Chapitre 1

Présentation générale de CobiT

Historique de CobiT

CobiT est le résultat des travaux collectifs réalisés par les principaux acteurs de la profession, auditeurs internes ou externes, fédérés au sein de l'ISACA (*Information System Audit and Control Association*). Cette association mondiale basée aux États-Unis est déployée dans les plus grandes villes du monde. Elle est représentée en France par l'AFAI (Association française pour l'audit et le conseil en informatique).

Dans ses premières versions, publiées à partir de 1996, CobiT (*Control OBjectives for Information and related Technology*) se positionne comme un référentiel de contrôle. Il décline sur le domaine IT les principes du référentiel COSO (*Committee of Sponsoring Organizations of the Treadway Commission*), publiés pour la première fois en 1992 et dont l'objectif est d'aider les entreprises à évaluer et à améliorer leur système de contrôle interne.

La mise en chantier de CobiT résultait donc de la volonté des auditeurs de répondre aux exigences du COSO et de partager les mêmes plans d'audit. La plupart des grands cabinets d'audit internationaux (les *big* 6 à l'époque) y ont participé. C'est ainsi devenu un standard de fait, au moins pour les auditeurs informatiques. On y trouvait l'essentiel de la structuration actuelle en domaines, processus et objectifs de contrôle détaillés.

En 1998, l'ITGI (*Information Technology Governance Institute*) a été créé sur l'initiative de l'ISACA, en réponse à la place de plus en plus importante occupée par les technologies de l'information. En effet, dans la plupart des organisations ou des entreprises, l'un des principaux facteurs de succès réside dans la capacité des systèmes d'information à apporter à la fois la

Des Big 8 aux Big 4

Dans les années 1970-1980, les principaux groupes d'audit mondiaux étaient surnommés les *Big 8* ; il s'agissait de : Arthur Andersen, Arthur Young, Coopers & Lybrand, Ernst & Whinney, Haskins & Sells (fusionné avec Deloitte), KPMG, Price Waterhouse, Touche Ross.

Dans les années 1990, les *Big 8* deviennent les *Big 6* suite à la fusion d'Erns & Whinney avec Arthur Young pour former Ernst & Young, et de la fusion de Deloitte, Haskins & Sells avec Touche Ross pour créer Deloitte & Touche.

En 1998, les *Big 6* deviennent les *Big 5,* suite à la fusion de Price Waterhouse et Coopers & Lybrand pour former PricewaterhouseCoopers.

Depuis 2002 et le scandale Enron qui a abouti au démantèlement d'Andersen, on parle des *Big 4*. (Deloitte, Ernst & Young, KPMG, PricewaterhouseCoopers).

différenciation stratégique et le support des activités. Dans un tel contexte, la « gouvernance » des systèmes d'information devient aussi critique que la gouvernance d'entreprise.

Depuis une dizaine d'années, l'ITGI a mené de nombreuses recherches au travers de groupes de travail répartis dans le monde entier. Le résultat de ces recherches a notamment donné lieu en 2000 à la publication de la version V3 du référentiel CobiT proposant, parallèlement à un « guide d'audit », un « guide de management » préfigurant les versions ultérieures.

À la suite des scandales ayant eu lieu au début des années 2000 (Enron, etc.), le Congrès américain vote, en 2002, la loi Sarbanes-Oxley (SOX) afin de redonner confiance aux investisseurs et aux actionnaires en garantissant à la fois la transparence des comptes, l'existence de processus d'alerte et l'engagement des dirigeants (PDG, DAF). Ceci se traduit par un renforcement des contrôles liés aux processus financiers. On retiendra, par exemple, la section 404 qui exige un contrôle strict des accès et des autorisations. CobiT a été reconnu comme une réponse à ces nouvelles exigences, tant en termes de contrôle que de gouvernance.

La généralisation de la loi SOX ou de ses déclinaisons locales ou sectorielles (IFRS, I*nternational Financial Reporting Standards*, LSF, Loi de sécurité financière, normes Bâle II) a considérablement renforcé le rôle des auditeurs. Ces dispositions réglementaires ont accéléré la diffusion de CobiT comme référentiel de contrôle et de gouvernance des SI. Ensuite, l'ISACA a publié successivement la version 4 (décembre 2005) puis la version 4.1 (2007) de CobiT, en regroupant deux visions : le « contrôle » et le « management » des systèmes d'information (SI) et, plus largement, des technologies de l'information (TI)[1].

1. Information Technology (IT) : se rapporte tantôt au potentiel global offert par les technologies de l'information (TI), ou à leur utilisation dans l'entreprise sous forme de systèmes d'information (SI).

