

Certifié sur la gouvernance COBIT® 5, **Alphonse Carlier** est formateur et consultant IT depuis plus de 30 ans. En tant que professionnel, il intervient régulièrement sur des actions de conseil, de chef de projet et de programme sur le développement des systèmes d'information. Ses spécialités couvrent les bases de données, les projets DevOps, agilité avec SCRUM et PSM, l'urbanisation et le déploiement des nouvelles architectures, mais aussi l'ETL *open source* et *salesforce*, ITIL 2011, *lifecycle* des services, ISO 20000, ISO 27001 et bien sûr le *cloud computing* et l'environnement *Big Data Hadoop*. Il intervient aussi sur des synthèses en tant qu'animateur de réunions autour du *Web* et des technologies de la communication, référencement des processus et auditeur interne ISO 9001 dans plusieurs entreprises.

Enfin, il est l'auteur de plusieurs ouvrages publiés chez AFNOR Éditions et chez Hermès-Lavoisier : *Intelligence économique et Knowledge Management*, *Management de la qualité pour la maîtrise des systèmes d'information*, *Manuel qualité pour les systèmes d'information*, *Le pilotage des évolutions des SI, SI élargis*, *Gestion des connaissances*, *Business intelligence et management*, *Management des projets collaboratifs*, *Premiers pas avec le CMMI*.



Vous voulez nous faire partager  
une remarque ou une suggestion ?  
Contactez-nous :  
[fabrication-editions@afnor.org](mailto:fabrication-editions@afnor.org)

© AFNOR 2018

Édition : Catherine Dô-Duc

Couverture (création et exécution) : Gilda Masset

Fabrication : Philippe Malbec

Crédit photo : Adobe Stock, 2018

Mise en pages : Axelle Felgine Lallement

ISBN 978-2-12-465672-1



Toute reproduction ou représentation intégrale ou partielle, par quelque procédé que ce soit, des pages publiées dans le présent ouvrage, faite sans l'autorisation de l'éditeur est illicite et constitue une contrefaçon. Seules sont autorisées, d'une part, les reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective et, d'autre part, les analyses et courtes citations justifiées par le caractère scientifique ou d'information de l'œuvre dans laquelle elles sont incorporées (loi du 1<sup>er</sup> juillet 1992, art. L 122-4 et L 122-5, et Code pénal, art. 425).

AFNOR – 11, rue Francis de Pressensé, 93571 La Plaine Saint-Denis Cedex  
Tél. : + 33 (0) 1 41 62 80 00 – [www.afnor.org/editions](http://www.afnor.org/editions)

# Sommaire

<b>Présentation du référentiel COBIT® 5.....</b>	<b>9</b>
<b>1 Pourquoi COBIT® 5?.....</b>	<b>23</b>
1.1 Gouvernance de l'entreprise .....	23
1.2 En quoi consiste COBIT® 5? .....	25
1.3 Principales cibles de gestion.....	26
1.4 Les principaux référentiels .....	29
1.5 Si la gouvernance n'existait pas? .....	29
1.6 Les principaux acteurs autour de COBIT® 5.....	30
1.7 Positionnement dans les référentiels et les normes .....	33
1.8 En résumé .....	36
<b>2 Le modèle COBIT® 5.....</b>	<b>37</b>
2.1 Quelle est la vision globale du modèle COBIT® 5? .....	37
2.2 Les 7 facilitateurs .....	40
2.3 La matrice RACI des rôles et des responsabilités de COBIT® 5 ..	43
2.4 Appliquer des actions d'amélioration continue.....	45
2.5 Fondamentaux des niveaux de maturité .....	48
2.6 En résumé .....	49
<b>3 Les principes COBIT® 5.....</b>	<b>51</b>
3.1 Les 5 principes de COBIT® 5.....	51
3.2 Répondre aux besoins des parties intéressées.....	54
3.3 En résumé .....	61

