'évaluation de l'aptitude des prestataires ;
- Donner aux prestataires un standard leur permettant de se différencier de leurs concurrents.

La chose la plus importante concernant ces deux versions est qu'elles sont construites symétriquement, comme le montre le schéma ci-dessous.

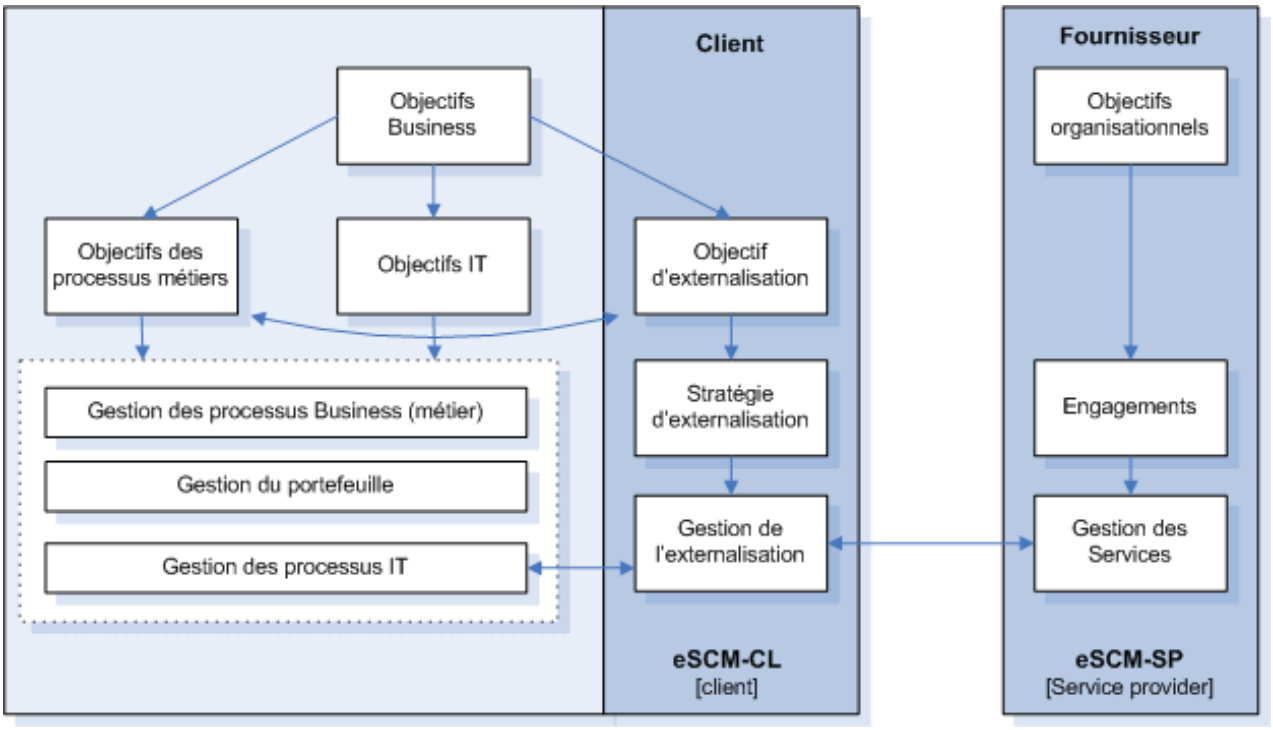

Figure 18 : Représentation du référentiel eSCM (source: itil.fr)

Ce schéma montre parfaitement la symétrie des deux parties de ce référentiel avec à gauche la version cliente ou *eSCM-CL* et à droite la partie fournisseur de service ou *eSCM-SP*.

En résumé, eSCM va permettre :

- Une entente client/fournisseur sur des objectifs communs ;
- Un alignement et maîtrise des processus de part et d'autre ;
- Une confiance mutuelle dans les relations client/fournisseur.

L'architecture du modèle eSCM

L'eSCM est un modèle structuré sur 3 dimensions :

- Niveau d'aptitude ;
- Cycle de vie ;
- Domaine d'aptitude.

Ces modèles sont développés dans le tableau ci-dessous :

		Niveaux d'aptitudes			
Cycle de vie du e-Sourcing	**Domaines d'aptitude**	**Niveau 2**	**Niveau 3**	**Niveau 4**	TOTAL
Cycle de vie	Gestion des connaissances	3	4	1	8
	Gestion des ressources humaines	3	7	1	11
	Gestion de la performance	3	3	5	11
	Gestion des relations	3	4	1	8
	Gestion de la technologie	4	1	1	6
	Gestion des menaces	6	1	n/a	7
Initialisation	Contractualisation	9	2	n/a	11
	Conception et déploiement des services	6	2	n/a	8
	Transfert des Services (in)	2	n/a	n/a	2
Livraison	Livraison du Service	7	1	n/a	8
Fin du Service	Transfert des Services (out)	2	1	1	4
	TOTAL	**48**	**26**	**10**	**84**

Figure 19 : L'architecture du modèle eSCM (source: itil.fr)

La première dimension correspond au niveau d'aptitude qui comprend 5 niveaux matérialisant chacun une trajectoire d'amélioration de service. Cela va de la fourniture du service sans pratiques particulières (niveau 1), au maintien de l'excellence pour laquelle une mise en œuvre de toutes les pratiques est requise et reconnue suite à deux évaluations consécutives (niveau 5). Chaque pratique est associée à un et un seul niveau. Par conséquent, seuls les niveaux 2, 3 et 4 contiennent des pratiques, le niveau 5 n'étant qu'une résultante qualité de toutes les activités issues des niveaux inférieurs.

Niveau 1	Fournir le service
Niveau 2	Fournir un service aligné sur le besoin
Niveau 3	Mettre en œuvre une organisation performante
Niveau 4	Gestion proactive
Niveau 5	Amélioration permanente de la valeur

Figure 20 : Niveaux d'aptitude de l'architecture eSCM (source: itil.fr)

La seconde dimension est le cycle de vie. Celui-ci couvre 4 phases que sont l'initialisation, la livraison, la clôture et enfin le cycle de vie du service (*On Going*).

L'initialisation recouvre les pratiques de mise en œuvre du service "infogéré" et de la relation client/fournisseur tel que la qualification des exigences, de la conception et de la mise en œuvre du service.
La livraison concerne le déploiement du service "infogéré" conformément aux spécifications réalisées et engagements contractés.

La clôture recouvre les activités de fin de cycle de vie et de réversibilité. Le cycle de vie du service concerne les pratiques mises en œuvre durant l'exécution du contrat et durant tout le cycle de vie du service.

2.1.5. Six Sigma, une approche statistique

Six Sigma est un référentiel présentant une méthodologie de management permettant une amélioration de la qualité et de l'efficacité des processus. La méthode Six Sigma trouve son origine chez Motorola en 1986. Motorola cherchait alors une méthode permettant d'optimiser ses processus de fabrication afin de satisfaire ses clients. Le Six Sigma peut se définir en cinq phases que sont : définir, mesurer, analyser, améliorer, contrôler. La première phase s'occupe de déterminer les exigences du client ainsi que les processus adaptés.
La mesure consiste au rassemblement des informations disponibles sur la situation courante afin d'obtenir les données de référence concernant les performances actuelles du processus et d'identifier les zones à problèmes.
Vient ensuite la phase d'analyse, dont le but est d'identifier les causes les plus probables des problèmes de qualité, puis de les confirmer à l'aide d'outils analytiques appropriés. La phase "Améliorer" permet la mise en place de solutions pour résoudre les problèmes identifiés précédemment, cette phase étant alors suivie par la phase de contrôle, dernière phase de la stratégie Six Sigma consistant à évaluer et à suivre l'évolution des précédents résultats.

