

ROYAUME DU MAROC

مكتب التكوين المهني وإنعاش الشغل

Office de la Formation Professionnelle et de la Promotion du Travail

Modèle Cobit  
[www.ofppt.info](http://www.ofppt.info)



OFPPT

DIRECTION RECHERCHE ET INGENIERIE DE FORMATION  
SECTEUR NTIC

## Sommaire

1. Introduction .....	2
2. Chapitre 1 .....	<b>Erreur ! Signet non défini.</b>
2.1.1. Item .....	<b>Erreur ! Signet non défini.</b>
2.1.2. Item .....	<b>Erreur ! Signet non défini.</b>

# 1.Introduction

Le référentiel **CobIT (Control Objectives for Information & related Technology)** est une méthode de Maîtrise des Systèmes d'Information (IT Gouvernance) et d'audit de systèmes d'information, éditée par l'Information System Audit & Control Association (ISACA) en 1996. C'est un cadre de **contrôle** qui vise à aider le management à gérer les risques (sécurité, fiabilité, conformité) et les investissements.

Cobit est une approche orientée processus : les tâches et activités définies sont intégrées dans les 34 processus établis, ces derniers sont eux-mêmes regroupés en 4 domaines de processus.

Cobit est une approche multi-critères, qui permet à chaque utilisateur de ce référentiel d'obtenir pour chaque processus les informations qui l'intéressent.

Il y a un certain nombre d'outils qui ont été mis en place afin de coller aux besoins des entreprises selon leur importance et la complexité de leur SI.

L'IT Governance affirme la responsabilité du Comité de Direction et de l'encadrement, au même titre que d'autres préoccupations essentielles relevant du management de l'entreprise, pour ce qui concerne :

1. l'alignement des évolutions du SI avec la stratégie "business",
2. la création de valeur en permettant de saisir les opportunités et générer du profit,
3. la gestion de risques liés au SI,
4. la bonne utilisation des ressources informatiques,
5. la mesure des performances.

Ces 5 exigences que devraient exprimer les dirigeants (selon l'ITGI) peuvent être prise en compte dans l'établissement d'une normalisation des processus avec le COBIT.

## 2.Historique et acteurs

La nécessité d'avoir un cadre de référence en matière de sécurité et de contrôle des technologies de l'information a poussé l'ISACA (Information Systems Audit and Control Association) à créer la méthode COBIT en 1996. Cette méthode est diffusée en France par sa branche française l'AFAI (Association Française de l'Audit et du Conseil Informatique).

L'objectif était de faire le lien entre les risques métiers, les besoins de contrôle et les questions techniques en se basant sur les meilleures pratiques en audit informatique et SI.

<b>www.ofppt.info</b>	Document	Millésime	Page
	Modele Cobit.doc	août 14	2 - 11

## Titre du document

Le COBIT se destine aussi bien au management (qui doit décider des investissements à effectuer pour assurer la sécurité et la maîtrise des TI, et les ajuster suivant les risques de l'environnement) qu'aux utilisateurs (sécurité, mise sous contrôle des services informatiques fournis). La méthode COBIT se veut le modèle de référence de la gouvernance des TI.

Récemment, et afin de faciliter l'évolution et la formalisation de la maîtrise des risques relatifs aux TI notamment dans le cadre de la loi Sarbane-Oxley, l'IT Governance Institute (créé par l'ISACA en 1998) a lancé une version interactive en ligne de COBIT appelée COBIT Online.

Cette version permet de rechercher facilement les meilleures pratiques, modèles de maturité, indicateurs clés d'objectifs et de rendement, etc. dans une base regroupant plus de 300 objectifs détaillés. Elle permet d'aider les managers à justifier les risques liés à leur gestion informatique.

La version 4 de CobiT est sortie en décembre 2005 aux Etats-Unis. Les principales évolutions sont :

- une volonté de couverture de l'IT Governance plus globale (selon les cinq axes) et pas seulement focalisée sur la fonction audit et contrôle interne,
- une démarche résolument orientée "action", plus que contrôle,
- une volonté de rapprochement avec les autres référentiels majeurs que sont ITIL, COSO, ISO 17799.

Une version pdf de Cobit V4 est disponible, en anglais, pour les membres de l'AFAI sur le site de **l'ISACA**.

L'AFAI publiera la version française de COBIT V4 en décembre 2006.

## 3. Les outils mis à notre disposition

### 3.1. COBIT QuickStart



COBIT Quickstart propose une première approche aux nombreuses PME et autres entités pour lesquelles les TI ne sont ni un enjeu stratégique ni un élément clé de leur survie ; pour d'autres entreprises il constitue un point de départ dans leur évolution vers un niveau de contrôle et de gouvernance des TI adapté à leurs besoins.

