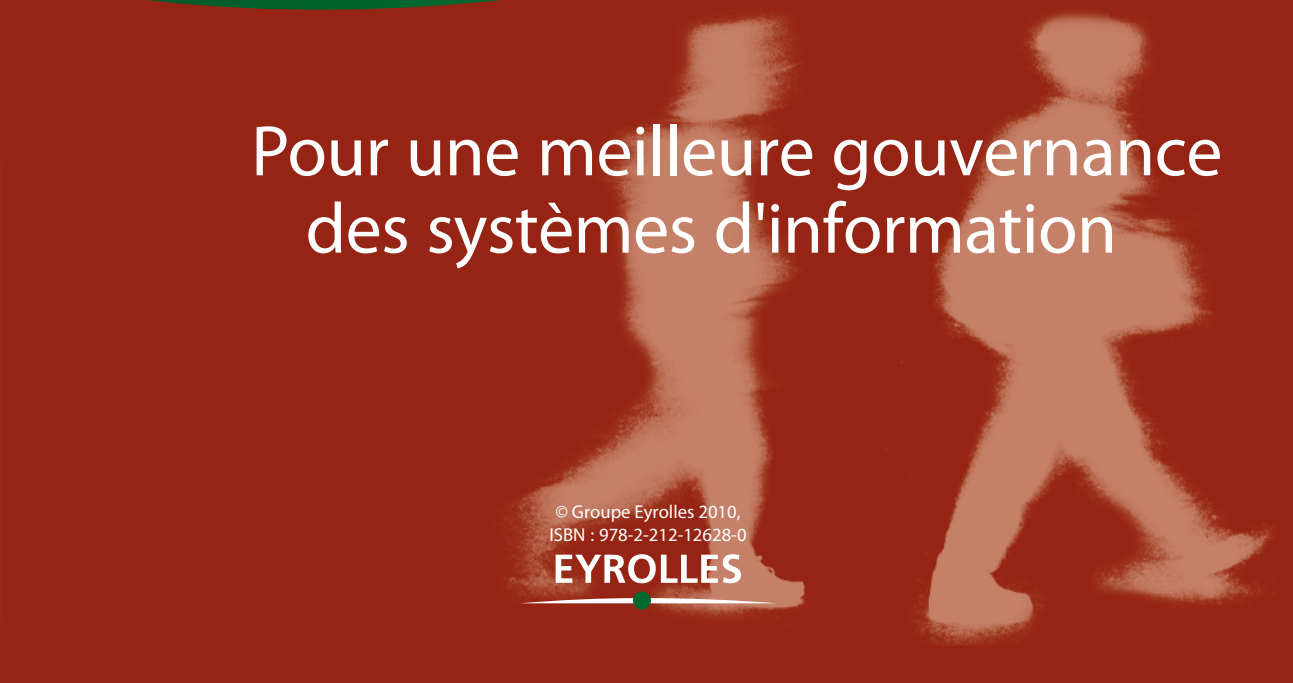
DOMINIQUE MOISAND
FABRICE GARNIER DE LABAREYRE
Préface de Bruno Ménard, président du Cigref

CobiT

2e édition

Pour une meilleure gouvernance des systèmes d'information



ISBN : 978-2-212-12628-0
EYROLLES

Table des matières

Partie I

CobiT et la gouvernance TI

Partie II

Description détaillée des processus

Avant-propos

Cet ouvrage s'adresse à tous ceux qui s'intéressent à la gouvernance des systèmes d'information. En raison du foisonnement des référentiels et des standards, il est indispensable de situer CobiT V4.1 dans cet ensemble. Nous avons retenu quatre grands courants qui alimentent cette recherche incessante : l'ISACA (*Information System Audit and Control Association*), association basée aux États-Unis, très active dans le monde entier et qui est à l'origine de CobiT ; le SEI (*Software Engineering Institute*) dont les recherches ont abouti à la création de CMMI ; l'OGC (*Office of Government Commerce*), très présent en Grande-Bretagne, en particulier à l'origine d'ITIL, et enfin l'ISO (Organisation internationale de normalisation) qui accompagne ces travaux en les insérant dans un cadre juridique normatif.

La première partie de ce livre est consacrée à une présentation générale de CobiT et des autres référentiels. Le chapitre 1 rappelle l'historique qui a conduit des premières versions de CobiT, orientées référentiels d'audit, à la série des versions 4, axées en priorité « guide de management ». Le chapitre 2 brosse un rapide tableau des principaux référentiels auxquels le DSI doit se confronter, soit parce qu'il s'agit de standards de facto ou parce que leur apport dans la gouvernance des systèmes d'information est incontournable. Le chapitre 3 permet d'appréhender CobiT comme fédérateur des principaux référentiels. Il reprend tout d'abord l'essentiel de la présentation de l'ouvrage de l'AFAI sur la V4.1 de CobiT, puis décrit la multitude de documents disponibles sur le site ***www.isaca.org*** (en anglais) à la date de parution de ce livre. Ce chapitre sert d'introduction à la partie suivante.