Six Sigma est donc centré sur la satisfaction du client, satisfaction qui va directement influencer la performance, la croissance et la santé économique d'une entreprise. Pour permettre cela, Six Sigma mesure la performance en ne se contentant pas de moyennes obtenues à l'aide d'indicateurs ou tableaux de bord par exemple mais en tentant de maîtriser la variation. En effet, Six Sigma est né du constat que la moyenne ne suffisait pas à obtenir une performance pertinente. Un très bon exemple ci-dessous permet de bien comprendre le concept (source : Newsletter Avril 2009 du portail des meilleures pratiques ITIL.fr) :

"Vous êtes à l'hôtel pour trois nuits et vous demandez à être réveillé le matin à 7h. La première fois, on vous réveille à 6h45, la deuxième fois à 7h et la troisième fois à 7h15. En moyenne, on vous a réveillé à 7h, c'est conforme. Pourtant, vue du client, vous n'avez pas été satisfait deux fois sur trois à cause de la variation."

Ici, le client se souviendra de n'avoir été satisfait qu'une seule fois, non pas d'avoir été réveillé en moyenne à la bonne heure. Le but de Six Sigma dans un premier temps est de mesurer la variation des enchaînements de tâches qui doivent être accomplie pour répondre aux exigences des clients, ceci en utilisant une échelle normée. Il en découle la notion de

capabilité, calculée en termes de sigma, lettre grecque utilisée en statistiques pour désigner l'écart type.

La seconde étape va être de comprendre les causes de cette variation afin de mieux pouvoir la réduire et la maitriser. En effet, 20% des causes expliquent jusqu'à 80 % de la variation. L'objectif est donc d'identifier à l'aide d'outils statistiques ces 20% qui expliquent à elles seules 80% de la variation et qui, une fois prises en charge permettront de réduire et de maitriser la variation.

Un autre point important dans la façon de faire de Six Sigma est le "coût de la non-qualité". Concernant ce dernier, Six Sigma permet de quantifier les coûts de non-qualité, montrant ainsi les gains financiers attribués à la réduction de ces coûts.

La collaboration entre ITIL et SIX SIGMA…

Comme nous l'avons vu précédemment ITIL est un ensemble de pratiques de gestion de services IT qui va permettre la fourniture et le soutien des services IT. Cependant, ITIL n'intègre pas de mécanismes d'évaluation des niveaux de qualité de référence, ni de mesures d'amélioration de la qualité et c'est donc ici qu'il peut être intéressant de le faire collaborer avec Six Sigma. En effet, ITIL et Six Sigma ont tout deux des objectifs complémentaires, d'un côté ITIL permet d'augmenter la qualité, et de l'autre Six Sigma s'occupe quand à lui de la satisfaction client.

Les avantages de cet apport sont alors les suivants :

- La mesure de l'amélioration des niveaux de qualité ;
- L'identification des processus critiques pour la qualité ainsi que leurs imperfections ;
- L'évaluation du coût de la mauvaise qualité ;
- Un gain en rapidité de la part de Six Sigma car les processus sont déjà en place.

Les motifs précis de complémentarité entre Six Sigma et ITIL peuvent se répartir en quatre catégories : (source **:** *ITIL.fr*)

Aligner l'informatique sur le métier :

- Six Sigma fournit un mécanisme non-subjectif de communication sur l'amélioration de la qualité des services auprès des responsables business, en termes business ;
- Six Sigma contribue à renforcer la crédibilité de l'informatique de par sa parfaite lisibilité par les responsables business ;
- Six Sigma participe à la réduction des risques opérationnels et soutient les initiatives de mise en conformité ;
- Six Sigma incite à rendre prioritaire les projets d'amélioration des services sur la base de la *criticalité* pour le business.

Mesurer la qualité des services :

- Six Sigma encourage l'utilisation de modèles prédictifs selon une démarche proactive d'amélioration des processus ;
- ITIL préconise une approche en termes de services, ce qui n'est pas le cas de Six Sigma ;
- Six Sigma peut contribuer à mettre en évidence les services à plus forte valeur ajoutée pour le business et qui de fait devraient se voir attribuer une plus haute priorité ;
- ITIL n'intègre ni dispositif de mesure et d'analyse de la qualité, ni méthodologie détaillée d'amélioration continue des processus. Six Sigma peut répondre à ces deux carences d'ITIL ;
- Six Sigma facilite l'élimination des défauts (en termes de réduction des coûts liés à la mauvaise qualité) au sein des processus supportant les fonctions business critique pour la qualité ;
- Six Sigma fournit de meilleures métriques.

Adaptabilité :

- Six Sigma s'adapte aux changements du business et à l'évolution de la demande du client ;
- Six Sigma n'est pas complexe et est basé sur des principes statistiques communément admis que le business et le personnel technique peuvent comprendre facilement.

Tendances du marché :

- Six Sigma tend à devenir de plus en plus populaire au sein de la communauté ITIL grâce à sa démarche pragmatique, orientée business et ce pour l'amélioration des services informatiques ;
- Six Sigma a démontré son efficacité basée sur l'utilisation d'outils et de techniques statistiques.

Concernant l'intégration de Six Sigma à ITIL, il faut garder à l'esprit que ces deux référentiels diffèrent sur de nombreux points étant donné qu'ils ont deux approches différentes (orientée statistique pour Six Sigma, processus pour ITIL). Cette différentiation implique le fait de bien prendre en compte 4 aspects lors de l'intégration qui sont la maturité de l'organisation, les compétences requises pour le personnel impliqué, le modèle en triangle (temps vs coût vs valeur), et enfin comment l'approche DMAIC[15] de Six Sigma peut être combinée avec le cycle PDCA[16] de ITIL.

[15] *Define, Measure, Analyse, Improve, Control*
[16] *Plan, Do, Check, Act*

… une collaboration fructueuse

Les Technologies de l'Information ont un besoin de processus standardisés et de méthodologies d'amélioration de la qualité qui ne cesse de croitre or ITIL et Six Sigma ont clairement montré leurs efficacités dans l'atteinte de l'excellence de service. Cependant, il manquait au référentiel ITIL un modèle de processus d'amélioration de qualité, modèle que possède Six Sigma. De ce fait, on peut dire que Six Sigma complète parfaitement ITIL dans la mesure où ce dernier vient ajouter une structure de mesure et d'amélioration des processus. En revanche, l'intégration de Six Sigma à ITIL nécessite réflexion et attention en prenant en compte les aspects cités un peu plus haut, en plus de bien prendre en compte et de différencier l'aspect "analystes de données" de Six Sigma contre celui de concepteur de processus d'ITIL.

2.1.6. Le projet FUSING

FUSING [17] est un projet de fusion des principaux standards actuels de meilleures pratiques IT au sein d'un standard unique qui est adapté aux PME/PMI.

L'origine de FUSING vient du fait que les entreprises concernées ont souvent du mal a comprendre l'intérêt des référentiels pris individuellement, ces référentiels étant souvent considérés comme trop complexes, inadaptés, et coûteux.

FUSING se veut ouvert et simplifié afin d'être adapté aux petites et moyennes entreprises en leur apportant les bénéfices issus de l'adoption des meilleures pratiques IT. Il représente donc pour ces entreprises un cadre de référence en matière de management et de gouvernance IT en utilisant une méthodologie simple et pragmatique car intégralement basée sur les problématiques typiques des PME/PMI.

