Chapitre 9

CobiT fédérateur

L'implémentation pragmatique de CobiT vise à donner une réponse rapide et évolutive au souci de gouvernance des TI. En s'appuyant sur l'existant, on choisit l'angle d'attaque le plus approprié aux priorités à gérer. La question est à chaque fois de savoir jusqu'où aller dans les processus à déployer en restant dans les limites d'un projet d'envergure appropriée.

Le pilotage stratégique

L'une des conditions essentielles du pilotage stratégique est l'engagement de la direction générale et des métiers. De la même façon, la stratégie d'entreprise est une condition nécessaire à sa déclinaison sur le domaine des TI.

Le Balanced Scorecard (BSC) est une représentation intéressante pour illustrer le pilotage stratégique des SI. Certains clients nous demandent souvent s'il est nécessaire que le BSC soit adopté au niveau de l'entreprise. Il est certain que ce serait bon signe mais ce n'est pas indispensable à la tenue d'un BSC sur la gouvernance des TI.

Les sections suivantes présentent l'utilisation des quatre cadrans du BSC.

Cadran 1 – Contribution stratégique

La contribution stratégique se reflète au travers des résultats des processus de haut niveau.

On y trouve en particulier le plan à trois ans (processus PO1), les investissements (processus PO5), la gestion des risques (processus PO9), le portefeuille de projets (processus PO10) et la surveillance de la gouvernance

(processus SE4). D'autres processus peuvent y être ajoutés mais ceux précités nous semblent être les plus importants.

Cadran 2 – Relation client

La relation aux clients de l'informatique concerne essentiellement les utilisateurs du SI (internes ou externes à l'entreprise) et les donneurs d'ordre dans les métiers (maîtrises d'ouvrage). Ce cadran est piloté par la contractualisation des niveaux de services (processus DS1) qui fixe non seulement des seuils aux objectifs de performance mais aussi des devoirs pour les métiers (former les utilisateurs) et des limites (c'est-à-dire consommation des services prévue, comme le nombre d'utilisateurs susceptibles de contacter l'assistance).

Les processus DS8 et DS10 sont essentiels au fonctionnement de cette relation client.

Interpréter la vision et la stratégie : quatre perspectives

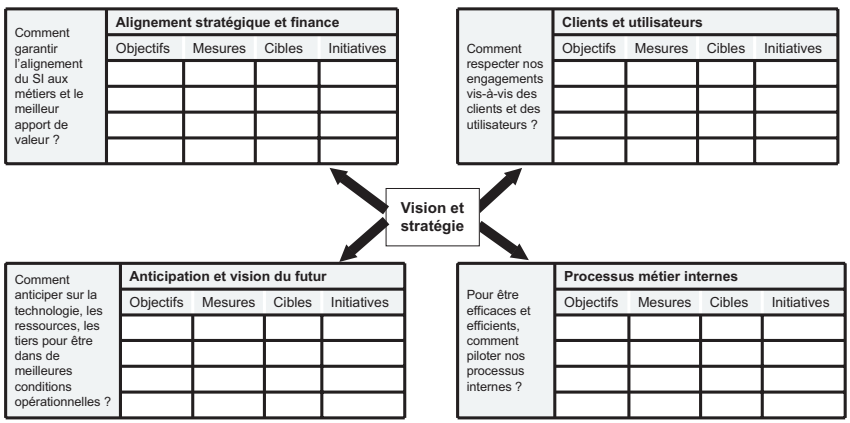

Figure 9-1 : Le Balanced Scorecard (BSC)

Cadran 3 – Futur et anticipation

C'est d'une certaine façon le domaine de la stratégie de la DSI : comment anticiper les besoins en ressources humaines (processus PO7), s'organiser (processus PO4 et PO8), assurer une veille des fournisseurs (processus DS2), anticiper les évolutions technologiques et les besoins métier (processus PO2 et AI1) ou encore faire évoluer les architectures (processus PO3). Tout cet ensemble conditionne le fonctionnement du SI et son coût.

Cadran 4 – Excellence opérationnelle

C'est le fonctionnement de la DSI au quotidien. Il faut, par exemple, gérer l'exploitation (processus DS13), l'environnement physique (processus DS12), les changements (processus AI6), etc.

Les performances opérationnelles sont liées pour partie à des questions intrinsèques et pour une grande part à des considérations autres (anticipation, niveau de risque et alignement stratégique, contrats avec les clients).

