



AB Consulting
Conseil en Gouvernance IT

<http://www.ab-consulting.eu>

Gouvernance IT et Normalisation

Alain Bonneaud
AB Consulting
v1.1 - 03/11/2008

Livre blanc rédigé par Alain Bonneaud, CEO de AB Consulting et QualiTI7 France, certifié ISO 20000 consultant auprès de l'ITSMF UK

© AB Consulting – 2008

Tous droits réservés. Ce document ne peut être reproduit et/ou diffusé en tout ou partie sans l'autorisation explicite et écrite de la société AB Consulting. Aucune partie de ce document ne peut être reproduite, archivée ou transmise sous quelque forme ou par quelque moyen que ce soit sans l'autorisation préalable de la société AB Consulting.

Les informations contenues dans ce document sont susceptibles d'être modifiées sans préavis par la société AB Consulting. Elles sont données uniquement à titre indicatif, et la société AB Consulting ne saurait être tenue pour responsable de l'usage qui en sera fait.

Les marques et noms déposés qui sont cités dans ce document appartiennent à leurs propriétaires respectifs.

Pour toute information complémentaire, contacter AB Consulting – 38 rue des Mathurins – 75008 Paris (France) – Tél +33 (0)662 254 501 - Fax : +33 (0) 142 652 840 – Web : <http://www.ab-consulting.eu> – email : webmaster@bonneaud.net

GOVERNANCE IT vs GOVERNANCE CORPORATE

Pour se développer dans un marché globalisé et hyper concurrentiel, les entreprises, qu'elles soient publiques ou privées, doivent désormais offrir à leurs actionnaires des garanties quant à leur capacité à créer et à préserver de la valeur. Cette approche, directement héritée des scandales financiers qui ont ébranlé l'économie américaine dans les années 2000, impose au management d'appréhender l'IT comme une ressource stratégique et non plus comme un moyen technique de soutien à l'activité de l'entreprise. Cette recomposition des éléments fondamentaux de l'entreprise implique, de fait, de nouvelles règles au niveau du management des technologies de l'information. L'IT Gouvernance qui incarne cette évolution change donc profondément le mode de fonctionnement des directions informatiques. Afin d'éviter une certaine réserve, voire une réticence, chez certains collaborateurs, notamment lorsqu'ils sont en charge de la gestion de systèmes d'information, la démarche de gouvernance doit être impulsée et accompagnée par les plus hautes instances de l'organisation. Ce point est fondamental car les enjeux n'ont jamais été aussi importants pour l'entreprise ou pour les ressources IT. En effet, depuis quelques années, les nouvelles règles de management permettent aux services informatiques d'être reconnus comme étant les principales fondations de l'entreprise. Ce passage du niveau tactique, porté par une logique de support, au niveau stratégique est l'aboutissement de l'IT Gouvernance qui représente un véritable phénomène de fond.

On parle fréquemment de Gouvernance d'Entreprise, de Gouvernance Publique ou de Gouvernance des Marchés pour expliquer que, grâce à ces nouveaux dispositifs, les institutions, les organisations, les entreprises (publiques ou privées) peuvent fonctionner plus efficacement dans un contexte globalisé, mondialisé et plus exigeant que jamais.

Pour comprendre les enjeux que cache le mot « Gouvernance », il faut bien comprendre le sens même de ce mot. La gouvernance d'entreprise est la traduction d'une expression nord-américaine « Corporate Governance ». La Gouvernance est la base d'un concept assez simple qui cherche à rassembler les institutions, les relations, les règles et les comportements dans le but d'obtenir des relations puis des décisions bénéfiques ou, pour le moins, acceptables pour l'ensemble. Soucieux d'apporter une meilleure clarté vis-à-vis de l'idée de gouvernance d'entreprise, certains experts ont synthétisé ce principe à partir de 3 éléments clés : Structure, Procédure, Comportement.

La gouvernance d'entreprise est intimement liée à la séparation entre les parties détentrices des droits (les actionnaires) et les mandataires en charge de l'administration de l'entreprise (le management). Cette notion de dissociation est le fondement même de la gouvernance qui trouve son champ d'application dans les entreprises bâties sur un mode managérial.