Le projet FUSING se présente sous la forme d'un recueil de meilleures pratiques directement inspirées des référentiels existants tels que : ITIL, CobiT, Six Sigma, etc.
Le standard FUSING est toujours en cours de développement et une première version officielle devrait être achevée d'ici la fin de l'année. Un dispositif de feedback sera alors mis en œuvre afin d'initier un cycle d'amélioration continue du standard basé sur les retours d'expérience.

2.1.7. L'avenir des référentiels

L'ensemble des auteurs de référentiels cherche continuellement à améliorer leurs ouvrages. Pour cela, ils mettent en place des cycles d'optimisation basés sur les retours d'expériences des utilisateurs.

De plus en plus de petites organisations adoptent des référentiels comme ITIL en les adaptant à la taille de leurs structures. Ils sont simplifiés au point de ne plus respecter

[17] *Fusing is a Unified Standard for Information techNologies Governance* ou *standard unifié pour la gouvernance des technologies de l'information*

l'ensemble des recommandations des référentiels originaux. C'est pourquoi, on peut s'attendre à ce que de nouveaux référentiels apparaissent pour les PME (tel FUSING). Cette situation est aussi vraie pour l'ensemble des types d'organisations qui cherchent à adapter des référentiels à leurs spécificités.

2.2.Les certifications

En plus des référentiels que nous venons de décrire, les entreprises peuvent faire certifier leurs collaborateurs à certaines pratiques de gouvernance IT. Dans le cas de l'utilisation du référentiel ITIL, on ne peut faire certifier les individus et non les organisations. Ainsi, une entreprise ne peut pas être certifiée ITIL. Si elle veut démontrer son application des processus ITIL, elle devra aller vers la normalisation ISO/CEI 20000 par exemple.

2.3.Les normes

En compléments des référentiels de Gouvernance IT, les organismes peuvent utiliser un certain nombre de normes qui sont à leur disposition. C'est un moyen pour les DSI, d'assurer un niveau de qualité envers les autres directions de l'entreprise.

Il existe aujourd'hui plusieurs organismes de normalisation du SI. Le principal étant l'ISO[18] qui définit plusieurs standards mondiaux pour le SI. Ces derniers sont basés ou adapté dans chaque pays par les organismes nationaux.

On peut noter le lien étroit entre le référentiel ITIL et la norme ISO/IEC 20000. En effet, ITIL offre la possibilité de certifier une partie ou la totalité de la démarche de gestion de services IT au travers de cette norme.

Cette norme de l'Organisation Internationale de Normalisation (ISO), publiée en Décembre 2005 est compatible avec les livres des meilleures pratiques d'ITIL. Cette norme est formée de deux parties. La partie 1, ISO-IEC 20000-1, énonce les spécifications pour le management des services IT. La partie 2, ISO-IEC 20000-2, offre un guide d'application et formule des recommandations pour la mise en œuvre des spécifications énoncées à la partie 1.

[18] International Organization of Standardization : cf. Les acteurs de la Gouvernance

3. La Gouvernance IT en action

Nous allons maintenant tenter de présenter des démarches d'intégration de la gouvernance dans les SI. Pour cela, nous nous baserons sur des études et rapports de plusieurs organismes dont notamment le *Club Urba-EA*, une association d'entreprises regroupées autour de la thématique de l'urbanisation et de l'architecture des SI. Cet organisme compte aujourd'hui plus de 55 membres dont AXA, FNAC, RATP,…

On s'attache à répondre à la question "qu'est ce qu'une entreprise qui gouverne bien son informatique?" de la façon suivante : c'est une entreprise qui a mis en place et fait évoluer un dispositif de management, fondé sur des bonnes pratiques, lui permettant :

- D'optimiser ses investissements informatiques dans le but de :
  - Contribuer à ses objectifs de création de valeur ;
  - Accroître la performance des processus informatiques et leur orientation client ;
  - Maîtriser les aspects financiers du Système d'Information ;
  - D'anticiper et de développer les solutions et les compétences en SI dont elle aura besoin dans le futur ;
  - S'assurer que les risques liés au Système d'Information sont sous contrôle.
- Développer la transparence dans les relations informatiques avec les clients.

Pour amorcer la mise en place d'une stratégie de gouvernance IT, l'entreprise doit se poser les bonnes questions. Il y a une démarche à suivre permettant d'avoir les réponses à ces questions et ainsi d'obtenir les meilleurs résultats possibles.
Pour savoir comment bien démarrer et élaborer sa stratégie de mise en œuvre, l'entreprise doit effectuer un diagnostic des dispositifs de gouvernance IT déjà existants si c'est le cas. En fonction, il faudra entreprendre la définition d'une stratégie d'amélioration ou de création de tels dispositifs.

Au début de cette démarche, les questions inévitables à se poser sont :

- *Comment savoir si l'entreprise gouverne bien son Informatique ?*
- *Comment identifier une cible réaliste à atteindre pour s'améliorer ?*
- *Comment identifier les actions à mener pour attendre la cible ?*

Il est impératif d'avoir les réponses à ces questions avant de se lancer dans un plan de gouvernance IT.

La mise en place des référentiels de bonnes pratiques est importante. On peut sereinement préconiser l'utilisation des trois principaux référentiels de gouvernance. Il s'agit de CobiT pour le pilotage du SI, ITIL pour l'amélioration de la production et CMMi pour l'amélioration du développement du SI. D'autres référentiels sont aussi disponibles et peuvent être utiles selon les cibles à atteindre.

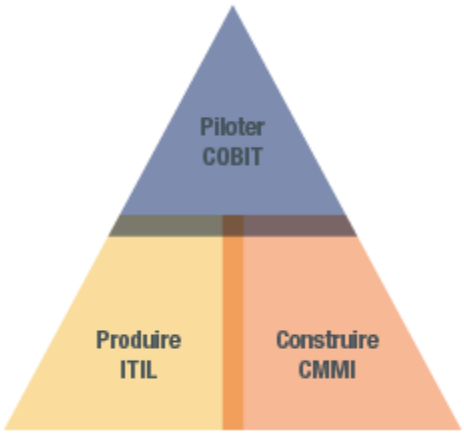

Figure 21 : Les trois référentiels majeurs de la fonction Informatique (source IT expert)

D'autres outils de méthodologie et logiciels de mise en œuvre de gouvernance existent. Selon une enquête sur le sujet réalisée en octobre 2003 par le cabinet IDC France sur un échantillon de 205 DSI, les directeurs informatiques français s'appuieraient en ordre décroissant de priorité sur : la gestion du budget, la gestion des projets, les priorités et les SLA (niveaux de services), la gestion des temps (planning et cycle de vie des applications) ; et enfin sur la gestion des ressources humaines et du changement.
Du côté des outils de gestion, plus de 80% des entreprises sondées utilisent les outils bureautiques. Les suites logicielles intégrées ne viennent qu'en dernière position, citées par seulement 40% des DSI.

Réduction des budgets opérationnels, implication de l'IT dans la stratégie business, externalisation croissante, recherche de ressources qualifiées... Les défis des DSI sont multiples. Les entreprises cherchent sans cesse à améliorer la qualité, la disponibilité et la livraison des services, à accroître la satisfaction de leurs clients internes et externes et à réduire le *Time to Market*.
La gestion optimisée des services informatiques devient alors l'une de leurs priorités majeures. À la recherche de référentiels pour viser l'excellence dans le service management, les DSI se tournent de plus en plus vers ITIL. Brique par brique (gestion des incidents, service desk, gestion des problèmes, etc.), cette méthodologie s'impose comme le standard incontesté de la gestion des services informatiques, parfois en complément d'autres référentiels.