Certains exemples de situations observées chez des clients illustrent ce qui ressemble à des compromis :

- administration de 60 serveurs Lotus, là où un projet de regroupement de ces serveurs aboutirait à trois serveurs seulement. Il est clair que tant que ce projet n'a pas été décidé, leur maintenance coûtera plus cher et sera moins fiable ;
- palier technologique permettant de réduire les coûts de maintenance des postes de travail ;
- veille sur les contrats des infogérants et choix d'un redécoupage des domaines externalisés afin d'optimiser la performance des sous-traitants et de minimiser les ressources internes en gestion de contrat ;
- négociation avec les utilisateurs sur la nécessité de développer des programmes spécifiques plutôt que de s'accommoder d'un standard. Arbitrage entre développements et évolution de la demande.

À chaque fois, l'excellence opérationnelle dépend des conditions négociées à d'autres niveaux.

ITIL et le management des services TI

ITIL est le cadre de référence le plus diffusé dans le monde pour le management des services TI ; il est devenu un standard de fait. Notons que le référentiel, qui se présente comme une vaste librairie, comprend aussi d'autres processus mais que le cœur du système et des certifications associées se réfère au management des services TI. C'est le cas en particulier de la certification de la norme ISO/IEC 20000.

Il comporte 10 processus classés en deux domaines, à savoir le support aux services (aspect opérationnel) et la fourniture des services (aspect tactique).

ITIL et CobiT : la complémentarité

ITIL structure son approche du management des services autour de la relation avec les parties prenantes : utilisateurs des TI au quotidien et

maîtrises d'ouvrage pour le pilotage (directions métiers, etc.). CobiT, de la même manière, a mis systématiquement en avant la finalité des TI, à savoir la réponse aux besoins des métiers et le souci d'aligner l'offre à la demande. Les deux approches partagent donc les mêmes valeurs s'agissant du management des services TI.

La figure ci-dessous liste les processus CobiT qui sont les plus proches des processus ITIL. Notons que les noms des processus sont souvent les mêmes, ce qui illustre la prise en compte croissante d'ITIL par les concepteurs de CobiT au fil des versions.

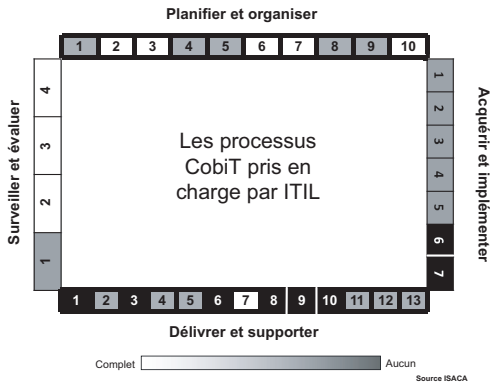

Figure 9-2 : Les processus de CobiT couverts par ITIL V3

Une publication (COBIT M*apping* : *mapping of* ITIL V3 *with* COBIT 4.1) est consacrée aux correspondances (*mapping*) entre CobiT et ITIL ; elle décrit deux niveaux de comparaison. Un niveau global compare les objectifs d'ITIL aux objectifs globaux de CobiT. Pour un détail plus fin, on se base sur la granularité des objectifs de contrôle de CobiT. ITIL a été détaillé en sous-parties associées à un ou plusieurs objectifs de contrôle de CobiT.

Ceux qui s'intéressent ainsi aux correspondances entre CobiT et d'autres référentiels ne manqueront pas d'être frappés du degré très élevé de similitude entre les processus concernés. Sur ITIL V2 par exemple, il semble que l'on puisse pratiquement substituer les 10 processus correspondants de CobiT et réciproquement.

En revanche, deux différences apparaissent clairement : la première concerne la complétude, et CobiT couvre délibérément l'ensemble de la gouvernance des TI ; la seconde concerne le classement en domaines. CobiT privilégie le distinguo entre la fourniture des services (domaine DS) et tout ce qui concerne la mise en œuvre (domaine AI) correspondant à des changements impactant les ressources informatiques.

Pourquoi les associer ?

Les démarches ITIL et CobiT sont souvent menées de façon séparée. ITIL a été une réponse au souci de mieux structurer les centres de services ; c'est pour cette raison que le centre de services est la seule fonction représentée au cœur des processus. Les procédures du centre de services autour de la gestion des incidents (structuration en niveaux, escalade, enregistrement des tickets d'appel, enrichissement des bases de données de résolution, etc.) avaient à s'industrialiser pour faire face aux sollicitations à moindre coût.

Simultanément, un nombre croissant d'organismes a cherché à externaliser ces fonctions de support, qui n'entraient pas forcément dans leur cœur de métier et se révélaient compliquées à gérer et à optimiser en interne. Du côté des outils, les éditeurs en ont proposé des plus en plus complets permettant de gérer l'ensemble des procédures et d'y associer une base de données des ressources informatiques au sens large (tickets d'appel, objets de configuration, mais aussi les descriptions de poste, etc.). Tout cet « arsenal » a été bâti avec le cadre de référence d'ITIL.