<b>4</b>	<b>Les fondamentaux COBIT® 5 (partie 1)</b> .....	<b>63</b>
4.1	La démarche COBIT® 5 .....	63
4.2	Mécanisme de fonctionnement de la gouvernance .....	67
4.3	En résumé .....	70
<b>5</b>	<b>Les fondamentaux COBIT® 5 (partie 2)</b> .....	<b>73</b>
5.1	Synthèse des domaines de processus .....	73
5.2	Synthèse sur des domaines de processus .....	74
5.3	En résumé .....	81
<b>6</b>	<b>Les domaines avec COBIT® 5</b> .....	<b>83</b>
6.1	Les 5 domaines et les 37 processus .....	83
6.2	Les niveaux de la capacité des processus .....	84
6.3	Normes ISO 15504 .....	87
6.4	En résumé .....	88
<b>7</b>	<b>Les fondamentaux COBIT® 5 (partie 3)</b> .....	<b>89</b>
7.1	Points importants du modèle COBIT® 5 .....	89
7.2	Modèle global de référence.....	89
7.3	Modes d'évaluation de la capacité des processus.....	93
7.4	Comité de gouvernance .....	96
7.5	Gérer les changements.....	97
7.6	En résumé .....	101
<b>8</b>	<b>Gestion des risques</b> .....	<b>103</b>
8.1	Comprendre le positionnement des risques .....	103
8.2	COBIT® 5 et sécurité de l'information .....	104
8.3	Les méthodes d'analyse des risques .....	108
8.4	La norme ISO/IEC 27002:2013 .....	110
8.5	La norme ISO 27001 .....	115
8.6	La norme NF ISO 31000:2018 .....	118
8.7	En résumé .....	120
<b>9</b>	<b>Maîtriser le domaine EDS (Évaluer, Diriger et Surveiller)</b> ..	<b>121</b>
9.1	Généralités .....	121
9.2	Présentation du domaine EDS.....	121
9.3	Maîtriser les processus du domaine EDS.....	122

9.4	En résumé .....	130
<b>10</b>	<b>Maîtriser le domaine APO (Aligner, Planifier et Organiser) ..</b>	<b>133</b>
10.1	Généralités .....	133
10.2	Présentation du domaine APO.....	133
10.3	Maîtriser les processus du domaine APO .....	134
10.4	En résumé .....	146
<b>11</b>	<b>Maîtriser le domaine BAI (Bâtir, Acquérir et Implémenter)...</b>	<b>147</b>
11.1	Présentation du domaine BAI .....	147
11.2	Maîtriser les processus du domaine BAI .....	148
11.3	En résumé .....	159
<b>12</b>	<b>Maîtriser le domaine LSS (Livrer, Servir et Soutenir) .....</b>	<b>161</b>
12.1	Présentation .....	161
12.2	Maîtriser les processus du domaine LSS .....	161
12.3	En résumé .....	168
<b>13</b>	<b>Maîtriser le domaine SEM (Surveiller, Évaluer et Mesurer) ..</b>	<b>169</b>
13.1	Présentation .....	169
13.2	Maîtriser les processus du domaine SEM .....	169
13.3	En résumé .....	174
<b>14</b>	<b>Mise en œuvre COBIT® 5 : cas FORCE1 .....</b>	<b>177</b>
14.1	Contexte de l'entreprise .....	177
14.2	Quelles démarches mettre en œuvre ? .....	180
14.3	Outils disponibles .....	181
14.4	Mise en place des contrôles internes.....	188
14.5	Audits internes .....	189
14.6	Mettre en place des questionnaires .....	191
14.7	En résumé .....	193
	<b>Conclusion.....</b>	<b>195</b>
	Éléments clés de la gouvernance COBIT® 5 .....	195
	Des changements culturels.....	197
	<b>Annexes .....</b>	<b>201</b>
	<b>Bibliographie .....</b>	<b>207</b>
	<b>Sigles et abréviations .....</b>	<b>213</b>

# Présentation du référentiel COBIT® 5

« La culture n'est pas un luxe, c'est une nécessité. »

Gao Xingjian

Tableau 1 Carte d'identité COBIT® 5

Carte d'identité COBIT® 5		
<b>Angle de vue</b>	Direction générale DSI Auditeurs Contrôleurs de gestion	Le référentiel COBIT® 5 décrit comment appliquer, contrôler et suivre l'ensemble des actions de la gouvernance dans les systèmes d'information de l'entreprise. C'est à la fois un référentiel d'amélioration continue et un moyen pour mesurer le niveau de la performance globale atteint dans l'organisation.
<b>Norme</b>	–	
<b>Auteur</b>	ISACA ( <i>Information Systems Audit and Control Association</i> )	
<b>Nationalité</b>	Américaine	