La deuxième partie offre une lecture commentée de CobiT en détaillant ses 34 processus selon quatre chapitres, correspondant aux quatre domaines de processus du référentiel : Planifier et Organiser, Acquérir et Implanter, Délivrer et Supporter, Surveiller et Évaluer. Au sein de ces chapitres, les processus sont décrits en respectant un plan standardisé.

La troisième partie aborde la mise en œuvre de CobiT, avec trois cibles : la première correspond à l'audit, le cœur de cible initial de CobiT depuis quinze ans environ, la deuxième place CobiT en fédérateur des autres référentiels de la gouvernance, et la troisième aborde le déploiement de CobiT à partir d'exemples précis. En synthèse, nous proposons une sorte de

modèle progressif de déploiement, tiré des expériences de mission menées depuis une dizaine d'années sur ces sujets.

Cet ouvrage se veut pragmatique et utile. Aussi n'avons-nous pas hésité à prendre position sur la pertinence de certains composants du référentiel, sur ce qui, à nos yeux, fait la force de CobiT ou au contraire ne figure qu'à titre indicatif.

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*.

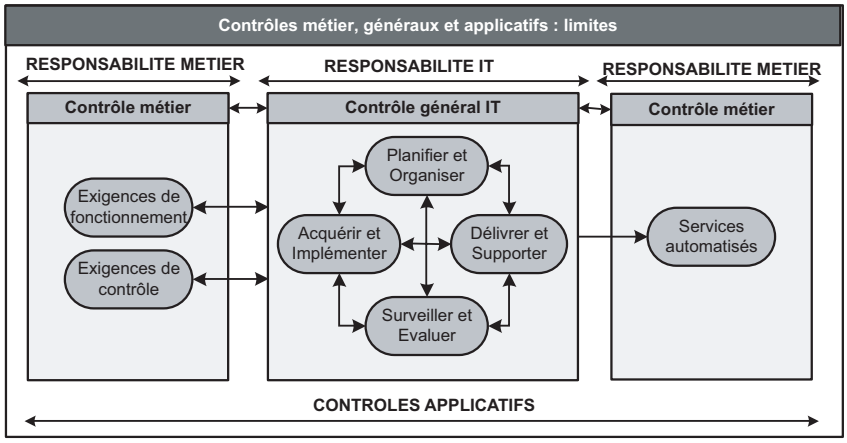


Figure 1-1 : Répartition des responsabilités de la gouvernance TI

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 Infrastructure Library* ou CMMI pour C*apability Maturity Model Integration*) 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.

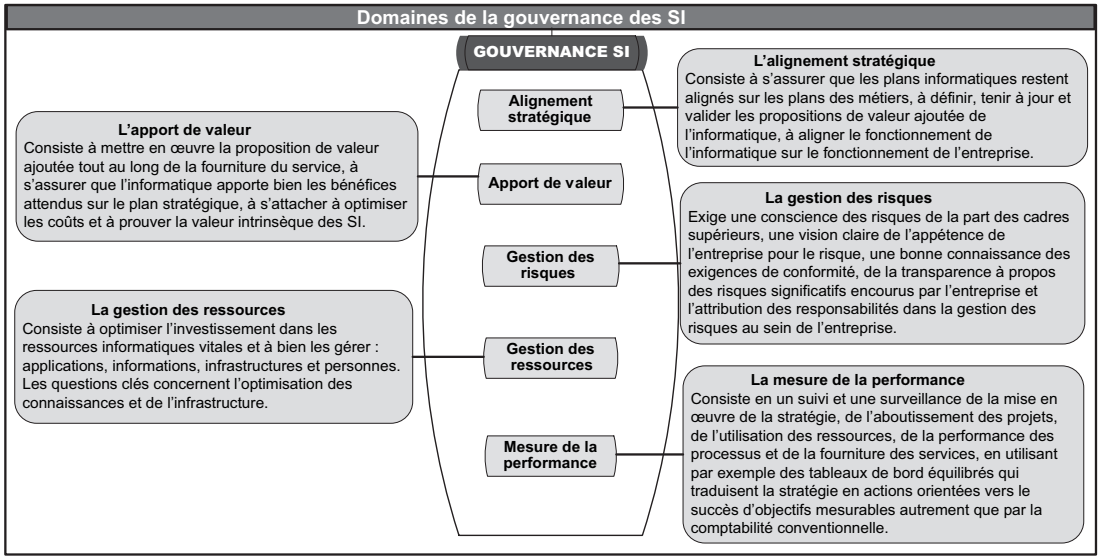


Figure 1-2 : Les domaines de la gouvernance des TI

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 (*Balanced 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.

Chapitre 3

Appréhender CobiT

Le référentiel CobiT a suscité toute une série de travaux et de publications. Dans les premières versions, V3 et antérieures, la publication principale était le guide d'audit. À partir de la version 4, c'est le guide de management qui est devenu le principal ouvrage descriptif de CobiT.

Dans ce chapitre, CobiT est décrit en termes de structure générale et d'approche à travers plusieurs points de vue : celui du guide de management pour CobiT V4.1, qui constitue le document de base, puis ceux de diverses ressources. En complément, il est utile de consulter périodiquement le site ***http://www.isaca.org*** pour connaître les dernières publications proposées.

