



PREPARATION EXAMEN COBIT5



COBIT[®]
AN ISACA[®] FRAMEWORK

TABLE DES MATIÈRES

Liste des figures.....	11
COBIT 5 : Un référentiel orienté affaires pour la gouvernance et la gestion des TI de l'entreprise	13
Sommaire de gestion	15
Chapitre 1. Vue d'ensemble de COBIT 5	17
Vue d'ensemble de la publication	18
Chapitre 2. Principe 1 : Répondre aux besoins des parties prenantes.....	19
Introduction	19
Cascade d'objectifs de COBIT 5	19
Étape 1. Les motivations des parties prenantes influencent leurs besoins.....	19
Étape 2. Les besoins des parties prenantes se déclinent en objectifs d'entreprise.....	19
Étape 3. Les objectifs d'entreprise se déclinent en objectifs liés aux TI.....	20
Étape 4. Les objectifs liés aux TI et leur déclinaison en objectifs facilitants	21
Utilisation de la cascade d'objectifs de COBIT 5	22
Avantages de la cascade d'objectifs de COBIT 5	22
Utilisation prudente de la cascade d'objectifs de COBIT 5	22
Utilisation pratique de la cascade d'objectifs de COBIT 5	22
Questions de gouvernance et de gestion des TI.....	24
Comment trouver des réponses à ces questions?	24
Chapitre 3. Principe 2 : Couvrir l'entreprise de bout en bout	25
Approche de gouvernance	25
Facilitateurs de la gouvernance.....	26
Portée de la gouvernance	26
Rôles, activités et relations	26
Chapitre 4. Principe 3 : Appliquer un référentiel unique et intégré	27
Intégrateur du référentiel de COBIT 5	27
Chapitre 5. Principe 4 : Faciliter une approche globale	29
Les facilitateurs de COBIT 5	29
Gouvernance et gestion systémiques au moyen de facilitateurs interreliés	29
Dimensions des facilitateurs de COBIT 5.....	30
Caractéristiques des facilitateurs.....	30
Gestion de la performance des facilitateurs	31
Exemples pratiques de facilitateurs.....	31
Chapitre 6. Principe 5 : Distinguer la gouvernance de la gestion	33
Gouvernance et gestion.....	33
Interactions entre la gouvernance et la gestion.....	33
Modèle de référence du processus COBIT 5.....	34
Chapitre 7. Orientations de mise en œuvre	37
Introduction	37
Tenir compte du contexte de l'entreprise	37
Créer un environnement approprié	38
Reconnaître les points sensibles et les événements déclencheurs	38
Favoriser le changement	39
Une approche fondée sur le cycle de vie	39
Pour commencer : réaliser le dossier d'affaires.....	41
Chapitre 8. Le modèle de capacité des processus de COBIT 5	43
Introduction	43
Différences entre le modèle de maturité de COBIT 4.1 et le modèle de capacité des processus de COBIT 5.....	43

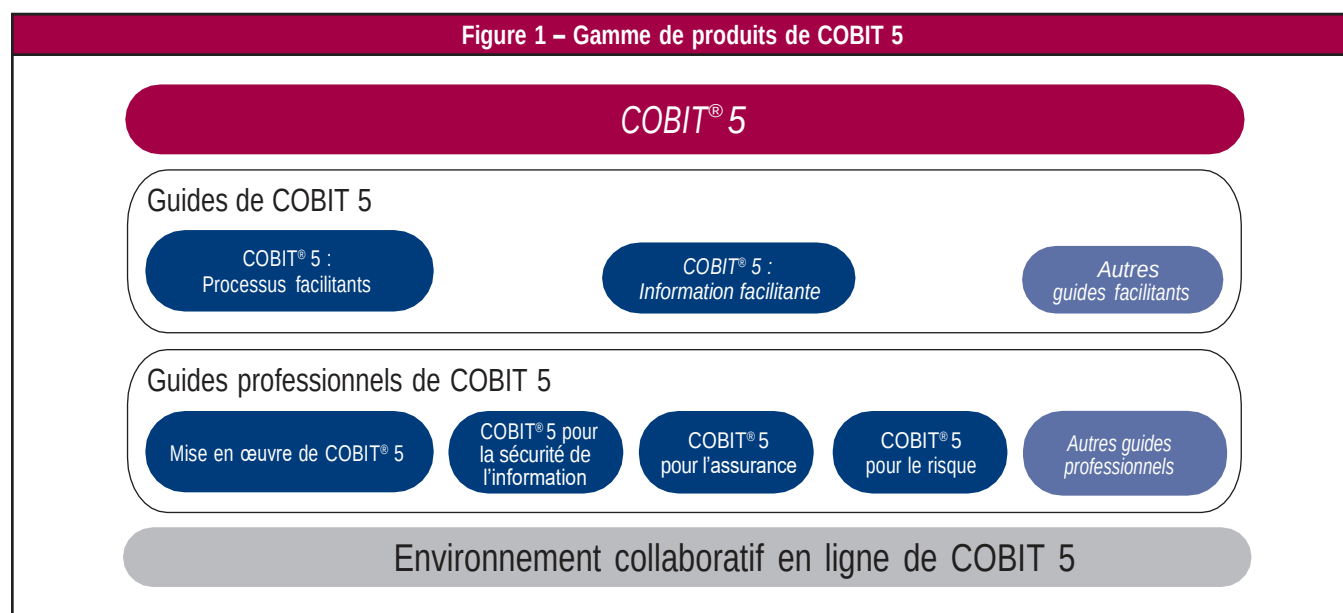
Différences dans la pratique	46
Avantages des changements	48
Exécution des évaluations de la capacité des processus dans COBIT 5	48
Annexe A. Références	51
Annexe B. Correspondance détaillée entre les objectifs d'entreprise et les objectifs liés aux TI	53
Annexe C. Correspondance détaillée entre les objectifs et les processus liés aux TI.....	55
Annexe D. Besoins des parties prenantes et objectifs d'entreprise.....	59
Annexe E. Correspondance entre COBIT 5 et les normes et référentiels connexes les plus pertinents	61
Introduction	61
COBIT 5 et ISO/CEI 38500.....	61
Principes ISO/CEI 38500	61
ISO/CEI 38500 Évaluer, diriger et surveiller.....	64
Comparaison à d'autres normes.....	64
ITIL® V3 2011 et ISO/CEI 20000.....	64
Série de normes ISO/CEI 27000	64
Série de normes ISO/CEI 31000	65
TOGAF®.....	65
Capability Maturity Model Integration (CMMI) (développement).....	65
PRINCE2®.....	65
Annexe F. Comparaison entre le modèle d'information de COBIT 5 et les critères d'information de COBIT 4.1.....	67
Annexe G. Description détaillée des facilitateurs de COBIT 5.....	69
Introduction	69
Caractéristiques des facilitateurs.....	69
Gestion de la performance des facilitateurs	70
Facilitateur de COBIT 5 : principes, politiques et cadres.....	70
Facilitateur de COBIT 5 : processus	73
Gestion de la performance des facilitateurs	75
Exemple pratique de processus facilitant.....	75
Modèle de référence du processus COBIT 5.....	75
Facilitateur de COBIT 5 : structures organisationnelles	79
Facilitateur de COBIT 5 : culture, éthique et comportement	82
Facilitateur de COBIT 5 : information.....	84
Introduction – Le cycle de l'information	84
Facilitateur de l'information de COBIT 5.....	84
Facilitateur de COBIT 5 : services, infrastructures et applications	88
Facilitateur de COBIT 5 : personnes, aptitudes et compétences	90
Annexe H. Glossaire	93

LISTE DES FIGURES

Figure 1 – Gamme de produits de COBIT 5	13
Figure 2 – Principes de COBIT 5	15
Figure 3 – Objectif de la gouvernance : création de valeur	19
Figure 4 – Vue d'ensemble de la cascade d'objectifs de COBIT 5	20
Figure 5 – Objectifs d'entreprise de COBIT 5	21
Figure 6 – Objectifs liés aux TI	21
Figure 7 – Questions de gouvernance et de gestion à propos des TI	24
Figure 8 – Gouvernance et gestion dans COBIT 5	25
Figure 9 – Rôles, activités et relations clés	26
Figure 10 – Référentiel unique et intégré de COBIT 5	27
Figure 11 – Gamme de produits de COBIT 5	28
Figure 12 – Facilitateurs d'entreprise de COBIT 5	29
Figure 13 – Facilitateurs de COBIT 5 : générique	30
Figure 14 – Interactions entre la gouvernance et la gestion selon COBIT 5	33
Figure 15 – Zones clés de gouvernance et de gestion de COBIT 5	34
Figure 16 – Modèle de référence du processus COBIT 5	35
Figure 17 – Les sept étapes du cycle de vie de la mise en œuvre	40
Figure 18 – Résumé du modèle de maturité de COBIT 4.1	44
Figure 19 – Résumé du modèle de capacité des processus de COBIT 5	45
Figure 20 – Tableau de comparaison entre les niveaux de maturité (COBIT 4.1) et les niveaux de capacité des processus (COBIT 5)	47
Figure 21 – Tableau de comparaison des attributs de maturité (COBIT 4.1) et des attributs de processus (COBIT 5)	47
Figure 22 – Correspondance entre les objectifs d'entreprise de COBIT 5 et les objectifs liés aux TI	54
Figure 23 – Correspondance entre les objectifs liés aux TI de COBIT 5 et les processus	56
Figure 24 – Correspondance entre les objectifs d'entreprise de COBIT 5 et les questions de gouvernance et de gestion	59
Figure 25 – Couverture des autres normes et référentiels par COBIT 5	66
Figure 26 – Équivalents des critères d'information de COBIT 4.1 dans COBIT 5	67
Figure 27 – Facilitateurs de COBIT 5 : générique	69
Figure 28 – Facilitateur de COBIT 5 : principes, politiques et cadres	71
Figure 29 – Facilitateur de COBIT 5 : processus	73
Figure 30 – Zones clés de gouvernance et de gestion de COBIT 5	77
Figure 31 – Modèle de référence du processus COBIT 5	78
Figure 32 – Facilitateur de COBIT 5 : structures organisationnelles	79
Figure 33 – Rôles et structures organisationnelles de COBIT 5	80
Figure 34 – Facilitateur de COBIT 5 : culture, éthique et comportement	82
Figure 35 – Métadonnées de COBIT 5 – Cycle de l'information	84
Figure 36 – Facilitateur de COBIT 5 : information	84
Figure 37 – Facilitateur de COBIT 5 : services, infrastructures et applications	89
Figure 38 – Facilitateur de COBIT 5 : personnes, aptitudes et compétences	90
Figure 39 – Catégories de compétences de COBIT 5	91

COBIT 5 : UN RÉFÉRENTIEL ORIENTÉ AFFAIRES POUR LA GOUVERNANCE ET LA GESTION DES TI DE L'ENTREPRISE

Figure 1 – Gamme de produits de COBIT 5



Le cadre de COBIT 5 repose sur cinq principes de base, décrits en détail, et comprend des orientations détaillées sur les facilitateurs pour la gouvernance et la gestion des TI de l'entreprise.

La gamme de produits de COBIT 5 est composée des produits suivants :

- COBIT 5 (le référentiel)
- Les guides de COBIT 5, qui traitent en détail des facilitateurs de la gouvernance et de la gestion. Ils comprennent :
 - *COBIT 5 : Processus facilitateurs*
 - *COBIT 5 : Information facilitante*
 - Autres guides (consultez le www.isaca.org/cobit)
- Les guides professionnels de COBIT 5, qui comprennent :
 - *COBIT 5 Mise en œuvre*
 - *COBIT 5 pour la sécurité de l'information*
 - *COBIT 5 pour l'assurance*
 - *COBIT 5 pour le risque*
 - Autres guides professionnels (consultez le www.isaca.org/cobit)
- Un environnement de collaboration en ligne disponible pour soutenir l'utilisation de COBIT 5

SOMMAIRE DE GESTION

L'information est une ressource clé pour toutes les entreprises, et de sa création jusqu'à sa destruction, la technologie joue un rôle important. Les technologies de l'information sont de plus en plus perfectionnées et sont devenues omniprésentes dans les entreprises comme dans les milieux privés, publics et d'affaires.

Par conséquent, aujourd'hui plus que jamais, les entreprises et leurs dirigeants s'efforcent de :

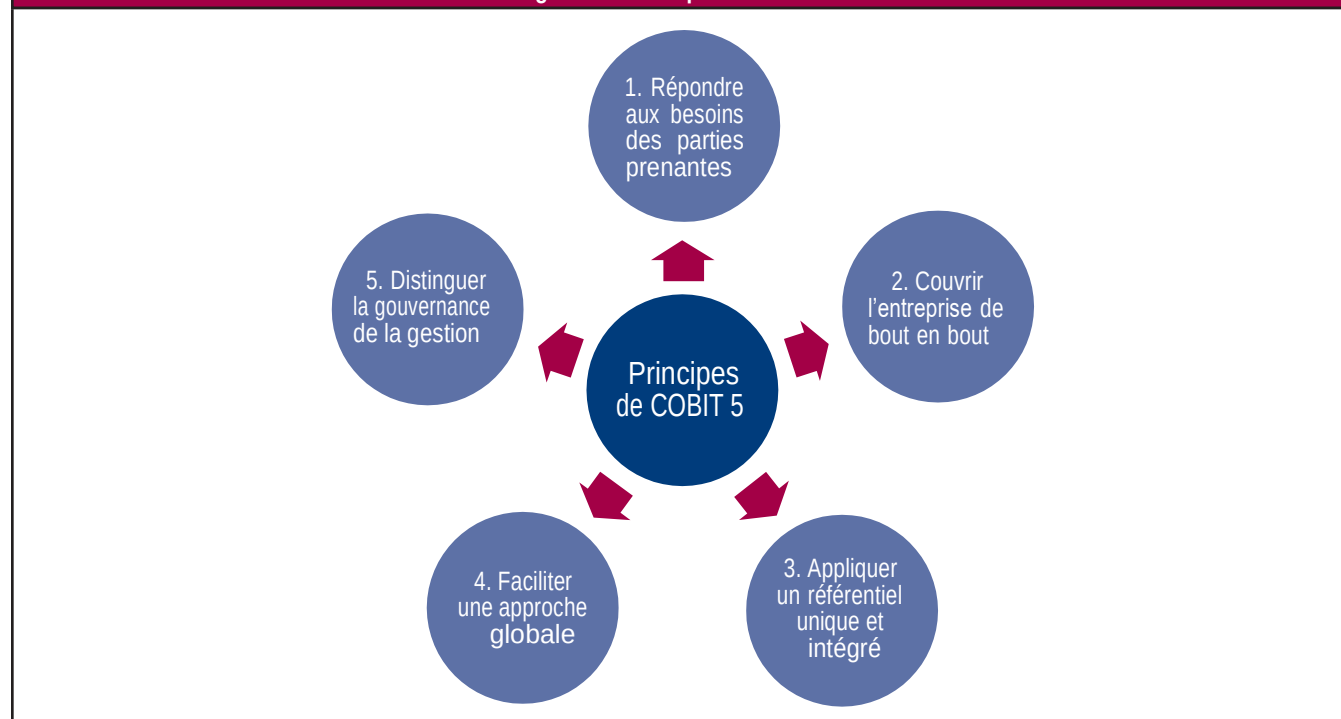
- Maintenir une information de grande qualité pour appuyer les décisions d'affaires.
- Générer une valeur pour les investissements en TI, c'est-à-dire contribuer à l'atteinte des objectifs stratégiques et tirer des bénéfices de l'utilisation efficace et innovante des TI.
- Atteindre l'excellence opérationnelle grâce à l'application fiable et efficace de la technologie.
- Maintenir les risques liés aux TI à un niveau acceptable.
- Optimiser le coût des services et des technologies liés aux TI.
- Se conformer aux lois applicables, dont le nombre ne cesse de croître, aux règlements, aux accords contractuels et aux politiques.

Au cours de la dernière décennie, le terme « gouvernance » est passé à l'avant-plan de la réflexion des entreprises. Des entreprises de par le monde ont su tirer profit de la mise en place d'une bonne gouvernance alors que d'autres, dépourvues d'une telle gouvernance, ont subi des revers marquants.