Le référentiel COBIT®5 (*Control Objectives for Information and related Technology* ou Objectifs de contrôle de l'information et des technologies associées) est la référence pour une gouvernance efficace et la gestion des technologies de l'information. C'est le guide pour maîtriser les démarches IT (*Information Technology*) des systèmes d'information des entreprises. Il est développé par l'ISACA<sup>1</sup> (*Information Systems Audit and Control Association*)

.....  
1 Lien : [www.isaca.org](http://www.isaca.org)

et l'ITGI (*IT Governance Institute*). La dernière version COBIT® 5 a été publiée en avril 2012. Elle remplace la version COBIT® 4.1 de 2007.

COBIT® 5 propose un système de mesures du **niveau de maturité** atteint par l'entreprise dans les contrôles des techniques informatiques. On utilise parfois le terme TI (traitement informatique). La Direction de l'entreprise fixe des objectifs aux équipes informatiques puis des contrôles opérationnels comparent les niveaux réalisés par rapport aux niveaux attendus.

COBIT® 5 est un outil de pilotage complet à destination de la DSI. En ce sens, il constitue une aide pour diriger l'organisation et toutes les fonctions de la DSI jusqu'à l'amélioration de la performance. Il permet des audits des systèmes d'information de l'entreprise.

COBIT® 5 est la démarche holistique par excellence pour une approche globale de développement des systèmes d'information. Elle s'applique tout à la fois aux différents domaines concernés dans l'organisation : son fonctionnement, sa culture qui favorise la confiance, la responsabilité, l'autonomie, le goût de l'excellence avec le sens du partage tout en développant les compétences et de nouveaux savoir-faire novateurs.

## Bénéfices de la démarche COBIT® 5

La mise en œuvre d'une gouvernance informatique, que l'on nomme *IT Governance* pour gagner en efficacité, est un des moteurs essentiels pour les organisations et toutes les entreprises qui veulent être assurées que leurs projets informatiques ne gaspillent pas les budgets, et donc économisent. Dans un mode de fonctionnement basé sur la gouvernance COBIT® 5, l'entreprise sera en capacité de réaliser des bénéfices et les économies significatives de productivité et/ou d'apporter des avantages compétitifs par rapport aux investissements.

### Les 6 bénéfices avec COBIT® 5

COBIT® 5 est un moyen pour conduire et amplifier les démarches de changement sur 3 aspects : sur le plan de l'organisation, sur le plan de la culture et sur le plan technique.

COBIT® 5 ne se veut pas normatif mais préconise que les organisations mettent en œuvre des processus de gouvernance et de management. L'ensemble des bonnes pratiques couvrent les domaines clés qui les concerneront : sécurité, risques, technologies, environnement, etc.

De ces démarches, il résulte **6 bénéfices importants** avec COBIT® 5 :

- ▶ la prise en compte des **besoins** et des **exigences** des métiers ;
- ▶ une **organisation** adaptée ;
- ▶ la prise en compte de l'ensemble des **risques** auxquels l'entreprise peut être confrontée ;
- ▶ l'intégration des **mutations technologiques** ;
- ▶ l'adaptation des **moyens** pour créer, accroître et préserver la valeur ajoutée dans l'ensemble de l'entreprise (voir figure 1).