Quickstart est utile à tous les types d'utilisateurs de COBIT dans les entreprises concernées : auditeurs, responsables des TI et acteurs de la mise en place de la gouvernance des TI qui ont de grandes chances de s'intéresser à la gouvernance et à COBIT pour la première fois, et qui

<b>www.ofppt.info</b>	Document	Millésime	Page
	Modele Cobit.doc	août 14	3 - 11

## Titre du document

souhaitent trouver une approche simplifiée et facile à mettre en œuvre pour commencer.

Lorsqu'on applique Quickstart il faut bien veiller à ce qu'il soit utilisé intelligemment en fonction des besoins et des spécificités de l'entreprise. Par ailleurs, même si Quickstart est un puissant outil de démarrage qui suggère les "choses intelligentes à faire", dans de nombreux cas il faudra ajouter des contrôles complémentaires pour constituer la base d'une gouvernance efficace de tous les processus informatiques.

Quickstart est donc une version allégée de COBIT plus facile d'accès et plus simple à mettre en œuvre.

### **3.1.1. Les hypothèses du Quick Start :**

- L'infrastructure informatique n'est pas complexe.
- Du fait de la taille de l'entreprise, les TI et l'activité sont bien alignées.
- Les tâches les plus complexes sont confiées à des services externes.
- Le but est de fabriquer moins et d'acheter plus.
- Les compétences informatiques internes sont limitées.
- La tolérance au risque est relativement élevée.
- L'entreprise est très attentive aux coûts.
- La structure de commandement est simple.
- L'éventail des contrôles est peu étendu.

Ces hypothèses correspondent à la culture du contrôle et de l'environnement informatique de la plupart des PME, et sans doute aussi à celle de petites entités secondaires ou autonomes d'organisations de plus grande taille.

Quickstart garde la structuration classique de COBIT en domaines, processus, objectifs de contrôle, mais il ne conserve que :

- 30 processus sur les 34,
- et surtout 62 objectifs de contrôle détaillés sur les 318 habituels.

La description des objectifs de contrôle est succincte, et renvoie aux objectifs de contrôle détaillés du COBIT « classique » référencés sous forme de liste de numéros d'objectifs.

Pour chaque objectif, 2 à 3 facteurs clés de succès sont présentés alors qu'une dizaine est proposée dans le COBIT « classique ».

Pour chaque objectif, Quickstart fournit 2 à 3 mesures recommandées, plutôt que la dizaine d'indicateurs clés de performance et d'indicateurs clés de d'objectifs présentés systématiquement dans le COBIT « classique ».

L'ouvrage, en annexe, montre le lien entre les 62 objectifs de contrôle détaillés et les principaux axes de gouvernance et de fonctionnement des technologies de l'information, sous forme de deux tableaux de

<b>www.ofppt.info</b>	Document	Millésime	Page
	Modele Cobit.doc	août 14	4 - 11

## Titre du document

diagnostics. Ceci a pour ambition d'aider l'utilisateur à définir rapidement les contrôles à utiliser face à un certain nombre de problèmes courants de gestion qui touchent les TI. Si un ou plusieurs de ces problèmes concernent l'entreprise de l'utilisateur, ces tables peuvent aider à identifier les contrôles importants.

Le premier tableau répartit des attributs "risque" selon deux catégories de "thèmes". Les cinq premiers thèmes correspondent aux aspects de la gouvernance des TI : alignement stratégique, délivrance de valeur, gestion des ressources des technologies de l'information, gestion des risques, gestion des performances. Les neuf thèmes suivants sont les problèmes informatiques qui préoccupent souvent les dirigeants : optimisation des coûts, délivrance de service, externalisation, sécurité, architecture, intégration des systèmes, fixation des priorités et planification, contrôles programmés, sécurité des applications. On peut aussi s'en servir de table de référence supplémentaire pour les objectifs de contrôle de Quickstart.