CobiT et la gouvernance TI

L'apport de CobiT

En tant que référentiel de la gouvernance des systèmes d'information, le périmètre de CobiT dépasse celui dévolu à la direction des systèmes d'information pour englober toutes les parties prenantes des SI dans l'entreprise (*stakeholders*[1]). Ainsi, selon CobiT, « la gouvernance des systèmes d'information est de la responsabilité des dirigeants et du conseil d'administration, elle est constituée des structures et processus de commandement et de fonctionnement qui conduisent l'informatique de l'entreprise à soutenir les stratégies et les objectifs de l'entreprise, et à lui permettre de les élargir ».

1. Stakeholders : représente l'ensemble des acteurs concernés par la gouvernance des SI, aussi bien les actionnaires et la direction générale que les métiers. Ce terme est souvent traduit par les *parties prenantes*.

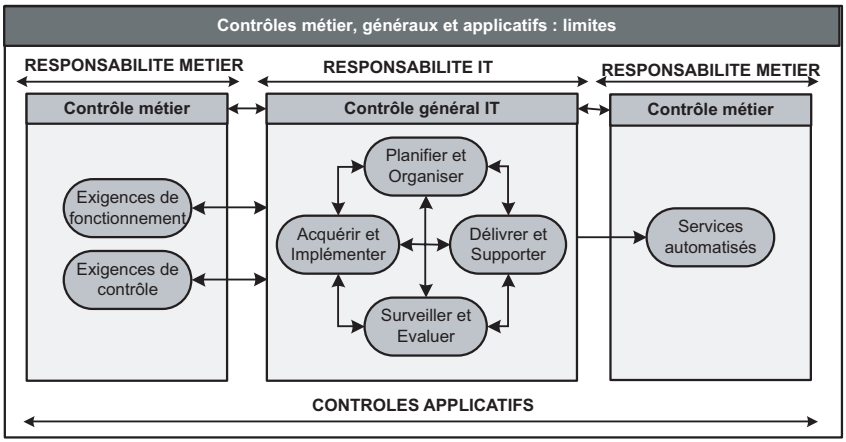

Figure 1-1 : Répartition des responsabilités de la gouvernance TI

La figure 1-1 illustre aussi bien la responsabilité de la fonction IT sur les quatre grands domaines de la gouvernance selon CobiT (planifier et organiser, délivrer et supporter, surveiller et évaluer, acquérir et implémenter) que les responsabilités des métiers.

CobiT se fixe des objectifs très pragmatiques reflétant les préoccupations de la direction générale, tels que :

- articuler le système d'information aux besoins des métiers, c'est l'alignement stratégique ;
- apporter des avantages concrets au fonctionnement des processus métier (efficacité et efficience) ;

- utiliser l'ensemble des ressources en liaison avec les SI (infrastructures, applications, informations et personnes) de façon optimisée et responsable ;
- maîtriser les risques liés au SI et leurs impacts pour les métiers.

1. On entend par processus un ensemble d'activités corrélées qui transforme des éléments entrants en éléments sortants, les activités étant elles-mêmes décrites dans des procédures.

Structuré en processus[1], CobiT prend en compte les besoins des métiers, et plus généralement des parties prenantes, dans une logique d'amélioration continue. Le préalable à toute diffusion de CobiT est donc la diffusion d'une culture de l'amélioration au service des clients de la DSI. Cette approche rappelle l'ISO 9001.

Les entrées des processus CobiT sont basées sur les exigences négociées des parties prenantes (métiers, etc.) conduisant à des objectifs. Ensuite, l'exécution des processus est garantie par des responsabilités clairement affectées et des mesures de performances face aux objectifs fixés. La satisfaction des « clients » fait partie des mesures de performance.

À ce stade, l'originalité de CobiT est sans doute de créer systématiquement un lien entre parties prenantes et DSI, ce qui nécessite bien souvent une petite révolution culturelle aussi bien pour les acteurs de la DSI dans leur tour d'ivoire que pour les métiers et la direction générale qui ignoreraient superbement le caractère stratégique des SI. Le point clé sous-jacent à cette démarche est l'instauration de dialogues constructifs à tous les niveaux de l'organisation, entre parties prenantes et DSI.

Ce postulat posé, chaque processus propose une liste d'objectifs de contrôle qui nous semble solide et une vision du management du processus (activités principales, responsabilités et indicateurs) qui nous paraît plutôt indicative et sujette à contextualisation.