Les entreprises qui réussissent reconnaissent que le conseil d'administration et les dirigeants doivent se préoccuper de la gestion des systèmes d'information au même titre que des autres activités de l'entreprise. Les conseils d'administration et les dirigeants, tant ceux des lignes d'affaires que ceux des TI, doivent collaborer pour intégrer les TI dans les approches de gouvernance et de gestion. De plus, un nombre croissant de lois sont adoptées et des règlements sont établis pour répondre à ce besoin.

COBIT 5 fournit un référentiel complet qui aide les entreprises à atteindre leurs objectifs en matière de gouvernance et de gestion des TI. En bref, il aide les entreprises à tirer le maximum des TI en maintenant l'équilibre entre la réalisation de bénéfices, l'optimisation des niveaux de risque et l'utilisation des ressources. COBIT 5 offre une approche holistique de la gouvernance et de la gestion des TI appliquée à l'ensemble de l'entreprise. Il tient compte de toutes les activités de l'entreprise et des domaines fonctionnels des TI et prend également en considération les intérêts des parties prenantes tant internes qu'externes en matière de TI. COBIT 5 est générique et utile pour les entreprises de toutes tailles, qu'il s'agisse d'organisations commerciales, d'organismes sans but lucratif ou du secteur public.

Figure 2 – Principes de COBIT 5



COBIT 5 se fonde sur cinq principes clés (présentés à la **figure 2**) pour la gouvernance et la gestion des TI de l'entreprise :

- **Principe 1 : Répondre aux besoins des parties prenantes** – Le rôle des entreprises est de générer de la valeur pour leurs parties prenantes en maintenant un équilibre entre la réalisation de bénéfices d'une part et la gestion optimale des risques et de l'utilisation des ressources d'autre part. COBIT 5 fournit tous les processus et autres facilitateurs requis pour appuyer la création de valeur grâce à l'utilisation des TI. Puisque les buts visés varient en fonction de l'entreprise, une organisation peut adapter COBIT 5 à son contexte grâce à la cascade d'objectifs, qui permet de convertir des objectifs d'entreprise généraux en objectifs TI clairs, gérables et liés à des pratiques et processus précis.
- **Principe 2 : Couvrir l'entreprise de bout en bout** – COBIT 5 intègre la gouvernance des TI à la gouvernance d'entreprise :
 - Il couvre tous les processus et les fonctions au sein de l'entreprise; COBIT 5 n'est pas centré uniquement sur la « fonction TI », mais traite aussi l'information et les technologies connexes en tant qu'actifs devant être gérés comme tout autre actif dans l'entreprise.
 - Il considère que tous les facilitateurs pour la gouvernance et la gestion des TI touchent l'entreprise de bout en bout, c'est-à-dire qu'ils incluent tous les éléments et les individus, à l'interne et à l'externe, pertinents pour la gouvernance et la gestion de l'information d'entreprise et de ses TI.
- **Principe 3 : Appliquer un référentiel unique et intégré** – Il existe de nombreuses normes et bonnes pratiques en matière de TI, chacune proposant des orientations pour un sous-ensemble d'activités. COBIT 5 s'harmonise aux autres normes et référentiels de haut niveau et peut donc servir de référentiel général pour la gouvernance et la gestion des TI de l'entreprise.
- **Principe 4 : Faciliter une approche globale** – Une gouvernance et une gestion efficaces et efficientes des TI de l'entreprise exigent une approche globale qui tient compte de plusieurs éléments interagissant entre eux. COBIT 5 définit un ensemble de facilitateurs pour appuyer la mise en œuvre d'un système complet de gouvernance et de gestion pour les TI de l'entreprise. Au sens large, on entend par facilitateur tout ce qui peut aider à atteindre les objectifs de l'entreprise. Le référentiel de COBIT 5 définit sept catégories de facilitateurs :
 - Principes, politiques et référentiels
 - Processus
 - Structures organisationnelles
 - Culture, éthique et comportement
 - Information
 - Services, infrastructures et applications
 - Personnel, aptitudes et compétences
- **Principe 5 : Distinguer la gouvernance de la gestion** – Le référentiel de COBIT 5 établit une distinction claire entre la gouvernance et la gestion. Ces deux fonctions englobent différents types d'activités, exigent différentes structures organisationnelles et répondent à des besoins différents. Le point de vue de COBIT 5 quant à cette distinction clé entre la gouvernance et la gestion est le suivant :
 - Gouvernance

La gouvernance consiste à évaluer les besoins, les règles et les options des parties prenantes dans le but de déterminer des objectifs d'entreprise équilibrés qui font consensus. Elle permet de déterminer l'orientation par les priorités et la prise de décisions. Enfin, elle permet de contrôler la performance et la conformité au regard des orientations et des objectifs convenus.

Dans la plupart des entreprises, la gouvernance générale relève du conseil d'administration, sous la direction de son président. Il est possible de déléguer des responsabilités de gouvernance précises à des structures organisationnelles spéciales à l'échelon approprié, particulièrement dans le cas de grandes entreprises complexes.

– Gestion

L'équipe de gestion planifie, bâtit, exécute et surveille les activités conformément à l'orientation fixée par le groupe de gouvernance afin d'atteindre les objectifs d'entreprise.

Dans la plupart des entreprises, la gestion relève de la haute direction, sous l'autorité du président-directeur général (PDG).

Ensemble, ces cinq principes permettent à l'entreprise de constituer un référentiel de gouvernance et de gestion efficace qui optimise les investissements en technologie et en gestion de l'information, de même que leur utilisation à l'avantage des parties prenantes.

CHAPITRE 1

VUE D'ENSEMBLE DE COBIT 5

COBIT 5 établit la nouvelle génération d'orientations de l'ISACA sur la gouvernance et la gestion des TI de l'entreprise. Elles s'appuient sur plus de 15 années d'expérience pratique et d'application de COBIT par de nombreuses entreprises et de nombreux utilisateurs du monde des affaires, des TI, du risque, de la sécurité et de l'assurance. Les objectifs majeurs du développement de COBIT 5 comprennent la nécessité de :

- Permettre aux parties prenantes d'exprimer davantage leurs attentes concernant l'information, les technologies associées (quels sont les avantages, à quel niveau de risque acceptable et à quel prix) et leurs priorités tout en s'assurant que la valeur attendue soit effectivement livrée. Certains voudront des rendements à court terme, tandis que d'autres viseront la durabilité. Certains seront prêts à prendre un risque élevé, d'autres non. Ces attentes divergentes et parfois contradictoires doivent être traitées efficacement. De plus, ces intervenants veulent non seulement participer davantage, mais souhaitent aussi obtenir plus de transparence dans le processus décisionnel et dans la communication des résultats obtenus.
- Traiter la dépendance croissante de la réussite de l'entreprise envers des entreprises extérieures et des fournisseurs de TI comme des sous-traitants, des fournisseurs, des consultants, des clients, l'infonuagique et d'autres fournisseurs de services, ainsi qu'envers un ensemble diversifié de moyens et de mécanismes internes pour créer la valeur attendue.
- Traiter la quantité d'information, qui a augmenté de manière significative. Comment les entreprises sélectionnent-elles l'information pertinente et crédible qui mènera à des décisions d'affaires judicieuses? L'information doit également être gérée efficacement; un modèle d'information efficace peut aider.
- Composer avec l'omniprésence des TI; elles font de plus en plus partie intégrante des lignes d'affaires. Comme elles sont désormais alignées sur les affaires, les TI doivent désormais faire partie intégrante des projets d'affaires, des structures organisationnelles, de la gestion des risques, des politiques, des compétences, des processus, etc. Les rôles du dirigeant principal de l'information (DPI) et de la fonction des TI sont en pleine évolution. De plus en plus de gens dans les fonctions d'affaires possèdent des compétences en TI et participent, ou participeront, aux décisions relatives aux TI et aux activités des TI. Les TI et les affaires devront être mieux intégrées.
- Fournir des orientations dans le domaine de l'innovation et des nouvelles technologies; il s'agit de créer, d'inventer, de concevoir de nouveaux produits, de rendre les produits existants plus attrayants aux yeux des clients et d'atteindre de nouveaux types de clients. L'innovation inclut également la rationalisation de la conception de produits, de la fabrication et des processus de la chaîne d'approvisionnement afin d'offrir plus efficacement et plus rapidement sur le marché des produits de meilleure qualité.
- Couvrir l'ensemble de l'entreprise et les responsabilités fonctionnelles des TI, de même que tous les aspects qui conduisent à une gouvernance et à une gestion efficaces des TI de l'entreprise, telles que les structures organisationnelles, les politiques et la culture, au-delà des processus.
- Obtenir un meilleur contrôle de l'accroissement des TI initiées et contrôlées par l'utilisateur.
- Assurer à l'entreprise :
 - La création de valeur grâce à l'utilisation efficace et innovante des TI de l'entreprise;
 - La satisfaction de la clientèle utilisatrice envers les engagements et les services des TI;
 - Le respect des lois applicables, des règlements, des accords contractuels et des politiques internes;
 - Une meilleure correspondance entre les besoins d'affaires et les objectifs des TI.
- Faire le lien et, le cas échéant, s'aligner avec d'autres référentiels et normes majeures du marché, comme l'Information Technology Infrastructure Library (ITIL®), The Open Group Architecture Forum (TOGAF®), Project Management Body of Knowledge (PMBOK®), PROjects IN Controlled Environments 2 (PRINCE2®), Committee of Sponsoring Organizations of the Treadway Commission (COSO) et l'Organisation internationale de normalisation (ISO). Cela aidera les parties prenantes à comprendre comment les différents référentiels, les bonnes pratiques et les normes se positionnent les uns par rapport aux autres et comment ils peuvent être utilisés ensemble.
- Intégrer les principaux référentiels et les orientations de l'ISACA en mettant l'accent sur COBIT, Val IT et Risk IT, mais en tenant également compte du Business Model for Information Security (BMIS), de l'IT Assurance Framework (ITAF), de la publication intitulée *Board Briefing on IT Governance* et de la ressource Taking Governance Forward (TGF). Ainsi, COBIT 5 couvre l'entreprise dans son ensemble et fournit une base pour intégrer d'autres référentiels, normes et pratiques dans un référentiel unique.

D'autres produits et orientations couvrant les divers besoins des parties prenantes seront élaborés à partir de la base de connaissances principale de COBIT 5 au fil du temps, faisant ainsi de l'architecture du produit un document vivant. Sa plus récente architecture se trouve sur les pages COBIT du site Web de l'ISACA (www.isaca.org/cobit).

Vue d'ensemble de la publication

Le référentiel de COBIT 5 contient sept autres chapitres :

- Le chapitre 2 traite du principe 1, **Répondre aux besoins des parties prenantes**. Il introduit la cascade d'objectifs de COBIT 5. Les objectifs d'entreprise en matière de TI, utilisés pour formaliser et structurer les besoins des parties prenantes, peuvent être liés à des objectifs TI, lesquels sont atteints grâce à l'utilisation optimale et à la mise en œuvre de tous les facilitateurs, incluant les processus. Cet ensemble d'objectifs connexes est appelé « cascade d'objectifs de COBIT 5 ». Le chapitre fournit également des exemples de questions typiques de gouvernance et de gestion se rapportant aux TI fréquemment soulevées par les parties prenantes des entreprises.
- Le chapitre 3 présente le principe 2, **Couvrir l'entreprise de bout en bout**. Il explique comment COBIT 5 intègre la gouvernance des TI de l'entreprise à la gouvernance de l'entreprise en couvrant l'ensemble de ses fonctions et processus.
- Le chapitre 4 traite du principe 3, **Appliquer un référentiel unique et intégré**, et décrit brièvement l'architecture de COBIT 5 qui permet cette intégration.
- Le chapitre 5 porte sur le principe 4, **Faciliter une approche globale**. En se fondant sur le principe voulant que la gouvernance des TI de l'entreprise soit systémique et soutenue par un ensemble de facilitateurs, ce chapitre présente les facilitateurs ainsi qu'une façon commune de les aborder : le modèle générique de facilitateur.
- Le chapitre 6, qui présente le principe 5, **Distinguer la gouvernance de la gestion**, élabore sur la différence entre la gestion et la gouvernance ainsi que sur la façon dont elles interagissent. Le modèle de référence des processus de COBIT 5 de haut niveau est inclus à titre d'exemple.
- Le chapitre 7 contient une introduction aux **orientations de mise en œuvre**. Il décrit comment il est possible de créer l'environnement approprié, quels sont les facilitateurs nécessaires, les points sensibles et les événements déclencheurs typiques pour la mise en œuvre, ainsi que le cycle de vie de mise en œuvre et d'amélioration continue. Ce chapitre est basé sur la publication intitulée *COBIT® 5 Implementation*, qui renferme tous les détails sur la façon de mettre en œuvre la gouvernance des TI de l'entreprise en s'appuyant sur COBIT 5.
- Le chapitre 8 présente **le modèle de capacité des processus de COBIT 5** dans le schéma d'approche du programme d'évaluation de COBIT (www.isaca.org/cobit-assessment-programme). Ce chapitre explique également comment COBIT 5 diffère des évaluations de la maturité des processus de COBIT 4.1 et comment les utilisateurs peuvent migrer vers la nouvelle approche.

Les annexes contiennent de l'information de référence, des tables de correspondances et de l'information plus détaillée sur des sujets particuliers :

- Annexe A. Les **références** utilisées lors de l'élaboration de COBIT 5 sont répertoriées.
- Annexe B. **Correspondance détaillées entre les objectifs d'entreprise et les objectifs liés aux TI**. Cette annexe décrit comment les objectifs d'entreprise sont habituellement pris en charge par un ou plusieurs objectifs liés aux TI.
- Annexe C. **Correspondance détaillée entre les objectifs liés aux TI et les processus liés aux TI**. Cette annexe décrit comment les processus de COBIT soutiennent la réalisation des objectifs liés aux TI.
- Annexe D. **Besoins des parties prenantes et objectifs d'entreprise**. Cette annexe décrit comment les besoins typiques des parties prenantes sont liés aux objectifs d'entreprise de COBIT 5.
- Annexe E. **Correspondance entre COBIT 5 et les normes et référentiels connexes les plus pertinents**.
- Annexe F. **Comparaison entre le modèle d'information de COBIT 5 et les critères d'information de COBIT 4.1**.
- Annexe G. **Description détaillée des facilitateurs de COBIT 5**. Cette annexe s'appuie sur le chapitre 5 et détaille les différents facilitateurs, y compris un modèle détaillé décrivant les composants particuliers. Elle est illustrée de plusieurs exemples.
- Annexe H. **Glossaire**.

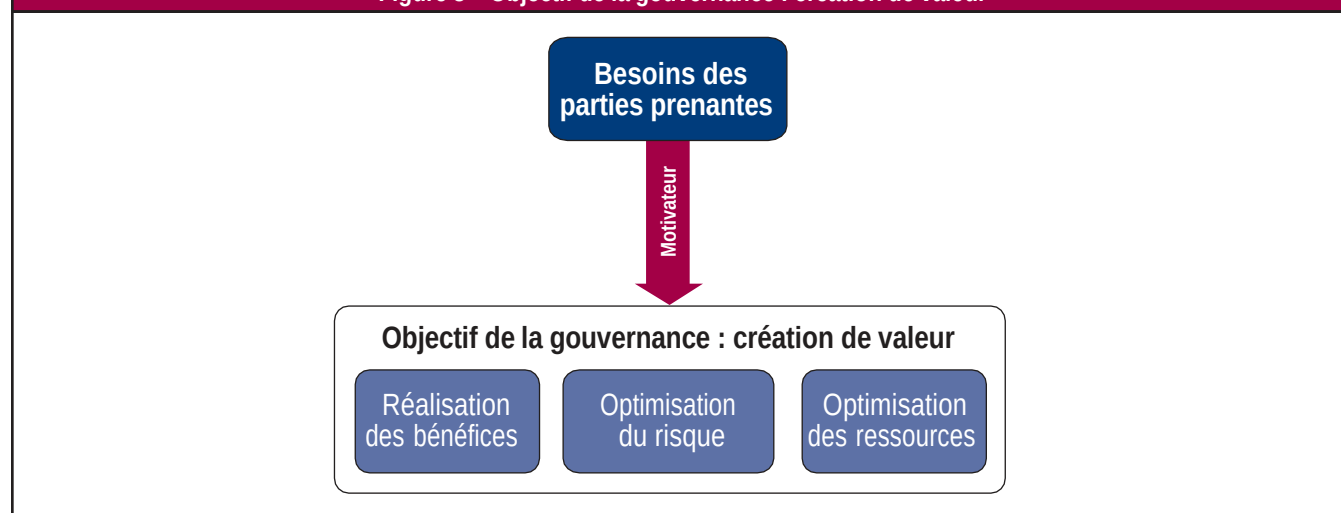
CHAPITRE 2

PRINCIPE 1 : RÉPONDRE AUX BESOINS DES PARTIES PRENANTES

Introduction

Le rôle des entreprises est de créer de la valeur pour leurs parties prenantes. Par conséquent, toute entreprise, commerciale ou non, aura la création de valeur comme objectif de gouvernance. Créer de la valeur signifie réaliser des bénéfices à un coût optimal des ressources, tout en optimisant les risques (voir la **figure 3**). Les bénéfices peuvent prendre plusieurs formes : pour les entreprises commerciales, il pourront être financiers, tandis que pour les entités gouvernementales, il pourra s'agir d'un meilleur niveau de services publics.