La suite de cet ouvrage a pour vocation de fournir un guide de lecture pour tous ceux qui souhaitent mettre en œuvre CobiT au sein de leur organisation informatique.

Description générale

CobiT offre un cadre de référence de contrôle structuré des activités informatiques selon 34 processus répartis en quatre domaines :

- Planifier et Organiser (PO) ;
- Acquérir et Implémenter (AI) ;
- Délivrer et Supporter (DS) ;
- Surveiller et Évaluer (SE).

La figure 3-1 présente les différents domaines et processus associés.

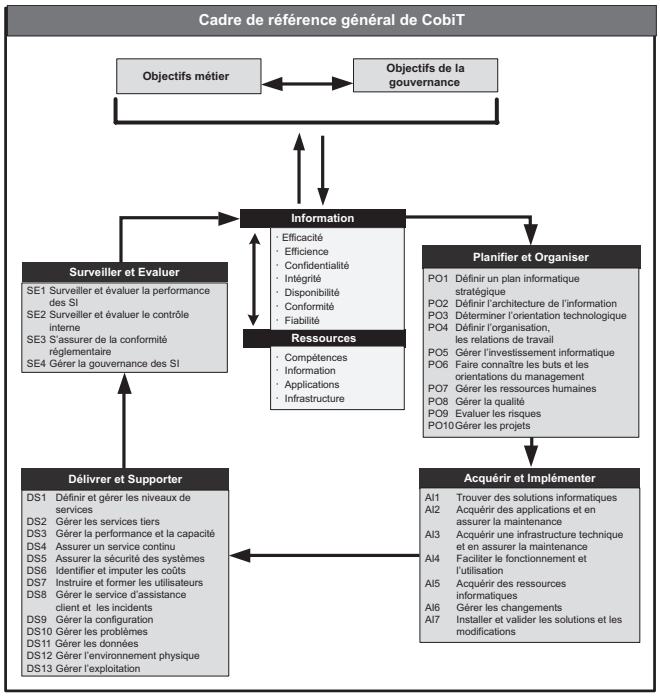


Figure 3-1 : Organisation du référentiel CobiT

Les composants de CobiT

Les quatre domaines de CobiT regroupent des ensembles cohérents de processus. Le domaine PO représente la dimension stratégique de la gouvernance des TI. Le domaine AI rassemble tous les processus qui impactent les ressources, de l'acquisition à l'implémentation : on y trouve aussi bien les projets que la mise en exploitation. Le domaine DS est consacré aux services offerts aux clients de la DSI. Enfin, le domaine SE couvre largement la dimension de contrôle, d'audit et de surveillance de l'ensemble.

Les processus de CobiT

Pour chacun des 34 processus, CobiT en décrit le périmètre et l'objet pour ensuite lister et développer :

- **les objectifs de contrôle** destinés aux auditeurs informatiques, qui sont détaillés dans d'autres publications ;
- **un guide de management** inscrit dans une logique de gouvernance des SI ;
- **un modèle de maturité** propre à chaque processus.

Les critères d'information

Pour la gouvernance des TI, CobiT prend en compte une très riche segmentation de l'information selon des critères précis (efficacité, efficience, confidentialité, intégrité, disponibilité, conformité et fiabilité). Ces critères correspondent aussi bien au point de vue d'un auditeur qu'à celui du manager :

- **efficacité** : la mesure par laquelle l'information contribue au résultat des processus métier par rapport aux objectifs fixés ;
- **efficience** : la mesure par laquelle l'information contribue au résultat des processus métier au meilleur coût ;
- **confidentialité** : la mesure par laquelle l'information est protégée des accès non autorisés ;
- **intégrité** : la mesure par laquelle l'information correspond à la réalité de la situation ;
- **disponibilité** : la mesure par laquelle l'information est disponible pour les destinataires en temps voulu ;
- **conformité** : la mesure par laquelle les processus sont en conformité avec les lois, les règlements et les contrats ;
- **fiabilité** : la mesure par laquelle l'information de pilotage est pertinente.

Les ressources informatiques

Cette dénomination regroupe les quatre classes suivantes : applications, informations, infrastructures et personnes.

- **Application** : les systèmes automatisés et les procédures pour traiter l'information.
- **Information** : les données, comme entrées ou sorties des systèmes d'information, quelle que soit leur forme.
- **Infrastructure** : les technologies et les installations qui permettent le traitement des applications.
- **Personnes** : les ressources humaines nécessaires pour organiser, planifier, acquérir, délivrer, supporter, surveiller et évaluer les systèmes d'information et les services.

Objectifs métier et objectifs informatiques

De façon globale, CobiT propose 17 objectifs métier répartis selon les quatre axes d'un BSC, à savoir : perspective financière, perspective client, perspective interne à la DSI et perspective future ou anticipation. Ces 17 objectifs métier renvoient à 28 objectifs informatiques, eux-mêmes liés aux processus CobiT, un même objectif informatique étant

associé à un ou plusieurs processus CobiT. Ainsi, CobiT offre une transitivité entre objectifs métier et informatiques, processus et activités. Cette structuration permet d'obtenir une sorte de synthèse de la gouvernance des SI.

Les processus dans CobiT V4.1

Chaque processus est décrit sur quatre pages, ce qui correspond à l'approche générale, l'audit, le management du processus et le modèle de maturité.