Le DSI qui s'intéresse aux référentiels constate donc rapidement que tout un pan du système d'information de la DSI pour elle-même existe ou pourrait rapidement exister, entre le centre de services et l'exploitation, entre les services internes et les tiers. Le travail considérable de structuration, de conception de SI interne, de conduite du changement et de tableaux de bord est fait, et mieux encore, il est opérationnel, à un niveau de détail que CobiT n'atteint pas. La question n'est plus de savoir s'il faut garder ITIL mais comment l'intégrer au mieux dans une vision complète pour la gouvernance des TI.

Conjuguer ITIL et CobiT

Les points clés à prendre en compte pour conjuguer les deux approches sont les suivants.

- **Concilier deux cultures**

  La culture ITIL est pragmatique, sans cesse confrontée aux réalités quotidiennes et orientée plutôt vers le service offert (continuité de service, performance). Elle gère souvent les objets informatiques à un niveau de détail qui ne concerne que les acteurs du support, de la maintenance ou de l'exploitation.

  CobiT, au contraire, risque d'être perçu comme trop théorique, peu applicable et pas assez concret pour être déployé facilement et utilement.

- **Structurer le référentiel d'ensemble**

  Il faut éviter les doublons de processus, ce qui se produit inexorablement si l'on ne décrit pas une cartographie des processus garantissant une cohérence d'ensemble.

- **Réaliser le lien avec les études et les développements**

  ITIL a du mal à se propager vers les équipes d'études et de développements et parfois même, vers l'exploitation. Il n'est reconnu ni dans le pilotage de projets au niveau élémentaire, ni dans la gestion globale des portefeuilles ou des investissements.

  CobiT présente l'avantage de donner un cadre complet qui offre un processus de transition, le PO10, entre ITIL et les études.

- **Bâtir progressivement le modèle de données de la DSI**

  Les acquis d'ITIL sont intéressants mais le risque est grand de tomber dans le détail. Il faut s'appuyer sur la CMDB pour créer le modèle de données de la DSI, veiller à s'en distancier et définir la granularité pertinente des données pour le pilotage.

Deux exemples concrets

Juxtaposition

Dans cet exemple, la DSI a lancé la réorganisation de son service support et exploitation. Cela s'est traduit par la création d'un service desk et la mise en place de contrats d'infogérance pour l'exploitation des ordinateurs centraux et des réseaux. Ensuite, l'externalisation du service desk a permis de gagner plus de 20 % sur les coûts du support.

Notons que l'infogérant avait été aussi choisi pour sa capacité à déployer ITIL. En apparence, la partie était gagnée et pourtant la situation s'est ensuite dégradée, essentiellement en raison de l'absence de vision systémique mais également par ignorance des points à mettre sous contrôle.

Simultanément, la DSI s'intéressait à CobiT, au moins pour le domaine PO, afin de lancer les bases d'une gouvernance stratégique des systèmes d'information.

Avec le recul, il est manifeste que l'organisation interne au service, la gestion des compétences et de la formation ont été des éléments clés. Les profils ne sont pas les mêmes entre ceux qui lancent une nouvelle organisation et ceux qui vont ensuite la faire fonctionner. Comme toujours, la situation était un peu hybride. Les principaux points de dérive observés sont les suivants.

- **Les processus et leur répartition interne/externe**

  Le service d'assistance et la gestion des incidents étaient clairement sous la responsabilité de l'infogérant, mais :

  – le niveau ultime d'expertise (niveau 3) restait à la charge du client, que ce soit sur des questions génériques (bureautique) ou spécifiques à la société (applications) ;

  – certains processus (par exemple, l'installation d'un nouveau PC) faisaient s'imbriquer les responsabilités selon les activités du processus

(achats, demande de rendez-vous, installation, configuration des droits, etc.) ;

– le processus de gestion des problèmes devenait une sorte d'instance aux frontières du contrat d'infogérance ;

– le service informatique interne avait tendance à rester sur un positionnement technique en recréant en double des activités de surveillance, de veille ou de contrôle minutieux.

- **L'absence de vision systémique au sein de la DSI**

  Le déploiement d'ITIL était limité aux processus liés à l'infogérant et au périmètre du support qui était externalisé. Les interfaces avec les autres services (exploitation, études, pilotage de la DSI) demeuraient des points de friction constants, concernant :

  – la faiblesse du processus de gestion des changements, ce qui réduisait considérablement les bénéfices du support ;

  – l'éclatement de la vision contractuelle « gestion des tiers » et ce, à des niveaux de compétence insuffisants, limitant l'alignement et la cohérence entre les contrats et les obligations. En conséquence, il était difficile de responsabiliser le sous-traitant, mais aussi de créer du travail en interne aux interfaces entre les sous-traitants ;

  – l' absence de levier sur les services études pour faire valoir les priorités à régler, d'où l'impuissance du responsable de gestion des problèmes ;

  – la croissance simultanée du domaine SAP avec son centre de compétences et son organisation propre (centre d'appels, support, TMA, mise en exploitation, etc.), limitant ainsi la pertinence du « point d'accès unique » vu du client.