Figure 3 – Objectif de la gouvernance : création de valeur



Les entreprises ont de nombreuses parties prenantes et ces dernières ont leurs propres définitions, parfois contradictoires, de la « création de valeur ». La gouvernance consiste à négocier et à prendre des décisions relatives aux intérêts des différentes parties prenantes, sur la base de la création de valeur. Par conséquent, le système de gouvernance doit prendre en compte toutes les parties prenantes dans les décisions d'évaluation des bénéfices, des risques et des ressources. Pour chaque décision, les questions qui suivent peuvent et doivent être posées : À qui profiteront les bénéfices ? Sur qui pèse le risque ? Quelles sont les ressources nécessaires ?

Cascade d'objectifs de COBIT 5

Chaque entreprise opère dans son propre contexte déterminé par des facteurs externes (le marché, l'industrie, la géopolitique, etc.) et des facteurs internes (la culture, l'organisation, la tolérance au risque, etc.). Ce contexte nécessite un système de gouvernance et de gestion personnalisé.

Les besoins des parties prenantes doivent être traduits en actions stratégiques pouvant être mises en place dans l'entreprise. La cascade d'objectifs de COBIT 5 représente le mécanisme de traduction des besoins des parties prenantes en objectifs d'entreprise précis, réalisables et personnalisés, en objectifs liés aux TI et en objectifs facilitateurs. Cette traduction permet de fixer des objectifs précis à tous les niveaux et dans tous les domaines de l'entreprise, en appui aux objectifs généraux et aux exigences des parties prenantes, afin de soutenir efficacement l'alignement entre les besoins d'entreprise et les solutions et services des TI.

La cascade d'objectifs de COBIT 5 est illustrée à la **figure 4**.

Étape 1. Les motivations des parties prenantes influencent leurs besoins

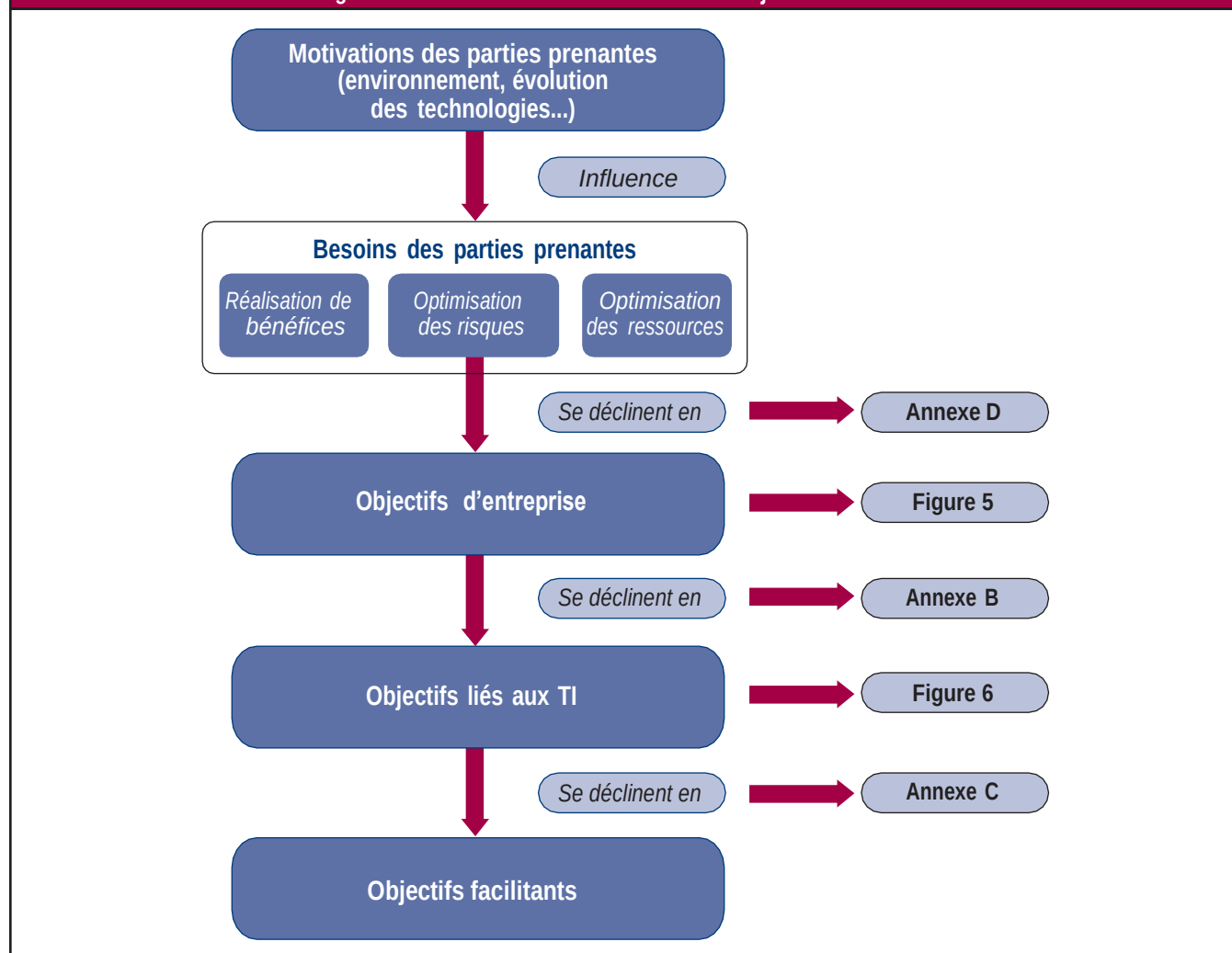
Les besoins des parties prenantes sont influencés par un certain nombre de facteurs, comme des changements de stratégie, un changement dans les affaires, l'évolution de la réglementation ou encore de nouvelles technologies.

Étape 2. Les besoins des parties prenantes se déclinent en objectifs d'entreprise

Les besoins des parties prenantes s'expriment sous forme d'objectifs d'entreprise génériques. Ces objectifs d'entreprise ont été établis en utilisant les dimensions du tableau de bord prospectif (TBP, ou BSC pour Balanced Scorecard en

anglais)¹, et ils représentent une liste d'objectifs couramment utilisés qu'une entreprise peut définir pour elle-même. Bien que cette liste ne soit pas exhaustive, la plupart des objectifs propres à l'entreprise peuvent être facilement mis en correspondance avec un ou plusieurs objectifs d'entreprise génériques. L'annexe D présente un tableau des besoins des parties prenantes et des objectifs d'entreprise.

Figure 4 – Vue d'ensemble de la cascade d'objectifs de COBIT 5



COBIT 5 définit 17 objectifs génériques, comme indiqué à la **figure 5**, qui comprennent les renseignements suivants :

- La dimension du TBP sous laquelle l'objectif de l'entreprise s'inscrit
- Les objectifs d'entreprise
- La relation avec les trois principaux objectifs de la gouvernance : la réalisation de bénéfices, l'optimisation des risques et l'optimisation des ressources (« P » représente les relations primaires et « S » les relations secondaires, c'est-à-dire les relations moins fortes)

Étape 3. Les objectifs d'entreprise se déclinent en objectifs liés aux TI

La réalisation des objectifs d'entreprise nécessite l'atteinte d'un certain nombre de résultats liés aux TI², ces derniers se rapportant aux objectifs liés aux TI. « Lié aux TI » signifie l'information et les technologies connexes. Les objectifs liés aux TI sont structurés selon les dimensions du tableau de bord prospectif des TI (TBP TI). COBIT 5 définit 17 objectifs liés aux TI, énumérés à la **figure 6**.

La table de correspondance entre les objectifs liés aux TI et les objectifs d'entreprise est fournie à l'annexe B. Elle montre comment chaque objectif d'entreprise est soutenu par un certain nombre d'objectifs liés aux TI.

Étape 4. Les objectifs liés aux TI et leur déclinaison en objectifs facilitants

L'atteinte des objectifs liés aux TI exige la mise en œuvre et l'utilisation réussies d'un certain nombre de facilitateurs, incluant les processus, les structures organisationnelles et l'information. Le chapitre 5 explique en détail le concept de facilitateur et indique, pour chacun d'eux, comment définir un ensemble d'objectifs précis pertinents pour les soutenir.

Les processus constituent l'un des facilitateurs. L'annexe C contient une table de correspondance entre les objectifs liés aux TI et les processus de COBIT 5 pertinents, lesquels contiennent des objectifs de processus connexes.

Figure 5 – Objectifs d'entreprise de COBIT 5

Dimension du TBP	Objectif d'entreprise	Relation avec les objectifs de gouvernance		
		Réalisation des bénéfices	Optimisation des risques	Optimisation des ressources
Financier	1. Valeur pour les parties prenantes	P		S
	2. Portefeuille de produits et services concurrentiels	P	P	S
	3. Gestion du risque d'affaires (protection des actifs)		P	S
	4. Conformité aux lois et à la réglementation		P	
	5. Transparence financière	P	S	S
Client	6. Culture de service orientée client	P		S
	7. Continuité et disponibilité des services d'affaires		P	
	8. Réponses agiles dans un contexte d'affaires en évolution	P		S
	9. Prise de décisions stratégiques basées sur l'information	P	P	P
	10. Optimisation des coûts de livraison des services	P		P
Interne	11. Optimisation de la fonctionnalité des processus d'affaires	P		P
	12. Optimisation des coûts des processus d'affaires	P		P
	13. Programmes de gestion du changement	P	P	S
	14. Productivité opérationnelle et productivité du personnel	P		P
	15. Conformité aux politiques internes		P	
Apprentissage et croissance	16. Personnes qualifiées et motivées	S	P	P
	17. Culture d'innovation des produits et des affaires	P		

Figure 6 – Objectifs liés aux TI

Dimension du TBP des TI	Objectif lié à l'information et aux technologies connexes	
Financier	01	Alignement des TI et de la stratégie d'affaires
	02	Conformité des TI et soutien à la conformité de l'entreprise aux lois et à la réglementation
	03	Engagement de la haute direction dans la prise de décisions liées aux TI
	04	Gestion du risque d'affaires lié aux TI
	05	Bénéfices réalisés sur les investissements en TI et sur le portefeuille de services
	06	Transparence des coûts, des bénéfices et des risques des TI
Client	07	Livraison de services des TI conformes aux exigences opérationnelles
	08	Utilisation adéquate des applications, de l'information et de solutions technologiques
Interne	09	Agilité des TI
	10	Sécurité de l'information, des infrastructures de traitement et des applications
	11	Optimisation des actifs, des ressources et des capacités des TI
	12	Mise en œuvre et soutien des processus d'affaires par leur intégration dans les applications et les technologies
	13	Livraison de programmes procurant des avantages, en temps opportun, en respectant le budget, les exigences et les normes de qualité
	14	Disponibilité d'informations fiables et utiles pour la prise de décision
	15	Conformité des TI aux politiques internes
Apprentissage et croissance	16	Personnel des TI et des lignes d'affaires compétent et motivé
	17	Connaissances, compétences et initiatives pour l'innovation d'affaires

Utilisation de la cascade d'objectifs de COBIT 5

Avantages de la cascade d'objectifs de COBIT 5

La cascade d'objectifs³ est importante, car elle permet de définir des priorités pour la mise en œuvre, l'amélioration et l'assurance de la gouvernance des TI de l'entreprise et est basée sur des objectifs (stratégiques) de l'entreprise ainsi que sur des risques connexes. Dans la pratique, la cascade d'objectifs :

- Définit des objectifs pertinents et concrets pour divers niveaux de responsabilité.
- Filtre la base de connaissances de COBIT 5 en se basant sur les objectifs d'entreprise, afin d'extraire des orientations pertinentes à inclure dans des projets spécifiques de mise en œuvre, d'amélioration ou d'assurance.
- Définit et communique clairement l'importance des facilitateurs (parfois très opérationnels) dans l'atteinte des objectifs d'entreprise.

Utilisation prudente de la cascade d'objectifs de COBIT 5

La cascade d'objectifs – avec les tableaux de correspondance entre les objectifs d'entreprise et les objectifs liés aux TI et entre les objectifs liés aux TI et les facilitateurs de COBIT 5 (y compris les processus) – ne contient pas la vérité absolue. Les utilisateurs ne doivent pas tenter de l'utiliser de façon purement mécanique, mais doivent plutôt s'en servir comme ligne directrice, et ce, pour plusieurs raisons, notamment :

- Chaque entreprise a des priorités différentes concernant ses objectifs et celles-ci peuvent changer au fil du temps.
- Les tableaux de correspondance ne font pas de distinction selon la taille de l'entreprise et son secteur d'activité. Ils représentent une sorte de dénominateur commun de la façon dont, en général, les différents niveaux d'objectifs sont interreliés.
- Les indicateurs utilisés dans la table de correspondance comportent deux niveaux d'importance ou de pertinence, ce qui suggère qu'il existe des niveaux « distincts » de pertinence, alors qu'en réalité, la correspondance s'apparente à un continuum de divers degrés de correspondance.

Utilisation pratique de la cascade d'objectifs de COBIT 5

Compte tenu de l'avertissement précédent, il est évident que la première étape à réaliser par l'entreprise lors de l'utilisation de la cascade d'objectifs consiste à personnaliser la table de correspondances en tenant compte de sa situation particulière. En d'autres termes, chaque entreprise doit élaborer sa propre cascade d'objectifs, la comparer avec COBIT, puis la préciser.

Par exemple, l'entreprise pourrait souhaiter :

- Traduire les priorités stratégiques en attribuant un « poids » précis ou une importance précise à chacun des objectifs d'entreprise.
- Valider les correspondances de la cascade d'objectifs en tenant compte de son milieu particulier, de son secteur d'activité, etc.

EXEMPLE 1 – CASCADE D'OBJECTIFS

Une entreprise s'est défini un certain nombre d'objectifs stratégiques, dont le plus important est l'amélioration de la satisfaction de sa clientèle. En se basant sur ce principe, elle souhaite identifier les sphères nécessitant une amélioration en matière de TI.

L'entreprise établit que le fait de prioriser la satisfaction du client équivaut à augmenter la priorité des objectifs d'entreprise ci-dessous (voir la figure 5) :

- 6. Culture de service orientée vers le client
- 7. Continuité et disponibilité des services d'entreprise
- 8. Réponses agiles à un environnement d'affaires en évolution

L'entreprise passe ensuite à la prochaine étape de la cascade d'objectifs : analyser quels objectifs liés aux TI correspondent à ses objectifs d'entreprise. Une proposition de table de correspondance est présentée à l'annexe B.

Ensuite, les objectifs liés aux TI les plus importants sont proposés ci-dessous (tous des relations « P ») :

- 01 Alignement des TI et de la stratégie d'affaires
- 04 Gestion du risque d'affaires lié aux TI
- 07 Livraison de services des TI conformes aux exigences opérationnelles
- 09 Agilité des TI
- 10 Sécurité de l'information, des infrastructures de traitement et des applications
- 14 Disponibilité d'informations fiables et utiles pour la prise de décision
- 17 Connaissances, compétences et initiatives pour l'innovation d'affaires

L'entreprise valide cette liste et décide de prioriser les quatre premiers objectifs.