Les objectifs de contrôle

Les objectifs de contrôle sont décrits en termes d'attendus résultant de la mise en œuvre des processus. Des documents plus détaillés (*Guide d'audit des systèmes d'information – Utilisation de CobiT*, ou en version anglaise : IT *Assurance Guide*: U*sing CobiT*) déclinent la structure de contrôle à des fins opérationnelles. Il apparaît clairement que CobiT est un outil opérationnel pour les auditeurs qui y trouveront toute la matière nécessaire pour établir des questionnaires et des grilles d'investigation.

Le guide de management

La page consacrée au guide de management comprend un descriptif des entrées-sorties du processus, un RACI avec rôles et responsabilités associés aux activités du processus, et enfin, une proposition d'indicateurs de contrôle.

Les activités

CobiT distingue les objectifs de contrôle (vision destinée à l'auditeur) des activités (vision management). Cette distinction peut surprendre car la liste des activités reprend certains objectifs de contrôle dans ses intitulés. Parfois, ces activités sont directement extraites de la description des objectifs de contrôle. De plus, les activités sont listées mais non décrites. Le lecteur doit donc faire l'effort de déterminer dans la description des objectifs de contrôle ce qui relève de la description d'activité. Il devrait décortiquer chaque objectif de contrôle en tentant d'isoler l'information attachée aux activités, aux instances/organisations, aux fonctions, aux documents/livrables et enfin au contexte.

Pour la mise en œuvre de CobiT, partir des activités est intéressant à condition de ne pas s'y enfermer. Il vaut mieux prendre cette liste comme un « pense-bête » pour donner du corps à une description personnalisée en fonction de l'organisation.

Les responsabilités et fonctions dans CobiT (RACI)

CobiT ne distingue pas moins de 19 parties prenantes ou fonctions pour la gouvernance des systèmes d'information. Chacune d'elles peut avoir un ou plusieurs rôles pour chaque activité.

On peut ainsi être responsable ou garant, ou simplement consulté ou informé, selon la situation. Ceci est décrit dans un tableau croisé activités/fonctions.

CobiT ne propose pas à proprement parler une organisation, mais les objectifs de contrôle font parfois référence à des instances comme le comité stratégique informatique ou le comité de pilotage informatique dont les missions sont clairement énoncées. Là encore, le RACI[1] est indicatif. Selon la taille et l'organisation de la DSI, certaines fonctions « génériques » peuvent être plus ou moins structurées en postes et emplois. Le RACI de CobiT est une base à affiner au cas par cas.

1. RACI : en anglais *Responsible, Accountable, Consulted, Informed*, traduit par Responsabilité, Autorité (celui qui est garant), Consulté, Informé. L'autorité (A) dicte la « politique » qui sera appliquée par le responsable (R).

Tableau 3-1 : Exemple de RACI (pocessus POI)

ACTIVITÉS	DG	DF	Direction métier	DSI	Propriétaire processus métier	Responsable exploitation	Responsable architecture	Responsable développements	Responsable administratif	Bureau projet	Conformité, audit, risque et sécurité
Lier objectifs métier et objectifs informatiques.	C	I	A/R	R	C						
Identifier les dépen-dances critiques et les performances actuelles.	C	C	R	A/R	C	C	C	C	C		C
Construire un plan informatique stratégique.	A	C	C	R	I	C	C	C	C	I	C
Élaborer des plans informatiques tactiques.	C	I		A	C	C	C	C	C	R	I
Analyser les portefeuilles de programmes et gérer les portefeuilles de projets et de services.	C	I	I	A	R	R	C	R	C	C	I

Les objectifs et les indicateurs

Pour chaque processus, on détaille les objectifs et les métriques associées. Un processus est considéré comme piloté lorsque des objectifs lui ont été assignés et que des indicateurs ont été définis pour atteindre les objectifs[1].

Nul doute que cette construction garantisse la bonne gouvernance en reliant ainsi les différents indicateurs de l'activité élémentaire au métier. Ceci étant, il faut disposer d'un vrai système d'information de pilotage pour le mettre en œuvre, ce qui correspond au stade ultime de la gouvernance SI. Autant les objectifs de contrôle nous semblent très structurants et invariants, autant la partie « guide de management » est à considérer comme un exemple méritant d'être contextualisé, complété et personnalisé au cas par cas.

1. Chacun de ces objectifs donne lieu à une mesure de performance qui permet de savoir si l'objectif est atteint (*lag indicator* en anglais), ce qui constitue en même temps le contexte de l'objectif suivant (*lead indicator*). Ainsi, l'objectif informatique « s'assurer que les services informatiques sont capables de résister à des attaques et d'en surmonter les effets », par exemple, s'inscrit à la fois dans un contexte (*lead* : le nombre d'accès frauduleux) et s'avère mesuré par un résultat (*lag* : le nombre d'incidents informatiques réels qui ont eu un impact sur l'activité de l'entreprise).