- **La multiplicité des outils de pilotage**

  La DSI est bien sûr le cordonnier le plus mal chaussé quand il s'agit du système d'information sous-tendant son activité interne. ITIL donne une réponse partielle, sur un périmètre réduit, limité à la gestion des incidents et à la gestion du parc (embryon de gestion des configurations). Les points à régler ne sont pas simples :

  – l'outil de gestion du service d'assistance avait été développé et maintenu par le client et l'infogérant en était un des utilisateurs. Ce point limite bien sûr la responsabilité du tiers mais permet d'assurer un support aux processus aussi bien internes qu'externes. Le choix inverse aurait conduit à créer une interface entre l'outil de l'infogérant et l'outil interne de gestion de la DSI ;

  – les autres services avaient leurs outils (études, centre de compétences SAP, exploitation) et la communication avec les interfaces s'effectuait par e-mails ;

– le service études était assez peu homogène. Un système de management de la qualité et des procédures de gestion de projets existaient mais, dans les faits, les pratiques étaient assez variées et les outils disparates (Excel), voire inexistants.

Dans ce contexte, les principaux indicateurs de pilotage qui émergent durablement sont ceux qui servent aussi à gérer les contrats tiers, dans la mesure où ils sous-tendent des enjeux financiers.

En résumé, l'analyse de la situation doit prendre en compte le contexte de la DSI et de l'entreprise. Le changement doit se faire un peu partout simultanément, il ne peut y avoir immobilisme d'un côté (les métiers ou les études, par exemple) et révolution de l'autre (les services de la DSI). La mise en œuvre de l'opération peut s'analyser comme une montée progressive en maturité. En ce sens, lancer simultanément une approche stratégique sur les processus PO et une refonte des services autour d'ITIL (ou des processus DS) peut se révéler efficace si elle est bien managée. Ensuite, il faut faire « bouger » les études et établir la jonction entre les processus PO et AI.

Intégration

Dans cet exemple, la DSI décide d'implanter simultanément CobiT et ITIL en créant un référentiel d'entreprise commun. Il faut dire que les services partent d'une situation où un grand travail a été effectué sur la structuration du centre d'assistance aux utilisateurs, la certification ISO 9001 de la production (avec une culture des indicateurs et de l'amélioration) et la mise en place d'un outil de gestion des incidents.

La durée qui sépare le cas précédent de celui-ci est de l'ordre de trois ans. Il nous semble que, pour la plupart, les grandes DSI sont plus proches de ce cas récent que du précédent.

L'intégration passe par une vision stratégique partagée au sein de la DSI et la définition d'un référentiel de processus dans une logique ISO 9001 reprenant les processus PO de CobiT et l'ISO/IEC 20000 (ITIL V2). Simultanément, une démarche très volontariste est menée sur les études (nomination de PMO, formation et déploiement de CMMI). Il faut dire que le périmètre études de la DSI est important (plus de 800 personnes avec les externes).

Les principales difficultés rencontrées sont :

- **le décalage entre la logique d'entreprise et celle de la DSI**

  Les services de support (comptabilité, budget, ressources humaines, achats) de l'entreprise ont leur logique propre et des systèmes d'information adaptés à leurs besoins. Pour la DSI, il faut à la fois s'y conformer et créer une vision adaptée à la gouvernance des SI, par exemple :

  – une comptabilité analytique et un contrôle de gestion adaptés aux objets à gérer dans le cadre de la gouvernance ;

  - la réconciliation entre les dépenses de personnel internes et les achats externes, de façon à alimenter le suivi des consommations (temps passé, coût) ;
  - une procédure d'achat plus conforme aux exigences (réactivité) et aux enjeux (référencement) ;
  - des achats mieux coordonnés au plus haut niveau de la DSI pour rendre une vision homogène et définir une stratégie claire (processus DS2) ;
  - une gestion des compétences qui permette de réduire le grand écart entre les compétences nécessaires dans le cadre d'une DSI et le référentiel de compétences de l'entreprise qui est le fil rouge de la carrière des agents.

- **les processus aux interfaces**

  La DSI est de facto organisée en silos (études, réseau, exploitation, centre de services, etc.) et les problèmes surgissent aux interfaces. Les principaux processus impactés sont les suivants :

  - tests et mise en production (processus AI7) ;
  - gestion des problèmes (processus DS10) et des changements (processus AI6) ;
  - relations avec les métiers (processus DS1) ;
  - gestion des données (processus DS11) à défaut de relation efficace avec les métiers ;
  - PMO (processus PO10) et gestion du portefeuille de projets.