À l'étape suivante de la démarche, en utilisant le concept de facilitateur (voir le chapitre 5), ces objectifs liés aux TI conduiront à un certain nombre d'objectifs, y compris les objectifs de processus. À l'annexe C, une table de correspondance est proposée entre les objectifs liés aux TI et les processus de COBIT 5. Cette table permet de définir les processus liés aux TI qui soutiennent les objectifs liés aux TI les plus pertinents. Toutefois les processus à eux seuls ne sont pas suffisants. Les autres facilitateurs, comme la culture, le comportement et l'éthique, les structures organisationnelles ou les compétences et l'expertise sont tout aussi importants et nécessitent un ensemble d'objectifs clairs.

Lorsque cet exercice est terminé, l'entreprise dispose d'un ensemble d'objectifs cohérents pour tous les facilitateurs qui lui permet d'atteindre les objectifs stratégiques fixés; l'entreprise possède aussi un ensemble d'indicateurs associés pour mesurer la performance.

EXEMPLE 2 – BESOINS DES PARTIES PRENANTES : DÉVELOPPEMENT DURABLE

Après avoir mené une analyse des besoins des parties prenantes, une entreprise décide que le développement durable constitue une priorité stratégique. Dans ce cas-ci, le développement durable englobe non seulement les aspects environnementaux, mais aussi tous les éléments qui contribuent à la réussite à long terme de l'entreprise.

En se basant sur ces résultats, l'entreprise décide de se concentrer sur les cinq objectifs qui suivent, avec quelques précisions supplémentaires :

1. Valeur pour les parties prenantes des investissements de l'entreprise, en particulier pour la communauté des parties prenantes.
4. Conformité aux lois et à la réglementation, en se concentrant sur les lois environnementales et les lois relatives à la réglementation du travail dans les ententes d'impartition (accords d'externalisation).
8. Réponses agiles dans un contexte d'affaires en évolution.
16. Personnes qualifiées et motivées, conscientes que le succès de l'entreprise dépend de ses collaborateurs.
17. Culture d'innovation des produits et des affaires, axée sur les innovations à long terme.

Questions de gouvernance et de gestion des TI

Le respect des besoins des parties prenantes dans toute entreprise, compte tenu de la forte dépendance aux TI, soulèvera un certain nombre de questions sur la gouvernance et la gestion des TI de l'entreprise (**figure 7**).

Figure 7 – Questions de gouvernance et de gestion à propos des TI	
Parties prenantes internes	Questions aux parties prenantes internes
• Conseil d'administration • Chef de la direction • Directeur financier • Dirigeant principal de l'information • Directeur de la gestion des risques • Dirigeants d'entreprise • Propriétaires des processus d'affaires • Gestionnaires d'entreprise • Gestionnaires de risques • Gestionnaires de sécurité • Gestionnaires de services • Gestionnaires des ressources humaines (RH) • Audit interne • Gestionnaires de la protection de la vie privée • Utilisateurs des TI • Gestionnaires des TI • Etc.	• Comment puis-je tirer profit de l'utilisation des TI? Les utilisateurs finaux sont-ils satisfaits de la qualité du service des TI? • Comment puis-je gérer la performance des TI? • Comment puis-je exploiter au mieux les nouvelles technologies pour en tirer de nouvelles opportunités stratégiques? • Comment puis-je bâtir et structurer au mieux mon service des TI? • Dans quelle mesure suis-je dépendant des fournisseurs externes? Dans quelle mesure les accords d'impartition (externalisation) des TI sont-ils bien gérés? • Comment puis-je obtenir une assurance envers les fournisseurs externes? • Quelles sont les exigences (de contrôle) en matière d'information? • Ai-je considéré tous les risques liés aux TI? • Mon exploitation des TI est-elle efficace et résiliente? • Comment puis-je contrôler le coût des TI? Comment puis-je utiliser les ressources TI de la manière la plus efficace? • Quelles sont les options d'impartition (externalisation) les plus efficaces? • Ai-je suffisamment de personnel pour les TI? Comment puis-je développer et maintenir leurs compétences, et comment puis-je gérer leur performance? • Comment puis-je obtenir une assurance envers les TI? • L'information que je traite est-elle bien sécurisée? • Comment puis-je améliorer l'agilité de l'entreprise au moyen d'un environnement des TI plus flexible? • Les projets en TI ne réussissent pas à livrer ce qu'ils avaient promis, si oui, pourquoi? Les TI entravent-elles l'exécution de la stratégie d'entreprise? • Quelle est l'importance des TI pour soutenir l'entreprise? Que dois-je faire si les TI ne sont pas disponibles? • Quels processus critiques de l'entreprise sont dépendants des TI et quelles sont les exigences des processus d'affaires? • Quel a été le dépassement moyen des budgets opérationnels des TI? À quelle fréquence et de combien les projets des TI dépassent-ils leur budget? • Quelle fraction de l'effort en TI sera consacré à la résolution de problèmes plutôt qu'à l'amélioration des affaires? • Les ressources et l'infrastructure des TI disponibles sont-elles suffisantes pour répondre aux objectifs stratégiques de l'entreprise? • Combien de temps faut-il pour prendre des décisions importantes en matière de TI? • Les efforts et les investissements en TI sont-ils transparents? • Les TI aident-elles l'entreprise à respecter la réglementation et les niveaux de service? Comment puis-je savoir si l'entreprise est conforme à toute la réglementation en vigueur?
Parties prenantes externes	Questions aux parties prenantes externes
• Partenaires commerciaux • Fournisseurs • Actionnaires • Organismes de réglementation et gouvernement • Utilisateurs externes • Clients • Organismes de normalisation • Auditeurs externes • Consultants • Etc.	• Comment puis-je savoir si les activités de mon partenaire d'affaires sont sûres et fiables? • Comment puis-je savoir si l'entreprise est conforme aux règles et à la réglementation applicables? • Comment puis-je savoir si l'entreprise maintient un système efficace de contrôle interne? • Les partenaires d'affaires ont-ils le contrôle sur leur chaîne d'échange d'information?

Comment trouver des réponses à ces questions?

Toutes les questions mentionnées à la **figure 7** peuvent être liées aux objectifs d'entreprise et servent d'intrants à la cascade d'objectifs, grâce à laquelle ils peuvent être traités efficacement. L'annexe D contient un exemple de correspondance entre les questions des parties prenantes internes mentionnées à la **figure 7** et les objectifs d'entreprise.

CHAPITRE 3

PRINCIPE 2 : COUVRIRE L'ENTREPRISE DE BOUT EN BOUT

COBIT 5 traite de la gouvernance ainsi que de la gestion bout en bout de l'information et des technologies connexes de l'entreprise. Cela signifie que COBIT 5 :

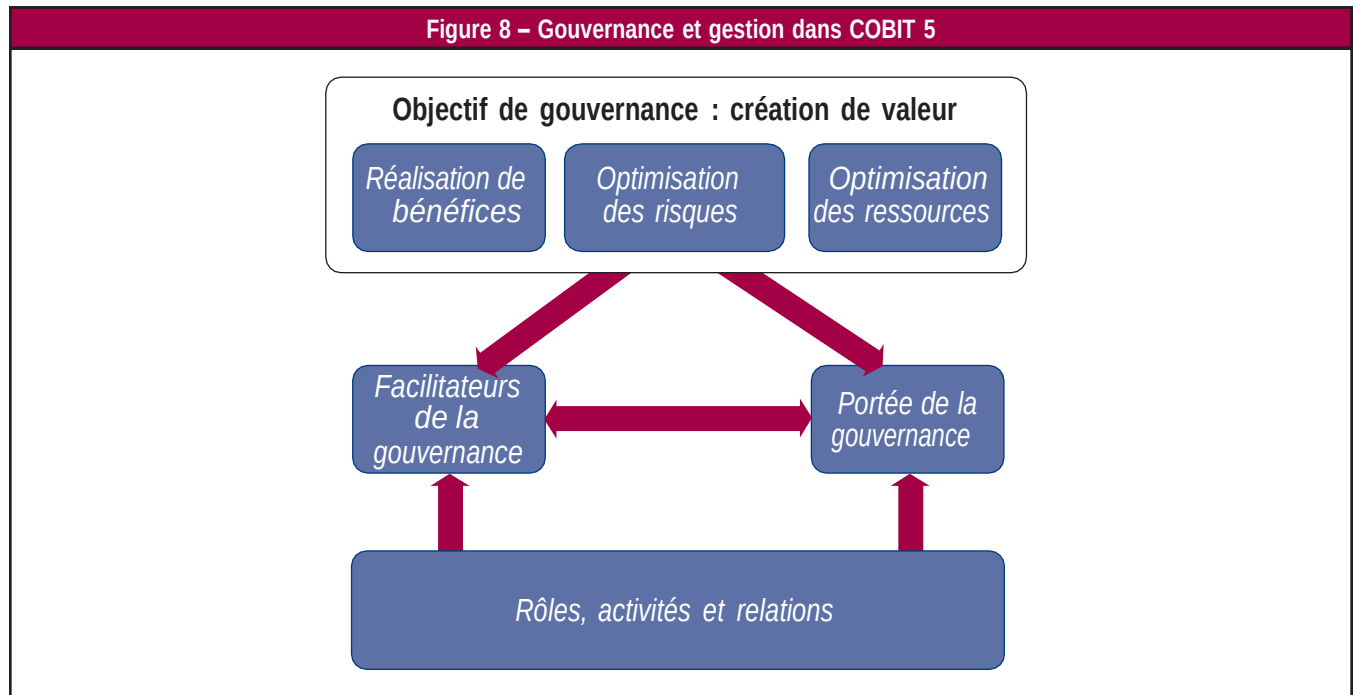
- Intègre la gouvernance des TI dans la gouvernance d'entreprise. Autrement dit, le système de gouvernance des TI proposé par COBIT 5 s'intègre parfaitement à tout système de gouvernance. COBIT 5 est aligné sur les derniers développements en matière de gouvernance.
- Couvre toutes les fonctions et les processus nécessaires pour gouverner et gérer l'information et les technologies liées à l'entreprise, quel que soit l'endroit où cette information est traitée. Compte tenu de l'étendue de sa portée, COBIT 5 aborde tous les services pertinents fournis par les TI et les processus d'affaires, internes comme externes.

COBIT 5 fournit une vision globale et systémique de la gouvernance et de la gestion des TI de l'entreprise (voir principe 4) en se basant sur un certain nombre de facilitateurs considérés à l'échelle de l'entreprise et comprenant les éléments et le personnel, interne comme externe, impliqués dans la gouvernance et la gestion de l'information et des TI connexes. Ils comprennent également les activités et les responsabilités des fonctions de tout ce qui est ou non concerné par les TI dans l'entreprise.

L'information est l'un des facilitateurs de COBIT. Le modèle au moyen duquel COBIT 5 définit les facilitateurs permet à toutes les parties prenantes de définir l'ensemble des exigences liées à l'information et au cycle de vie du traitement de l'information. Ainsi, il permet de relier l'entreprise, son besoin d'information adéquate et la fonction TI, tout en soutenant les opérations et en s'adaptant à son contexte.

Approche de gouvernance

L'approche de gouvernance de bout en bout à la base de COBIT 5 est représentée à la **figure 8**, illustrant les éléments clés d'un système de gouvernance⁴.



Outre son objectif, les principaux éléments constituant l'approche de gouvernance sont les facilitateurs, la portée, les rôles, les activités et les relations.

Facilitateurs de la gouvernance

Les facilitateurs de la gouvernance sont les ressources organisationnelles, comme les référentiels, les principes, les structures, les processus et les pratiques, par lesquels ou vers lesquels l'action est dirigée de façon à atteindre les objectifs fixés. Les facilitateurs comprennent également les ressources de l'entreprise. Par exemple, les capacités de service (infrastructure des TI, applications, etc.), le personnel et l'information. Un manque de ressources ou de facilitateurs peut affecter la capacité de l'entreprise à créer de la valeur.

Compte tenu de l'importance des facilitateurs en matière de gouvernance, COBIT 5 présente une façon unique de considérer et de traiter les facilitateurs (voir le chapitre 5).

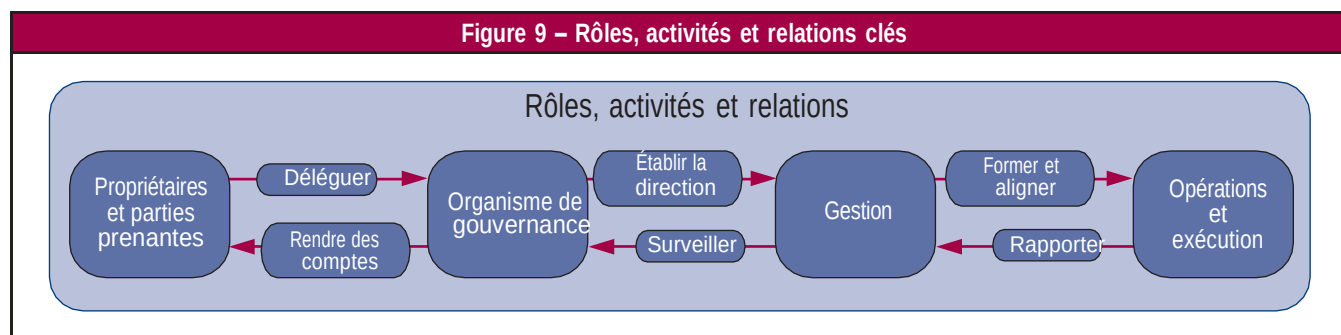
Portée de la gouvernance

La gouvernance peut être appliquée à toute l'entreprise, à une entité, à un actif tangible ou intangible, etc. Autrement dit, il est possible de ne définir que certains aspects de l'entreprise auxquels s'applique la gouvernance. Il est essentiel de bien définir cette portée du système de gouvernance. COBIT 5 considère l'entreprise dans son ensemble, mais fondamentalement, COBIT 5 peut traiter tout aspect individuellement.

Rôles, activités et relations

Les rôles, les activités et les relations définissent les personnes qui participent à la gouvernance, la façon dont elles sont impliquées, ce qu'elles font et comment elles interagissent dans le cadre d'un système de gouvernance. COBIT 5 établit une différenciation claire entre les activités de gouvernance et celles de gestion ainsi qu'une interface entre ces activités et les rôles des acteurs impliqués. La **figure 9**, qui détaille la partie inférieure de la **figure 8**, présente les interactions entre les différents rôles.

