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 ;
- Acquérir et Implémenter ;
- Délivrer et Supporter ;
- Surveiller et Évaluer.

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

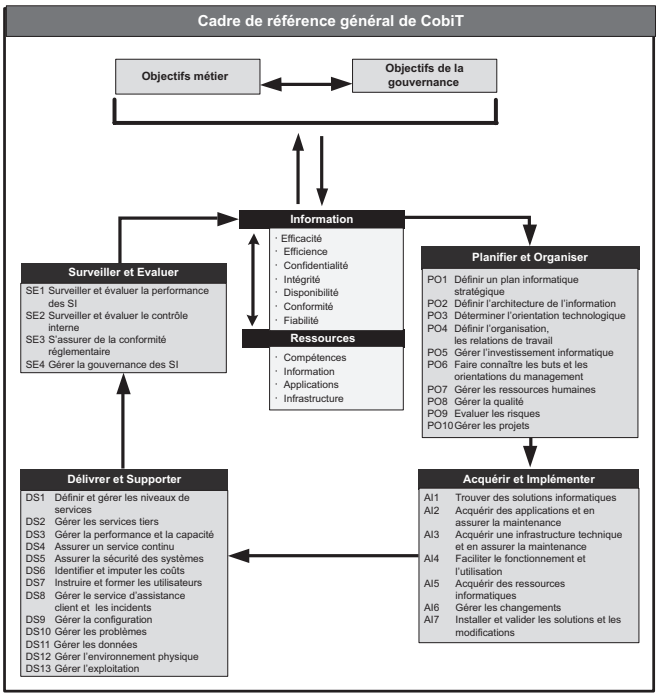

Figure 3-1 : Organisation du référentiel CobiT

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.
- **Infrastructure** : les technologies et les installations qui permettent le traitement des applications.
- **Information** : les données, comme entrées ou sorties des systèmes d'information, quelle que soit leur forme.
- **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 20 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 20 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 (IT *Assurance Guide*: U*sing Cobi*T) 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 (processus PO1)

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 dépendances 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.

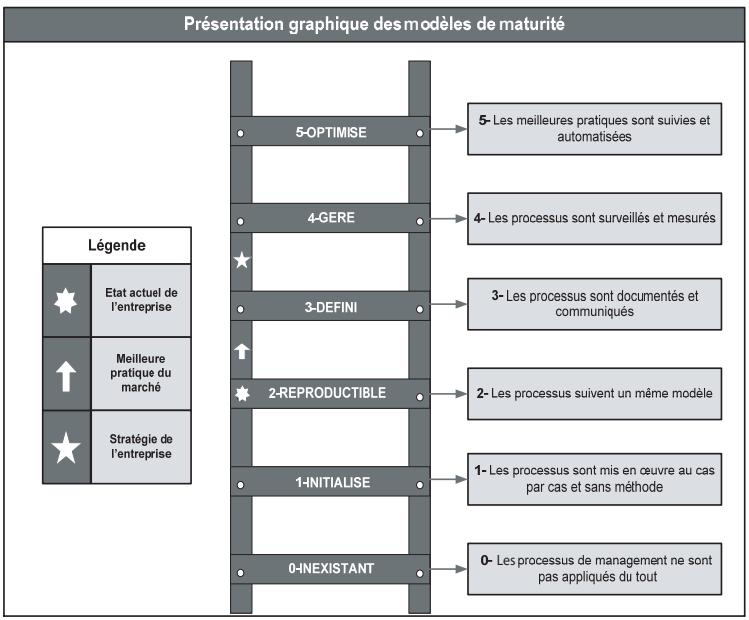

Figure 3-2 : Modèle de maturité

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.