- **le système d'information de la DSI**

  En partant des systèmes existants, le système de gestion de l'entreprise et la base de gestion des appels (embryon de la CMDB), on a évidemment la mauvaise surprise de constater que le système d'information de la DSI ne sera ni l'un (trop global, trop orienté entreprise) ni l'autre (trop détaillé). Il reste donc à le construire.

- **la culture de la mesure et de l'amélioration de processus**

  Il est bon de rappeler que la description des processus n'est rien sans culture de la mesure pour l'amélioration. Le défaut de système d'information fiable excuse l'absence d'indicateur. Ne faut-il pas prendre la question dans l'autre sens : bâtir des indicateurs, même temporaires, et améliorer l'ensemble, y compris la production d'indicateurs ?

Cet exemple illustre la difficulté à trouver les leviers de progrès de la DSI tant les chantiers à ouvrir sont nombreux, chacun semblant être le préalable à la réussite du tout !

La sécurité

Jusqu'à un passé récent, la sécurité s'est limitée à la protection des systèmes informatiques concernés par le stockage et le traitement des informations plutôt que de la protection de l'information elle-même. Avec CobiT, la sécurité devient l'une des composantes de la gouvernance en proposant des bonnes pratiques de gouvernance de la sécurité de l'information. Cette dernière rejoint ainsi l'univers de la gestion des risques.

La sécurité de l'information n'est plus seulement un sujet de technicien mais devient un enjeu de direction générale et métiers. CobiT, en développant l'alignement stratégique et l'apport de valeur des systèmes d'information, met bien en évidence les risques que l'absence de mesure de sécurité de l'information fait courir à l'entreprise.

CobiT aborde la gouvernance de la sécurité de l'information en s'intéressant à :

- la prise en compte de la sécurité de l'information dans l'alignement stratégique ;
- la prise de mesures appropriées pour limiter les risques et leurs conséquences potentielles à un niveau acceptable ;
- la connaissance et la protection des actifs ;
- la gestion des ressources ;
- la mesure pour s'assurer que les objectifs de sécurité sont bien atteints ;
- l'apport de valeur par l'optimisation des investissements en matière de sécurité de l'information ;
- les bénéfices retirés ;
- l'intégration de la sécurité de l'information dans les processus.

Globalement, CobiT aborde la sécurité de l'information dans plus de 20 processus sur 34. Mais les processus suivants font apparaître une dimension sécurité importante dans les objectifs de contrôle :

- PO6 – Faire connaître les buts et orientations du management
- PO9 – Évaluer et gérer les risques
- DS4 – Assurer un service continu
- DS5 – Assurer la sécurité des systèmes

CobiT et la norme ISO/IEC 27002

L'ITGI a produit un rapport de correspondance entre les 34 processus CobiT et les 133 mesures préconisées par la norme ISO/IEC 27002. Ce rapport fait apparaître que CobiT offre une vision des mesures de plus haut niveau que celle proposée par l'ISO/IEC 27002. Ainsi, CobiT offre un cadre de gouvernance, et l'ISO/IEC 27002 complète ce cadre par la description de mesures de sécurité de l'information.

CobiT et l'ISO/IEC 27001

La norme ISO/IEC 27001, qui s'appuie sur l'ISO/IEC 27002, décrit les exigences de mise en place d'un système de management de la sécurité de l'information (SMSI). Les principes utilisés sont identiques à ceux exprimés dans la norme ISO 9001. CobiT, à travers le processus PO8, préconise la mise en place d'un système de management de la qualité (SMQ) qui reprend les finalités de l'ISO 9001. Quant aux exigences de l'ISO/IEC 27001, elles se retrouvent également dans les processus PO6, PO9, DS4 et DS5. En ce sens, CobiT est parfaitement compatible avec la mise en place d'un SMSI.

La mise en place d'un SMSI relève de la même logique que celle d'un SMQ ; c'est une question de stratégie et d'affichage. En effet, la mise en place d'un système de management ISO 9001 ou ISO/IEC 27001 est souvent motivée par un besoin de reconnaissance, lequel est matérialisé par la certification. Il est cependant important de noter que la manière de définir les périmètres est différente selon que l'on traite de l'ISO 9001 ou de l'ISO/IEC 27001. Pour le management de la qualité, le périmètre est défini par la détermination des activités réalisées par une organisation identifiée. Pour le management de la sécurité de l'information, le périmètre est déterminé par l'identification des actifs devant être protégés.

Cette question du périmètre est importante et CobiT, de par sa dimension de gouvernance de la sécurité de l'information, permet de mieux l'appréhender. Il est donc à utiliser en amont de la mise en place d'un SMSI. Le résultat d'un Quick Scan peut d'ailleurs être, pour une direction, l'événement déclencheur de la mise en place d'un SMSI.