Figure 9 – Rôles, activités et relations clés



PRINCIPE 3 : APPLIQUER UN RÉFÉRENTIEL UNIQUE ET INTÉGRÉ

CHAPITRE 4

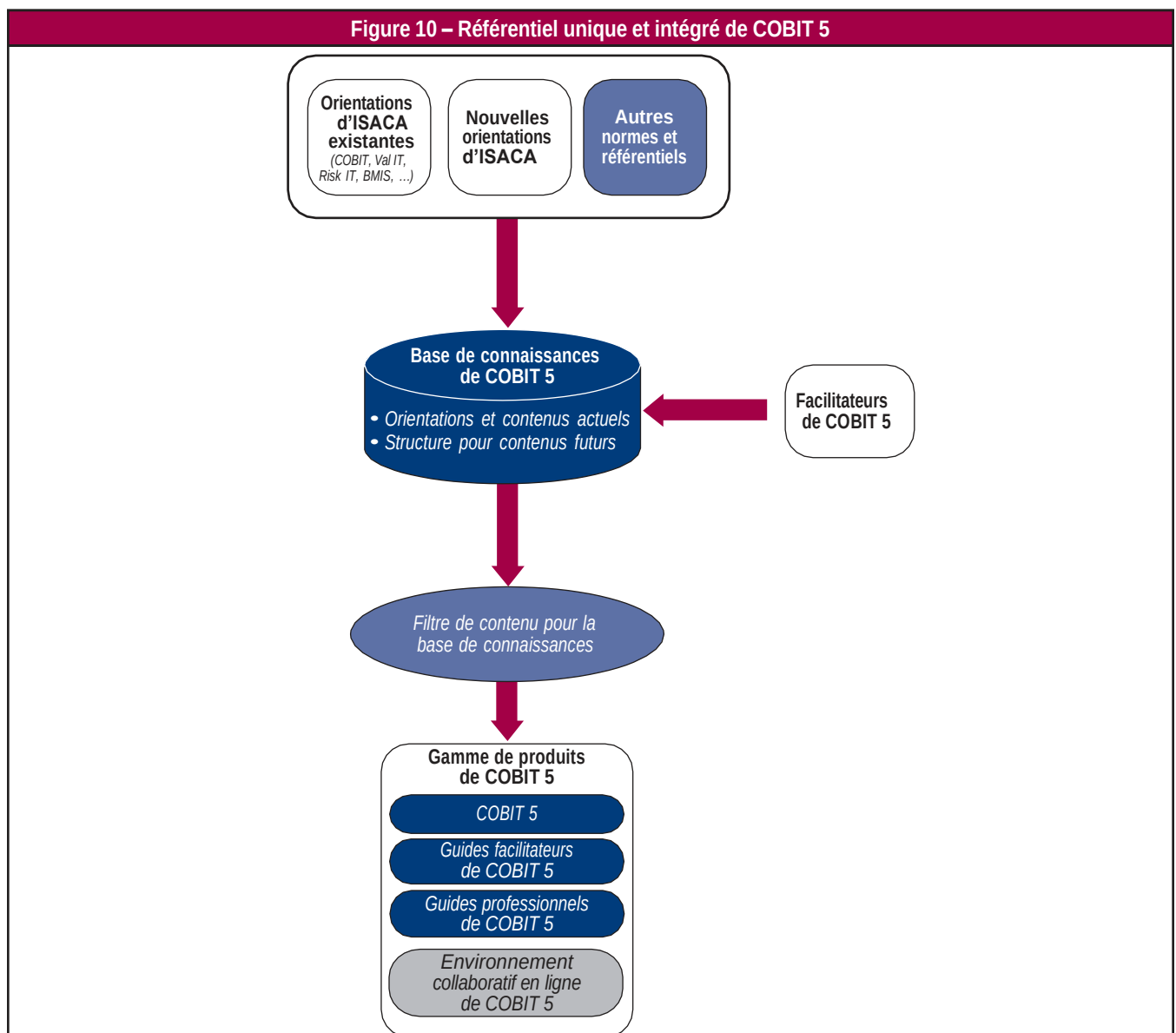
PRINCIPE 3 : APPLIQUER UN RÉFÉRENTIEL UNIQUE ET INTÉGRÉ

COBIT 5 est un référentiel unique et intégré pour les raisons suivantes :

- Il s'aligne avec les normes et référentiels d'importance les plus récents, permettant ainsi à l'entreprise d'utiliser COBIT 5 comme intégrateur global du référentiel de gouvernance et de gestion.
- Il couvre complètement l'entreprise, fournissant une base pour intégrer efficacement d'autres référentiels, normes et pratiques. Un référentiel global unique constitue une source cohérente et intégrée d'orientations dans un langage commun, non technique et indépendant des technologies.
- Il fournit une architecture simple pour structurer les documents d'orientation et générer un ensemble cohérent de documents.
- Il intègre toutes les connaissances précédemment réparties dans les différents référentiels élaborés par l'ISACA. Cette dernière étudie le domaine clé de la gouvernance d'entreprise depuis de nombreuses années et a élaboré des référentiels comme COBIT, Val IT, Risk IT, BMIS, la publication *Board Briefing on IT Governance* et ITAF afin de fournir des orientations pratiques et des conseils aux entreprises. COBIT 5 intègre toutes ces connaissances.

Intégrateur du référentiel de COBIT 5

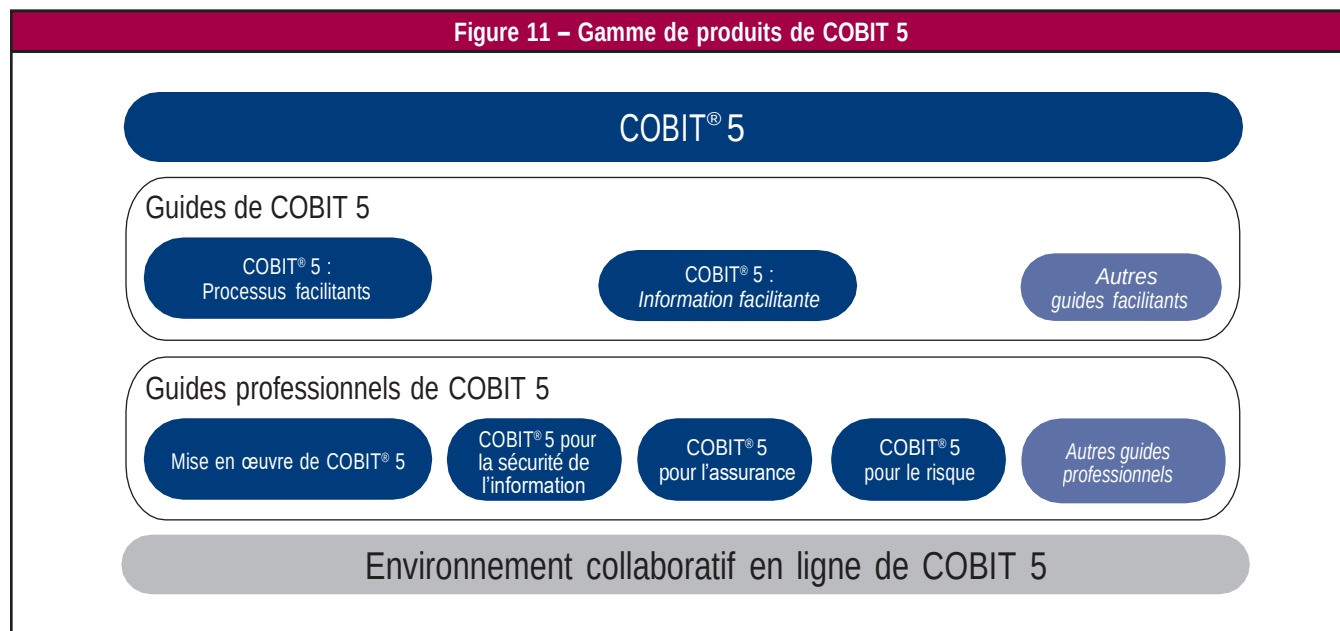
La **figure 10** fournit une description graphique de la façon dont COBIT 5 remplit son rôle en tant que référentiel aligné et intégré.



Le référentiel de COBIT 5 fournit à ses parties prenantes des conseils plus complets et à jour (voir la **figure 11**) sur la gouvernance et la gestion des TI de l'entreprise par :

- La recherche et l'utilisation d'un ensemble de sources qui ont mené à l'élaboration du nouveau contenu, y compris :
 - Réunir les orientations existantes de l'ISACA (COBIT 4.1, Val IT 2.0, Risk IT, BMIS) dans ce référentiel unique.
 - Compléter ce contenu avec les domaines nécessitant un approfondissement et des mises à jour.
 - S'aligner sur d'autres normes et référentiels pertinents, comme ITIL, TOGAF et les normes ISO. La liste complète des références se trouve à l'annexe A.
- La définition d'un ensemble de facilitateurs de gouvernance et de gestion, qui fournissent une structure pour tous les documents d'orientation.
- La constitution d'une base de connaissances COBIT 5 qui contient toutes les orientations et les contenus déjà développés, et qui fournira une structure permettant l'évolution des contenus.
- L'établissement d'une base de référence solide et complète en matière de bonnes pratiques.

Figure 11 – Gamme de produits de COBIT 5



CHAPITRE 5

PRINCIPE 4 : FACILITER UNE APPROCHE GLOBALE

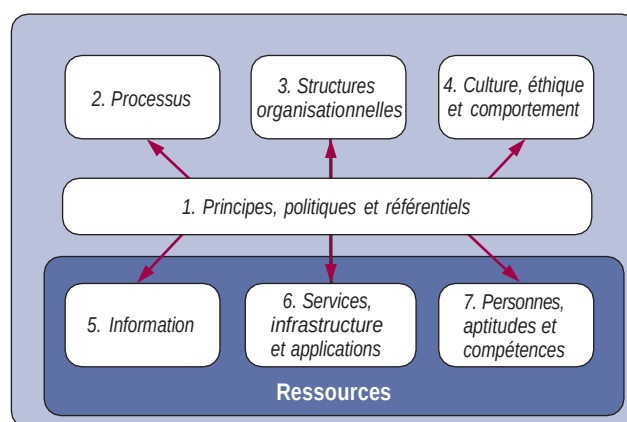
Les facilitateurs de COBIT 5

Les facilitateurs sont des facteurs qui, individuellement ou collectivement, influencent la réussite d'une activité; dans ce cas-ci, la gouvernance et la gestion des TI de l'entreprise. Les facilitateurs sont influencés par la cascade d'objectifs, c'est-à-dire que des objectifs de plus haut niveau liés aux TI définissent ce que les différents facilitateurs devraient permettre d'atteindre.

Le référentiel de COBIT 5 décrit sept catégories de facilitateurs (**figure 12**) :

- **Les principes, les politiques et les référentiels** représentent le véhicule permettant de traduire le comportement désiré en orientations pratiques pour la gestion quotidienne.
- **Les processus** décrivent un ensemble organisé de pratiques et d'activités requises pour atteindre des objectifs et pour produire un ensemble de résultats permettant la réalisation des objectifs globaux liés aux TI.
- **Les structures organisationnelles** sont les principales entités de décision dans l'entreprise.
- **La culture, l'éthique et le comportement** des individus et de l'entreprise sont très souvent sous-estimés en tant que facteurs de réussite dans les activités de gouvernance et de gestion.
- **L'information** est omniprésente dans toute organisation. Elle comprend toute l'information produite et utilisée par l'entreprise. L'information est nécessaire pour maintenir l'organisation fonctionnelle et bien gouvernée, mais au niveau opérationnel, elle est souvent le produit phare de l'entreprise elle-même.
- **Les services, l'infrastructure et les applications** comprennent l'infrastructure, la technologie et les applications qui fournissent à l'entreprise les traitements et les services en matière de technologies de l'information.
- **Le personnel, les aptitudes et les compétences** sont liées aux individus et sont nécessaires pour la réussite de toutes les activités ainsi que pour la prise de décisions éclairées et de mesures correctives.

Figure 12 – Facilitateurs d'entreprise de COBIT 5



Certains facilitateurs précédemment définis sont également des ressources d'entreprise qui doivent être gérées et gouvernées. Ceci s'applique à :

- L'information. Certaines informations, comme les rapports de gestion et les veilles stratégiques, constituent des facilitateurs importants pour la gouvernance et la gestion de l'entreprise.
- Le service, l'infrastructure et les applications.
- Le personnel, les aptitudes et les compétences.

Gouvernance et gestion systémiques au moyen de facilitateurs interreliés

La **figure 12** illustre la relation de la gouvernance d'entreprise, dont celle des TI, avec les divers éléments ainsi que son rôle, qui consiste à atteindre les principaux objectifs de l'entreprise. Toute entreprise doit tenir compte d'un ensemble de facilitateurs interreliés. Par ailleurs, chaque facilitateur :

- Nécessite l'apport des autres facilitateurs pour être pleinement efficace; par exemple, les processus requièrent de l'information, les structures organisationnelles ont besoin de compétences et de comportements adéquats.
- Fournit un résultat au profit d'autres facilitateurs; par exemple, les processus fournissent de l'information, les aptitudes et les comportements rendent les processus efficaces.

Ainsi, en matière de gouvernance et de gestion des TI de l'entreprise, de bonnes décisions ne peuvent être prises que lorsque la nature des ententes est prise en compte. Cela signifie que pour faire face à tous les besoins des parties prenantes, les facilitateurs interreliés doivent être analysés pour leur pertinence et leur éventuelle considération. Cet état d'esprit doit émaner de la haute direction de l'entreprise, comme l'illustrent les exemples suivants.

EXEMPLE 3 – GOUVERNANCE ET GESTION DES TI DE L'ENTREPRISE

Fournir des services de TI opérationnelles à tous les utilisateurs nécessite le bon fonctionnement de certains services (infrastructures, applications) et l'apport de personnel détenant des compétences particulières et adoptant un comportement approprié. Un certain nombre de processus de livraison de services doivent aussi être mis en œuvre et soutenus par les structures organisationnelles.

EXEMPLE 4 – GOUVERNANCE ET GESTION DES TI DE L'ENTREPRISE

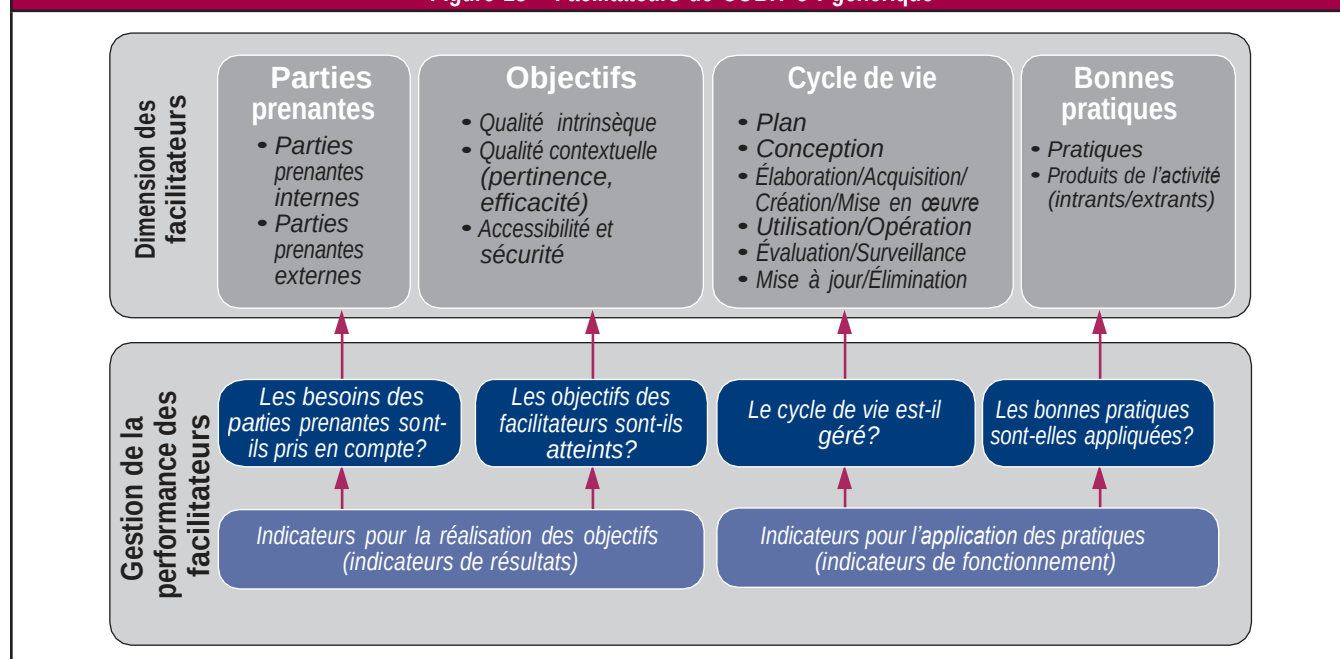
Le besoin de sécurité de l'information exige la création et la mise en œuvre d'un certain nombre de politiques et de procédures. Ces politiques, à leur tour, exigent la mise en œuvre d'un certain nombre de pratiques liées à la sécurité. Toutefois, si la culture et l'éthique de l'entreprise et du personnel ne sont pas appropriées, les processus et procédures de sécurité de l'information ne seront pas efficaces.

Dimensions des facilitateurs de COBIT 5

Tous les facilitateurs présentent un ensemble de caractéristiques communes qui (figure 13) :

- Fournit une façon commune, simple et structurée pour gérer les facilitateurs.
- Permet à une entité de gérer ses interactions complexes.
- Facilite l'obtention de résultats positifs par les facilitateurs.

