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

	Niveau 1 - Sécurité et fonctionnement	Niveau 2 - Mesures et pilotage	Niveau 3 - Apport de valeur	Niveau 4 - Gouvernance des SI
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	✓			
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		✓		
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			✓	
PO1 – Définir un plan informatique stratégique SE4 – Mettre en place une gouvernance des SI				✓