DES CONSTATS ALARMANTS

En 2000, face à la progression alarmante des fraudes financières de la part des sociétés sur le marché américain, la SEC (Securities and Exchange Commission) et l'administration américaine décident d'appliquer une tolérance zéro vis-à-vis des rapports comportant des informations financières frauduleuses. Une majorité d'entreprises nord-américaines vont alors engager des audits internes pour s'assurer de la fiabilité de leur Système d'Information Financier. Sur le plan financier, les premiers résultats révèlent que le coût global des infrastructures informatiques représente de 10 à 40% des coûts de fonctionnement de l'entreprise, en fonction de son secteur d'activité.

Pour des moyens considérés jusqu'alors comme du support logistique, le coût semble totalement disproportionné. Face à ce constat, beaucoup de managers vont chercher à mieux appréhender les enjeux et à vérifier le rendement et l'efficacité de leur direction informatique. Les rapports remis sont à tel point accablants que certains vont engager des audits complémentaires pour vérifier les premiers résultats. Les chiffres sont désastreux : 30 à 35% des projets initiés ne voient jamais le jour, environ 25% de ceux qui arrivent à terme ont du retard, dépassent les budgets ou ne sont pas opérationnels lors de leur mise en place. Le taux d'incidents sur les projets est en augmentation constante de 2 à 4% par an sur les dix dernières années. Les entreprises les plus importantes constatent un taux d'échec presque deux fois supérieur. Dans un grand nombre de cas, seuls 15 à 20% du budget est réellement productif (**Source : Standish Group**). Les systèmes d'information ne valent guère mieux, leurs structures reposent sur des briques empilées depuis plus de vingt ans et forment des ensembles instables dont le coût de maintenance est exorbitant. Les services de support technique sont, quant à eux, dans l'incapacité de gérer les phases de changement dans des conditions acceptables. Pour les grands groupes internationaux, y compris dans le monde bancaire, les problèmes ne se limitent pas aux projets ou aux systèmes d'information. Certaines directions des services informatiques ignorent jusqu'à l'existence de plusieurs dizaines voire de centaines de machines en production. En termes de sécurité, cela signifie un niveau de risque très élevé, inacceptable dans le monde bancaire en particulier. Côté des serveurs, on constate qu'ils sont exploités à hauteur de 20 à 30% de leur capacité. Quant aux comportements, tout y passe : prés carrés dans les services, baronnies au niveau des directions, choix techniques aberrants, autisme des équipes, ... etc.

Par conséquent pour changer cet état de fait et améliorer fortement l'efficacité des services informatiques en mettant en place des moyens de supervision et de contrôle, une notion va voir le jour, c'est l'IT Management qui permet de se focaliser sur les objectifs suivants :

- Meilleure gestion décisionnelle au niveau du management
- Meilleur contrôle de l'activité informatique



- Clarification du rôle de chaque intervenant en amont et en aval de la DSI
- Responsabilisation accrue du personnel et des prestataires
- Maîtrise optimisée des pratiques qui amènent à la fourniture d'un service

Et afin de développer un modèle de management propre à l'IT, les managers doivent prendre en compte plusieurs contraintes spécifiques :

- La technologie : elle implique des facteurs restrictifs dans le périmètre fonctionnel, des facteurs de risques liés à la sécurité, aux délais et aux coûts mais aussi des facteurs de captation d'activité (par exemple la téléphonie sur IP). En outre, l'évolution naturelle de la technologie augmente la difficulté à stabiliser un schéma directeur à moyen terme et donc à mesurer son impact global.
- La responsabilité : toutes les directions d'une entreprise dépendent du fonctionnement de l'ensemble des services informatiques.
- L'organisation : l'externalisation des moyens (BPO : Business Process Outsourcing) implique un management permettant de faire face à des problématiques spécifiques.
- L'adaptation : puisque la définition même de l'informatique est d'être un outil permettant de développer des solutions métiers offrant des services adaptés aux besoins de chacun.
- L'influence sur l'organisation de l'entreprise : depuis près de vingt ans, ce sont, le plus souvent, les structures qui ont évolué autour de l'outil informatique et non l'inverse.
- Enfin l'IT Management doit être applicable à toute entité, indépendamment de sa localisation, de son statut et de son activité.