La gouvernance IT se positionne comme un vrai challenge pour les entreprises. En effet, en pleine période de crise, l'entreprise qui place son système d'information au cœur de son activité augmente ses chances de réussite. On a souvent tendance à assimiler la gouvernance à l'utilisation de référentiels de bonnes pratiques or la gouvernance IT n'est pas uniquement basée sur ces référentiels. Elle est basée sur les cinq ou huit domaines

stratégiques que nous avons définis auparavant. Les référentiels ne sont là que pour aider les entreprises à mettre en place facilement une bonne gouvernance IT. Et dans la mise en place de ces référentiels, les entreprises utilisent entre autres des solutions applicatives dédiées à cette tâche.

La grande majorité des solutions qui existent sur le marché en matière de gouvernance IT est destinée aux grands groupes et PME qui désirent mettre en place un plan de gouvernance et qui ont les moyens de supporter le coût d'une telle démarche. Les grands éditeurs ne cessent de proposer des solutions applicatives utiles à la gouvernance. Ces dernières sont souvent des solutions d'aide à la mise en œuvre. Dans ce sens, les éditeurs leurs offrent des outils permettant de facilité cette mise en place.

3.1. Les solutions pour la mise en place de gouvernance

Certains outils sont destinés à mettre en place un plan de gouvernance IT, plus précisément implémenter les référentiels de bonnes pratiques. Nous avons choisi de vous présenter quelques solutions présentes sur le marché.

GRC Accelerator (Governance, Risk & Compliance) est une solution qui permet d'implémenter facilement ITIL. Elle permet de gérer les processus et systèmes d'information en implémentant les pratiques via un portail web.
Cette approche basée sur des diagrammes favorise l'optimisation de la gestion du Service Informatique en permettant à toute organisation de rationaliser ses services IT.
La solution offre aux DSI une vision plus précise des processus d'ITIL ainsi que la possibilité d'évaluer la performance de ses services informatiques. Toutes les procédures de mises en place du référentiel sont accessibles sous forme de schémas détaillés de déroulement des processus. Pour évaluer la performance des services informatiques, la solution comprend un outil de consolidation des données permettant de créer une base de données complète de la situation actuelle. Un calendrier totalement interactif permet aux équipes de suivre l'implémentation en fonction d'indicateurs clés.
La solution GRCA se positionne comme l'un des principaux outils de mise en place des bonnes pratiques d'ITIL.

WorkflowGen est un moteur qui permet d'implémenter facilement et rapidement des processus d'entreprise. Workflow/BPM WorkflowGen permet d'automatiser rapidement et efficacement les processus ITIL tout en respectant les contraintes les plus fortes de la conformité avec les lois du secteur d'activité de l'entreprise.

On peut aussi suivre l'activité de plusieurs éditeurs qui sont présents sur ce marché.
Casewise apparaît aujourd'hui comme être un leader en modélisation d'entreprise pour l'amélioration des processus, l'architecture d'entreprise, les meilleures pratiques et la conformité. Les logiciels et solutions Casewise ont été choisis par plus de 3000 organisations

majeures dans le monde, que ce soit dans les domaines de l'amélioration des processus métier, de l'architecture d'entreprise, de l'architecture orientée services ou des meilleures pratiques.

Pytheas propose à ses clients à travers le monde des logiciels de gestion de parc et de help desk. PYTHEAS est également un acteur impliqué dans l'évolution des *Meilleures Pratiques* de gestion des services informatiques.

3.2.Les logiciels pour la gouvernance IT…

Les outils pour la gestion des risques IT

Maillon clé de la gouvernance informatique des entreprises, la gestion des risques se positionne aujourd'hui comme une problématique centrale pour les entreprises. Les entreprises souhaitent une meilleure représentation des risques IT afin de pouvoir prendre des mesures permettant de les limiter. L'objectif est l'amélioration sur le long terme de l'efficacité opérationnelle de toute l'organisation.
De ce fait, des solutions applicatives de gestion des risques existent afin de permettre au DSI de mieux gérer les menaces pesantes sur le SI. Nous définirons un logiciel de gestion des risques comme une solution permettant d'identifier, évaluer et cartographier les risques. Ils pourront éventuellement proposer des mesures de contrôles adéquates. Cet outil s'adapte aux besoins spécifiques des entreprises afin de les aider à dresser la meilleure cartographie de leurs risques.

Des outils de gestion de Portefeuille d'Applications

Une gestion de portefeuille de projets permet d'améliorer le partage et la transparence autour des projets informatiques avec les directions métiers et la direction générale. Elle professionnalise les engagements réciproques entre Directions métiers et DSI : nomination de chefs de projet, disponibilité de ressources, délais… De plus, grâce à elle, les DSI maîtrisent mieux les délais et les budgets. Elle favorise une vision transverse de l'entreprise et propose une première approche d'urbanisation du Système d'Information. Enfin, elle renforce l'importance des techniques de gestion de projets simples, rigoureuses et adaptées au sein de la DSI. La gestion de portefeuille de projets est une brique clé de la réussite d'une nouvelle gouvernance informatique.

De nombreux enjeux sont à citer concernant le PPM[19]. Cette gestion doit accroître le bon alignement stratégique des projets. Elle doit améliorer la prise de décisions, optimiser l'allocation des ressources dédiées aux projets. De plus, le pilotage doit être facilité par une meilleure cohérence des informations. Enfin, des moyens de reporting et de communication doivent être offerts par cette gestion du portefeuille.

[19] Project Portfolio Management : Gestion de portefeuille de projet

Compuware tente d'évoluer dans le domaine, en lançant *Application Portfolio Management Accelerator*, une solution de gestion de portefeuille de projets. Elle permet aux DSI de prendre des décisions afin de réduire le nombre d'applications, à minimiser les coûts ainsi qu'à optimiser les investissements en fonction des objectifs de l'entreprise et des besoins métier. *"Avec les processus de l'Application Portfolio Management, les entreprises ont une idée précise des coûts, des risques et de la valeur métier des applications déployées", constate* Jim Duggan, vice-président chargé de la recherche chez Gartner *"…Sans stratégie rigoureuse d'Application Portfolio Management, les entreprises sont tributaires d'hypothèses souvent mal fondées et peinent à surmonter l'inertie institutionnelle"*

La BI au service de la gouvernance

Pour évaluer la performance du service rendu par le SI aux processus métier, on peut utiliser des outils d'aide à la décision tel que celui fournit par l'éditeur I-Cosoft. Leur logiciel est destiné à mesurer et piloter la performance du DSI. Elle leur permet de garantir l'optimisation des processus métier, d'assurer la performance, la sécurité en élaborant des tableaux de bord pour la DSI.

Les éditeurs de logiciels de gouvernance

Il existe aujourd'hui plusieurs éditeurs sur ce marché. Ces derniers proposent des solutions aidant les DSI à assurer une bonne gouvernance de leur SI.

- IBM ;
- Effisoft ;
- Compuware ;
- …

IBM met à la disposition des entreprises la palette de ressources la plus complète, compétences, systèmes, logiciels, services, financement, technologies, pour les aider et leur permettre de devenir des entreprises d'innovation.
Grâce à son expérience en matière d'expertise métier, IBM aide non seulement les entreprises à inventer de nouveaux produits mais aussi à s'organiser différemment, à comprendre les enjeux des marchés et à mieux réagir à leurs évolutions.

Effisoft est un groupe international qui conçoit des logiciels pour les professionnels de l'assurance, de la réassurance et de la gestion des risques depuis 15 ans. Effisoft compte parmi ses clients un assureur sur 2, de nombreuses grosses PME et les acteurs majeurs du CAC40, du FTSE ou du NYSE.

