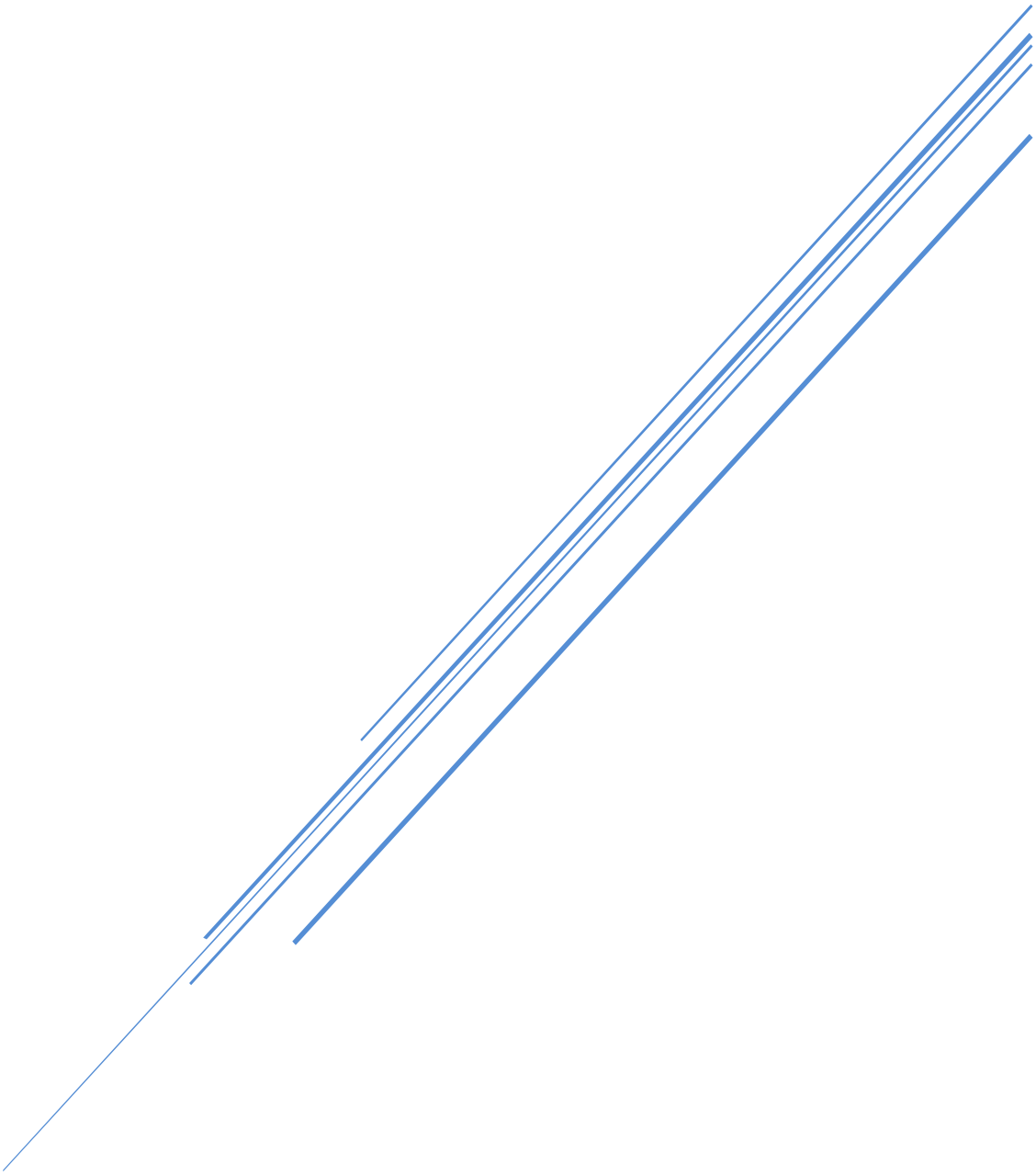
PRESENTATION DE COBIT



Christophe JUBRAN, Lauriane VIGIER, Quentin BRIOUDES

Génie Logiciel – CobiT

CobiT

Table des matières

Présentation générale de COBIT

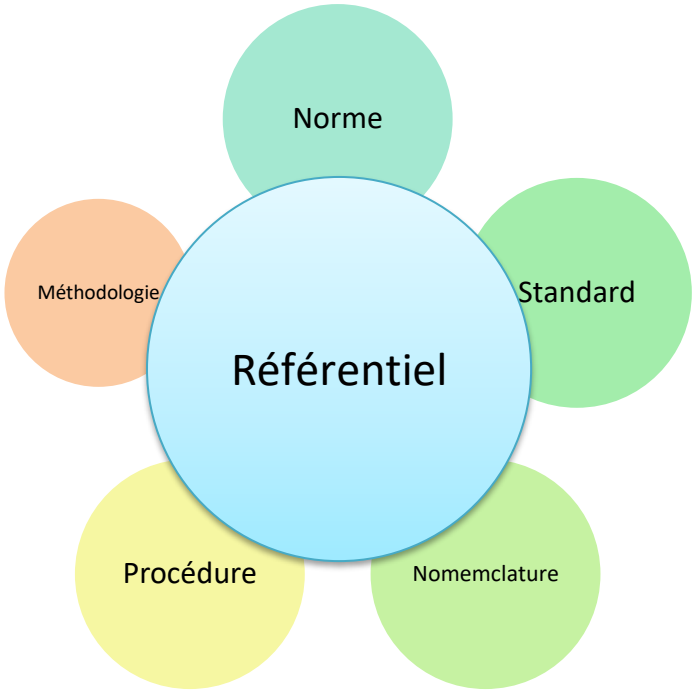
Définition générale

COBIT (**C**ontrol **OB**jectives for **I**nformation and related **T**echnologies) est un référentiel pour l'audit et la gouvernance des technologies de l'information.

CobiT a la particularité de s'intéresser tout particulièrement aux objectifs liés à l'informatique. Le principe de fonctionnement de CobiT est de dire quoi faire mais pas comment.

Référentiel – Définition

Le référentiel se situe à la frontière entre norme, standard, nomenclature, procédure et méthodologie. Il « fédère » ces différents principes



Historique

Le référentiel CobiT a été conçu par l'ISACA (**I**nformation **S**ystems **A**udit and **C**ontrol **A**ssociation), l'association pour le contrôle et l'audit des systèmes d'information, qui est une organisation internationale. Le but de CobiT est d'améliorer la gouvernance des technologies de l'information au sein des entreprises.

L'ISACA est représentée en France par l'AFAI, l'**A**ssociation **F**rançaise pour l'**A**udit et le conseil en **I**nformatique.