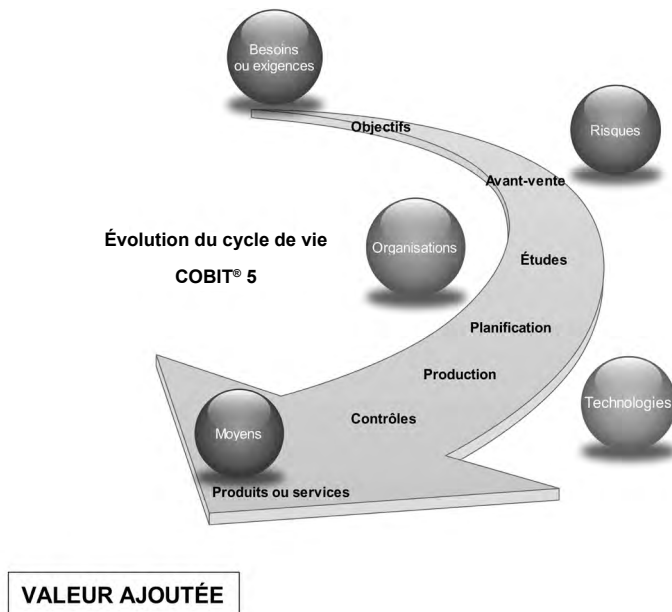


Figure 1 Six bénéfices importants du référentiel COBIT® 5

COBIT® 5 est donc le référentiel pour la gouvernance de l'entreprise et la gestion de l'informatique de l'entreprise. Il est le point de départ commun reconnu par l'ensemble des professionnels impliqués par la gouvernance. Il s'adapte pour trouver un équilibre et évoluer vers une organisation adaptée et efficace. Ce référentiel permet notamment de :

- ▶ préparer les projets et des programmes ;
- ▶ suivre et contrôler des activités ;
- ▶ acquérir une certification externe.

## Piloter les SI avec COBIT® 5

Pour le pilotage des SI, avec les systèmes d'information distribués, les activités de pilotage mettent en œuvre un modèle de maturité sur 5 niveaux (voir figure 2). Cela permet d'évaluer l'état d'avancement de l'entreprise. Ces six niveaux sont, par ordre décroissant :

- ▶ le niveau « leader » (niveau 5) ;
- ▶ le niveau « prédictif » (niveau 4) ;
- ▶ le niveau « efficient » (niveau 3) ;
- ▶ le niveau « géré » (niveau 2) ;
- ▶ le niveau « réactif » (niveau 1).

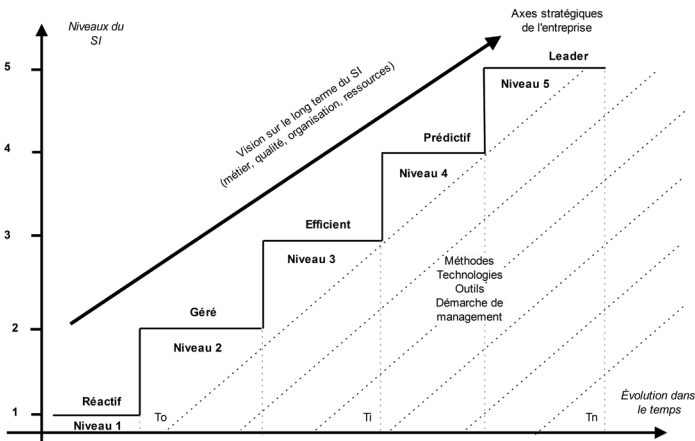


Figure 2 Évaluation du niveau de performance et de valeur ajoutée par le référentiel COBIT® 5

Dans un premier temps, nous allons retracer l'histoire de la gouvernance des TI, en commençant par la technologie de l'information<sup>2</sup> ou plus simplement l'informatique au sens large, son évolution au sein de l'industrie des affaires en coordination avec les nombreuses mutations dans l'IT.

COBIT®5 se positionne pour accompagner et garantir des niveaux de rentabilité dans les organisations.

2 Le terme *Information Technology* (IT) se rapporte soit au potentiel global offert par les technologies de l'information (TI), soit à leurs utilisations dans l'entreprise (systèmes d'information – SI – par exemple). En dehors de tout contexte, IT désigne les techniques informatiques au sens général.



Les entreprises et toutes les organisations privées ou publiques cherchent à améliorer leurs processus de management sur les domaines métiers afin de s'adapter aux évolutions, à la mondialisation, aux changements technologiques, en intégrant plusieurs contraintes (sécurité, clients, métiers...) et avec plusieurs objectifs : produire des services auprès des clients, rationaliser progressivement les *workflows* et garantir que les processus d'entreprise constituent un ensemble homogène géré pour obtenir la valeur ajoutée attendue. On représentera les principaux mots clés de COBIT®5 au moyen d'un nuage (voir figure 3).