Compuware, spécialiste de la fiabilité et de la performance des systèmes d'information fait partie des grands éditeurs de logiciels et fournisseur de services. Sa mission consiste à fournir aux directions informatiques des solutions complètes pour leur système d'information afin de mieux maîtriser les risques, les budgets et les ressources. Son offre se compose de solutions (logiciels et services) pour le test et le pilotage des applications, de leur conception à leur exploitation en production.

3.3. Vers une Gouvernance IT dans l'Administration...

3.3.1. Quelle gouvernance IT pour les collectivités ?

Lorsque nous avons défini la Gouvernance IT, nous l'avons fait dans le cadre d'entreprises et notamment des grandes entreprises. Cependant la Gouvernance IT n'est pas réservée à ces dernières. Un autre type d'organisation peut y trouver son compte. Il s'agit de l'administration publique et les collectivités territoriales. Nous allons donc voir dans quelles mesures une DSI publique peut appliquer une véritable gouvernance IT.

Si l'on considère une collectivité territoriale classique, on s'aperçoit qu'elle ne diffère que de peu d'une entreprise au niveau de son système d'information. En effet, celui-ci est géré par une DSI qui dispose d'un budget, lequel doit être justifié auprès d'une direction. Dans le cadre de son activité, cette DSI doit assurer la réactivité, la performance et l'efficacité de son SI afin de permettre à l'ensemble de l'organisation d'être opérationnelle. Il n'y a donc pas de différence et c'est pourquoi on peut sereinement envisager la possibilité d'appliquer une réelle Gouvernance IT au sein des DSI d'organismes publics.

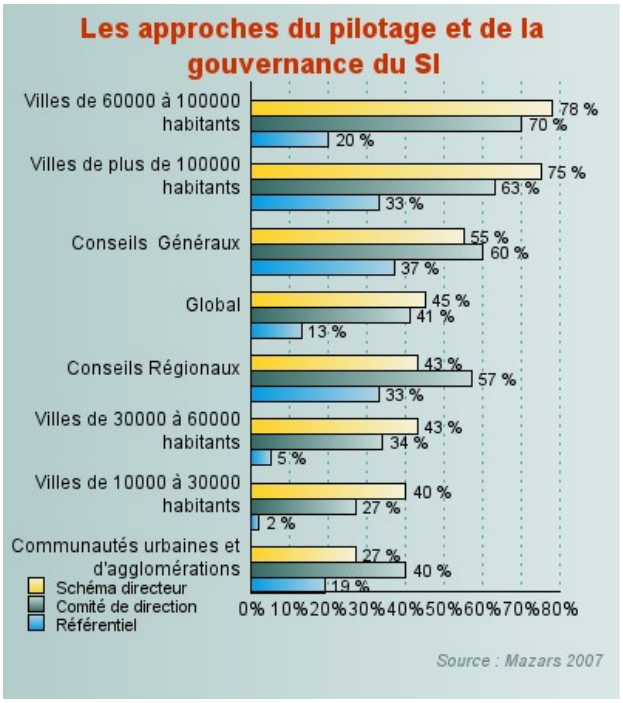

Figure 22 : Les approches du pilotage et de la gouvernance du SI selon le type de collectivités (source : Mazars)

D'après une étude du cabinet d'audit Mazars réalisée en 2007, dont une partie des résultats sont présentés sur la figure précédente, on remarque que l'approche de la gouvernance IT diffère en fonction du type de collectivités et donc de la taille du SI de l'organisme. Il s'agit là encore d'une similarité par rapport au monde de l'entreprise: les grandes organisations ressentent plus tôt le besoin de disposer d'une approche formalisée du SI. On peut expliquer ce phénomène par le fait que les SI des grandes collectivités sont plus assujettis à être

composés de beaucoup d'applications métiers rendant le SI hétérogène. De la même façon, les SI de petites collectivités sont plus restreints à cause des budgets réduits mais aussi de la compétence réduite de ceux-ci. Il est donc évident que les grandes collectivités seront donc plus concernées par une approche pluralisée du pilotage du SI. On remarque donc que ce sont les conseils généraux, régionaux et les communes de plus de 100 000 habitants qui sont les plus utilisatrices de référentiels de gouvernance IT.

Cependant, une des questions à se poser est de savoir dans quelles mesures on peut appliquer un référentiel tel que CobiT ou ITIL dans une DSI "publique". En effet, ces référentiels ont été créés pour des DSI d'entreprises et non pour des organisations d'intérêts collectifs. Cependant, à priori, rien ne contre-indique l'utilisation d'un référentiel tel qu'ITIL au sein d'une DSI de collectivités territoriales.

Un des exemples les plus parlants est celui de la Mairie de Bordeaux qui a entrepris l'implémentation du référentiel ITIL au sein de sa DSI il y a quelques années de cela. En novembre 2008, lors de la dernière conférence annuelle de l'itSMF, les promoteurs d'ITIL en France, la directrice du système d'information de la Mairie de Bordeaux, Pascale Avargues, a été mis à l'honneur pour le succès du projet d'implémentation du référentiel au sein de son service informatique. Cela montre que même le monde des DSI des collectivités peut se prêter aux référentiels classiques de Gouvernance IT.

Il n'existe aujourd'hui pas de référentiels de gouvernance ou d'outil de gouvernance en général spécifiques aux DSI des collectivités. Cela s'explique par le simple fait que ce besoin n'existe pas. En effet, comme nous l'avons indiqué précédemment, il n'y a pas de différences entre les missions des DSI, privées ou publiques.
Cependant, dans le cadre d'une bonne gouvernance IT, on veille à aligner son SI à la stratégie de l'entreprise. Dans le cas des collectivités, cette stratégie évolue au rythme des choix politiques définis par des élus dont le mandat est souvent plus court que celui des membres d'une direction d'entreprise.

3.3.2. Perspectives pour les DSI territoriales

Nous avons vu que les DSI institutionnelles pouvaient aujourd'hui tout à fait envisager l'utilisation d'outils classiques dans le cadre de projet de gouvernance IT. Avec les retours d'expérience des collectivités qui ont déjà franchi le pas, on peut s'attendre dans les prochains mois à l'expression de besoins spécifiques par rapport au monde des entreprises.

En effet, nous avons vu que les stratégies des collectivités peuvent évoluer beaucoup plus vite que celles des entreprises. Il apparaît évident que les DSI territoriales devront être particulièrement sensibles à une conduite du changement fréquente notamment dans le cas de changement de direction suite à des élections. Il faut donc pour ces DSI adopter des méthodologies en adéquation avec cette situation. Or celles-ci n'existent pas à ce jour.
D'autre part, l'essor de l'e-administration aura indéniablement un impact dans un proche

avenir sur les SI des collectivités. Ces derniers devront prendre en charge de nouveaux besoins des directions des organisations mais aussi des usagers.

Outre tous les référentiels de gouvernance connus dont nous avons détaillé les principes et le fonctionnement dans les parties précédentes, on peut noter que l'État par l'intermédiaire de la Direction Générale de Modernisation de l'État (DGME) est actuellement en train de publier des référentiels de bonnes pratiques pour les SI des administrations et des collectivités territoriales. Il ne s'agit ici pas de référentiels de gouvernance IT "pure" telle qu'on l'a décrite précédemment. En effet, ces ouvrages ne comportent que des bonnes pratiques en termes de conception des SI. Il ne s'agit en aucun cas de considération du SI en termes d'alignement stratégique, d'apport de valeur, de gestion des risques, de gestion des ressources ou de mesures de la performance, c'est pourquoi on ne pourra pas parler de référentiel de gouvernance. Cependant, un de ces ouvrages, le Référentiel Général d'Interopérabilité (RGI) devra être mis en centre des considérations sur les SI dans les institutions. Effectivement, dès la parution du décret relatif à ce texte, l'ensemble des collectivités et des services de l'État devront être en conformité avec celui-ci dans un délai de 2 à 3 ans. Cela signifie que l'on peut s'attendre à une hausse du nombre de projet d'urbanisation des SI institutionnels dans les mois à venir dès lors que le RGI aura été validé.