COBIT a évolué dans le temps selon diverses versions :

Premières versions

- **Création en 1996**

Version 3

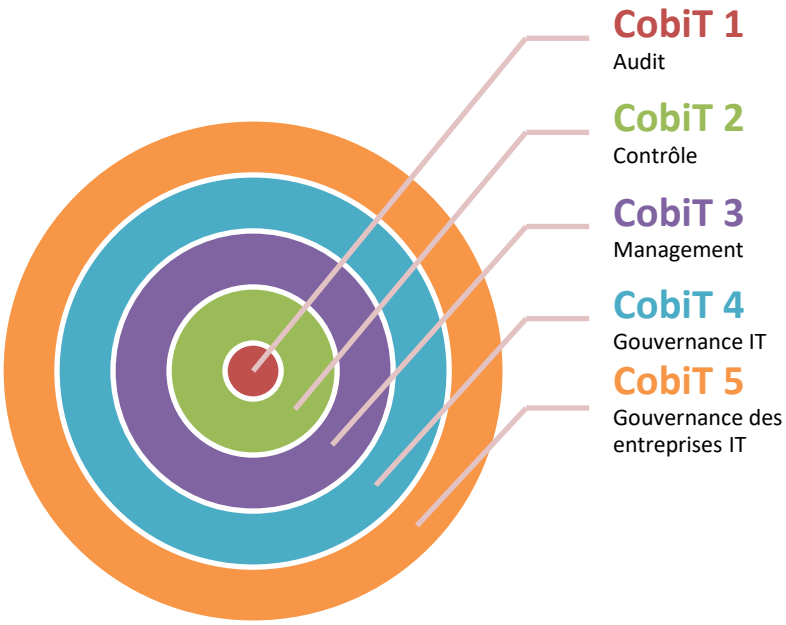
- **Création en 2000**

Version 4

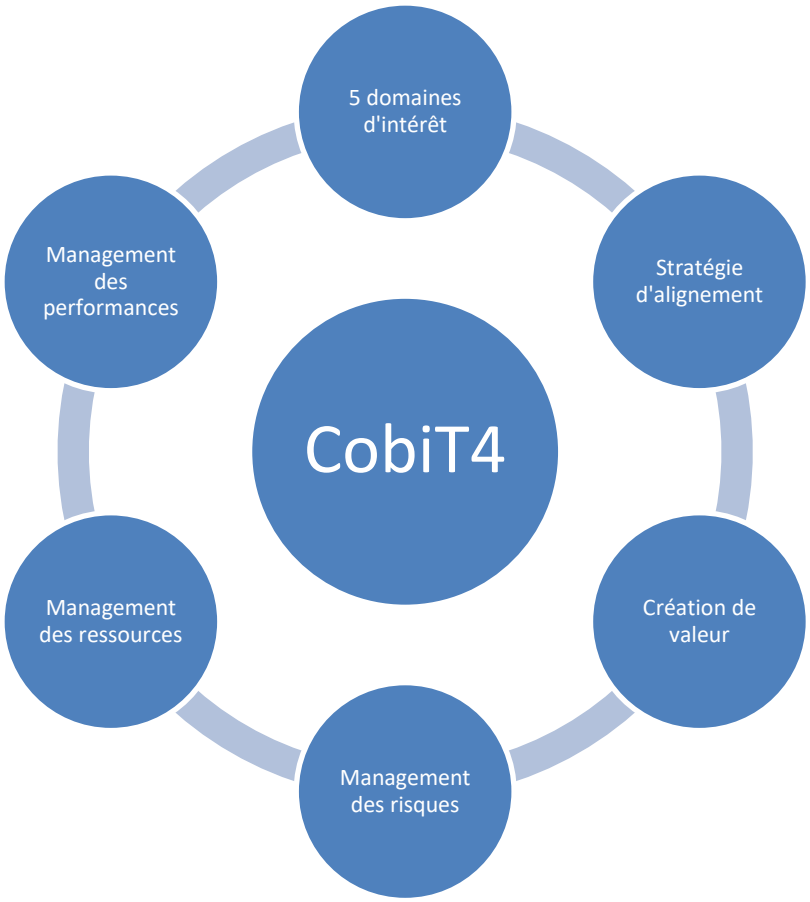
- **Création en 2005**
- **Création en 2007 de la version 4.1**