Le référentiel CobiT, avec ses 34 processus génériques, est une proposition qui pourra être revue pour s'adapter à la cartographie propre de l'organisation considérée. De la même façon, on pourra facilement coupler CobiT à d'autres référentiels du marché (ISO 27001, ITIL pour I*nformation Technology* I*nfrastructure* L*ibrary* ou CMMI pour C*apability* M*aturity* M*odel* I*ntegration*) en bâtissant un cadre de référence satisfaisant l'ensemble des exigences. Ceci est d'autant plus vrai que les processus de CobiT sont parfois globaux et s'interprètent souvent comme des « macroprocessus » de référentiels plus spécialisés. CobiT est donc un cadre fédérateur.

CobiT sert aussi à comparer entre elles (*benchmark*) différentes entités de l'entreprise. Il permet également, avec les restrictions d'usage, de se comparer à d'autres entreprises. Plus couramment, il conduit à la définition de ses propres objectifs et à leur évaluation périodique.

Les membres de l'ISACA utilisent CobiT dans de nombreux secteurs d'activité à travers le monde. Les spécificités culturelles et les différences d'avance de développement sur le plan technologique ne semblent pas limiter l'adéquation de CobiT pour l'alignement des systèmes d'information aux objectifs stratégiques de l'entreprise.

Les cinq axes stratégiques

En réponse à la volonté d'exercer une bonne gouvernance des SI, CobiT s'attache aux cinq axes présentés ci-après.

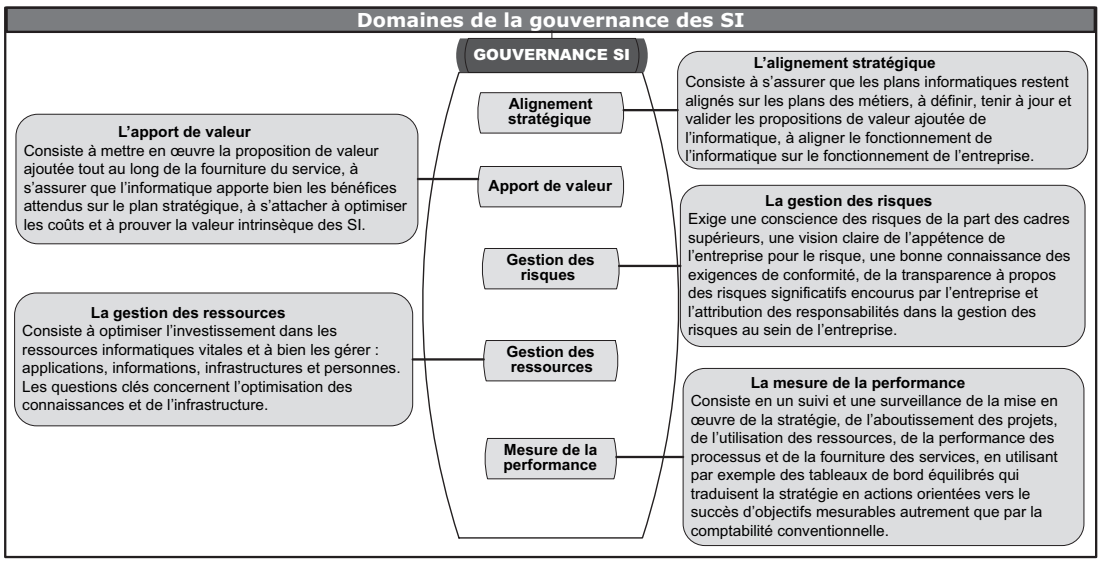

Figure 1-2 : Les domaines de la gouvernance des TI

L'alignement stratégique

Les activités informatiques prennent de plus en plus d'importance dans le fonctionnement des métiers de l'entreprise. Il est donc indispensable que la réponse de l'informatique soit celle attendue par les métiers. Prenons, par exemple, une direction marketing qui souhaite lancer un nouveau produit ou service. Il est indispensable de s'assurer que les exemplaires de ce produit, lorsqu'ils seront disponibles, pourront être commandés puis facturés. Si le canal de commande est le Web, la disponibilité de l'application de commande en ligne doit être assurée avec l'ensemble des éléments nécessaires à la commande du produit (références, prix, conditions particulières, etc.). Par alignement stratégique, il faut donc entendre la capacité à fournir les services souhaités en temps et en heure avec le niveau de qualité requis.