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

En synthèse, Quickstart propose une démarche de mise en oeuvre, résumée comme suit :

ETAPE	DESCRIPTION DES PROCESSUS	RESULTAT
1. Evaluer le bien-fondé	Utiliser les tests fournis avec Quickstart pour déterminer si l'approche Quickstart est adaptée à l'entreprise. Le résultat montrera si on peut utiliser ce programme tel quel ou s'il faut le compléter avec certains composants plus détaillés de la version complète de COBIT, ou encore s'il faut recourir à cette version complète dès le début.	Décision d'utiliser ou non COBIT Quickstart
2. Evaluer la situation actuelle	Utiliser les graphes de Quickstart pour définir la situation actuelle de l'entreprise. Pour cette étape il s'agit le plus souvent de rechercher des données, d'interviewer des personnels clés responsables de ces processus, et d'examiner des résultats de performances et des rapports d'audits. On peut aussi réunir une équipe de travail avec des personnels qui connaissent la question pour travailler avec un animateur et suivre le processus dans son déroulement.	Processus tel qu'il est
3. Déterminer la cible	Considérer l'environnement de travail de l'entreprise et positionner la situation visée sur les tableaux de situation des processus de Quickstart. Les considérations les plus courantes sont : 1. Nature de l'activité 2. Contraintes légales et réglementaires 3. Confidentialité des informations traitées 4. Dépendance vis-à-vis de la technologie. Il est important que ce positionnement soit, si possible établi, mais en tout cas approuvé par les dirigeants et par les propriétaires de l'entreprise.	Situations visées par le processus
4. Analyser les écarts	Examiner les pratiques de contrôles et les FCS (facteurs clés de succès) qui correspondent à l'écart de chaque processus (différence entre la situation actuelle et la situation visée), pour déterminer la nature et l'importance des améliorations nécessaires.	Énoncé des modifications de processus
5. Définir	Regrouper les modifications de processus individuelles dans des projets d'amélioration, améliorations qui permettront à l'entreprise de faire de réels progrès par étapes successives faciles à gérer.	Projets d'amélioration des processus
6. Elaborer un programme intégré de mise en place de la gouvernance	Organiser les projets d'amélioration selon des séquences et des priorités en un plan programme intégré qui prenne en compte les besoins immédiats de l'entreprise, les interdépendances entre les projets et la disponibilité des res-	Plan programme intégré

### 3.1.2. Tests : savoir si COBIT QuickStart répond à vos besoins

COBIT Quickstart propose deux tests pour évaluer l'intérêt qu'il peut y avoir pour une entreprise de mettre en place des contrôles des TI inspirés de ceux de Quickstart :

1. Le premier test (Restez dans la zone bleue), aide l'entreprise à déterminer si elle est susceptible d'utiliser Quickstart pour gérer

<b>www.ofppt.info</b>	Document	Millésime	Page
	Modele Cobit.doc	août 14	5 - 11

## Titre du document

ses risques informatiques ou si elle doit envisager d'utiliser la version complète de COBIT.

2. Le second test (Surveillez le thermomètre) peut aider à évaluer les situations particulières qui doivent conduire à envisager d'aller au-delà de COBIT Quickstart.

### 3.1.3. COBIT Online



COBIT ONLINE est un site web réalisé par l'IT Governance Institute accessible par abonnement à l'adresse : [www.isaca.org/cobitonline](http://www.isaca.org/cobitonline)

Il offre diverses fonctionnalités comme la possibilité de pouvoir consulter et télécharger le contenu de COBIT en ligne, de réaliser des analyses comparatives (benchmark) et d'échanger avec d'autres utilisateurs (forum).

### 3.1.4. COBIT Advisor



L'AFAI a contribué à la version française du logiciel COBIT Advisor réalisé par la société METHODWARE.

En automatisant le référentiel COBIT, le logiciel COBIT Advisor (Audit) facilite la conduite d'un audit informatique et la génération de rapports et de représentations graphiques des résultats.

COBIT Advisor (Audit) donne la possibilité de :

- appliquer le Cadre de Référence COBIT dans un processus complet et cohérent
- consacrer plus de temps à l'audit et moins à l'enregistrement des données
- préparer les rapports d'audits informatiques, consolider et analyser les résultats en fonction de l'organisation concernée
- fournir un meilleur feed-back aux clients de l'audit, à l'aide de meilleurs rapports et de graphiques aisément adaptables
- analyser et interpréter les résultats de l'audit informatique à l'aide de fonctions performantes de tri et de filtre
- ajouter de nouveaux processus reflétant l'organisation des systèmes d'information de l'organisation.

Conçu par et pour les Auditeurs informatique, COBIT Advisor (Audit) vous assure une intégration cohérente du Cadre de Référence COBIT au travers de votre organisation.