L'APPORT DES REFERENTIELS DE BONNES PRATIQUES

L'idée de ce mode de management est basée sur une approche privilégiant l'utilisateur, les processus, la technologie et les services. La bibliothèque ITIL va, à partir de 2000, servir de référence, dans le cadre de cette approche, à l'intégration de démarches dites de « Best Practices » largement popularisées en Angleterre ainsi qu'aux Pays-Bas depuis les années 90. Le contrôle étant également au centre des nouvelles préoccupations. Les travaux de l'ISACA sur le COBIT offrent un cadre d'IT Management de plus en plus précis.

A partir de 2002 naît le concept d'IT Governance qui peut se résumer ainsi : *la Gouvernance IT est une conséquence du mécanisme de Gouvernance d'Entreprise visant à réduire les risques opérationnels engendrés par les technologies de l'information à travers des processus*



d'audit et de contrôle destinés à garantir l'intégrité, la complétude et la traçabilité des informations.

Ce concept primitif de Gouvernance IT n'intègre que très partiellement l'IT Management, ce qui semble pour le moins paradoxal pour un dispositif dédié aux technologies de l'information. Des référentiels comme ITIL, ISPL, PMBOK, etc. ne sont pas pris en compte, ce qui s'explique aisément par le fait que les principes de contrôle interne et d'audit des systèmes d'information ont, à l'origine, été définis dans une optique de contrôle des systèmes financiers uniquement. Ce mécanisme de gouvernance ne protège, par conséquent, que très partiellement les actionnaires puisqu'il est principalement destiné à la prévention des malversations financières.

Fin 2002, l'idée de plusieurs chercheurs anglo-saxons est de redéfinir le concept d'IT Gouvernance pour l'appréhender de façon globale. Cette démarche est motivée par le constat que les technologies de l'information sont désormais la fondation primaire de toute activité de l'entreprise. En tant que telles, elles doivent donc, au même titre que la finance, disposer d'un mécanisme de gouvernance spécifique destiné à protéger et soutenir les processus de création de valeur par l'organisation.

Cette vision globale a plusieurs avantages :

- Elle intègre le concept primitif axé sur *le contrôle et l'audit*
- Elle s'appuie sur le dispositif d'*IT Management*
- Elle offre une meilleure protection aux actionnaires

La Gouvernance Informatique comporte huit domaines stratégiques :

- L'alignement IT (alignement stratégique et alignement sur les processus métiers)
- Le management IT
- La gestion des ressources IT
- La gestion des risques IT
- La gestion de la performance IT
- Le contrôle et l'audit
- La valeur financière de l'IT
- La maturité IT

Quel que soit le domaine où elle s'applique, la gouvernance est intimement associée à la notion de meilleures pratiques sur le plan éthique, managérial, financier, sociétal et environnemental. La Gouvernance IT n'échappe pas à cette règle. Le principe de bonnes



pratiques ou de pratiques de références est essentiellement basé sur l'enseignement de l'expérience des autres entreprises, permettant ainsi de capitaliser des connaissances vis-à-vis de processus, de méthodes et de technologies.

De nombreux groupes de travail en Europe et en Amérique du Nord ont élaboré des référentiels de management dédiés au monde de l'IT en se fondant sur le principe des meilleures pratiques. Ces derniers ont généralement une approche verticalisée sur certains domaines comme le développement de logiciel, la fourniture de services, la gestion de projets, la modélisation de processus ou la gestion des risques.

GOVERNANCE IT ET CERTIFICATION

L'enjeu de la certification étant une question de plus en plus présente dans le monde informatique, l'introduction des référentiels IT et leur succès actuel ont conduit à se poser la question de la certification au niveau des personnes et des organisations. Bien souvent, les directions générales, dans le cadre d'une démarche de mise en conformité (SOX), les tiers (tels que les clients), les assureurs et les investisseurs voient dans la certification un gage de fiabilité, de sécurité et de maturité. L'IT Gouvernance permet, grâce à une approche pragmatique d'entamer des démarches de certification, notamment par l'approche des services. Il faut toutefois garder à l'esprit que le principe même de gouvernance implique une forte notion de retour sur investissement. Il est donc indispensable, avant d'entamer une démarche de certification, d'évaluer au préalable la pertinence de cette démarche et de définir le type de certification recherchée : processus de travail, compétences ou bien les deux, en s'assurant que le niveau de risque inhérent à l'activité informatique est minimisé.