Figure 13 – Facilitateurs de COBIT 5 : générique



Caractéristiques des facilitateurs

Les quatre caractéristiques communes des facilitateurs sont :

- **Parties prenantes** – Chaque facilitateur comporte des parties prenantes (éléments qui jouent un rôle actif ou qui ont un intérêt dans le facilitateur). Par exemple, les processus comportent différents éléments qui réalisent les activités du processus ou qui ont un intérêt dans les résultats du processus; les structures organisationnelles sont composées de parties prenantes ayant chacune leurs propres rôles, intérêts et besoins, qui sont parfois contradictoires. Les besoins des parties prenantes se traduisent par des objectifs d'entreprise, qui à leur tour se traduisent par des objectifs liés aux TI de l'entreprise. Une liste de parties prenantes est présentée à la figure 7.
- **Objectifs** – Chaque facilitateur a un certain nombre d'objectifs, et tous procurent de la valeur en permettant d'atteindre ces objectifs, qui peuvent être définis en fonction des éléments suivants :
 - Résultats attendus du facilitateur
 - Application ou fonctionnement du facilitateur

Les objectifs facilitants représentent la dernière étape de la cascade d'objectifs de COBIT 5 et peuvent encore être divisés en différentes catégories :

- **Qualité intrinsèque** – La mesure selon laquelle les facilitateurs agissent avec précision, de façon objective et fournissent des résultats précis, objectifs et fiables.
- **Qualité contextuelle** – La mesure selon laquelle les facilitateurs et leurs résultats sont appropriés au contexte dans lequel ils opèrent. Par exemple, les résultats doivent être pertinents, complets, actuels, appropriés, uniformes, compréhensibles et faciles à utiliser.
- **Accès et sécurité** – La mesure selon laquelle les facilitateurs et leurs résultats sont accessibles et sécurisés, tels que :
 - Les facilitateurs sont disponibles au moment opportun et au besoin.
 - Les résultats sont sécurisés, c'est-à-dire que l'accès est limité aux personnes qui en ont besoin.
- **Cycle de vie** – Chaque facilitateur possède un cycle de vie, qui va de sa création à son élimination, en passant par sa durée de vie opérationnelle et utile. Ceci s'applique à l'information, aux structures, aux processus, aux politiques, etc. Les étapes du cycle de vie sont les suivantes :
 - Planifier (y compris l'élaboration et la sélection des concepts)
 - Concevoir
 - Bâtir, acquérir, créer, mettre en œuvre
 - Utiliser, exploiter
 - Évaluer, surveiller
 - Mettre à jour, éliminer
- **Bonnes pratiques** – Pour chacun des facilitateurs, il est possible de définir de bonnes pratiques. Celles-ci contribuent à l'atteinte des objectifs facilitants. Les bonnes pratiques fournissent des exemples ou des suggestions sur la meilleure façon de mettre en œuvre les facilitateurs en précisant les produits, les intrants ou les extrants requis. COBIT 5 fournit des exemples de bonnes pratiques pour certains facilitateurs proposés (par exemple, les processus). Pour les autres facilitateurs, il est possible d'utiliser des orientations provenant d'autres normes, référentiels, etc.

Gestion de la performance des facilitateurs

Les entreprises s'attendent à des résultats positifs de la mise en œuvre et de l'utilisation des facilitateurs. Pour gérer la performance des facilitateurs, les questions qui suivent doivent être considérées, et il faut par la suite y répondre sur une base régulière en fonction des indicateurs :

- Les besoins des parties prenantes sont-ils pris en compte?
- Les objectifs facilitants sont-ils atteints?
- Le cycle de vie des facilitateurs est-il géré?
- Les bonnes pratiques sont-elles appliquées?

Les deux premiers points concernent le résultat concret du facilitateur. Les indicateurs utilisés pour évaluer dans quelle mesure les objectifs sont atteints peuvent être appelés « indicateurs de résultats ».

Les deux derniers points traitent du fonctionnement réel du facilitateur lui-même et les indicateurs qui y sont associés peuvent être appelés « indicateurs de fonctionnement ».

Exemples pratiques de facilitateurs

L'exemple 5 illustre les facilitateurs, leurs interconnexions et leurs caractéristiques ainsi que la façon de les utiliser pour en tirer un bénéfice concret.

EXEMPLE 5 – FACILITATEURS

Une organisation a nommé des « gestionnaires de processus » chargés de définir et d'exploiter des processus efficaces liés aux TI, dans le cadre de la bonne gouvernance et de la bonne gestion des TI de l'entreprise.

Au départ, ces gestionnaires de processus analyseront les processus facilitateurs, en regard de leurs caractéristiques :

- **Parties prenantes** : Les parties prenantes du processus incluent tous les acteurs du processus, soit tous les approbateurs des activités reliées aux processus de même que tous ceux qui en sont responsables ou doivent être consultés ou informés (RACI). Le tableau RACI décrit dans *COBIT 5 : Les processus facilitateurs* peut être utilisé.
- **Objectifs** : Pour chaque processus, des objectifs adéquats ainsi que leurs indicateurs connexes doivent être définis. Par exemple, pour le processus *Gestion des relations* (processus APO08 dans *COBIT 5 : Processus facilitateurs*) il est possible d'extraire un ensemble d'objectifs de processus et d'indicateurs tels que :
 - **Objectif** : Les stratégies, les plans et les exigences d'affaires sont bien compris, documentés et approuvés.
 - **Indicateurs** : Pourcentage des programmes alignés avec les exigences et les priorités d'affaires de l'entreprise
 - **Objectif** : De bonnes relations existent entre l'entreprise et le service des TI.
 - **Indicateurs** : Notation par sondage de la satisfaction des utilisateurs et du personnel des TI
- **Cycle de vie** : Chaque processus dispose d'un cycle de vie, c'est-à-dire qu'il doit être créé, exécuté, surveillé et optimisé si nécessaire. Éventuellement, les processus sont amenés à être remplacés. Dans ce cas, les gestionnaires de processus devront au préalable concevoir et définir le processus. Ils peuvent utiliser plusieurs éléments de *COBIT 5 : Processus facilitateurs* pour définir les responsabilités et scinder le processus en pratiques et en activités, ainsi que pour définir les intrants et les extrants. Éventuellement, le processus doit devenir plus robuste et plus efficace. Dans ce but, les gestionnaires de processus peuvent optimiser les capacités du processus. La norme ISO/CEI 15504 a inspiré le modèle de capacité des processus de COBIT 5 et les attributs de capacité du processus peuvent être utilisés à cette fin.
- **Bonne pratique** : Les bonnes pratiques pour les processus sont décrites dans *COBIT 5 : Processus facilitateurs*, comme mentionnés au point précédent. Ce document renferme des exemples et couvre tout l'éventail des activités nécessaires à la bonne gouvernance et à la bonne gestion des TI de l'entreprise.

En plus des orientations sur les processus facilitateurs, les gestionnaires de processus peuvent décider de considérer d'autres facilitateurs tels que :

- Les tableaux RACI, qui décrivent les rôles et les responsabilités. D'autres facilitateurs permettent d'approfondir cette dimension, par exemple :
 - Dans le facilitateur des aptitudes et compétences, les aptitudes et compétences nécessaires à chaque rôle peuvent être définies, et des objectifs appropriés (par exemple, les niveaux de compétences techniques et comportementales) ainsi que des indicateurs associés peuvent être définis.
 - Le tableau RACI contient également des structures organisationnelles pouvant être précisées dans le facilitateur des structures organisationnelles, où une description plus détaillée peut être fournie et où les résultats attendus et les indicateurs correspondants peuvent être définis (par exemple, les décisions). Les bonnes pratiques peuvent aussi être définies (par exemple, la portée du contrôle, les principes de fonctionnement de la structure, le niveau d'autorité).
- Les principes et les politiques formalisent les processus et justifient l'existence de ceux-ci; ils indiquent à qui ils s'appliquent et comment les processus doivent être utilisés. Il s'agit du domaine d'action des facilitateurs des principes et des politiques.

L'annexe G présente plus en détail les sept catégories de facilitateurs. La lecture de cette annexe est recommandée pour mieux comprendre les facilitateurs et toute leur importance dans l'organisation de la gouvernance et de la gestion des TI de l'entreprise.

CHAPITRE 6

PRINCIPE 5 : DISTINGUER LA GOUVERNANCE DE LA GESTION

Gouvernance et gestion

Le référentiel de COBIT 5 établit une distinction claire entre la gouvernance et la gestion. Ces deux fonctions englobent différents types d'activités, nécessitent différentes structures organisationnelles et répondent à des besoins différents. Le point de vue de COBIT 5 quant à cette distinction clé entre la gouvernance et la gestion est le suivant :

- **Gouvernance**

La gouvernance consiste à évaluer les besoins, les règles et les options des parties prenantes dans le but de déterminer des objectifs d'entreprise équilibrés qui font consensus. Elle permet de déterminer l'orientation par les priorités et la prise de décisions. Enfin, elle permet de contrôler la performance et la conformité au regard des orientations et des objectifs convenus.

Dans la plupart des entreprises, la gouvernance relève du conseil d'administration, sous la direction de son président.

- **Gestion**

L'équipe de gestion planifie, bâtit, exécute et surveille les activités conformément à l'orientation fixée par le groupe de gouvernance afin d'atteindre les objectifs d'entreprise.

Dans la plupart des entreprises, la gestion relève de la haute direction, sous l'autorité du président-directeur général.

Interactions entre la gouvernance et la gestion

D'après les définitions de la gouvernance et de la gestion, il est clair que ces deux fonctions comprennent différents types d'activités et de responsabilités. Étant donné le rôle de la gouvernance (évaluer, diriger et surveiller), un ensemble d'interactions est nécessaire entre la gouvernance et la gestion afin d'obtenir un système de gouvernance efficace. En se servant de la structure des facilitateurs, ces interactions sont représentées sommairement à la **figure 14**.

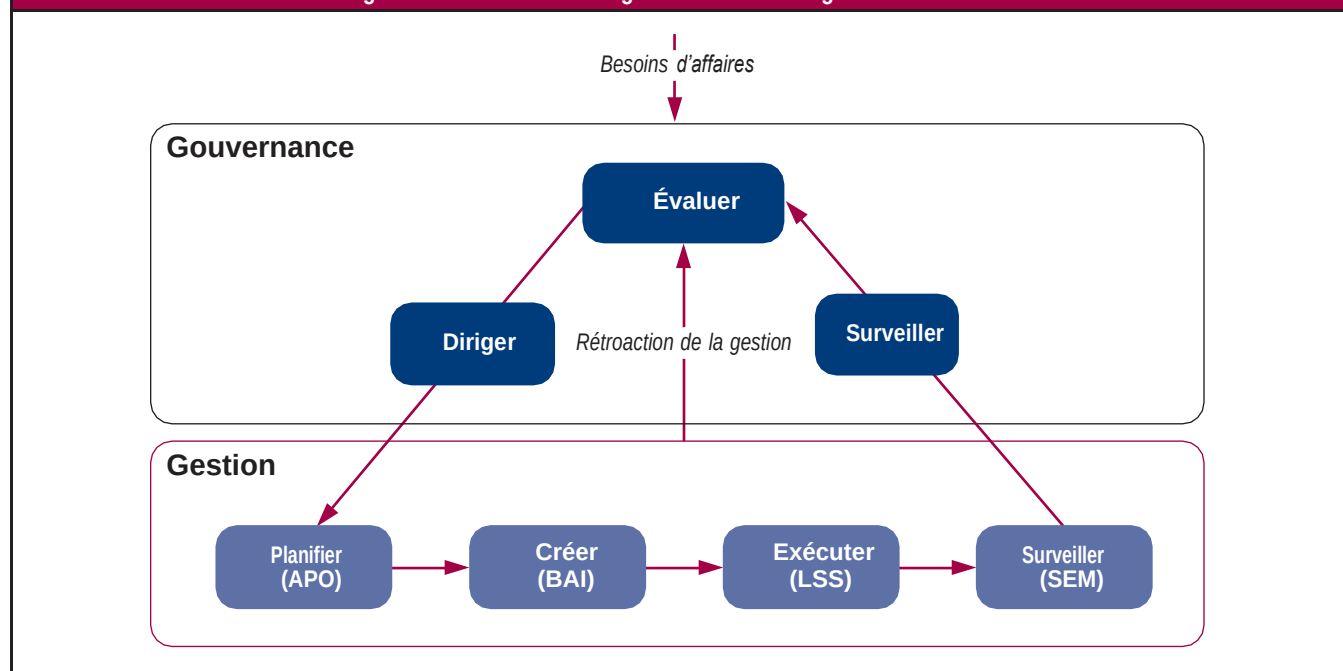
Figure 14 – Interactions entre la gouvernance et la gestion selon COBIT 5

Facilitateurs	Interaction gouvernance-gestion
Processus	Dans le modèle de processus de COBIT 5 illustré (<i>COBIT 5 : Processus facilitateurs</i>), une distinction est faite entre les processus de gouvernance et de gestion, comprenant des ensembles précis de pratiques et d'activités pour chacun d'entre eux. Des tableaux RACI sont rattachés aux processus et décrivent les responsabilités des différentes structures organisationnelles et des différents rôles au sein de l'entreprise.
Information	Le modèle de processus décrit les intrants et les extrants des différentes pratiques d'un processus. L'information utilisée pour évaluer, diriger et surveiller les TI de l'entreprise est échangée entre la gouvernance et la gestion, comme cela est décrit dans les intrants et les extrants du modèle de processus.
Structures organisationnelles	Un certain nombre de structures organisationnelles sont définies dans chaque entreprise; elles peuvent reposer sur la gouvernance ou sur la gestion, en fonction de leur composition et de la portée des décisions. Puisque la gouvernance concerne l'établissement d'une orientation, une interaction a lieu entre d'une part les décisions prises par les structures de gouvernance (par exemple, le fait de choisir le portefeuille d'investissement et d'établir la tolérance au risque) et d'autre part les décisions et les actions qui les mettent en œuvre.
Principes, politiques et référentiels	Les principes, les politiques et les référentiels constituent le véhicule par lequel les décisions de gouvernance sont institutionnalisées au sein de l'entreprise. Pour cette raison, une interaction existe entre les décisions de gouvernance (établissement de l'orientation) et de gestion (exécution des décisions).
Culture, éthique et comportement	Le comportement constitue également un facilitateur clé de la bonne gouvernance et de la bonne gestion de l'entreprise. Il se place au premier plan puisqu'il représente l'exemple à suivre, et constitue donc une interaction importante entre la gouvernance et la gestion.
Personnes, aptitudes et compétences	Les activités de gouvernance et de gestion nécessitent différentes aptitudes essentielles de la part de leurs responsables, dont celle de comprendre les tâches de chacun et ce qui les différencie.
Services, infrastructures et applications	Les services, soutenus par les applications et les infrastructures, permettent de fournir au groupe de gouvernance les informations nécessaires à ses activités d'évaluation, de gestion et de surveillance.

Modèle de référence du processus COBIT 5

COBIT 5 se défend d'imposer sa vision, mais recommande fortement aux entreprises de mettre en œuvre des processus de gouvernance et de gestion de telle sorte que les principaux piliers soient couverts, comme le montre la **figure 15**.

Figure 15 – Zones clés de gouvernance et de gestion de COBIT 5



Une entreprise peut décider de ses propres processus, à condition que tous les objectifs de gouvernance et de gestion nécessaires soient couverts. Les petites entreprises peuvent avoir moins de processus, tandis que les entreprises plus grandes et plus complexes peuvent avoir de nombreux processus.

Le modèle de référence de COBIT 5 définit et décrit en détail un certain nombre de processus de gouvernance et de gestion. Il représente tous les processus qui se trouvent normalement dans une entreprise en matière d'activités liées aux TI, fournissant un modèle de référence commun compréhensible par les gestionnaires des opérations des TI et des lignes d'affaires. Le modèle de processus proposé en est un global et complet, mais il ne s'agit pas du seul modèle de processus possible. Chaque entreprise doit définir son propre ensemble de processus en tenant compte de sa situation particulière.

L'intégration d'un modèle opérationnel et d'un langage commun pour toutes les parties de l'entreprise participant aux activités des TI est l'une des étapes les plus importantes et critiques menant à une bonne gouvernance. Elle fournit également un référentiel pour évaluer et surveiller la performance des TI, auditer les TI, communiquer avec les fournisseurs de services et intégrer des meilleures pratiques de gestion.