Version 5

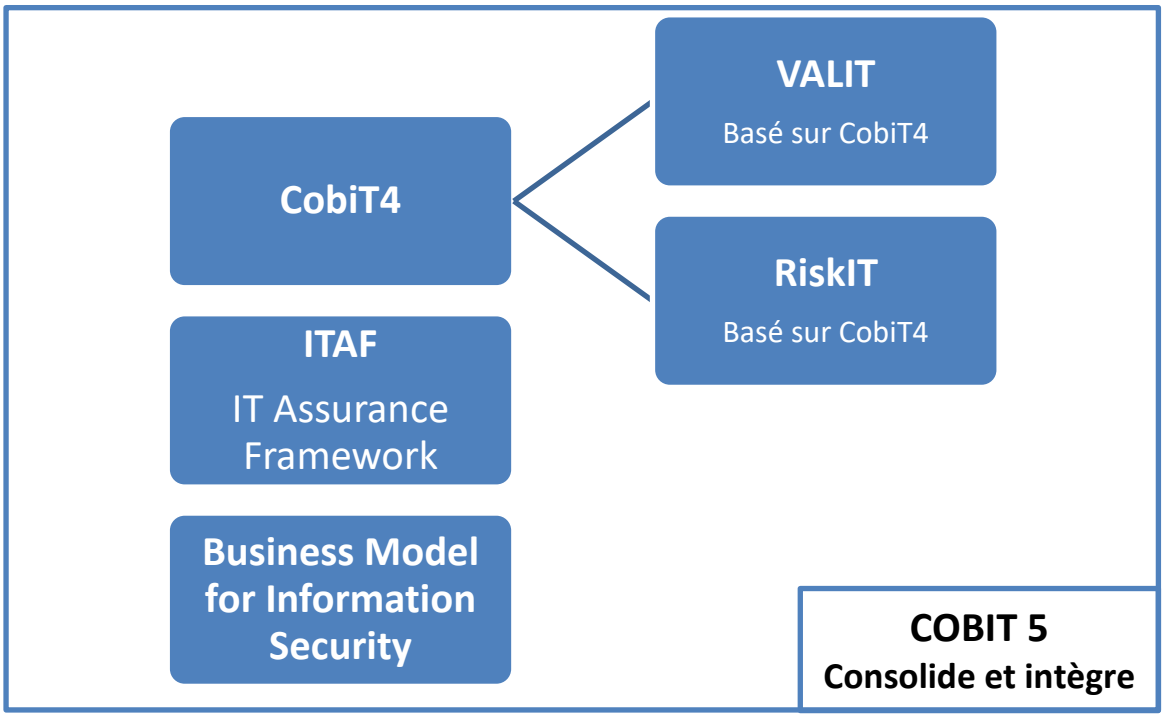
- **Création en 2013**

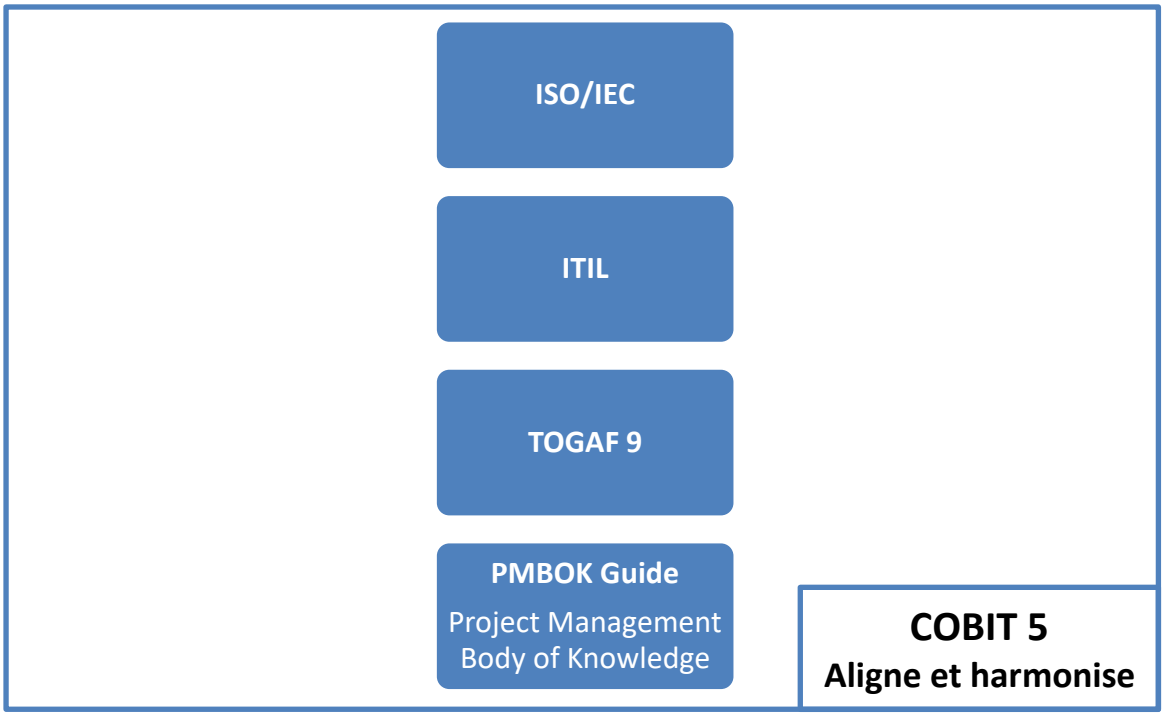


Ajouts de CobiT 4



Ajouts de CobiT 5





Dès les premières versions, COBIT a été conçu pour être un référentiel de contrôle. En 1996 on trouve donc déjà une liste de plus de 300 objectifs de contrôle permettant à l'auditeur de cadrer ses travaux.

Depuis la version 5, COBIT a évolué pour prendre en compte :

- **Le « business model » des entreprises utilisant COBIT,**
- **Les environnements technologiques de ces entreprises**

CobiT5 peut ainsi être appliqué à toutes les industries, peu importe leur lieu géographique ou leur culture d'entreprise.

CobiT peut être appliqué à de nombreux domaines d'une entreprise, comme :

- La sécurité de l'information
- La gestion des risques
- La gouvernance et la gestion du Système d'Information de l'entreprise
- Les activités d'audit
- La conformité avec la législation et la règlementation
- Les opérations financières ou les rapports sur la responsabilité sociale de l'entreprise

Avant d'aller plus loin : quelques définitions clés

Qu'est-ce qu'un système d'information (SI) ?

Le Système d'Information **(*)** est un ensemble organisé de ressources qui permet de collecter, stocker, traiter et distribuer de l'information.

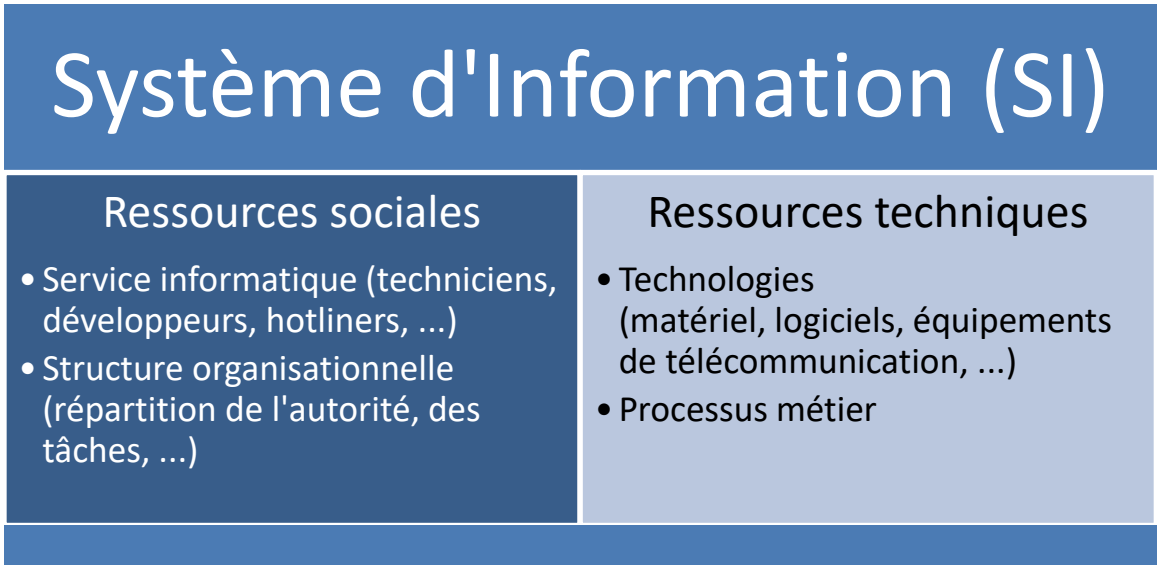
Les ressources de ce système se distinguent en deux catégories : la catégorie « social » et la catégorie « technique ».

La catégorie « social » correspond aux personnes liées au SI et à la structure organisationnelle qui les regroupe.

La catégorie « technique » est composée des technologies (matériel, logiciels, et équipements de télécommunication) et des processus métier.

(*) NOTE : Dans la suite de ce document, l'abréviation **SI** sera utilisée.

Résumé : Le SI



Qu'est-ce que les Technologies de l'information (TI) ?

Les Technologies de l'Information et de la communication (TIC) **(*)** désignent les techniques de l'informatique, de l'audiovisuel, des multimédias, d'Internet et des télécommunications qui permettent aux utilisateurs de communiquer, d'accéder aux sources d'information, de stocker, manipuler, produire et transmettre l'information sous toutes ses formes (texte, son, image, vidéo, musique, …). Les textes juridiques et réglementaires parlent de « communications électroniques ».

(*) NOTE : Dans la suite de ce document, les abréviations **TI** ou **IT** seront utilisées.

Qu'est-ce que la gouvernance des Technologies de l'Information ?

La prise de conscience générale dans le fait que les TI peuvent avoir un impact important sur les performances de l'organisation à laquelle elles sont rattachées, a amené à la mise en place progressive de la gouvernance IT au sein des entreprises. La loi « Sarbanes-Oxley » aux États-Unis ou encore la réglementation bancaire « Bâle II » en Europe a initié cette prise de conscience.

L'une des idées clés de la gouvernance IT est d'éviter que l'informatique soit une boîte noire. En effet, traditionnellement, le management des entreprises se sent peu concerné par l'informatique et lorsqu'un problème survient, on s'en remet au responsable informatique de l'entreprise.