Afin de répondre à une attente forte en terme de norme pouvant conduire à une certification de personnes et d'organisations, l'organisation internationale de normalisation ISO a publié en décembre 2005 la norme ISO 20000 « IT Service Management » qui fait la promotion de démarches très répandues, basées sur ITIL, telles que

- l'approche processus,
- l'amélioration continue au niveau de la fourniture des services informatiques,
- l'alignement des exigences business de l'organisation ainsi que des besoins des clients...

Cette norme se compose de deux publications :

- « Part 1 Spécification for service management » énonçant les spécifications pour le management des services IT. Celles-ci peuvent être auditées en interne et par un Registraire reconnu.



- « Part 2 Code of practice for service management » propose un guide d'application et formule des recommandations pour la mise en œuvre des spécifications énoncées dans la partie 1.

Un groupe de travail (WG25) s'est formé au cours de l'année 2006 pour la faire évoluer dans le cadre d'un processus d'amélioration continue. Ce même groupe fait partie du comité JTC1/SC7 de l'ISO et comporte des représentants des organisations nationales de normalisation adhérentes de l'ISO.

Parallèlement, un second groupe de travail spécialisé sur l'intégration de la gouvernance IT à la gouvernance d'entreprise a vu le jour en 2006, au sein du comité JTC1/SC7, avec l'objectif d'étudier la relation entre la gouvernance IT les autres normes. Le but de son action est l'établissement des principes de base d'une bonne gouvernance et les composants essentiels des processus, des référentiels et des métriques démontrant la maturité d'une organisation. Il a d'ores et déjà abouti à des préconisations dans ce sens et des grandes orientations ont été déterminées lors de l'assemblée plénière qui s'est tenue à Berlin en Mai 2008. Une première publication de la norme « ISO 38500 » : Gouvernance des technologies de l'information par l'entreprise, a d'ores et déjà été réalisée en juin 2008.

A propos de AB Consulting

AB Consulting est un centre de compétences spécialisé dans les problématiques d'organisation, de maîtrise des coûts et de création de valeur pour les métiers de l'entreprise grâce à l'optimisation de leur système d'information, en s'appuyant sur les référentiels de bonnes pratiques, les modèles de maturité, les méthodologies et les normes associées à la gouvernance informatique (ITIL, ISO 20000, CobiT, CMMi, MOF, MSF). Tous les consultants de AB Consulting Eu sont certifiés et agréés pour assister les directions de grands groupes au niveau stratégique, dispenser des formations, intervenir en qualité de conseils à la mise en œuvre ainsi que pour réaliser des audits en entreprise.

AB Consulting est présent dans de nombreuses régions du monde (Europe, Amérique du Nord, Asie, Afrique) grâce à un réseau de partenaires locaux parmi lesquels Softnet Burkina à Ouagadougou et Advantech CI à Abidjan

A propos de l'auteur

Alain Bonneaud possède la certification ISO 20000 Consultant délivrée par l'ITSMF UK ainsi que les certifications ITIL délivrées par l'EXIN, la certification CobiT Foundation de l'ISACA et la certification MOF Foundation de Microsoft. Il possède également la reconnaissance de compétence CMMi délivrée par le Carnegie Mellon University (US).

Alain dirige le cabinet AB Consulting à Paris ainsi que QualiTI7 France, représentant pour l'EMEA le cabinet de conseil QualiTI7 International, dont le siège est situé au Canada. Il intervient régulièrement en qualité de conseil dans les domaines de l'organisation et de la refonte des processus SI ainsi que dans la mise en place de méthodologies et de référentiels "best practices" auprès d'organisations de toutes tailles dans le cadre de leurs projets de certification à la norme ISO 20000.

Membre de l'ITSMF, Alain est membre depuis 2008 du comité JTC1/SC7 de l'ISO au sein duquel il participe aux groupes de travail WG1A sur la Gouvernance IT et WG25 sur l'évolution de la norme ISO 20000, en qualité de chef de délégation pour la Côte d'Ivoire. Le comité JTC1/SC7 est chargé de la définition et de l'amélioration continue des normes ISO dans les domaines Software et System Engineering ainsi que des leur intégration avec les autres normes ISO (ISO 9001-2005 et ISO 27001 en particulier). Il anime fréquemment des séminaires et des conférences sur la gouvernance IT et l'intégration de la gouvernance SI à la gouvernance Corporate au niveau international.