Le management des études

Il existe de nombreux référentiels de processus pour l'amélioration du management de projet (PRINCE2, PMBOK, CMMI, etc.), et des méthodes sont également largement diffusées (PERT, GANTT, points de fonction, etc.). Nous nous intéressons ici à l'amélioration des processus de production de logiciel (couramment nommé « service études »). Ce chapitre ne concerne que les grandes DSI qui gardent en interne une part importante de développements.

CobiT et CMMI

Les raisons du déploiement de CMMI sont de deux ordres : la nécessité d'atteindre un certain niveau de maturité pour satisfaire des obligations contractuelles ou améliorer le pilotage des études, et l'amélioration de la performance. Dans les grandes DSI, il s'agit surtout de performance, des processus et des équipes. On part donc du principe que l'atteinte d'un niveau de maturité CMMI entraînera de facto des gains (durée, coût, qualité).

Notons qu'il est inutile de tenter de concilier les modèles de maturité de CobiT et de CMMI. Le premier est vraiment indicatif et destiné au management, le second conduit à une vraie certification.

Les processus de CMMI se répartissent en quatre domaines (management des processus, management de projet, engineering et support). Dans l'exemple qui suit, une DSI décide un programme important de déploiement de CMMI sans que les actions au niveau du référentiel qualité à partir de CobiT ne soient abouties. Les principales difficultés ou déconvenues qui apparaissent au fil du déploiement sont les suivantes :

- **La conduite du changement dans les équipes**

  Outre les méthodes qui peuvent se révéler plus ou moins adaptées, la conduite du changement pose deux problèmes assez cruciaux dans la pratique :

  – les processus de management de projet et d'engineering supposent l'existence de méthodes (planification, estimation, suivi du reste à faire, tests, etc.). La formation des groupes de travail révèle la disparité des méthodes et pose la question de leur harmonisation, ce qui met au second plan les processus CMMI ;

  – les domaines management des processus et processus support sont très fortement reliés aux processus CobiT ou ITIL. Il est nécessaire d'harmoniser le référentiel de la DSI plutôt que de prendre en compte CMMI comme tel.

  Dans les deux cas, le risque est grand de devoir faire marche arrière si ces questions ne sont pas tranchées en amont.

- **Le système de mesure**

  Lorsque les enjeux sont polarisés sur les coûts, on se demande comment mesurer la performance et l'amélioration espérée. Là encore, les préalables sont assez nombreux pour ne pas viser d'emblée un système intégré mais plutôt procéder par étapes. Citons quelques exemples.

  – Comment mesurer la durée d'un projet si la fin n'est pas certaine ? Par exemple, la fin du contrat d'un intégrateur et le passage en TMA peut signifier que le projet est terminé, mais aussi que le budget initial est consommé ! La mise en production n'est pas synchrone de la fin de contrat.

  – Comment agréger des coûts internes et externes ? et des temps passés lorsque l'on a recours à des forfaits ?

  – Comment estimer un projet (coût, délai) selon les situations (progiciels, logiciel, TMA, etc.) et les technologies ? A-t-on une courbe d'expérience de mesure des points de fonctions ?

  – Comment reconstituer l'ensemble des coûts d'un projet ?

CMMI n'est pas un référentiel de gouvernance des TI. Pour s'en assurer, il suffit d'examiner le tableau 9-1, traduit du *mapping* entre CobiT et CMMI (publication COBIT M*apping*: M*apping of* CMM*i with* COBIT *v*4.1). Il donne une idée de l'ampleur des objectifs de contrôle non couverts par CMMI et qui sont pourtant à déployer si l'on vise un minimum de gouvernance des TI.

Tableau 9-1 : Les objectifs de CobiT n'ayant pas de correspondance dans CMMI

Objectifs de contrôle non couverts par CMMI	**Mots-clés ou concepts non pris en compte par CMMI**
PO2 – Définir l'architecture de l'information	Architecture des données, dictionnaire des données, classification, management des données.
PO3 – Déterminer l'orientation technologique	Cible technologique, architecture, infrastructure, urbanisation.
PO5 – Gérer les investissements informatiques	Gestion des investissements, management des coûts, priorisation des programmes, cycle de vie, portefeuille de projets, budget TI, apport de valeur.
DS3 – Gérer la performance et la capacité	Management de la performance, de la capacité et de la disponibilité.
DS4 – Assurer un service continu	Continuité de service pour les métiers, référentiel de secours, ressources critiques, reprise de service, site de secours.
DS5 – Assurer la sécurité des systèmes	Sécurité.
DS6 – Identifier et imputer les coûts	Imputation des coûts, définition des services, catalogue des services, modèle de coût et de refacturation.
DS8 – Gérer le service d'assistance client et les incidents	Service d'assistance, gestion des incidents, enregistrement des demandes, escalade.
DS11 – Gérer les données	Intégrité des données, propriété des données et des systèmes, management des données, stockage.
DS12 – Gérer l'environnement physique	Environnement physique.
DS13 – Gérer l'exploitation	Gestion des opérations.
SE2 – Surveiller et évaluer le contrôle interne	Contrôles internes, référentiel de management des risques.
SE3 – Assurer la conformité aux obligations externes	Gouvernance TI, conformité réglementaire.