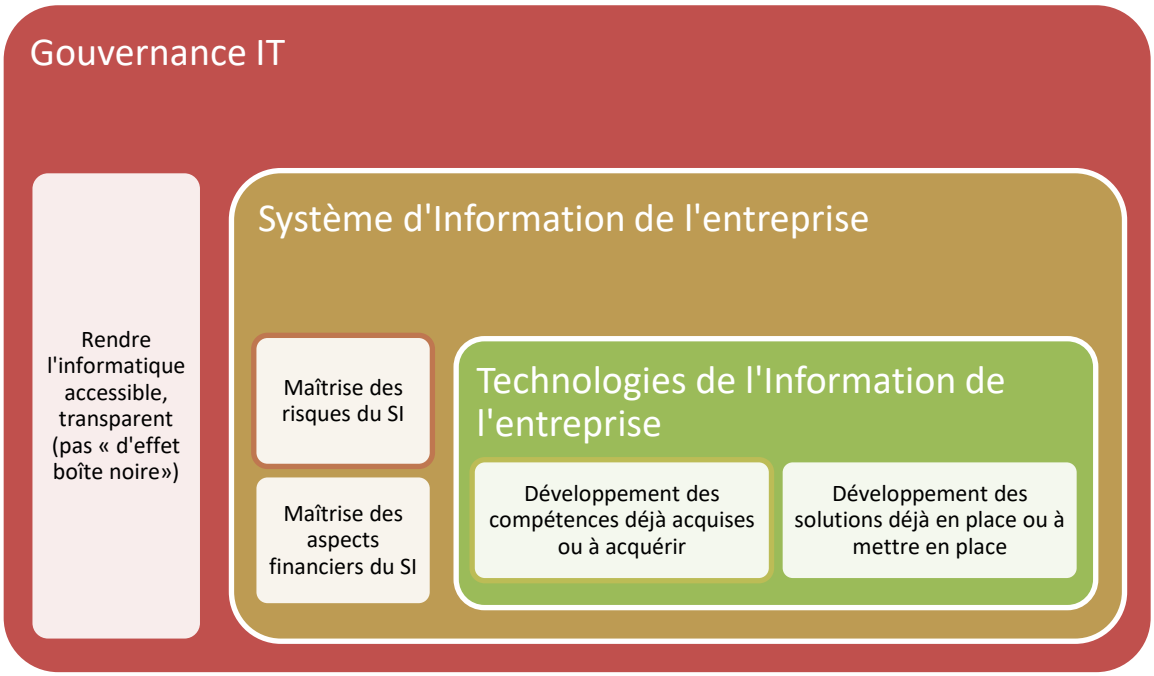
La gouvernance IT souhaite corriger cela et vise ainsi à impliquer toutes les parties prenantes (y compris les membres du Comité de Direction de l'entreprise et les principaux utilisateurs ; voire même le conseil d'administration).

La gouvernance IT repose sur la mise en œuvre de bonnes pratiques pour s'assurer que les investissements informatiques de l'entreprise contribuent à la création de valeur et à l'accroissement des performances des processus informatiques.

La maîtrise des risques liés au SI et la maîtrise des aspects financiers du SI représentent d'autres points clés de la gouvernance IT ; au même titre que le **développement des solutions et des compétences liées aux TI utilisées par l'entreprise**.

La transparence est primordiale pour éviter l'effet « boîte noire » traditionnellement ressenti par les parties prenantes au regard de l'informatique.

Résumé : La gouvernance IT



Principes et objectifs de CobiT

Objectifs

- Faire le lien entre risques métiers, besoins de contrôle et questions techniques afin d'apporter de meilleures pratiques en audit.

- Apporter une logique de contrôle et de management pour gérer les solutions techniques et les risques business.

- Fournir un langage commun pour permettre aux dirigeants d'entreprises de communiquer entre eux sur les objectifs et les résultats.

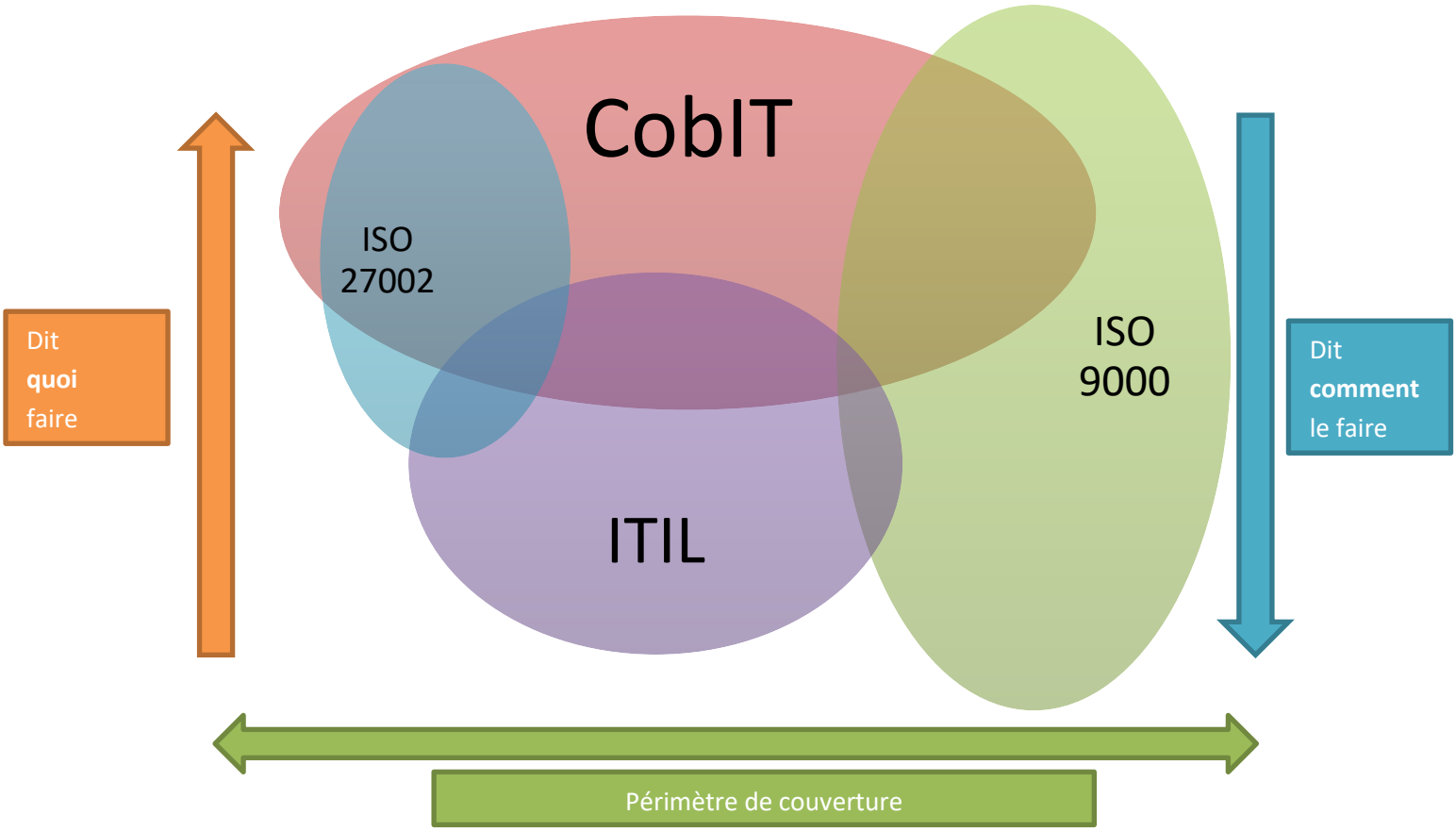
Périmètre d'application

Comme mentionné dans la partie « Qu'est-ce que la gouvernance des Technologies de l'Information ? », CobiT vise à impliquer toutes les parties prenantes du SI d'une entreprise.

CobiT repose sur une logique d'amélioration continue pour fonctionner à son plein potentiel. Il faut donc diffuser une culture d'amélioration au sein de l'entreprise pour que la logique de l'amélioration continue se mette en place d'elle-même et perdure.

La satisfaction des utilisateurs du SI représente un des facteurs centraux de la mesure des performances de l'application de CobiT.