Dans le cas de notre direction marketing, cela signifie que le projet de mise à disposition de commande en ligne doit être identifié et priorisé dès la réflexion amont par la direction marketing, ceci afin d'être dans les temps au moment de l'annonce du produit au marché. L'alignement stratégique se matérialise par un plan stratégique qui devra traiter des budgets d'investissements et de fonctionnement, des sources de financement, des stratégies de fourniture et d'achats tout en intégrant les exigences légales et réglementaires.

L'apport de valeur

L'informatique doit également pouvoir apporter un gain identifiable dans la bonne exécution des processus métier. Dans le cas de notre direction marketing, l'apport de valeur va se matérialiser par la mise en place d'un canal de distribution adressant une nouvelle clientèle. Il permettra la vente permanente du produit tout en s'affranchissant des contraintes de la distribution classique organisée autour d'un lieu géographique et de plages horaires plus limitées que l'accès Web. Dans le processus de distribution, l'apport de l'informatique doit pouvoir être mesuré afin d'identifier la valeur apportée en termes de volume de ventes, de progression de chiffre d'affaires et de marge par rapport aux prévisions. L'apport de valeur se concrétise par la maîtrise des processus de fonctionnement en termes d'efficacité et d'efficience. Ceci vient compléter le processus de pilotage des investissements qui traitera des coûts, des bénéfices et des priorités en fonction de critères d'investissement établis (ROI [*Return On Investment*], durée d'amortissement, valeur nette actuelle).

La gestion des ressources

Les ressources pour mesurer l'activité informatique doivent être optimales pour répondre aux exigences des métiers. Dans notre exemple de direction marketing, cela revient à dire que les ressources humaines et technologiques sont mobilisées au mieux en termes de volume, d'expertise/compétences, de délai et de capacité. Cette gestion des ressources se matérialise par une cartographie des compétences et un plan de recrutement/formation en ce qui concerne les ressources humaines. Cette gestion des ressources est articulée à la gestion des tiers afin d'optimiser le *make or buy*[1].

Les ressources technologiques font partie du périmètre et donneront lieu à un plan d'infrastructure. Celui-ci traitera des orientations technologiques, des acquisitions, des standards et des migrations. Dans ce cas, la responsabilité du métier consiste à exprimer ses besoins, par exemple, en termes de capacité (comme le nombre de clients en ligne simultanément).

1. Make or buy : décision stratégique de confier une activité à un tiers ou de la développer en interne. Ainsi, par exemple, les centres d'appel pour le support informatique sont souvent confiés à des tiers. Les raisons de ce choix sont multiples : compétences à mobiliser, masse critique, professionnalisation, logistique, temps de mise en œuvre, prix.

La gestion des risques

Dans certains secteurs, l'activité cœur de métier de l'entreprise peut être mise en péril en cas d'arrêt ou de dysfonctionnement de ses systèmes informatiques, car la dépendance des processus métier envers l'informatique est totale. Dans notre exemple de distribution par le Web, si ce canal est le seul prévu pour le produit en question, l'indisponibilité pour cause de panne ou de retard dans l'ouverture du service de commande en ligne se solde par une perte nette de revenus qui ne sera jamais récupérée. Dans le secteur du transport aérien, la panne du système de réservation peut clouer au sol l'ensemble des avions d'une compagnie. Dans le monde boursier, l'arrêt des systèmes informatiques stoppe immédiatement toutes les transactions. La gestion des risques informatiques ou des systèmes d'information correspond à un référentiel qui comprend une analyse de risque et un plan de traitement des risques associé. Ce plan de traitement des risques doit être établi selon des critères de tolérance par rapport au préjudice financier lié à la réalisation des risques. Cela veut dire en d'autres termes que les moyens engagés pour couvrir les risques ne doivent pas coûter plus cher que le préjudice lui-même.

La mesure de la performance

La mesure de la performance répond aux exigences de transparence et de compréhension des coûts, des bénéfices, des stratégies, des politiques et des niveaux de services informatiques offerts conformément aux attentes de la gouvernance des systèmes d'information. Là encore, CobiT tente de faire le lien entre les objectifs de la gouvernance et les objectifs à décliner sur les processus ou les activités. Ce faisant, on crée du lien et on donne du sens aux objectifs de performance des SI comme support aux métiers.

Ces mesures peuvent facilement se traduire par la mise en place d'un BSC (B*alanced Scorecard*[1]) qui va offrir une vision d'ensemble de la performance.

1. BSC, Balanced Scorecard (ou tableau de bord équilibré) : représentation de la performance de l'entreprise selon 4 quadrants – le financier, la relation client, l'anticipation et l'opérationnel. Le BSC a été développé en 1992 par Robert S. Kaplan et David Norton.