Il semble assez risqué et coûteux de déployer CMMI avant d'avoir réuni au niveau de la DSI certains préalables, que ce soit sur le plan de la gouvernance d'ensemble (CobiT), de l'évaluation des charges (évaluation de charge, estimation du reste à faire), des outils de mesure élémentaires (points de fonction, temps passés) ou sur le plan des méthodes diffusées et généralisées dans les équipes (pilotage de projet, tests, spécifications).

Une fois réunis les préalables de mise en cohérence des méthodes au sein des études et de déploiement des principaux processus de CobiT, CMMI vient très facilement s'intégrer dans le référentiel d'ensemble.

La certification

La certification ISO 9001 obéit à des règles strictes, en particulier concernant la structuration des processus en domaines (management, support, réalisation). Pour conjuguer CobiT et la certification, deux scénarios sont possibles.

- Scénario 1 : certifier ISO 9001 l'ensemble de la DSI en s'appuyant sur les bonnes pratiques CobiT, voire en y ajoutant les bonnes pratiques CMMI, ITIL et ISO/IEC 17799.
- Scénario 2 : identifier et sélectionner dans le référentiel CobiT, quelques processus suffisamment matures pour les intégrer au périmètre de certification ISO 9001 de l'entreprise.

Scénario 1

Conditions de mise en œuvre

Ce scénario implique la mise en œuvre de tous les processus de la DSI et de toutes les bonnes pratiques CobiT, CMMI, ITIL et ISO/IEC 17799.

Il impose de définir un système de management de la qualité (SMQ) dédié à la DSI qui accueille les processus en cours de définition, avec tout le référentiel documentaire exigé par la norme ISO 9001 :

- le manuel qualité ;
- les 6 procédures documentées :
  - maîtrise de la documentation ;
  - maîtrise des enregistrements qualité ;
  - audit interne ;
  - maîtrise du produit non conforme ;
  - actions correctives ;
  - actions préventives.
- mise en œuvre des revues de direction.

Le périmètre de ce scénario englobe tous les processus. La certification suppose donc une maturité importante du système de management dans son ensemble.

Effort de mise en œuvre

La mise en œuvre de ce scénario est assez lourde. En effet, il suppose de mettre en place une organisation dédiée au système de management, et de respecter toutes les exigences d'un système de management.

Une équipe projet spécifique doit être désignée pour mettre en place la démarche, composée, par exemple, d'une personne à mi-temps pour piloter le projet et des représentants des directions de la DSI avec une disponibilité d'environ 25 %.

Intérêt pour la DSI

Ce scénario résulte d'une décision stratégique de positionner la DSI comme un prestataire créateur de valeur et de s'inscrire dans la logique de gouvernance pouvant mener au BSC.

Scénario 2

Conditions de mise en œuvre

Ce scénario n'implique pas de définir une structure complète de processus. Il s'agit de sélectionner, dans le modèle proposé par CobiT, les processus les plus matures ou les plus déterminants afin de les piloter selon la logique du système management global de l'entreprise.

Pour être certifiables, les processus sélectionnés doivent être déployés au sein de la DSI, et être suffisamment mûrs pour être mesurés ou, pour les plus critiques, pilotés.

Ce scénario nécessite de définir une cartographie présentant une cohérence entre les processus sélectionnés pour la DSI et ceux déjà définis pour l'entreprise.

Effort de mise en œuvre

La démarche de la DSI s'intègre complètement dans la démarche globale de management de l'entreprise. Seules des actions d'harmonisation documentaire sont nécessaires. Ce scénario nécessite de se coordonner avec les autres directions de l'entreprise et la direction générale.

Intérêt pour la DSI

Ce scénario permet à la DSI d'insérer sa démarche processus dans un programme d'excellence de la direction de l'entreprise. Ainsi, les calendriers de la DSI dans ses démarches et celui de la direction générale peuvent s'aligner. Cet alignement laisse alors à la DSI le temps de progresser dans

son niveau de maturité. Il présente l'avantage de positionner les processus SI comme des contributeurs directs à la création valeur des processus produits (voir le référentiel des processus présenté à la figure 9-1).