Cependant, CobiT ne peut couvrir à lui seul tous les domaines, c'est pourquoi le référentiel CobiT consolide, intègre, aligne et harmonise d'autres référentiels, normes, standards ou méthodologies (voir « Ajouts de CobiT5 »). Mais ce n'est pas tout. En effet, CobiT est lié à la stratégie, mais rien n'empêche de le coupler à une surcouche ITIL pour gérer l'opérationnel ou encore à une couche PRINCE2 pour la gestion de projets.

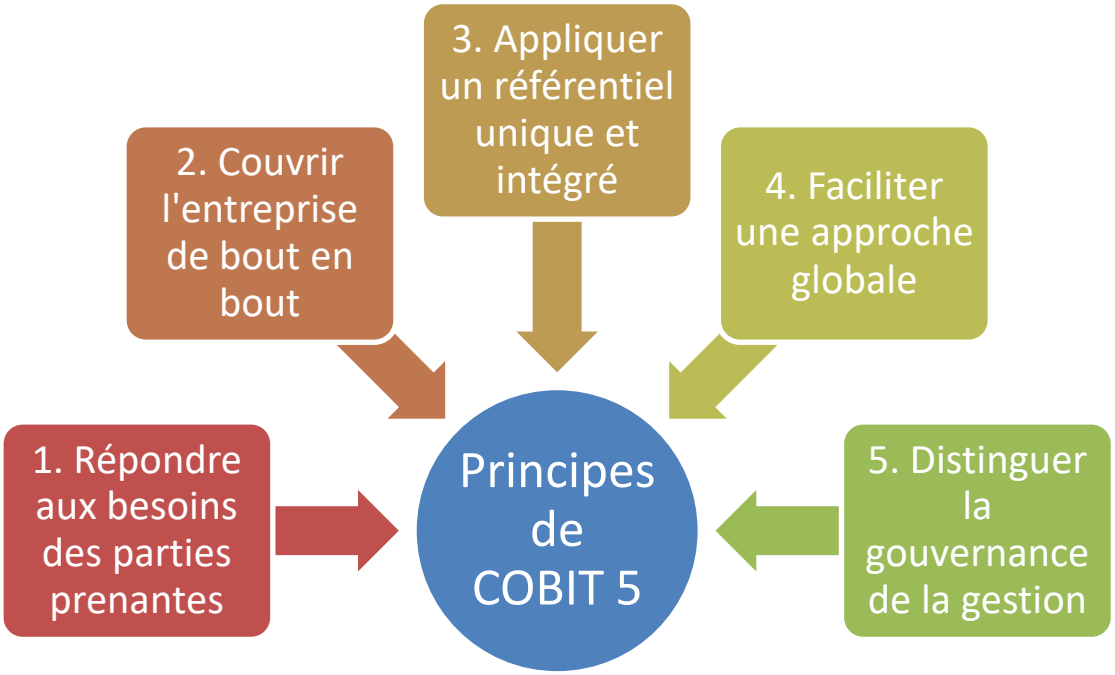


Principes

CobiT apporte un **cadre de pilotage orienté processus SI**, ce qui contribue efficacement à **aligner la gouvernance IT sur la stratégie de l'entreprise**. Cet alignement stratégique consiste à redessiner les structures organisationnelles, processus du SI et systèmes de production afin qu'ils soient en parfait accord avec la stratégie de l'entreprise.

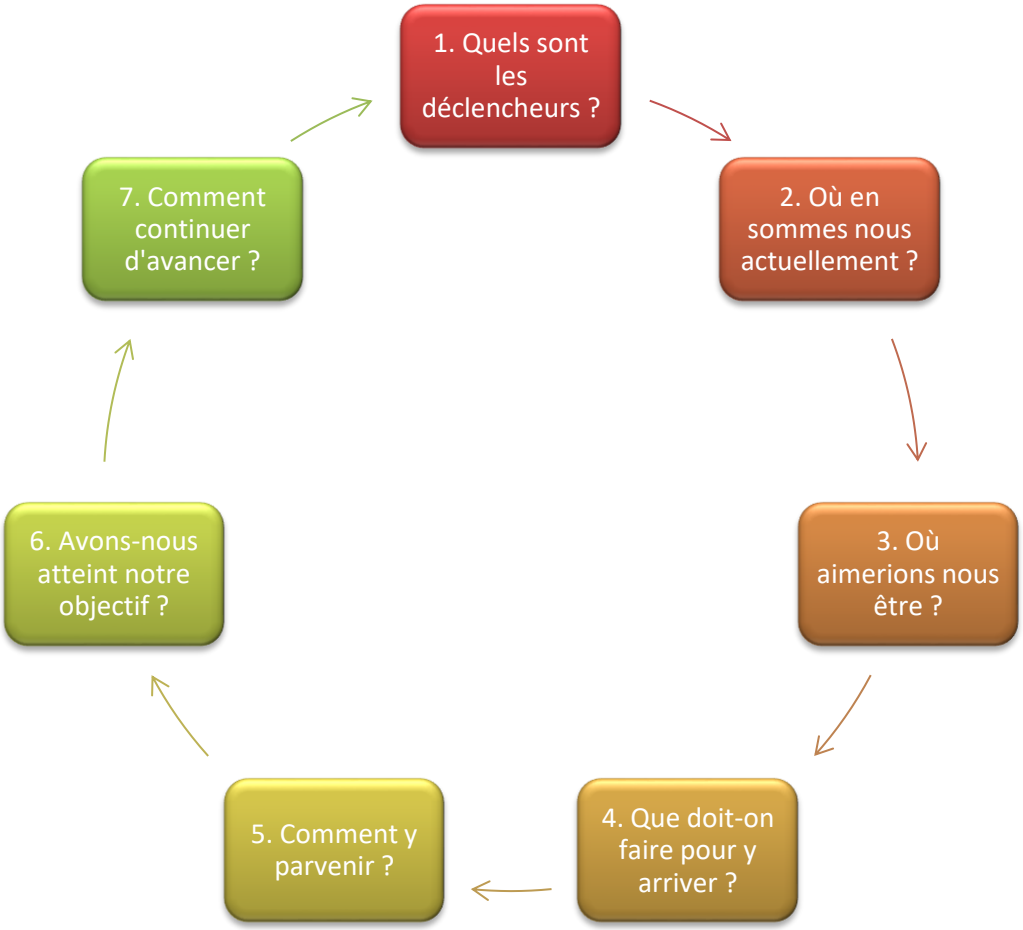
De plus, CobiT fournit des indicateurs clés **d'objectif**, des indicateurs clés de **performance** et des facteurs clés de **succès** pour chaque processus tout en se focalisant sur ce que l'entreprise a **besoin de faire** et non sur la façon de faire.

Les 5 principes de CobiT



1. Assurer la création de valeur au sens des parties prenantes tout en optimisant la gestion des ressources et la maîtrise des risques
2. Prendre en considération l'ensemble des processus de l'entreprise
3. Englober les autres référentiels
4. Assurer une approche globale
5. Mettre en évidence la distinction entre gouvernance et gestion de l'entreprise

Les 7 étapes du cycle de vie de la mise en œuvre de CobiT



Gestion des programmes

1. Initier le programme
2. Définir les problèmes et les opportunités
3. Définir un plan général
4. Planifier la gestion
5. Exécuter le plan
6. Réaliser des bénéfices
7. Revoir l'efficacité

Facilitateurs du changement

1. Établir les changements souhaités
2. Former une équipe pour l'implémentation
3. Établirles résultats à atteindre
4. Identifier les acteurs
5. Exploiter et utiliser
6. Intégrer les nouvelles approches
7. Soutenir la production

Cycle de vie de l'amélioration continue

1. Identifier les besoins auxquels répondre
2. Évaluer l'état actuel
3. Définir l'état à atteindre
4. Développer / acquérir les améliorations
5. Mettre en place les améliorations
6. Exploiter et mesurer
7. Surveiller et évaluer

Les domaines et processus de CobiT 4.1

Cobit 4.1 est structuré selon 34 processus regroupés en 4 domaines listés ci-dessous.