Le modèle de maturité

CobiT propose un modèle de maturité générique faisant l'objet d'une déclinaison spécifique pour chacun des 34 processus. Ainsi, la mise en œuvre de chacun des 34 processus peut être confrontée à des stades du modèle de maturité selon une échelle classique en la matière (voir figure 3-2). En se limitant à cette description générique, on peut donc mesurer de façon globale la maturité de chaque processus et piloter leur amélioration.

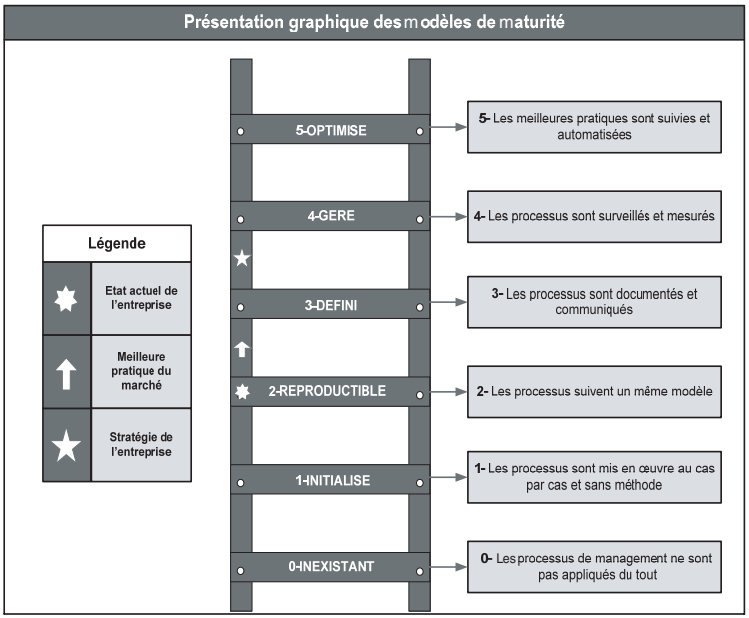


Figure 3-2 : Modèle de maturité

CobiT veut aller plus loin en groupant trois dimensions au modèle de maturité, pour chacun des 34 processus. Il propose ainsi les dimensions suivantes :

- quoi : contrôle (initialisé, reproductible, défini, géré et optimisé), stades de 0 à 5 ;
- combien : couverture en termes de périmètre ;
- comment : capacité à réaliser les objectifs.

En étudiant la description du modèle de maturité[1] par processus, il semble que chaque stade caractérise un palier de mise en œuvre en fonction de son périmètre de déploiement au sein de l'entreprise. Il peut ainsi y avoir confusion entre le périmètre spécifique de déploiement d'un processus (dimension « combien ») et le stade de maturité générique qu'il a atteint, au sens du CMM (dimension « contrôle »).

Pour un même processus, il est ainsi possible de fixer des objectifs différents de progression de la maturité en fonction de l'état de maturité observé sur plusieurs périmètres de sa mise en œuvre. Pour un métier ou un système donné, le processus peut être évalué au niveau 2 du modèle de maturité alors que, pour d'autres, il peut l'être au niveau 3. Selon les exigences métier et la criticité de l'informatique sur les métiers de l'entreprise, la cible en termes de niveau de maturité peut être différente.

Dans le cas d'un périmètre d'évaluation de la maturité globale selon CobiT (c'est-à-dire tous les métiers et tous les systèmes), il serait donc réducteur de dire par exemple qu'un processus donné est globalement au niveau 2 si, selon les endroits où il est applicable, il se trouve au niveau 3, 4 ou 1.

Le modèle de maturité CobiT est conçu pour offrir une grande flexibilité à l'évaluateur en fonction de ses objectifs et des besoins d'amélioration. Il est adapté à l'activité d'audit du ou des processus considérés plutôt qu'à une activité de mise en œuvre d'une démarche CobiT globale dans l'entreprise.

En effet, il n'y a aucune recommandation ni orientation quant à la priorité ou l'ordre de mise en œuvre des processus. Les 34 processus du référentiel CobiT ne sont pas présentés pour se loger dans un modèle de maturité étagé avec une logique de mise en place progressive comme dans CMMI.

En revanche, un ordre de mise en place des processus CobiT peut être envisagé mais, dans ce cas, il sera toujours spécifique à chaque entreprise en fonction de ses exigences métier et de ses objectifs informatiques. C'est d'ailleurs à partir d'une évaluation initiale des 34 processus CobiT et selon les exigences métier qu'il sera possible de définir un plan de mise en place. Ce plan spécifiera, processus par processus, les différents niveaux de maturité à atteindre en fonction des métiers et de la criticité des systèmes informatiques associés. Nous n'avons donc pas repris, dans la suite de la présentation des processus, les éléments spécifiques des modèles de maturité de CobiT.

1. Il y a au moins une centaine de modèles de maturité dont un bon nombre servent à des référentiels utilisés en DSI. Le précurseur est celui du SEI (*Software Engineering Institute*) qui a donné le CMM (*Capability Maturity Model*), conçu pour évaluer la maturité des organisations en charge du développement de logiciel. En général, un modèle de maturité a cinq niveaux : inexistant, intuitif, défini, géré et mesurable, optimisé.