Le modèle de référence de COBIT 5 divise l'ensemble des processus de l'entreprise en deux fonctions :

- **Gouvernance** – Contient cinq processus pour lesquels des pratiques d'évaluation, de direction et de surveillance (EDS)⁵ sont définies.
- **Gestion** – Contient quatre domaines en lien avec la planification, la création, l'exécution et la surveillance (PCES) et fournit une couverture des TI de bout en bout. Ils représentent une évolution des domaines et de la structure de processus de COBIT 4.1, dont les noms sont choisis en fonction de ces principales appellations. Ils contiennent cependant un plus grand nombre de verbes :
 - Aligner, planifier et organiser (APO)
 - Bâtir, acquérir et implanter (BAI)
 - Livrer, servir et soutenir (LSS)
 - Surveiller, évaluer et mesurer (SEM)

Chaque domaine renferme un certain nombre de processus. Bien que la plupart des processus fassent intervenir la planification, la création, l'exécution et la surveillance dans la résolution d'un problème particulier (en lien par exemple

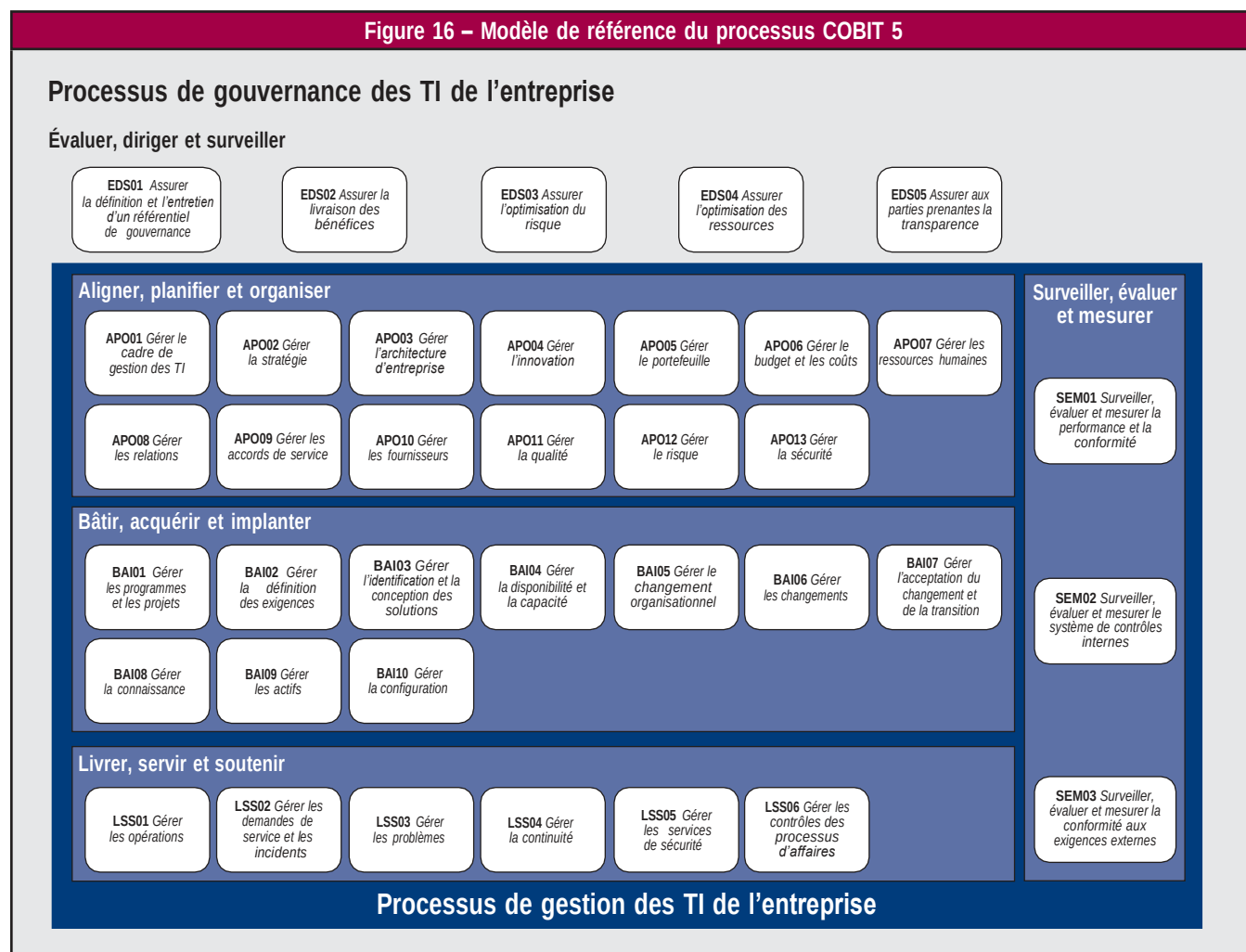
⁵ Dans le contexte du domaine de gouvernance, le mot « surveillance » désigne les activités où le groupe de gouvernance vérifie dans quelle mesure l'orientation qui a été définie pour la gestion est effectivement appliquée.

avec la qualité ou la sécurité), chacun d'eux est placé dans les domaines correspondant au secteur d'activité le plus pertinent si l'on considère les TI d'un point de vue général.

Le modèle de référence de processus de COBIT 5 représente l'évolution du modèle de processus de COBIT 4.1, avec l'intégration des modèles de processus de Risk IT et de Val IT.

La **figure 16** montre l'ensemble des 37 processus de gouvernance et de gestion de COBIT 5. Les détails de tous les processus, selon le modèle de référence décrit précédemment, sont inclus dans *COBIT 5: Processus facilitateurs*.

Figure 16 – Modèle de référence du processus COBIT 5



CHAPITRE 7

ORIENTATIONS DE MISE EN ŒUVRE

Introduction

Toute entreprise peut optimiser sa valeur en tirant profit de COBIT, pour autant qu'elle se l'approprie et l'adapte à son contexte particulier. Chaque approche de mise en œuvre sera assortie d'un lot de défis particuliers, dont la gestion des changements culturels et comportementaux.

L'ISACA fournit des orientations de mise en œuvre pratiques et approfondies dans sa publication *COBIT 5 Mise en œuvre*,⁶ qui se base sur une approche d'amélioration continue. Ce document ne se veut pas une approche normative, ni une solution exhaustive, mais plutôt un guide pour éviter les pièges couramment rencontrés, pour tirer parti des bonnes pratiques et pour contribuer à l'atteintes de résultats. Le guide comprend également une trousse d'outils de mise en œuvre contenant une variété de ressources qui seront continuellement améliorées. Son contenu comprend :

- Des outils d'autoévaluation, de mesure et de diagnostic
- Des présentations destinées à différents publics
- Des articles connexes et des explications supplémentaires

Le but de ce chapitre est d'introduire sommairement la mise en œuvre et l'approche d'amélioration continue et de mettre en évidence un certain nombre de sujets importants tirés de *COBIT 5 Mise en œuvre* tels que :

- Préparer un dossier d'affaires pour la mise en œuvre et l'amélioration de la gouvernance et de la gestion des TI.
- Reconnaître les points sensibles typiques et les événements déclencheurs.
- Créer un contexte propice à la mise en œuvre.
- Tirer parti de COBIT pour repérer les lacunes et orienter l'élaboration de facilitateurs tels que les politiques, les processus, les principes, les structures organisationnelles, les rôles et les responsabilités.

Tenir compte du contexte de l'entreprise

La gouvernance et la gestion des TI de l'entreprise ne se font pas en vase clos. Chaque entreprise doit concevoir son propre plan de mise en œuvre en fonction de facteurs environnementaux internes ou externes qui lui sont propres, tels que :

- L'éthique et la culture
- Les lois, les règlements et les politiques applicables
- La mission, la vision et les valeurs
- Les politiques et les pratiques de gouvernance
- Le plan d'affaires et les intentions stratégiques
- Le modèle d'exploitation et son niveau de maturité
- Le style de gestion
- La tolérance au risque
- Les capacités et les ressources disponibles
- Les pratiques de l'industrie

Il est également important de tirer parti des facilitateurs de gouvernance existants.

L'approche optimale pour la gouvernance et la gestion des TI sera différente pour chaque organisation. Le contexte doit être compris et considéré afin de s'approprier COBIT et de l'adapter efficacement dans la mise en œuvre des facilitateurs pour la gouvernance et la gestion des TI de l'entreprise. Les concepts de COBIT sont souvent étayés par d'autres référentiels, bonnes pratiques et normes. Ces derniers doivent aussi être adaptés aux contextes particuliers.

Les facteurs clés de succès pour une mise en œuvre réussie sont les suivants :

- Les membres de la direction doivent fournir une orientation et un mandat pour l'initiative, ainsi qu'un engagement et un soutien continus et visibles.
- Toutes les parties soutenant les processus de gouvernance et de gestion doivent comprendre les activités et les objectifs des TI.
- Assurer une communication efficace ainsi que l'habilitation des changements nécessaires.
- Ajuster COBIT et les autres bonnes pratiques et normes pour s'adapter au contexte particulier de l'entreprise.
- Mettre l'accent sur les gains rapides et prioriser les améliorations les plus profitables qui sont les plus faciles à mettre en œuvre.

⁶ www.isaca.org/cobit

Créer un environnement approprié

Il est important que les initiatives de mise en œuvre tirant parti de COBIT soient correctement dirigées et gérées. La plupart des initiatives liées aux TI échouent en raison d'une orientation, d'une supervision ou d'un soutien inadéquats de la part des différentes parties prenantes concernées; il en est de même pour la mise en œuvre de facilitateurs de gouvernance ou de gestion des TI tirant profit de COBIT. Le soutien et l'orientation des principales parties prenantes sont essentiels afin que les améliorations proposées soient adoptées et maintenues. Dans un environnement d'entreprise fragile (caractérisé par un modèle d'exploitation global imprécis ou par un manque de facilitateurs de gouvernance à l'échelle de l'entreprise), ce soutien et cette participation sont d'autant plus importants.

Les facilitateurs s'appuyant sur COBIT doivent fournir une solution qui répond aux besoins et aux problèmes réels de l'entreprise plutôt que d'être une fin en soi. Les exigences fondées sur les points sensibles et les motivations du moment doivent être définies et acceptées par la gestion comme étant des domaines qui doivent être pris en charge. Les bilans de santé, les diagnostics ou les évaluations de capacité de haut niveau basés sur COBIT constituent d'excellents outils pour sensibiliser, créer un consensus et susciter un engagement à agir. L'engagement et l'adhésion des parties prenantes doivent être sollicités dès le début. Pour y parvenir, les objectifs et les avantages de la mise en œuvre doivent être clairement exprimés en termes d'affaires et résumés dans un plan d'affaires sommaire.

Une fois que l'engagement a été obtenu, des ressources adéquates doivent être disponibles pour soutenir le projet. Les rôles et les responsabilités clés du projet doivent être définis et assignés et des mesures doivent être prises sur une base continue afin de maintenir l'engagement de toutes les parties prenantes concernées.

Des structures et des processus de surveillance et d'orientation appropriés doivent être établis et maintenus. Ceux-ci doivent également être en harmonie constante avec la gouvernance de l'entreprise et les approches de gestion des risques.

Un soutien et un engagement palpables doivent être démontrés par les parties prenantes clés, dont le conseil d'administration et les dirigeants, afin de donner le ton et de s'assurer de l'engagement de tous les intervenants du projet.

Reconnaître les points sensibles et les événements déclencheurs

Il existe un certain nombre de facteurs qui peuvent indiquer la nécessité d'améliorer la gouvernance et la gestion des TI de l'entreprise.

En utilisant les points sensibles ou les événements déclencheurs comme points de départ pour des initiatives de mise en œuvre, le dossier d'affaires visant l'amélioration de la gouvernance ou de la gestion des TI de l'entreprise peut être lié à des enjeux pratiques quotidiens vécus par l'entreprise. Cette pratique permet d'améliorer l'adhésion et de créer un sentiment d'urgence au sein de l'entreprise pour donner le coup d'envoi de la mise en œuvre. De plus, des gains rapides peuvent être identifiés et une valeur ajoutée peut être démontrée dans les domaines de l'entreprise les plus visibles ou reconnaissables. Ces éléments servent de plateforme pour introduire de nouveaux changements et peut aider à obtenir un engagement et un appui massif de la haute direction envers des changements plus importants.

Voici des exemples de quelques-uns des points sensibles courants pour lesquels une gouvernance ou une gestion nouvelle ou améliorée des facilitateurs des TI peut être une solution (ou une partie de la solution), comme le mentionne *COBIT 5 Mise en œuvre* :

- Une frustration des parties prenantes des lignes d'affaires liée à des initiatives qui ont échoué, à la hausse des coûts des TI et à une perception de faible valeur pour l'entreprise.
- Des incidents importants liés aux risques des TI, comme une perte de données ou l'échec d'un projet.
- Des problèmes de prestation de services en sous-traitance, par exemple une incapacité constante à répondre aux niveaux de service convenus.
- Le non-respect des exigences réglementaires ou contractuelles.
- La limitation par les TI des capacités d'innovation et de l'agilité de l'entreprise.
- Des résultats d'audits faisant régulièrement état de la piètre performance des TI ou de problèmes concernant la qualité des services des TI.
- Des dépenses en TI masquées et indésirables.
- La duplication ou le chevauchement entre les initiatives ou le gaspillage des ressources, par exemple la fin prématurée du projet.
- L'insuffisance des ressources en TI, un personnel épuisé, insatisfait ou aux compétences inadéquates.
- Des changements liés aux TI qui ne respectent pas les besoins de l'entreprise et livrés en retard ou dépassant les budgets.

- Des membres du conseil d'administration, des dirigeants ou des cadres supérieurs qui sont réticents à s'engager avec les TI, ou un manque d'engagement et de satisfaction des promoteurs d'affaires envers les TI.
- Des modèles complexes d'exploitation des TI.

En plus de ces points sensibles, d'autres événements dans le contexte interne et externe de l'entreprise peuvent soulever des préoccupations à l'égard de la gouvernance et la gestion des TI. Voici des exemples tirés du chapitre 3 de la publication *COBIT 5 Mise en œuvre* :

- Fusion, acquisition ou démantèlement
- Changement dans le marché, l'économie ou la position concurrentielle
- Changement dans le modèle de fonctionnement de l'entreprise ou dans les ententes d'approvisionnement
- Nouvelles exigences réglementaires ou de conformité
- Changement technologique important ou changement de paradigme
- Attention envers la gouvernance à l'échelle de l'entreprise ou du projet
- Nouveau chef de la direction, directeur financier, dirigeant principal de l'information, etc.
- Audit externe ou évaluations par des consultants
- Nouvelle stratégie ou priorité d'entreprise

Favoriser le changement

Une mise en œuvre réussie dépend du choix du changement (les facilitateurs appropriés de gouvernance ou de gestion) et de la façon de le faire. Dans de nombreuses entreprises, l'accent est mis sur le premier aspect, soit la gouvernance ou la gestion principale des TI, mais sans qu'il y ait suffisamment d'accent sur la gestion des aspects humains, comportementaux et culturels du changement ainsi que sur la motivation des parties prenantes à accepter le changement.

Il ne faut pas supposer que les différentes parties prenantes concernées ou touchées par des facilitateurs nouveaux ou améliorés accepteront et adopteront facilement le changement. La possibilité de l'ignorance ou de la résistance au changement doit être abordée au moyen d'une approche structurée et proactive. De même, il faut effectuer une sensibilisation optimale au projet de mise en œuvre grâce à un plan de communication qui définit ce qui sera communiqué, de quelle manière, par qui et ce tout au long des différentes étapes du programme.

Une amélioration durable peut être obtenue par l'engagement des parties prenantes (investissement pour gagner les cœurs et les esprits, obtenir du temps de la part des dirigeants et communiquer avec le personnel et répondre à ses attentes) ou, lorsque cela est encore requis, en faisant respecter la conformité (investissement dans les processus de gestion, de surveillance et de mise en exécution). En d'autres termes, les barrières humaines, comportementales et culturelles doivent être surmontées afin qu'il y ait un intérêt commun à adopter correctement ce changement et à assurer la capacité de l'adopter.