1) Planning and Organization: Planning et Organisation

Comment utiliser au mieux les technologies afin que l'entreprise atteigne ses objectifs ?
Contient 11 processus.

Dans ce domaine nous cherchons à savoir comment utiliser les technologies afin que l'entreprise atteigne ses objectifs.

2) Acquisition and Implementation: Acquisition et Mise en place

Comment définir, acquérir et mettre en oeuvre les technologies nécessaires en adéquation avec les business processus de l'entreprise ?
Contient 6 processus.

Ici CobiT cherche à définir, acquérir et mettre en œuvre des technologies en les alignant avec les processus métiers de l'entreprise.

3) Delivery and Support: Distribution et Support

Comment garantir l'efficacité et l'efficience des systèmes technologiques en action ?
Contient 13 processus.

L'objectif est de garantir l'efficacité et l'efficience des systèmes technologiques en action.

4) Monitoring: Surveillance

Comment s'assurer que la solution mise en œuvre corresponde bien aux besoins de l'entreprise dans une perspective stratégique ?
Contient 4 processus

Il convient ici de vérifier si la solution mise en place soit en adéquation avec les besoins de l'entreprise dans une vision stratégique.

Critères pour la qualification d'un jugement selon CobiT 4.1

Nous avons ensuite les critères pour la qualification d'un jugement. CobiT dispose de 7 critères pour qualifier un jugement :

1) Efficacité

2) Efficience

3) Confidentialité

4) Intégrité

5) Disponibilité

6) Conformité

7) Fiabilité

Selon ces cas, nous avons 5 types de ressources concernées :

1) Données

2) Applications

3) Technologies

4) Installation

5) Personnel

Le package CobiT

L'outil CobiT dispose d'un package qui contient les ressources suivantes :

- Executive Summary

Résumé synthétique pour les managers pressés

- Framework

Cadre de référence explicatif de la méthode, des domaines et processus

- Control Objectives

Les objectifs de contrôle : ils sont au nombre de 215

-Audit Guidelines

Le guide de l'audit : Comment assurer un audit efficace ?

- Implementation Tool Set

Les outils pour la mise en oeuvre de COBIT

- Management Guidelines

Le guide du management

L'objectif étant d'assurer l'adéquation durable entre les technologies, les processus métiers et la stratégie d'entreprise. Ce guide propose un cadre de pilotage (de type tableau de bord équilibré ou Balanced Scorecard) et d'évaluation. Nous sommes là tout à fait dans le cadre de la gouvernance du SI. Le guide de management propose aussi un modèle de maturité afin d'apprécier sur une échelle à 5 degrés le niveau d'évolution de chacun des processus. Le guide ne serait pas achevé s'il ne comportait l'identification des principaux facteurs de succès et des indicateurs de performance clés.

Exemple d'utilisation de CobiT 5

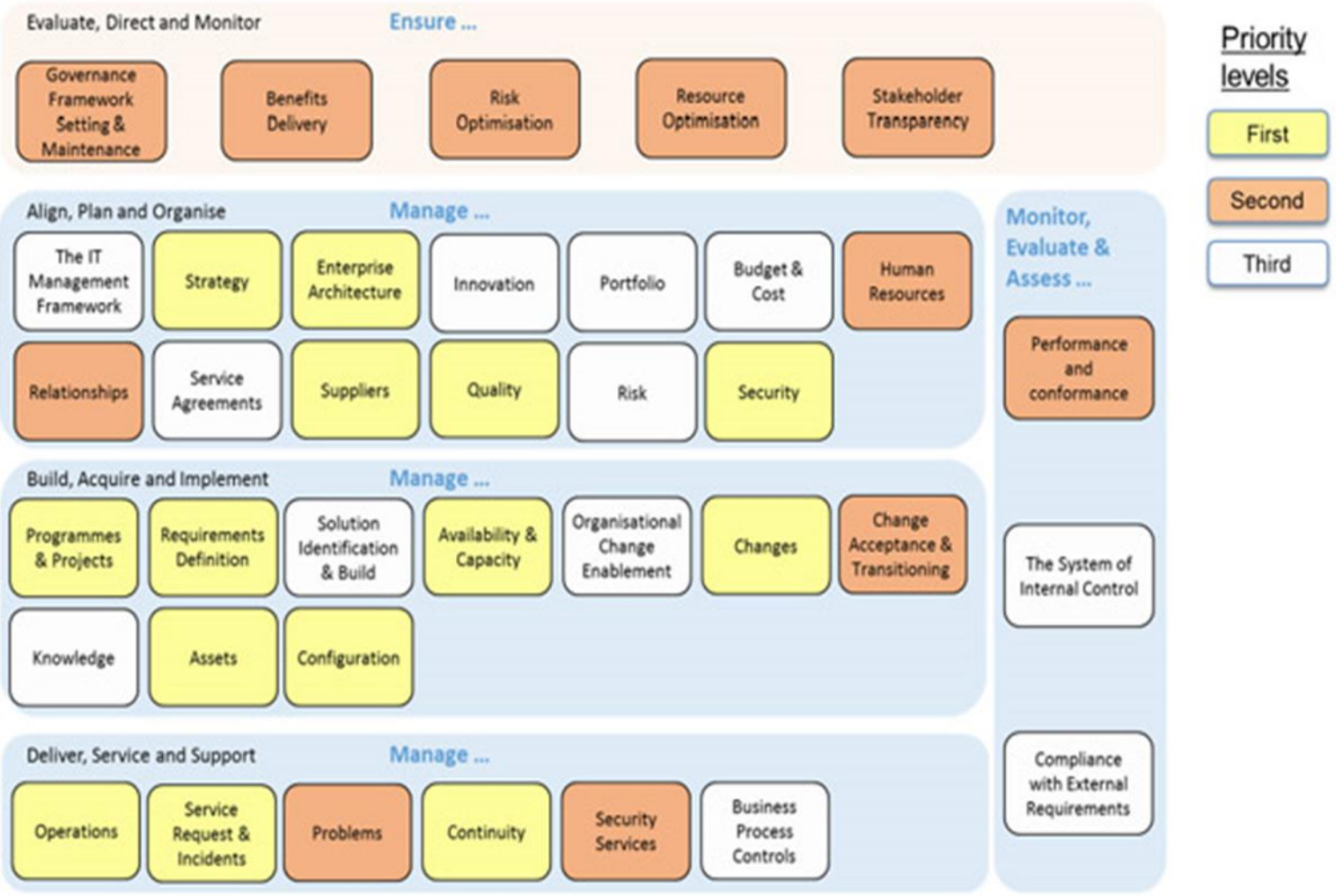
Catégorisation des processus

CobiT préconise de commencer par classifier les processus en diverses catégories. Comme CobiT dit « quoi faire » mais pas « comment » (voir Périmètre d'application), la liste de catégories pour classifier les processus n'est pas définie par CobiT, c'est l'entreprise utilisatrice de CobiT qui définit les catégories de processus. On peut ainsi retrouver, par exemple, la liste de catégories suivante :