# COBIT audit|advisor



## methodware

<b>www.ofppt.info</b>	Document	Millésime	Page
	Modele Cobit.doc	août 14	6 - 11

Titre du document

Ci-dessous des captures d'écran du logiciel développé par brochure de présentation du produit :

**Processus : Définir un plan informatique stratégique**

Fichier Modifier Fenêtre Aide

**P01 Planification et Organisation**

**Le contrôle du processus informatique**  
définir un plan informatique stratégique

**qui répond à l'impératif suivant**  
trouver l'équilibre optimal entre les possibilités offertes par les technologies de l'information et les besoins en TI de l'entreprise et en garantir la réalisation future

**est rendu possible par**  
un processus de planification stratégique entrepris à intervalles réguliers et débouchant sur des plans à long terme ; les plans à long terme doivent être régulièrement traduits en plans opérationnels dotés d'objectifs à court terme, clairs et concrets

Réponse de la Direction | Problèmes | Graphique | Pièces jointes | Arbre

Considérer | Objectifs de Contrôle | Guide d'Audit | Évaluation | Recommandation

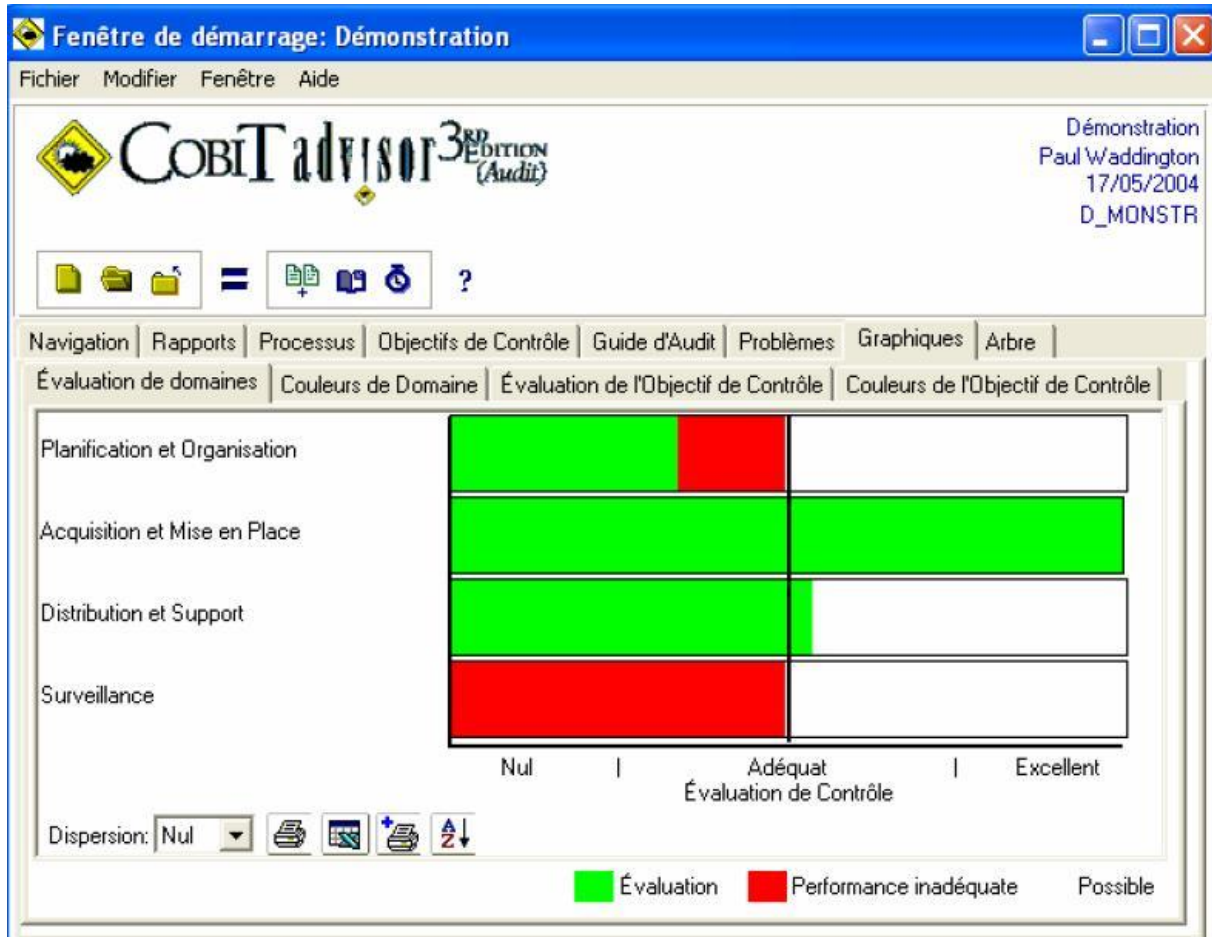
Num.	Libellé	Pertinent	Importance	Évaluation
1.1.1	Intégration des TI au plan à lo	Pertinent	Impact Important	Aucun Contrôle
1.1.2	Plan informatique à long terme	Pertinent	Impact Moyen	Aucun Contrôle
1.1.3	Approche et structure de la pl.	Pertinent	Impact Faible	Pas Évalué
1.1.4	Modifications du plan informat	Pertinent	Aucun Impact	Contrôles Adéqu
1.1.5	Planification informatique à co	Pertinent	Impact Important	Excellents Contr
1.1.6	Communication des plans info	Pertinent	Aucun Impact	Pas Évalué
1.1.7	Surveillance et évaluation des	Pertinent	Impact Très Impr	Contrôles Faibles