Comparaison des scénarios

Tableau 9-2 : Comparaison des scénarios de certification

	Scénario 1	Scénario 2
Principe	Certifier ISO 9001 l'ensemble de la DSI.	Certifier les processus les plus matures ou prioritaires déjà déployés dans le cadre DSI.
Effort DSI	Mise en place d'une organisation dédiée.	Démarche intégrée dans une démarche globale d'entreprise.
Délai de mise en œuvre	2 à 3 ans	Par tranches de 1 an
Intérêt pour la DSI	Stratégie du directeur des systèmes d'information, autonomie de la DSI.	Prise en compte des démarches DSI dans un programme d'excellence ou d'amélioration continue de l'entreprise.

Exemples de déploiement

Scénario 1

Étudions un exemple de mise en place du scénario 1 pour une entreprise ayant engagé une démarche de certification ISO 9001 et ISO/IEC 27001, en s'appuyant sur les bonnes pratiques CobiT et ITIL.

Le choix de cette DSI a été motivé par un besoin de reconnaissance de la qualité des prestations offertes, car celle-ci était exigée par les clients des directions métiers de l'entreprise, c'est-à-dire le marché.

La DSI s'est donc dotée d'un système de management intégré (qualité et sécurité de l'information). La cartographie des processus est structurée selon les trois catégories de processus : management, réalisation et support. Pour l'élaborer, la DSI a pioché parmi les 34 processus de CobiT en sélectionnant des pratiques ou activités issues des objectifs de contrôle et en les regroupant en macroprocessus. Cette sélection a été opérée en fonction de la capacité de la DSI à les mettre en œuvre dans un avenir à court terme, cette capacité ayant été appréciée après l'évaluation du niveau de maturité des pratiques existantes. La logique est ensuite d'améliorer ces processus dans le temps via la démarche de progrès continue induite par la mise en place du système de management.

CobiT a donc servi de guide pour modéliser les processus opérationnels en se centrant sur la responsabilité de la DSI en tant que fournisseur. Ainsi, toutes les responsabilités décrites dans CobiT extérieures à l'organisation de la DSI n'ont donc pas été mises en œuvre car elles n'étaient pas comprises dans le périmètre de management de la DSI.

Scénario 2

À présent, étudions un exemple de mise en place du scénario 2 pour une entreprise ayant engagé une démarche d'excellence ciblée sur l'obtention du prix EFQM.

Pour être intégrés dans le périmètre de certification de l'entreprise, les processus sélectionnés de CobiT doivent cependant répondre aux exigences classiques d'une démarche processus. Les critères sont les suivants :

- le processus est défini, décrit et documenté ;
- le processus est mis en œuvre ;
- le processus est mesuré et des indicateurs sont mis en place ;
- le périmètre d'application couvre l'ensemble de la DSI ;
- le processus est ouvert vers l'extérieur (orientation client).

Par ailleurs, les processus sont classés en trois catégories :

- les processus de management ;
- les processus de réalisation ;
- les processus supports.

Les processus de management

Dans cette catégorie, trois processus ont été identifiés :

- PO1 – Définir un plan informatique stratégique pour le SI
- PO10 – Manager les projets SI (guide de la gouvernance des SI)
- PO9 – Évaluer et gérer les risques (définir la politique de sécurité de gestion de l'information de l'entreprise)

Les processus de réalisation

Au niveau de la DSI, les processus de réalisation sont de deux types : le développement du SI (gérer le projet et fabriquer la solution) et la production (exploitation du SI).

- Processus de développement du SI (domaine AI)

  Mise en œuvre des processus CMMI de niveau 2 sur l'ensemble de la DSI.

- Processus de gestion des services (domaine DS)

  La démarche ITIL est utilisée pour définir les processus de gestion des services (fourniture et soutien des services) en suivant le modèle de maturité de l'itSMF (IT *Service Management Forum*) pour la priorité de mise en place (1 an par niveau).

Les processus supports

Les processus supports identifiés dans cette catégorie sont :

- manager les ressources humaines (processus groupe) ;
- gérer la refacturation des prestations (spécifique DSI) ;
- réaliser les achats (processus groupe) ;
- définir des directives de sécurité (spécifique DSI) ;
- maîtriser les risques business liés au SI (spécifique DSI) ;
- mettre en place un tableau de bord sécurité (spécifique DSI) ;
- définir un plan de reprise d'activité (PRA) et assurer le support au déploiement (spécifique DSI).

En résumé

CobiT a choisi de se positionner en fédérateur. Aucun référentiel n'a à ce jour la couverture que CobiT propose sur l'ensemble des TI. Les travaux permanents qui sont engagés et l'esprit d'ouverture qui préside au sein des groupes de bénévoles justifient cette image de fédérateur. Les autres standards ont une vision beaucoup plus limitée, se contentant de querelles aux frontières, chacun briguant la position de leader. Tant qu'il y aura des mondes aussi inconciliables que les études (projets) et les services, CobiT aura son rôle à jouer !