1. Évaluer, diriger, surveiller (Evaluate, Direct and Monitor)
2. Aligner, planifier et organiser (Align, Plan and Organise)
3. Construire, acquérir et mettre en œuvre (Build, Acquire and Implement)
4. Livraison, service et support (Deliver, Service and Support)

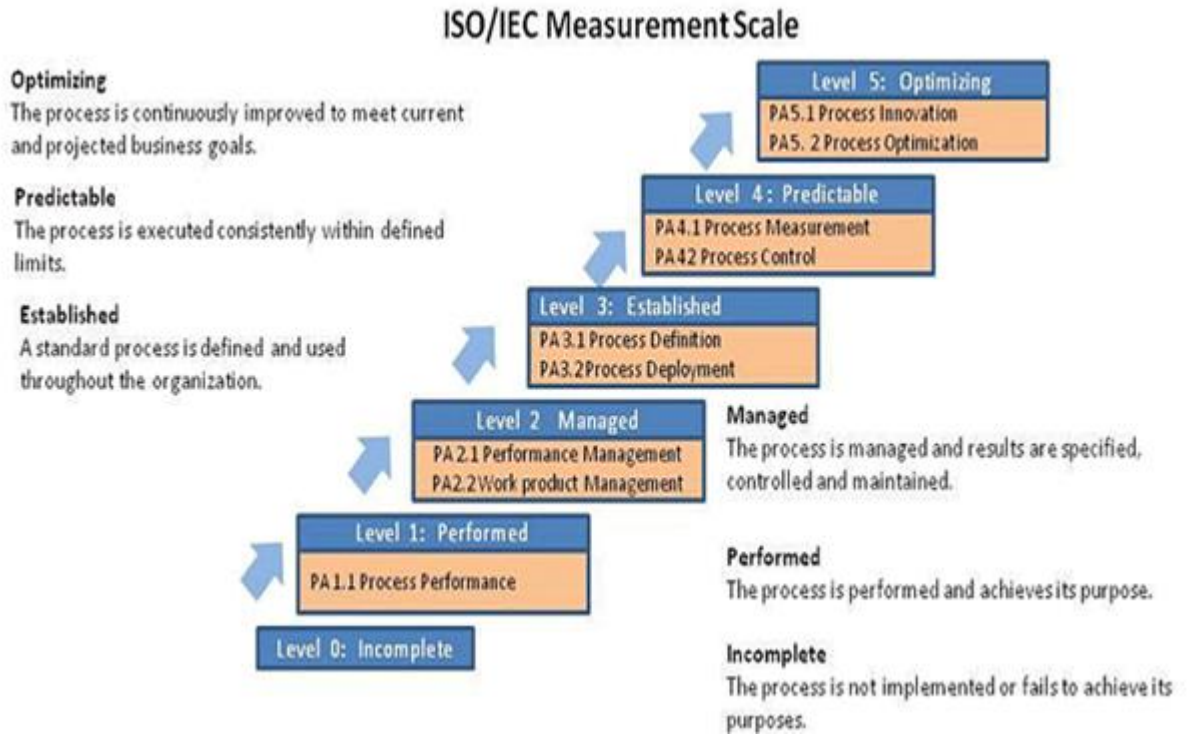
Hiérarchisation des processus

Les processus catégorisés sont ensuite classés par ordre de priorité ; là encore CobiT ne précise pas comment hiérarchiser les processus ; on peut donc par exemple retrouver un schéma comme suit :



Attribution d'un niveau aux processus

Une fois nos processus catégorisés et hiérarchisés, on leur attribue un niveau d'avancement. Pour cela on peut utiliser le « Process Assessment Model (**PAM**) » de CobiT ou le « Measurement Scale » d'ISO/IEC par exemple :



Level 0.	Incomplete	En développement, non implémenté ou processus à modifier
Level 1.	Performed	Processus est fonctionnel et atteint son but
Level 2.	Managed	Le processus est géré et ses résultats sont spécifiés, contrôlés et maintenus
Level 3.	Established	Le processus est défini et utilisé dans toute l'entreprise
Level 4.	Predictable	Le processus est exécuté de manière cohérente dans des limites définies
Level 5.	Optimizing	Le processus est continuellement amélioré pour atteindre les objectifs actuels et prévus

Attribution de tâches à chaque processus

Chaque processus se voit ensuite attribuer des tâches, avec de préférence une priorité, une date de début et de fin prévues et si possible la répartition des tâches (qui fait quoi). Par exemple :

Action name	Priority	Date action	What	Due date	Who
APO01	1	06.08	Validate findings and score	31.08	GVO
APO01	2	07.08	Complete process description	11.09	GVO
APO01	3	22.08	Valide process description	17.09	KDJ
EDM02	2	07.08	Define implementation steps	15.09	KBU
EDM03	2	07.08	Define stakeholders & ownership	17.09	KDJ

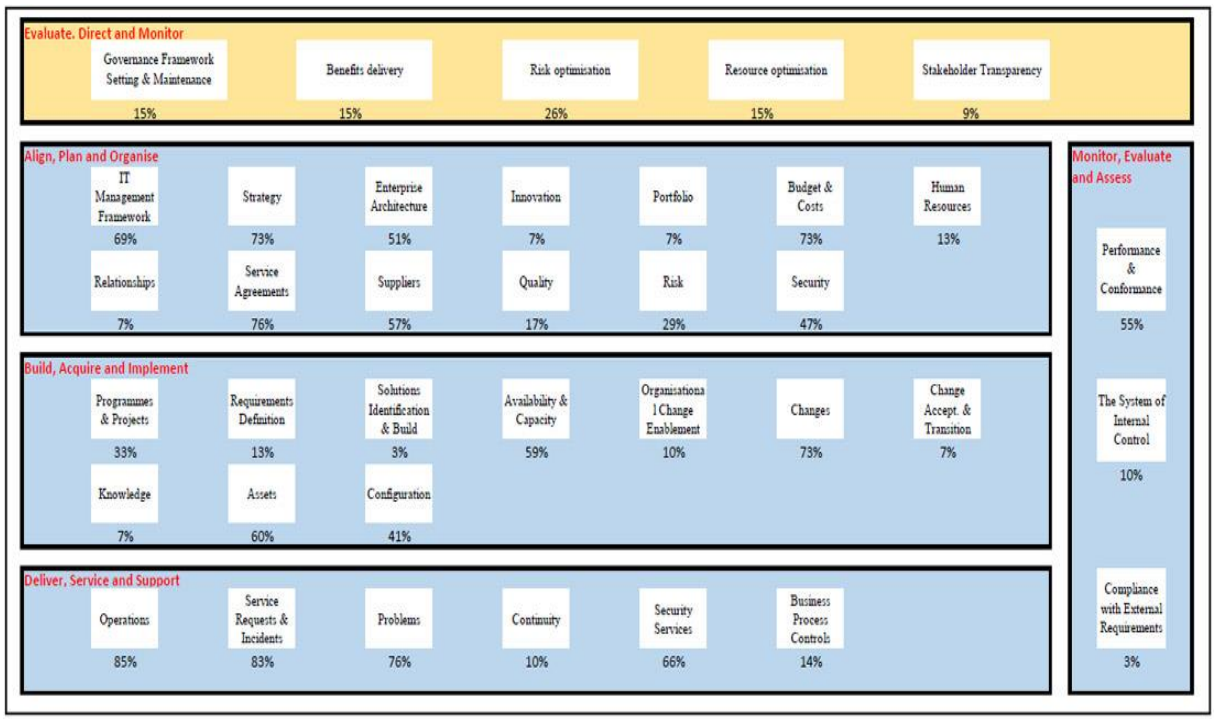
Suivi de l'avancement des processus

En connaissant l'avancement de chaque tâche reliée à chaque processus, il devient possible de calculer son avancement. Une fois de plus, CobiT n'impose pas de méthodologie. **Rappelons que le but de CobiT est de s'adapter à toutes les structures, c'est pourquoi le « comment » n'est jamais précisé**. Ici, un simple tableau Excel peut donc faire l'affaire, par exemple :