Évaluation  
 S/O Évaluation OC

Excellent - -  
- -  
Adéquat - -  
- -  
Nul - -

Démonstration  
Paul Waddington 17/05/2004





Le produit peut être testé en version de démonstration sur le site de l'éditeur à cette url : <http://www.methodware.com/demo/idx-demo.php3>.

### 3.1.5. COBIT v3 et v4

La **synthèse** est une présentation des concepts et principes de COBIT. Elle présente les domaines, les objectifs de contrôle généraux (aussi appelés processus) et le cadre de référence.

C'est une introduction à la méthode elle-même. Elle donne une vision générale de ce qu'est la méthode COBIT.

Le **cadre de référence** se décline en *check lists* méthodiques couvrant 4 domaines, 34 objectifs de contrôle généraux (très synthétiques) et 302 objectifs de contrôle détaillés. Chacun de ces objectifs répond à 3 familles d'impératifs : économiques et fiduciaires, sécuritaire et qualité.

**Le domaine Planification & Organisation** : 11 objectifs couvrent tout ce qui concerne la stratégie et les tactiques. Ils identifient les moyens permettant à l'informatique de contribuer le plus efficacement à la réalisation des objectifs commerciaux de l'entreprise.

**Le domaine Acquisition & Mise en place** : 6 objectifs concernent la réalisation de la stratégie informatique, l'identification, l'acquisition, le

<b>www.ofppt.info</b>	Document	Millésime	Page
	Modele Cobit.doc	août 14	8 - 11

Titre du document

développement, l'installation des solutions informatiques et leur intégration dans des processus commerciaux.

**Le domaine Distribution & Support** : 13 objectifs regroupent la livraison des prestations informatiques exigées (l'exploitation, la sécurité, les plans d'urgences et la formation).

**Le domaine Surveillance** : 4 objectifs permettent au management d'évaluer la qualité et la conformité des processus informatiques aux exigences de contrôle. Le **guide d'audit** permet d'évaluer et de justifier les risques et les faiblesses des objectifs généraux et détaillés et de mettre en place des actions correctives. Ce guide d'audit répond à 4 principes : l'acquisition d'une bonne compréhension, l'évaluation des contrôles, la vérification de la conformité, la justification du risque de ne pas atteindre les objectifs de contrôle.

Le **guide de management** fournit des indicateurs clés d'objectif et de performance et des facteurs clés de succès.

C'est aussi dans ce guide que l'on trouve le modèle de maturité. Il évalue l'atteinte d'un ou plusieurs objectifs généraux sous forme d'une échelle de 0 à 5 :

- 0 : Inexistant
- 1 : Existant mais non organisé (initialisé au cas par cas)
- 2 : Décrit (reproductible mais intuitif)
- 3 : Défini (avec documentation)
- 4 : Surveillé et mesuré
- 5 : Optimisé.

Les **outils de la mise en œuvre** contiennent une présentation de "*success story*" d'entreprises qui ont mis en place rapidement et avec succès la méthode COBIT. Cette partie intègre deux outils d'analyse de sensibilisation du management et de diagnostic de contrôle informatique.

Le COBIT est donc étroitement lié aux objectifs de l'entreprise tout en s'intéressant plus particulièrement à l'informatique. Il permet de rassurer le management, d'uniformiser les méthodes de travail et de garantir la sécurité et les contrôles de leurs services informatiques.

Une version pdf de Cobit V4 est disponible, en anglais, pour les membres de l'AFAI sur le site de l'[ISACA](#).

L'AFAI publiera la version française de COBIT V4 en décembre 2006.

La présentation effectuée par l'AFAI le 3 octobre 2006 portait sur 2 points dont **CobIT v4 : l'importance de la définition des objectifs et des métriques**.

<b>www.ofppt.info</b>	Document	Millésime	Page
	Modele Cobit.doc	août 14	9 - 11

### **Pour approfondir le sujet....**

Proposition de références utiles permettant d'approfondir le thème abordé

### **Sources de référence**

Citer les auteurs et les sources de référence utilisées pour l'élaboration du support