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

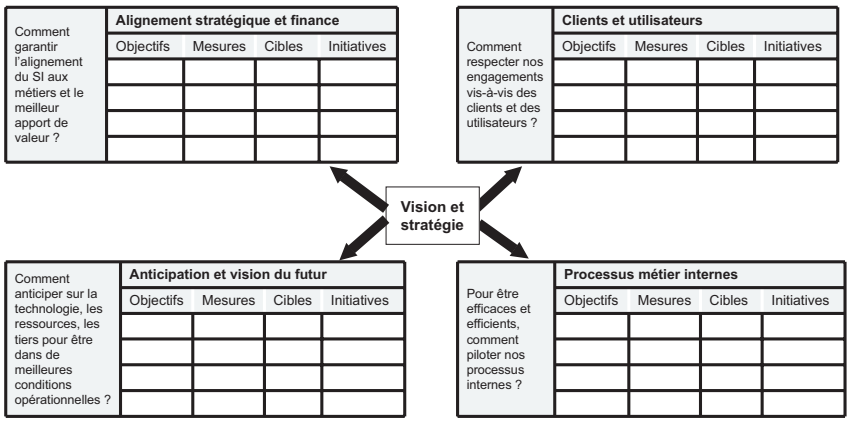


Figure 9-1 : Le Balanced Scorecard (BSC)

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 principaux, 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.

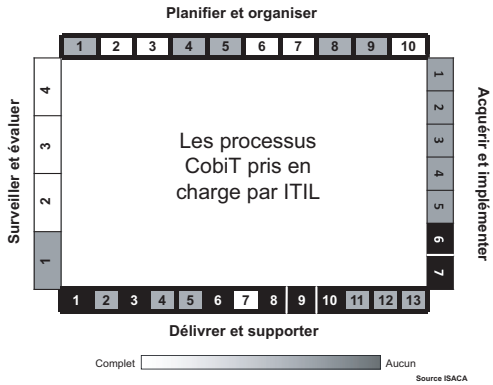


Figure 9-2 : Les processus de CobiT V4.1 couverts par ITIL V3

Une publication (*Cobi*T M*apping* : *mapping of* ITIL V3 *with Cobi*T 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 C*obi*T M*apping*: M*apping of* CMMI *with* C*obi*T *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 27002.
- 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 27002.

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 !

Une série de tableaux illustre les liens entre les 62 bonnes pratiques et les principaux axes de gouvernance TI.

Le premier tableau répartit des attributs « risques » selon deux catégories de « thèmes ».

- Les cinq premiers thèmes correspondent aux domaines de la gouvernance des TI (alignement stratégique, apport de valeur, gestion des ressources, gestion des risques et gestion des performances).
- Les neuf thèmes suivants résument concrètement les principales préoccupations des dirigeants (optimisation des coûts, délivrance de service, externalisation, sécurité, architecture, intégration des systèmes, priorités et planification, contrôles programmés et sécurité des applications).

Le second tableau répartit les objectifs de contrôle de CobiT Quickstart selon les mêmes thèmes généraux.

Pour résumer, CobiT Quickstart est orienté bonnes pratiques et guide de management des TI plus qu'audit ; il peut convenir à une première implémentation. Il met de côté le processus DS6, lequel peut représenter effectivement un très gros effort. Toutefois, même si le nombre d'objectifs est divisé par trois, il reste un grand nombre de processus à déployer, ce qui représente d'emblée une lourde charge et ne résout pas la question de la conduite du changement au sein de la DSI.

Pour un déploiement étagé

Si l'ampleur du déploiement de CobiT devient un risque en tant que tel, il faut imaginer des manières plus progressives de le mettre en place. La première approche consiste à se demander quelles sont les préoccupations auxquelles on souhaite répondre afin de mettre en priorité certains processus, la seconde partirait plutôt de l'ensemble des préalables à recueillir pour savoir ce que l'on peut faire et à quel stade ; une combinaison des deux serait idéale. Au fil des missions, nous avons dégagé une proposition de modèle de maturité « étagé » pour la mise en place progressive de CobiT.

Les préalables à recueillir

CobiT se place dans une situation un peu idéale dans laquelle l'organisation serait conforme au RACI, les mesures des indicateurs seraient remontées dans un système d'information de la DSI avec un effort minimum, les coûts seraient connus, les acteurs internes seraient rôdés à la notion de processus et de boucle d'amélioration, etc.

La situation réelle est bien différente, et tellement en deçà des attentes, que le projet de déploiement tourne court bien souvent. Il faut donc faire des choix, lesquels dépendent de la situation de la DSI mais aussi des

parties prenantes et des objectifs de gouvernance qui se font jour. Les principaux obstacles au déploiement de CobiT sont les suivants.

- **Le système de mesure des indicateurs de fonctionnement**

  Dans le meilleur des cas, il est hétérogène avec une couverture correcte ; le plus souvent, il est hétéroclite, incomplet et surtout centré autour des domaines qui bénéficient de systèmes d'information existants (automates d'exploitation, centre d'assistance, comptabilité, facturation, paie, achats). Les éléments sont donc parfois mesurés avec une finalité qui n'est pas celle de CobiT.

  De la même manière, le pilotage des projets informatiques mériterait d'être outillé pour produire des indicateurs cohérents (temps passé, coûts, estimations, etc.).

