

COBIT : Référentiel de gouvernance informatique ?

Par Karim El-Boustani
IETxpress, Mai 2006



COBIT est devenu un incontournable suite à l'introduction de la loi Sarbanes Oxley (SOX) aux États-Unis. En effet, l'aspect informatique de la conformité à cette loi se base sur les contrôles définis par COBIT. C'est pour cette raison que ce référentiel est actuellement mieux connu par les vérificateurs que les gestionnaires. Mais qu'est-ce que COBIT exactement? Est-il un référentiel de gouvernance informatique? Quelle est la différence avec d'autres pratiques telles que ITIL ou ISO17799?

Qu'est-ce que COBIT?

COBIT signifie « Control Objectives for Information and related Technologies » qui se traduit en français par Gouvernance, contrôle, et audit de l'information et des technologies associées.

COBIT a été créé par la fondation de l'ISACA (Information Systems Audit and Control Association) et a été repris par l'IT Governance Institute. Sa première version date de 1996, avec des mises à jour en 1998 (version 2), 2000 (version 3), et fin 2005 (version 4). COBIT est un cadre de meilleures pratiques qui vient intégrer les nombreux autres cadres et a le soutien d'un grand nombre d'experts mondiaux.

COBIT regroupe 34 processus TI organisés en quatre domaines :

- Planification et organisation (10 processus)
- Acquisition et mise en place (7 processus)
- Distribution et soutien (13 processus)
- Surveillance (4 processus)

À ces 34 processus correspondent 318 objectifs de contrôle pour lesquels des pratiques de contrôle détaillées ont été identifiées. Comme les vérificateurs ont été les premiers utilisateurs de COBIT, il contient un guide de vérification qui décrit les éléments nécessaires à la bonne compréhension de chaque processus, précise les contrôles à effectuer, fournit des éléments pour évaluer la conformité aux bonnes pratiques et évaluer les risques de la non atteinte des objectifs.

De plus, COBIT a été conçu pour aider les dirigeants TI en leur offrant un Guide de gestion. Avec ce guide, COBIT offre :

1. Le moyen d'évaluer les 34 processus TI par rapport aux meilleures pratiques sur le marché. À chaque processus on associe un modèle de maturité permettant de déterminer le niveau sur une échelle de 0 (inexistant) à 5 (optimisé). À chaque niveau on associe des facteurs clés de

succès correspondant aux actions à prendre afin de s'améliorer. De plus, un outil (COBIT Online) permet aux entreprises de se comparer à des organisations similaires afin de déterminer le niveau de maturité à atteindre pour être compétitive.

2. Des indicateurs clés afin de permettre la mise en œuvre de tableaux de bord pertinents. Il existe ainsi deux catégories d'indicateurs :

- des indicateurs clés de succès pour vérifier que les objectifs sont atteints. Ces indicateurs sont à utiliser par les dirigeants TI.
- des indicateurs clés de performance pour le suivi de la qualité des opérations. Ces indicateurs sont à surveiller par les équipes opérationnelles et influencent directement les indicateurs clés de succès.

Quelle est la différence entre COBIT, ITIL, ISO17799, etc. ?

COBIT est positionné à haut niveau et agit comme un intégrateur de ces autres standards et meilleures pratiques TI qui sont plus détaillés, tout en résumant leurs objectifs clefs sous un même référentiel. De plus, la version 4 présente un lien entre les objectifs d'affaires, les objectifs TI et les processus TI : une étape essentielle à la mise en place d'une gouvernance TI.

Il est certain qu'affirmer que COBIT, ITIL, ou ISO17799 sont des référentiels de gouvernance informatique n'est pas exact. Ce sont des meilleures pratiques de gestion interne, COBIT

étant le seul qui offre une vue globale des TI, en intégrant les autres à haut niveau, offrant ainsi une fondation solide pour la mise en place de la gouvernance informatique.

Comment COBIT peut-il aider votre organisation?

La première action dans la mise en place d'un cadre de gouvernance est de vous assurer d'une compréhension approfondie des objectifs de votre entreprise. COBIT vous permet de faire le lien entre les objectifs de l'entreprise et ceux des TI. Suite à cette analyse, vous pouvez identifier les processus TI qui viennent soutenir les objectifs TI les plus importants pour votre organisation.

Prenons un exemple concret. Si la protection des renseignements personnels est un objectif primordial de votre organisation, alors la gestion de la sécurité informatique devient un élément essentiel de votre stratégie informatique.

Votre prochaine étape serait d'analyser le niveau de maturité de vos activités : comment votre gestion de la sécurité informatique se compare-t-elle aux meilleures pratiques de l'industrie? Vous allez ainsi déterminer les actions à prendre, et mettre en place votre plan d'action. L'avantage principal de cette approche est d'intégrer les partenaires d'affaires dans la définition et mise en place d'un cadre de gouvernance qui répond à leurs besoins.