3.4. Gouvernance et nouvelles tendances

Les DSI cherchent constamment à fournir des services de qualité à un coût raisonnable, la crise intensifie cette exigence. Il faudra donc tout d'abord rapidement se conformer à cette obligation. Mais la seule manière de s'y conformer de manière réellement durable, pérenne et significative, passera par une approche radicalement nouvelle. Nous nous dirigeons vers des architectures basées sur Internet, le Cloud Computing. Les éditeurs devront alors proposer des solutions adaptées au changement des SI.

3.4.1. Le concept de Cloud Computing

Ces deux dernières années ont vu apparaître un nouveau concept dans le monde de l'informatique : le Cloud Computing qui peut se traduire par "l'informatique en nuages". Ce concept est résultat d'une externalisation toujours plus importante des Systèmes d'Information des entreprises dans un souci de réduction de coûts.

Il s'agit pour une entreprise d'utiliser l'infrastructure, les applications et/ou l'espace de stockage mis à disposition de manière quasi illimitée par une autre entreprise fournisseurs de solution Cloud Computing.

Il est possible de distinguer trois déclinaisons du concept de Cloud Computing :

- Les offres de type SaaS (Software as a Service) sont des applications déjà développées par un prestataire, complètes, et configurables en fonction des besoins de l'entreprise ;
- Les offres du type Paas (Platform as a Service) sont des plateformes de développement qui permettent de créer ses propres applications et services en fonction des besoins ;
- Les offres du type Iaas (Infrastructure as a Service) sont les ressources informatiques de base qui sont misent à disposition telles que la puissance de calcul, la mémoire ou le stockage.

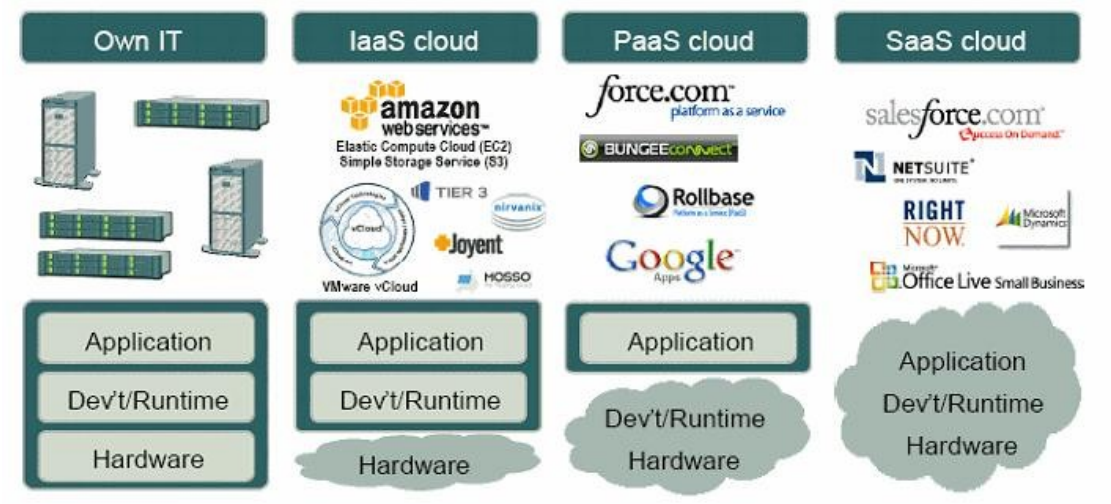

Figure 23 : Des infrastructures classiques au Cloud Computing (source : FCS/Novembre 2008)

Aujourd'hui, l'engouement des entreprises pour le Cloud Computing est bien réel, et ce quelque soit la taille et le type d'entreprise. Début 2009, le Cloud ne représentait que 4% du marché mais avec une prévision de croissance de 21% sur l'année dans le monde pour dépasser les 56 milliards de dollars (41 milliards d'euros). Un chiffre qui devrait tripler d'ici 2013.

La gouvernance et le Cloud Computing

À ce jour, aucun référentiel de Gouvernance IT ne fait état de l'utilisation ou non du Cloud Computing au sein du SI. Cependant, il semble que la version 3 d'ITIL puisse prendre en compte l'ensemble des contraintes du Cloud. C'est pour cela que l'on peut affirmer que c'est un des référentiels les mieux adaptés à cette pratique.

A l'heure actuelle, nous pouvons distinguer deux types de Cloud : le public et le privé. Nous confronterons ces derniers aux concepts de la gouvernance IT pour définir dans quelles mesures, cette nouvelle pratique de l'informatique aura une influence sur le SI.

Le Cloud public repose sur des plates formes publiques mise à disposition par des prestataires. Une des raisons pour laquelle une entreprise va choisir d'externaliser son Système d'Information dans une offre de Cloud Computing est l'importante réduction des coûts engendrée. En effet, les coûts de mise en place d'un plan de gouvernance vont diminuer de manière significative car une plus ou moins grosse part de celui-ci va désormais être gérée par le fournisseur de solutions Cloud. La solution publique fournie via le Net des services qui jusqu'à présent ne pouvaient l'être que par des applications. Elle permet de mettre en œuvre très rapidement de nouvelles formes d'organisation dans les entreprises.

Dans le cas d'une externalisation totale du SI, la DSI n'aura plus pour tâche que l'administration à distance du SI, la gestion des postes clients et de l'infrastructure du réseau. Les configurations des postes clients sont simplifiées du fait que l'ensemble des services est accessible par le biais du navigateur web. La DSI ne s'occupe plus du déploiement des serveurs, de mises à jour logicielles, du redimensionnement des espaces de stockages, des prévisions de ressources nécessaires à tel ou tel déploiement de services.

La mise en pratique de Cloud Computing au sein du SI permet d'apporter des réponses à deux des préoccupations de la gouvernance.
En effet, cette pratique permet une meilleure gestion des ressources matérielles puisque celle-ci est confiée à un prestataire extérieur qui se chargera d'en assurer le bon fonctionnement.
En outre, la gestion de la performance sera assurée puisque l'entreprise prestataire de solution de Cloud Computing garantie à l'entreprise cliente un certain niveau de service (SLA[20]).
Cependant, on peut affirmer que la DSI se dégage d'une partie de ses responsabilités en confiant son SI. Cela engendre automatiquement une hausse du risque IT.

Pour éviter cette hausse du risque IT, une entreprise peut choisir de ne pas externaliser son SI mais de transformer celui sous forme de Cloud privé grâce à des solutions applicatives et des outils proposés par des entreprises prestataires. Cette forme est bâtie sur des plates-formes privées, regroupant les différents centres de données, les automatisant et les virtualisant. Dans ce cas, la gouvernance du SI de l'entreprise ne changent pas mais est simplifiée car, une fois le Cloud privé mis en place, la DSI peut gérer plus facilement les incidents concernant les besoins de ressources. A l'instar du Cloud public, les solutions applicatives en Cloud permettent de simplifier les mises à jour logicielles et la configuration des postes clients.

[20] Service Level Agreement : Garantie de niveau de service

La Gouvernance et le Cloud : quel avenir ?