  En résumé, l'implémentation de CobiT nécessiterait de disposer d'un modèle de données adapté, propre à la DSI, conçu dans une logique de gouvernance IT.

- **Le contrôle de gestion de la DSI**

  Il se base généralement sur la comptabilité de la société sans qu'il existe un plan analytique de la DSI. Le préalable avant d'identifier et d'imputer les coûts peut se révéler très lourd.

- **La culture du management des processus**

  Il est fondamental que les équipes aient une culture de l'amélioration de processus, ce qui suppose d'accepter de parler des dysfonctionnements pour dépasser le stade élémentaire du chacun pour soi. Cette culture a pu être créée au fur et à mesure de la mise en place des processus (ISO 9001, etc.).

- **Les contrats avec les tiers**

  La gestion des tiers s'est faite au fil du temps. Son efficacité passe parfois par la renégociation de contrats (fournisseurs, constructeurs, intégrateurs, infogérants, éditeurs, etc.) et l'harmonisation des périmètres externalisés. Dans la réalité, certains contrats s'étalent sur de longues durées et le travail d'harmonisation et de négociation ne peut prendre place que dans certains intervalles de temps, plus ou moins espacés.

- **Les relations avec les métiers**

  La relation avec les métiers concerne l'ensemble de la DSI, aussi bien les services à fournir et la sécurité que les projets ou la maintenance. Ces relations sont plus ou moins formalisées et propres à s'inscrire dans une refonte des processus de la DSI.

- **Les méthodes mises en œuvre sur les projets**

  Les entreprises ont très souvent leur propre bibliothèque de procédures et de méthodes pour le cycle de développement de logiciels. Dans les

faits, il est rare que les méthodes soient déployées de façon uniforme, et exceptionnel de déterminer un système d'information complet pour piloter les projets.

Cette liste non exhaustive d'obstacles rencontrés couramment donne une idée de la difficulté de transformer une DSI.

Exemple de déploiement progressif

Le choix des processus à déployer dépend à la fois des objectifs de gouvernance et des obstacles rencontrés. Parmi les objectifs identifiés dans notre exemple, nous avons retenu :

- la conformité avec les exigences réglementaires de la loi Sarbanes-Oxley et, plus généralement, la réduction des risques ;
- le management des ressources.

Cela signifie que l'alignement stratégique, la mesure de la valeur et la mesure de performance ne sont pas dans ce premier lot.

Niveau 0

C'est l'inexistence de processus formalisés et déployés. On est au niveau le plus artisanal de l'organisation.

Niveau 1 – Sécurité et fonctionnement

Le choix stratégique se porte en priorité sur la mise en œuvre d'une politique de sécurité et le bon fonctionnement de la DSI. Cela correspond à plusieurs processus à déployer, essentiellement dans les domaines AI et DS qui contrôlent la grande partie des ressources TI.

- Groupe 1 – Sécurité, conformité SOX et disponibilité :
  - PO9 – Évaluer et gérer les risques
  - AI3 – Acquérir une infrastructure technique et en assurer la maintenance
  - AI6 – Gérer les changements
  - AI7 – Installer et valider des solutions et des modifications
  - DS1 – Définir et gérer les niveaux de services
  - DS2 – Gérer les services tiers
  - DS4 – Assurer un service continu
  - DS5 – Assurer la sécurité des systèmes
  - DS8 – Gérer le service d'assistance client et les incidents
  - DS9 – Gérer la configuration
  - DS10 – Gérer les problèmes
  - DS13 – Gérer l'exploitation

- Groupe 2 – Piloter les ressources TI (hormis les projets applicatifs) :
  - PO4 – Définir les processus, l'organisation et les relations de travail
  - AI3 – Acquérir une infrastructure technique et en assurer la maintenance
  - AI4 – Faciliter le fonctionnement et l'utilisation
  - AI5 – Acquérir des ressources informatiques
  - AI6 – Gérer les changements
  - AI7 – Installer et valider des solutions et des modifications
  - DS8 – Gérer le service d'assistance client et les incidents
  - DS9 – Gérer la configuration
  - DS13 – Gérer l'exploitation

Plusieurs processus sont communs aux deux groupes. L'ensemble donne un premier niveau de 15 processus à déployer (processus PO4, PO9, DS1, DS2, DS4, DS5, DS8, DS9, DS10, DS13, AI3, AI4, AI5, AI6 et AI7). Les puristes remarqueront que d'autres processus devraient être également embarqués à ce stade (processus PO10, AI1 et AI2, par exemple) mais le but est de se concentrer sur un projet pragmatique pour lequel le périmètre ne devient pas un risque.

Le parti pris de ne pas inclure les projets (processus PO10, AI1 et AI2) vient de l'ampleur des changements à mener et des préalables à réaliser (harmonisation des pratiques). Concrètement, il faut les démarrer parallèlement sans qu'ils ne soient encore matures à ce stade.

Déploiement

Il commence par une vision claire de l'organisation et de la politique de maîtrise des risques. Pour le fonctionnement, le déploiement de cet ensemble de processus couvre bien les processus ITIL (ou ISO/IEC 20000), la production, les contrats tiers et la sécurité. Sur ces zones, il existe des indicateurs remontés par les outils (gestion d'appels, etc.) ; il convient de les identifier et de les sélectionner pour le pilotage des processus.