				PAM level achieved				
Process	Total score	Owner	Process Title	Level 2	Level 3	Level 4	Total score on Oct.	Difference Nov. Vs. Oct.
EDM01	15%	KDJ	Governance Framework Setting & Maintenance	26%	12%		15%	0%
EMD02	15%	KDJ	Benefits delivery	26%	12%		15%	0%
EDM03	26%	NFR	Risk optimisation	58%	31%		26%	0%
APO09	76%	GVO	Service Agreements	80%	95%	75%	75%	1%
BAI09	60%	JFZ	Configuration	80%	73%		43%	17%

Avancement global des processus

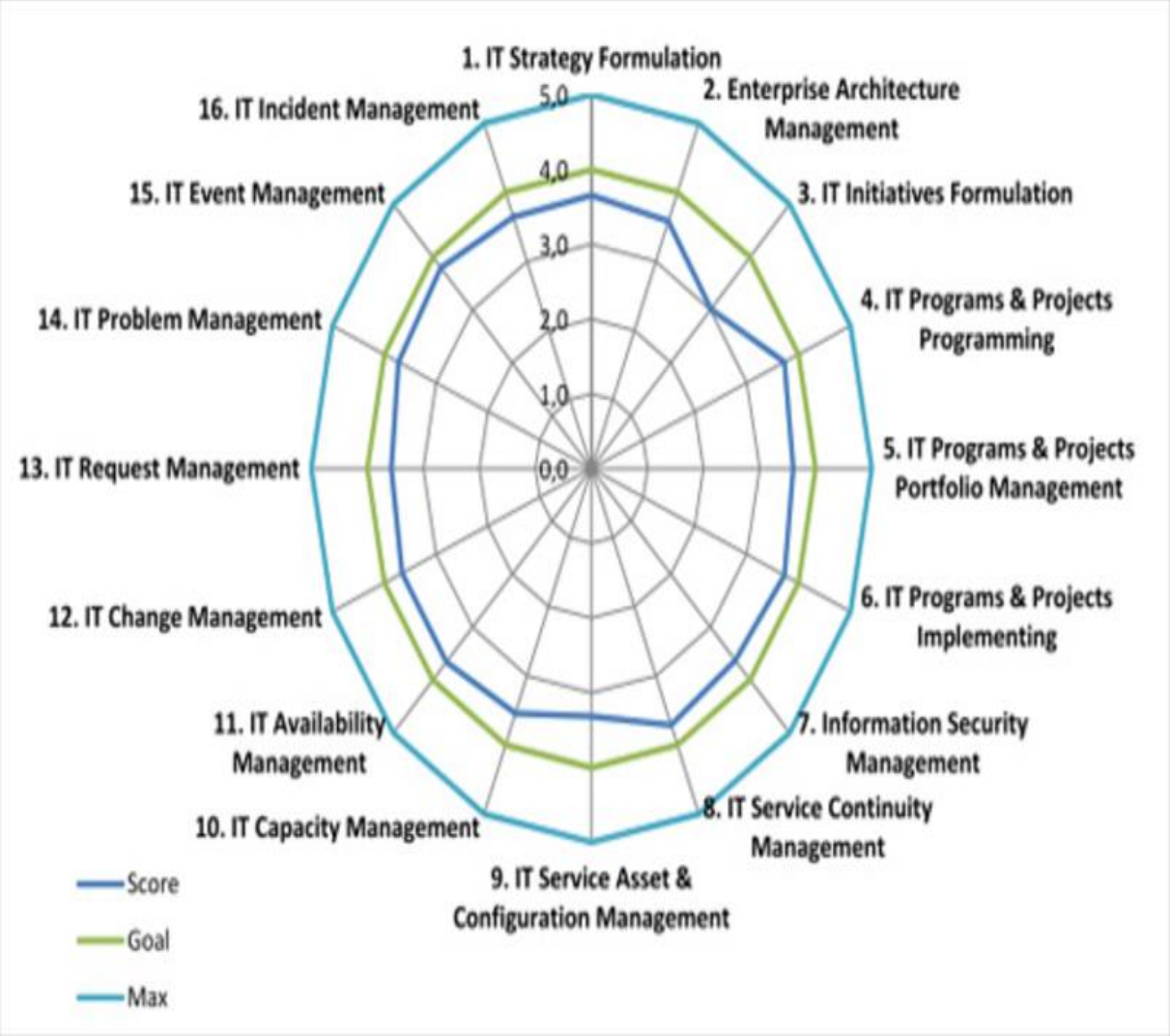
Le suivi de l'avancement des processus permet principalement de réaliser un suivi de l'avancement global des processus. On peut ainsi attribuer un pourcentage d'avancement à chaque processus et les lister des un schéma, tableau ou graphique afin d'avoir une visualisation globale de l'avancement. Par exemple :



Idéalement, les processus les plus simples à réaliser et à mettre en place ainsi que les processus prioritaires sont les processus les plus avancés.

Graphique des scores

Le graphique des scores est un autre moyen de visualiser l'avancement global des processus. Ici, on attribue simplement un « score » à un processus. Le score peut correspondre au pourcentage d'avancement du processus par exemple ; ou à une notation prenant en compte divers facteurs, en fonction de nos besoins. Il s'agit donc d'une visualisation globale encore plus générale, puisqu'elle peut englober de nombreux facteurs en fonction de ce à quoi correspond le score.



Matrice RACI

La répartition des tâches se base bien généralement sur une matrice RACI pour chaque tâche et chaque processus traités. La matrice RACI est simple et rapide à mettre en place, simple à comprendre, ne demande pas de ressources particulières et reste malgré tout complète. C'est pourquoi on la retrouve dans de nombreux projets. Toutefois, CobiT n'impose pas l'utilisation de matrice RACI.

Le fonctionnement d'une matrice RACI repose sur l'attribution de rôles à différentes personnes. Chaque personne pouvant endosser divers rôles pour diverses tâches. Par exemple, un collaborateur peut être à la fois réalisateur de la tâche 1 et en même temps approbateur de la tâche 2.

On retrouve les rôles suivants dans une matrice RACI :

- **Approbateur (A)** : La personne « Approbateur » est en charge de la tâche. Il s'organise comme il veut pour que la tâche en question soit réalisée. Il sous-traite le travail au(x) Réalisateur(s) et peut également participer à la réalisation de la tâche. Il n'y a qu'un seul Approbateur par tâche.
- **Réalisateur (R)** : Réalise la tâche en question. Il doit y avoir **au moins** un Réalisateur par tâche.
- **Consulté (C)** : Personne(s) ou entité(s) à consulter pour contribuer au bon déroulement de la tâche.
- **Informé (I)** : Personne(s) ou entité(s) à informer de l'avancement de la tâche.

Dans cet exemple, on pourrait retrouver la matrice RACI suivante :

	GVO	KDJ	KBU
APO01	A, R	R	I
EDM02	I	C	A, R
EDM03	I	A, R	C