D'ici 2 ans, le Cloud Computing devrait être adopté en masse par les entreprises dans les deux, trois prochaines années. Seul ITIL V3 est adapté au concept du Cloud. Il semble que ce ne soit pas le cas avec d'autres référentiels. C'est pourquoi ces derniers auront évolué de sorte à prendre en compte certaines problématiques propres au Cloud Computing telles que la sécurité des données ou l'importance d'un bon niveau de service garanti.
D'autre part, l'adoption du Cloud Computing devrait se formaliser dans les prochaines années et l'on devrait voir apparaître des standards et des référentiels permettant à la DSI de faire du Cloud Computing un véritable outil d'amélioration du SI.

Dans 5 ans, le Cloud est devenue une technologie mature. Elle est entrée dans les SI des entreprises il y a plusieurs années. Les référentiels de bonnes pratiques ont intégré les retours d'expérience sur l'utilisation du Cloud. De nouveaux référentiels spécifiques et des standards ont même été créés afin d'aider les DSI à adopter le Cloud Computing comme outil de Gouvernance IT.

4. Conclusion

Avec point comme de départ l'application des lois financières réglementant les Systèmes d'Information Financiers (*Sarbanes-Oxley*, 2002), la Gouvernance IT a connu une évolution spectaculaire.

Les grandes entreprises ont réalisé que leurs Systèmes d'Information n'étaient pas aussi efficaces qu'ils pouvaient l'être. Ces DSI ont alors décidé de collaborer en confrontant leurs expériences. Ces travaux ont débouché sur l'amélioration ou même sur la rédaction de nouveaux référentiels qui réalisent une synthèse des bonnes pratiques informatiques.

Une grande partie des décideurs informatiques ont maintenant connaissance de ces référentiels et beaucoup d'entre eux les ont mis en œuvre. La publication d'*ITIL V3* a fait connaître davantage les référentiels de gouvernance et a convaincu les hésitants.

L'efficacité des référentiels étant prouvée, les PME et les collectivités territoriales qui n'étaient pas directement concernées par ceux-ci ont tenté de les implémenter en les adaptant à leur échelle. Le référentiel *FUSING* est en cours d'élaboration, il se base en effet sur les retours d'expérience des PME ayant eu une démarche de gouvernance.

Favorisant la mobilité et la réduction des coûts, de nouvelles configurations d'architectures sont apparues : la virtualisation, l'architecture orientée services (*SOA*) et le *Cloud Computing* Nous pouvons nous attendre à ce que les référentiels s'adaptent à ces nouvelles pratiques informatiques grâce aux retours d'expérience des premiers utilisateurs.

Nous pouvons affirmer qu'il existe des processus continus d'amélioration des référentiels. Un référentiel ne pourra jamais être parfaitement adapté puisque les pratiques informatiques varient rapidement. Cependant, c'est grâce à leur maturité qu'ils peuvent s'adapter à toutes les évolutions.

Pistes de création d'entreprise

Cependant, même avec des référentiels à jour, l'application de ceux-ci peut s'avérer problématique et surtout difficile à gérer sur la durée. Le marché des logiciels d'assistance à la gouvernance peut encore être développé. Les grands éditeurs actuels bénéficient de leur notoriété mais l'efficacité et la valeur ajoutée apportée de leurs solutions n'est pas toujours démontrée. Il est possible de les concurrencer sur ce marché en proposant des solutions d'accompagnement à prix compétitif et basé sur les nouvelles tendances.

Références

Bibliographie

- Thierry Chamfrault et Claude Durand, *ITIL et la Gestion des Services*, *Éditions Dunod 2006*
- Club URBA-E, *Urbanisation des SI et Gouvernance*, *Éditions Dunod, 2006*
- Frédéric Georgel, *IT Gouvernance*, *Éditions Dunod, 2ème édition, 2009*
- Frédéric Parrat, *Le gouvernement d'entreprise*, *Éditions Dunod, 2003*
- Frédéric Peltier, *La Corporate gouvernance, Éditions Dunod, 2004*

Webographie

- 01 Informatique : www.01informatique.fr – 25 mai 2009
- AFAI : www.afai.fr – 25 mai 2009
- Best Practices SI : www.bestpractices-si.fr – 2 mai 2009
- CIO-Online : www.cio-online.com – 25 mai 2009
- ISACA: www.isaca.org – 2 février 2009
- ISO : www.iso.org – 2 février 2009
- ITGI : www.itgi.org – 20 mai 2009
- ITIL France : www.itilfrance.com – 25 mai 2009
- Portail des meilleurs pratiques : www.itil.fr – 25 mai 2009
- Piloter.org : www.piloter.org – 25 mai 2009
- Wikipedia : www.wikipedia.org – 25 mai 2009

Glossaire

AFAI

Association Française de l'Audit et du Conseil Informatique - Équivalent français du site américain de l'ISACA

Audit

L'audit des systèmes d'information) est l'évaluation du niveau de contrôle des risques associés aux activités informatiques. L'objectif apparent est d'améliorer la maîtrise des systèmes d'information d'une entité. L'objectif réel est d'assurer le niveau de service adéquat aux activités d'une organisation. Afin d'adapter ses investigations au sujet de son audit, l'auditeur peut se baser sur des référentiels tels que CobiT, ITIL, et les normes ISO.

ERP

Enterprise Resource Planning en anglais, littéralement « planification des ressources de l'entreprise », expression rendue généralement par « gestion intégrée », à savoir l'intégration des différentes fonctions de l'entreprise dans un système informatique centralisé configuré selon le mode client-serveur. ERP system sera traduit par « progiciel de gestion intégré »

Gouvernance d'entreprise

La gouvernance d'entreprise est l'ensemble des processus, réglementations, lois et institutions influant la manière dont l'entreprise est dirigée, administrée et contrôlée.

ISACA

Information Systems Audit and Control Association - Le site de l'ISACA est l'équivalent américain du site de l'AFAI. Il est la référence des sites Internet consacrés à l'Audit et au Conseil en Informatique. Avec plus de 86 000 membres répartis sur 160 pays, l'ISACA ® (www.isaca.org) est un acteur majeur, reconnu au plan international, de la gouvernance, du contrôle, de la sécurité et de l'audit des systèmes d'information. Fondée en 1969, l'ISACA sponsorise des conférences internationales, publie le journal ISACA Journal®, et développe des normes et référentiels en matière d'audit et de contrôle des systèmes d'information. L'association gère également les certifications professionnelles, reconnues au plan international.

ISO

L'Organisation internationale de normalisation (International Organization for Standardization), ou ISO est un organisme de normalisation international composé de représentants d'organisations nationales de normalisation de 158 pays. Cette organisation créée en 1947 a pour but de produire des normes internationales dans les domaines industriels et commerciaux appelées normes ISO. L'ISO est le plus grand organisme de normalisation au monde.

ITGI

The IT Governance Institute - L'Institut de la Gouvernance des Systèmes d'Information a été fondé par l'Afai et le Cigref en mai 2004. Il est un des premiers instituts nationaux de gouvernance des systèmes d'information affiliés à l'IT Governance Institute.

ITIL
ITIL (Information Technology Infrastructure Library pour "Bibliothèque pour l'infrastructure des technologies de l'information") est un ensemble d'ouvrages recensant les bonnes pratiques ("best practices") pour la gestion des services informatiques (ITSM), édictées par l'Office public britannique du Commerce (OGC).

Loi Sarbanes-Oxley
Aux États-Unis d'Amérique, la loi de 2002 sur la réforme de la comptabilité des sociétés cotées et la protection des investisseurs est une loi fédérale imposant de nouvelles règles sur la comptabilité et la transparence financière. Elle fait suite aux différents scandales financiers révélés dans le pays aux débuts des années 2000, tels ceux d'Enron et de Worldcom. Le texte est couramment appelée loi Sarbanes-Oxley, du nom de ses promoteurs les sénateurs Paul Sarbanes et Mike Oxley. Ce nom peut être abrégé en SOX, Sarbox ou SOA.