Figure 3 Mots-clés avec COBIT®5

## Positionnement du référentiel COBIT®5

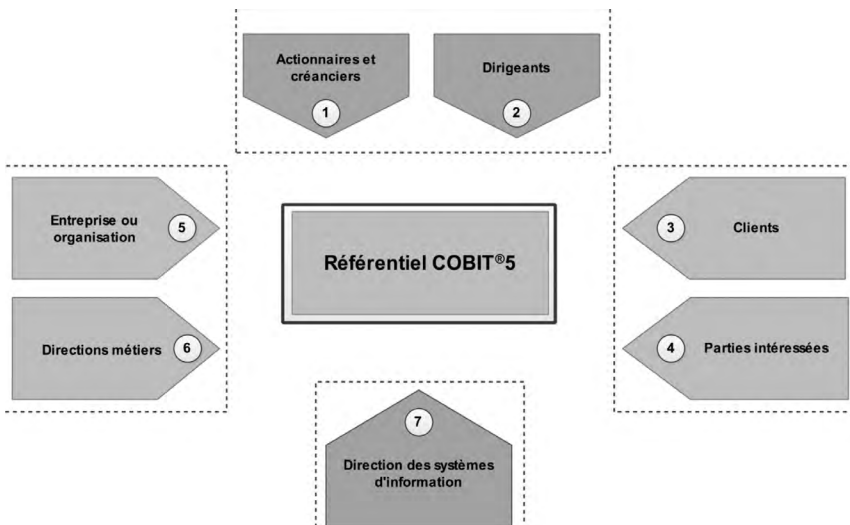


Figure 4 Les 7 éléments inclus dans le périmètre du référentiel COBIT®5

Le contenu de ce livre se focalise sur **7 points forts** majeurs qui impliquent toutes les parties intéressées et concernées par les enjeux de la gouvernance, les dirigeants, les actionnaires et créanciers, l'entreprise et ses équipes de Direction, les collaborateurs, jusqu'à l'ensemble des clients (voir figure 4).

## Portée de COBIT® 5

En effet, le référentiel COBIT® 5 s'applique véritablement à tous les types d'entreprises – qu'elles soient publiques ou privées, dans les domaines de la production, des services, de l'ingénierie, du conseil, et quelle que soit leur taille (groupes internationaux, grandes entreprises, PME ou PMI) –, mais aussi aux associations ou groupements d'intérêts.

## Les liens entre les référentiels

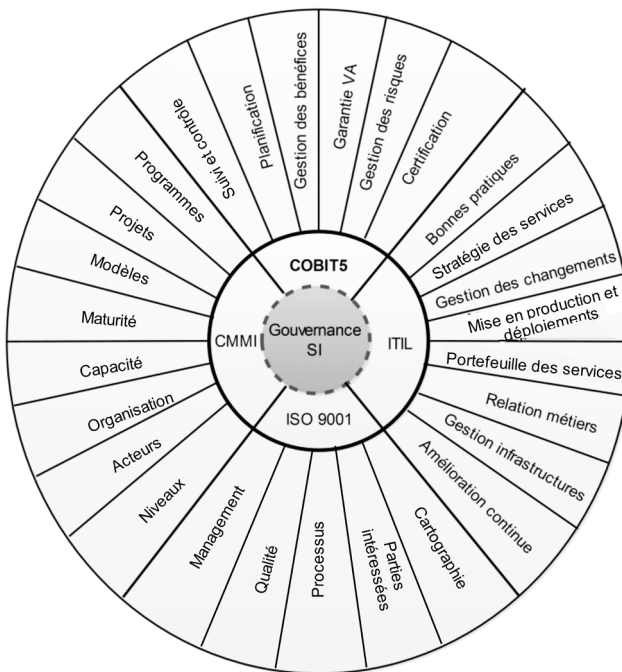


Figure 5 L'approche COBIT® 5 pour la gouvernance

COBIT® 5 s'inscrit dans une démarche globale en complément aux bonnes pratiques (COSO, ITIL, CMMI...) mais aussi aux normes (ISO 9100, ISO 9001, ISO 2700X, ISO 20000, ISO 15504, ISO 31000...) pour couvrir