Le déploiement s'accompagne d'une sérieuse conduite du changement sur les fonctions impactées dans les processus, en particulier entre service d'assistance, exploitation, tiers et études. Deux cas sont privilégiés pour cela, dans la mesure où ils concernent la plupart des fonctions de la DSI :

- la maintenance applicative sur son cycle de vie ;
- la gestion des problèmes en relation avec les acteurs de la DSI.

L'organisation doit être revue pour faire émerger les pilotes des processus, en particulier le responsable assistance/incidents et le responsable des contrats tiers.

Ce déploiement dure six mois environ et nécessite ensuite au moins six mois de fonctionnement pour être bien rôdé. Des consultants externes assurent un coaching périodique pour actionner la boucle d'amélioration permanente.

Niveau 2 – Mesures et pilotage

Au deuxième niveau de déploiement, on doit bénéficier des travaux qui auront été effectués en amont pour embarquer les projets et le service études. Il est toutefois prématuré de gérer les coûts, compte tenu du travail à faire en amont sur le système d'information concerné. À ce stade, on commence à piloter les processus déployés (processus SE1), ce qui représente en tant que tel un enjeu majeur et un effort considérable. La mise en place du responsable de ce pilotage est un facteur de succès pour la boucle d'amélioration à entretenir.

- PO6 – Faire connaître les buts et les orientations du management
- PO7 – Gérer les ressources humaines
- PO8 – Gérer la qualité
- PO10 – Manager les projets
- AI1 – Trouver des solutions informatiques
- AI2 – Acquérir des applications et en assurer la maintenance
- DS3 – Gérer la performance et la capacité
- DS7 – Instruire et former les utilisateurs
- DS11 – Gérer les données
- DS12 – Gérer l'environnement physique
- SE1 – Surveiller et évaluer la performance des SI

Ce niveau permet d'être quasiment complet sur les objectifs de management des ressources et de sécurité. Il comprend aussi le pilotage général (processus PO8 et SE1) et prévoit de s'occuper sérieusement de la communication. Simultanément, il faudra se préparer pour le niveau suivant. La gestion des coûts nécessite d'engager la conception du système d'information correspondant.

Niveau 3 – Apport de valeur

Au troisième niveau de déploiement, il devient crucial de gérer les coûts et les investissements (processus PO5 et DS6) : c'est l'objectif principal de ce niveau. Parallèlement, on complètera le dispositif sur les axes stratégiques (processus PO2 et PO3) et sur la surveillance du contrôle interne et de la conformité aux obligations externes (processus SE2 et SE3).

- PO2 – Définir l'architecture de l'information
- PO3 – Déterminer l'orientation technologique
- PO5 – Gérer les investissements informatiques
- DS6 – Identifier et imputer les coûts
- SE2 – Surveiller et évaluer le contrôle interne
- SE3 – S'assurer de la conformité aux obligations externes

Niveau 4 – Gouvernance des SI

Au dernier stade de déploiement, il reste à faire progresser en maturité les processus PO1 et SE4 qui finalisent la construction de l'alignement stratégique.

Le tableau 10-1 représente ce modèle de maturité pragmatique, résultat des travaux réalisés par les consultants de la société ASK Conseil chez leurs clients.

Tableau 10-1 : Proposition de modèle de maturité étagé, © ASK Conseil

PO4 - Définir les processus, l'organisation et les relations de travail PO9 - Évaluer et gérer les risques AI3 - Acquérir une infrastructure technique et en assurer la maintenance AI4 - Faciliter le fonctionnement et l'utilisation AI5 - Acquérir des ressources informatiques AI6 - Gérer les changements AI7 - Installer et valider des solutions et des modifications DS1 - Définir et gérer les niveaux de services DS2 - Gérer les services tiers DS4 - Assurer un service continu DS5 - Assurer la sécurité des systèmes DS8 - Gérer le service d'assistance client et les incidents DS9 - Gérer la configuration DS10 - Gérer les problèmes DS13 - Gérer l'exploitation	**Niveau 1 - Sécurité et fonctionnement**			
PO6 - Faire connaître les buts et les orientations du management PO7 - Gérer les ressources humaines PO8 - Gérer la qualité PO10 - Manager les projets AI1 - Trouver des solutions informatiques AI2 - Acquérir des applications et en assurer la maintenance DS3 - Gérer la performance et la capacité DS7 - Instruire et former les utilisateurs DS11 - Gérer les données DS12 - Gérer l'environnement physique SE1 - Surveiller et évaluer la performance des SI		**Niveau 2 - Mesures et pilotage**		
PO2 - Définir l'architecture de l'information PO3 - Déterminer l'orientation technologique PO5 - Gérer les investissements informatiques DS6 - Identifier et imputer les coûts SE2 - Surveiller et évaluer le contrôle interne SE3 - S'assurer de la conformité aux obligations externes			**Niveau 3 - Apport de valeur**	
PO1 - Définir un plan informatique stratégique SE4 - Mettre en place une gouvernance des SI				**Niveau 4 - Gouvernance des SI**