Loi de Sécurité financière
La loi de sécurité financière (LSF), aussi appelée Loi Mer du nom du Ministre des Finances en poste Francis Mer, a été adoptée par le Parlement français le 17 juillet 2003 afin de renforcer les dispositions légales en matière de gouvernance d'entreprise. La LSF est parue au JO no 177 du 2 août 2003 (no 2003-706 du 1er août 2003). Cette nouvelle loi s'applique à toutes les sociétés anonymes ainsi qu'aux sociétés faisant appel à l'épargne publique ; ces dispositions sont applicables pour les exercices comptables ouverts à partir du 1er janvier 2003.

Processus métier
Ensemble des activités internes d'un métier dont l'objectif est de fournir un résultat observable et mesurable pour un utilisateur individuel du métier.

Service
Une prestation immatérielle composable, manifestée de manière perceptible et qui, dans une condition d'utilisation définie est source de valeur pour le consommateur et le fournisseur.

Système d'information
Un système d'information (noté SI) représente l'ensemble des éléments participant à la gestion, au stockage, au traitement, au transport et à la diffusion de l'information au sein d'une organisation.

Annexes

- Annexe 1 : Acteurs de la Gouvernance IT
- Annexe 2 : Fiche création d'entreprise 1
- Annexe 3 : Fiche création d'entreprise 2

Annexe 1 : Les acteurs de la Gouvernance IT

En parlant de Gouvernance IT, il est essentiel de savoir qui sont les différents "acteurs" de celle-ci. Il apparait évident que l'on peut mettre dans cette liste les auteurs de référentiels ou les organismes de contrôle ou les associations d'utilisateurs,… Nous allons décrire les principaux organismes dans le monde et en France:

- **Organismes références sur la Gouvernance IT**
  - AIS (*Association for Information Systems*): Organisation professionnelle dédiée aux universitaires et chercheurs spécialisés dans les systèmes d'information.
    (http://www.aisnet.org)
  - ITGI (*IT Governance Institute*): Institut chargé d'assister les entreprises dans la définition et les objectifs de la gouvernance de systèmes d'information. (http://www.itgi.org)
- **Organismes auteurs de référentiels**
  - COSO (*The Committee of Sponsoring Organizations of the Treadway Commission*): Organisation spécialisée dans l'étude et l'approche du contrôle interne. (http://www.coso.org)
  - ISACA (*Information Systems Audit & Control Association*): Cette association compte 86000 membres dans le monde. L'ISACA édite le COBIT et élabore les certifications CISA et CISM.
    (http://www.isaca.org)
  - OGC (*Office of Government Commerce*): Ministère britannique du Commerce. Ils sont les administrateurs d'ITIL.
  - SEI (*Software Engineering Institute*): Organisme définissant les modèles d'évaluation de maturité (CMM)
    (http://www.sei.cmu.edu)
- **Organismes de normalisation, certification**
  - ISO (*International Organization for Standardization*): Organisme de normalisation.
    (http://www.iso.org)
  - BSI Group (British Standards Institution): Organisme britannique de normalisation.
    (http://www.bsi-global.com)

- **Organismes divers**
  - AFAI (*Association Française de l'Audit et du Conseil Informatique*): Fédération des acteurs de l'audit et du conseil en informatique.
    (http://www.afai.fr)
  - IGSI (*Institut de la Gouvernance des Systèmes d'Information*): Institut de recherche crée en partenariat du Cigref et de l'AFAI.
    (http://www.afai.asso.fr/index.php?m=130)
  - Cigref: (*Club Informatique des GRandes Entreprises Françaises*): Créé en 1970, cette association regroupe plus de cent très grandes entreprises et organismes français et européens de tous les secteurs d'activité (banque, assurance, énergie, distribution, industrie, services...).
    (http://www.cigref.fr)

Annexe 2 : Fiches création d'entreprise 1

Édition de logiciels appliqués à la Gouvernance IT

Service ou produit	La société est une société d'édition et d'intégration de solution (logiciel) dans le domaine de la gouvernance IT. En effet, la DSI a de plus en plus besoin de solutions efficaces afin de mieux gérer son SI, que ce soit en matière de gestion des risques, gestion des ressources…
Le marché	
- Actuel	Les solutions existent et sont assez nombreuses mais certaines solutions sont difficiles à mettre en place ou sont trop chère.
- Les tendances	L'offre tend vers la nouveauté, avec des solutions plus adaptée et plus efficaces, accessibles plus facilement par exemple grâce à des solutions sur Internet.
Concurrence	
- Actuelle	La concurrence n'est pas très rude mais les éditeurs actuels bénéficient de leur notoriété pour vendre leurs solutions.
- Future	Le nombre de société sur le marché ne semble pas augmenter contrairement à l'offre.
Localisation	Présence nationale voire internationale
Ressources	
- Humaines	Équipe d'Ingénieurs et de développeurs. Il sera aussi nécessaire, des spécialistes du domaine (gouvernance IT) afin qu'ils apportent leur expériences en matière de gouvernance IT.
- Matérielles	Local commercial de développement.
- Financières	Un certain capital sera nécessaire mais si la solution s'avère efficace et séduit les clients, le bénéfice est assuré.
Échéance	Le plus tôt possible serait le mieux. En effet, les solutions existantes se voient déjà concurrencées par ces nouvelles offres. La société aura intérêt pour survivre à proposer le plus tôt possible une offre convaincante et performante.

Annexe 3 : Fiche création d'entreprise 2

Société de Conseil en Gouvernance IT

Service ou produit	La société est une société de conseil telles qu'on les connait aujourd'hui. Cependant, celle-ci est spécialisée dans le domaine de la Gouvernance IT et vise le marché des PME/PMI. La mission de notre société est de les aider à développer des démarches d'adoption de référentiels de Gouvernance IT au sein de leur système d'information.
Les clients	5% des PME françaises ont plus de 10 employés et donc potentiellement un système d'information. Cela représente environ 130 000 entreprises qui sont aujourd'hui peu informée sur les enjeux de la gouvernance IT.
- Marché actuel	Très peu de PME ont mis en place des plans de gouvernance IT au sein de leur SI à cause de la complexité et de l'importance des ressources à mettre en œuvre. Cependant le besoin est là.
- Les tendances du marché	De nouveaux outils spécifiques aux PME sont en cours d'élaboration. Dès que ceux-ci seront à la disposition des entreprises, ces dernières pourront entreprendre sereinement l'adoption d'une démarche de gouvernance IT.
Concurrence	
- Actuelle	Le marché étant quasi-inexistant, il n'y a pas de réelle concurrence actuellement.
- Future	Les SSII et autres grands cabinets de conseil vont probablement vouloir occuper une place sur ce segment.
Localisation	Toute la France, mais l'Europe aussi.
Ressources initiales	
- Humaines	Consultants spécialistes de la gouvernance IT ; Commerciaux pour prospecter et développer le marché
- Matérielles	Pas de local commercial. Les missions peuvent s'exécuter chez le client.
- Financières	Le marché étant nouveau, il faut pouvoir vivre quelques mois sans l'assurance de signer des contrats de suite.
Échéance	Quelques mois… En effet, dans les mois prochains, de nouvelles offres d'outils (référentiels tel FUSING, normes,…) seront disponibles aux PME. Ces sur ces outils que l'on pourra appuyer notre activité.