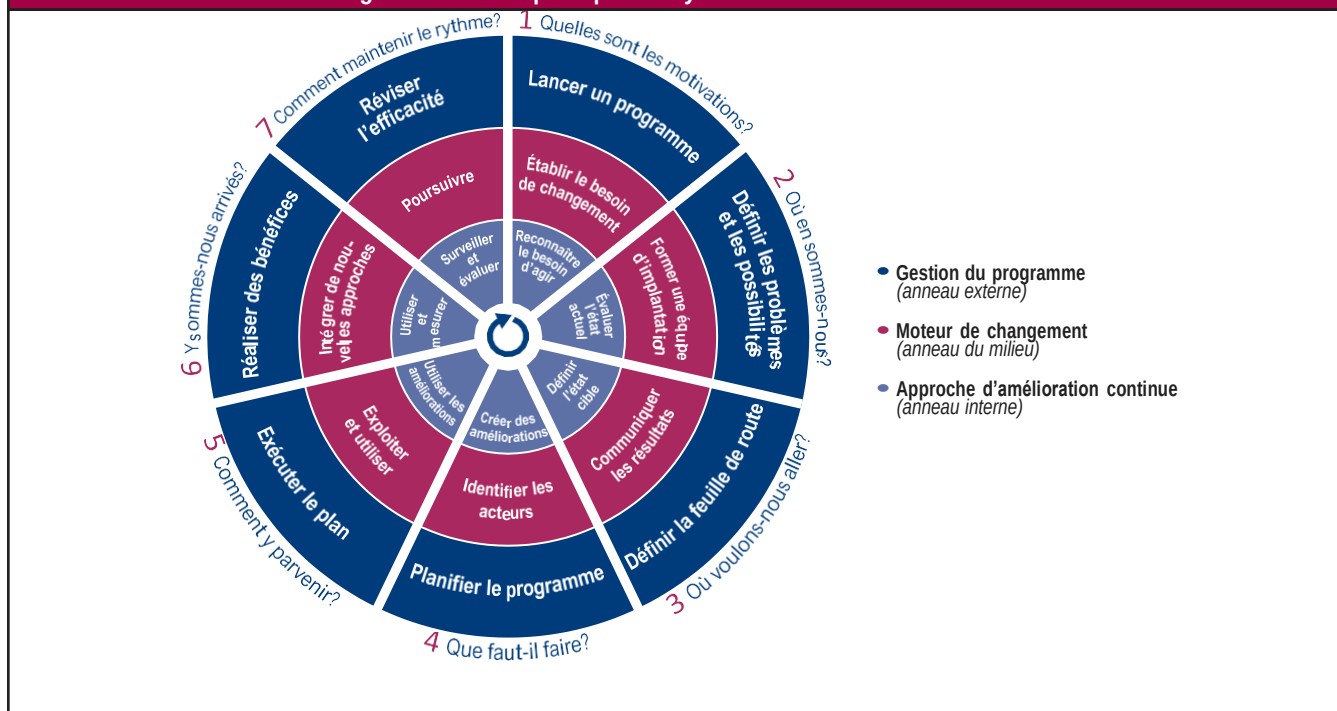
Une approche fondée sur le cycle de vie

Le cycle de vie de la mise en œuvre fournit aux entreprises une façon d'utiliser COBIT pour aborder la complexité et les défis qui se présentent généralement lors de sa mise en œuvre. Les trois éléments interreliés du cycle de vie sont :

1. Un processus d'amélioration continue – Il ne s'agit pas d'un projet ponctuel
2. La facilitation du changement – Aborder les aspects comportementaux et culturels
3. La gestion du projet

Comme mentionné précédemment, il faut créer un contexte favorable qui garantisse le succès de l'initiative de mise en œuvre ou d'amélioration. La **figure 17** illustre les sept étapes du cycle de vie.

Figure 17 – Les sept étapes du cycle de vie de la mise en œuvre



L'**étape 1** commence par le constat d'un besoin de mise en œuvre ou d'amélioration et le consentement à une telle initiative. Elle cerné les points sensibles et les déclencheurs actuels, et crée un désir de changement au sein de la haute direction.

L'**étape 2** se concentre sur la définition de la portée de l'initiative de mise en œuvre ou d'amélioration en se servant de COBIT pour mettre en correspondance les objectifs d'entreprise, les objectifs liés aux TI et les processus TI connexes, et en tenant compte des scénarios de risque qui pourraient également mettre en évidence des processus clés à cibler. Des diagnostics de haut niveau peuvent aussi être utiles pour cerner la portée et comprendre les domaines à prioriser. Une évaluation de l'état actuel doit ensuite être effectuée, de même qu'une évaluation de la capacité du processus pour cerner les problèmes ou lacunes. Les initiatives à grande échelle doivent être structurées sous forme d'itérations multiples du cycle de vie – pour toute initiative de mise en œuvre s'échelonnant sur plus de six mois, il existe un risque d'essoufflement, de perte de concentration et de démotivation des parties prenantes.

Durant l'**étape 3**, il faut fixer une cible d'amélioration, suivie d'une analyse détaillée tirant parti des orientations de COBIT pour repérer des lacunes et définir des solutions possibles. Certaines solutions peuvent produire des résultats instantanés, alors que d'autres peuvent être plus complexes et à plus long terme. La priorité doit être accordée aux initiatives faciles à appliquer et à celles susceptibles d'offrir les plus grands avantages.

L'**étape 4** vise à cerner des solutions pratiques en définissant des projets appuyés par des dossiers d'affaires justifiables. Un plan de changement est également élaboré pour la mise en œuvre. Un dossier d'affaires bien étayé contribue à assurer que les avantages du projet sont définis et surveillés.

Les solutions proposées sont appliquées aux pratiques quotidiennes durant l'**étape 5**. Il est possible de définir les mesures et d'établir une surveillance à l'aide des objectifs et des indicateurs de COBIT, afin d'assurer l'atteinte et le maintien de l'alignement d'affaires et afin que la performance puisse être mesurée. La réussite nécessite la participation et l'engagement actif de la haute direction ainsi que son appropriation par les parties prenantes d'affaires et des TI concernées.

L'**étape 6** est axée sur l'exploitation durable des nouveaux facilitateurs et ceux améliorés ainsi que sur la surveillance de la réalisation des bénéfices attendus.

Au cours de l'**étape 7**, la réussite globale de l'initiative est révisée, des exigences supplémentaires pour la gouvernance et la gestion des TI de l'entreprise sont identifiées et le besoin d'amélioration continue est renforcé.

Au fil du temps, le cycle de vie doit être répété pour que se bâtisse une approche durable quant à la gouvernance et à la gestion des TI de l'organisation.

Pour commencer : réaliser le dossier d'affaires

Pour que la mise en œuvre des initiatives issues de COBIT soit un succès, le besoin d'agir doit être largement reconnu et communiqué au sein de l'entreprise. Cela peut prendre la forme d'un appel à l'action (où l'on discute de points critiques précis, comme mentionné précédemment) ou d'une annonce d'une occasion d'amélioration à saisir et avant tout, des bénéfices qui en découleront. Il faut insuffler le juste sentiment d'urgence : les principales parties prenantes doivent prendre conscience des risques associés à l'inaction ainsi que des bénéfices d'entreprendre le programme.

L'initiative doit être prise en charge par un promoteur, impliquer toutes les parties prenantes majeures et être fondée sur un dossier d'affaires. En premier lieu, il peut être de haut niveau d'un point de vue stratégique, orienté du général au particulier : d'une bonne compréhension des objectifs organisationnels souhaités et en progressant vers une description détaillée des tâches critiques et des jalons cruciaux ainsi que des rôles et responsabilités clés. Le dossier d'affaires constitue un outil précieux à la disposition de la direction pour orienter la création de valeur. Il devrait comprendre au minimum les éléments suivants :

- Les bénéfices organisationnels ciblés, leur harmonisation avec la stratégie d'entreprise et les responsables concernés (ceux qui, au sein de l'entreprise, veilleront à la réalisation des bénéfices). Cet aspect peut être fondé sur des points critiques et des événements déclencheurs.
- Les changements organisationnels nécessaires pour créer la valeur souhaitée. Cet aspect peut être fondé sur des bilans de santé et des analyses d'écart de capacité. Les éléments inclus dans la portée et ceux qui en sont exclus doivent être indiqués clairement.
- Les investissements nécessaires pour apporter les changements en gouvernance et gestion des TI de l'entreprise (selon les estimations des projets requis).
- Les coûts continus administratifs et de TI.
- Les avantages que l'on espère tirer de cette nouvelle façon de fonctionner.
- Les risques intrinsèques aux éléments mentionnés précédemment, y compris toute contrainte ou dépendance (fondée sur les obstacles et les facteurs de réussite).
- Les rôles, les responsabilités et les approbations associés à l'initiative.
- Les moyens de contrôler l'investissement et la création de valeur tout au long du cycle de vie économique, ainsi que les indicateurs à utiliser (en fonction des objectifs et des indicateurs).

Le dossier d'affaires n'est pas un document statique, mais un outil opérationnel évolutif qui doit être mis à jour continuellement afin d'être représentatif de la vision actuelle de l'avenir. De cette manière, il sera toujours possible d'évaluer la viabilité du programme.

Les avantages des initiatives de mise en œuvre ou d'amélioration peuvent être difficiles à quantifier. Il faut prendre soin de choisir uniquement les bénéfices qui sont réalistes et réalisables. Des études menées dans différentes entreprises pourraient fournir de l'information utile à propos des avantages réalisés.

EXEMPLE 6 – STATISTIQUES SUR LA GOUVERNANCE DES TI

ITGI a commandé une analyse de marché sur la gouvernance des TI⁷ auprès de PwC. Plus de 800 répondants du domaine des TI et des affaires dans 21 pays y ont participé. 38 % des répondants ont mentionné une baisse des coûts en TI comme résultat des pratiques de gouvernance des TI; 28,1 % ont mentionné une compétitivité accrue et 27,1 % ont indiqué que le rendement de leurs investissements en TI avait augmenté. Différents avantages moins tangibles ont également été mentionnés parmi lesquels une meilleure gestion des risques liés aux TI (42,2 % des répondants), de meilleures communications et relations entre les activités d'entreprise et les TI (39,6 % des répondants) et une meilleure livraison des objectifs d'entreprise grâce aux TI (37,3 % des répondants).

L'ISACA a de plus entrepris des recherches⁸ qui explorent et démontrent la valeur de COBIT. L'ensemble de données issues des recherches offre de nombreuses possibilités d'analyse et précise la relation entre la gouvernance des TI et la performance de l'entreprise.

Une autre étude, menée auprès de 250 entreprises partout dans le monde, a permis de conclure qu'à objectifs égaux, les entreprises ayant une gouvernance des TI supérieure profitaient d'une rentabilité d'au moins 20 % supérieure à celle des entreprises ayant une piètre gouvernance⁹. Elle soutient que la valeur des TI pour l'entreprise découle directement d'une bonne gouvernance des TI.

Enfin, un autre cas de recherche, qui portait sur l'industrie du transport aérien, a conclu que la mise en œuvre et l'audit continu de la gouvernance des TI restaure la confiance entre les lignes d'affaires et les TI. Elle contribue également à une meilleure harmonisation des investissements aux objectifs stratégiques. D'autres avantages tangibles ont aussi été rapportés dans ce cas, incluant la baisse des coûts de continuité en TI par unité d'affaires et le dégagement de fonds pour l'innovation. D'autres recherches croisées dans le secteur des finances ont démontré que les organisations profitant d'une meilleure gouvernance des TI se classaient plus haut au chapitre de l'harmonisation entre les activités de l'entreprise et des TI¹⁰.

CHAPITRE 8

LE MODÈLE DE CAPACITÉ DES PROCESSUS DE COBIT 5

Introduction

Les utilisateurs de COBIT 4.1, de Risk IT et de Val IT connaissent les modèles de maturité des processus compris dans ces référentiels. Ces modèles servent à mesurer la maturité actuelle des processus liés aux TI d'une entreprise, à définir l'état de maturité souhaité, et à déterminer l'écart entre les deux ainsi que les moyens d'améliorer les processus de manière à obtenir la maturité désirée.

Les outils de COBIT 5 comprennent un modèle de capacité des processus fondé sur la norme reconnue mondialement ISO/CEI 15504 Génie logiciel – Norme d'évaluation des processus. Ce modèle permet d'atteindre les mêmes objectifs généraux d'évaluation et de soutien dans un contexte d'amélioration des processus, c'est-à-dire qu'il fournit un moyen de mesurer la performance de n'importe quel processus de gouvernance (fondé sur l'évaluation, la direction et la surveillance – « EDS ») ou de gestion (fondé sur la planification, la construction, l'exécution et la surveillance – « PCES »), et permet de cerner les domaines à améliorer.

Cependant, le nouveau modèle se distingue du modèle de maturité de COBIT 4.1 dans sa conception et son utilisation. C'est pour cette raison que les sujets qui suivent sont abordés :

- Différences entre les modèles de COBIT 5 et de COBIT 4.1
- Avantages du modèle COBIT 5
- Résumé des différences que les utilisateurs de COBIT 5 observeront dans la pratique
- Exécution d'une analyse de capacité selon COBIT 5

Les détails de l'approche de COBIT 5 quant à l'évaluation de la capacité se trouvent dans la publication de l'ISACA intitulée *COBIT® Process Assessment Model (PAM): Using COBIT® 4.1*.¹¹

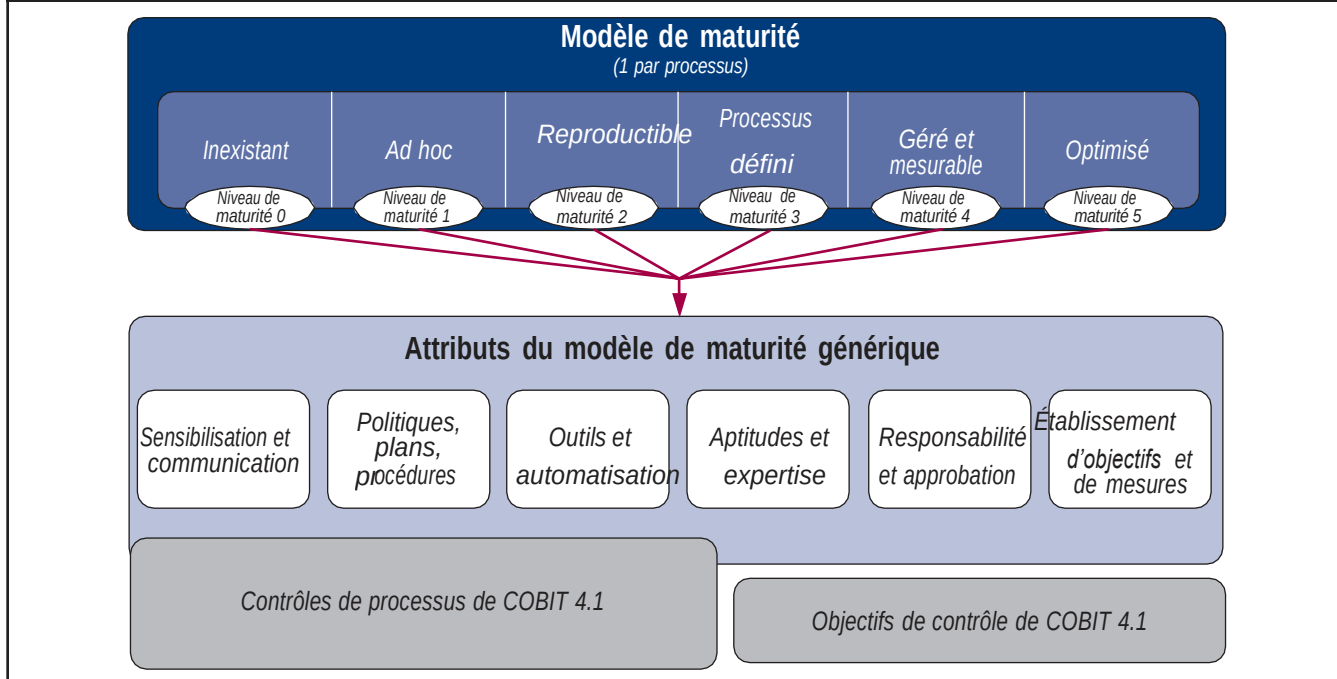
Même si cette approche fournit des renseignements précieux à propos de l'état des processus, ces derniers ne sont qu'un des sept facilitateurs en gouvernance et en gestion. Par conséquent, l'évaluation des processus ne permet pas de dresser un tableau complet de l'état de la gouvernance d'une entreprise. En effet, il faut également évaluer les autres facilitateurs.

Différences entre le modèle de maturité de COBIT 4.1 et le modèle de capacité des processus de COBIT 5

Les éléments du modèle de maturité de COBIT 4.1 sont illustrés à la **figure 18**.

¹¹ www.isaca.org/cobit-pam

Figure 18 – Résumé du modèle de maturité de COBIT 4.1

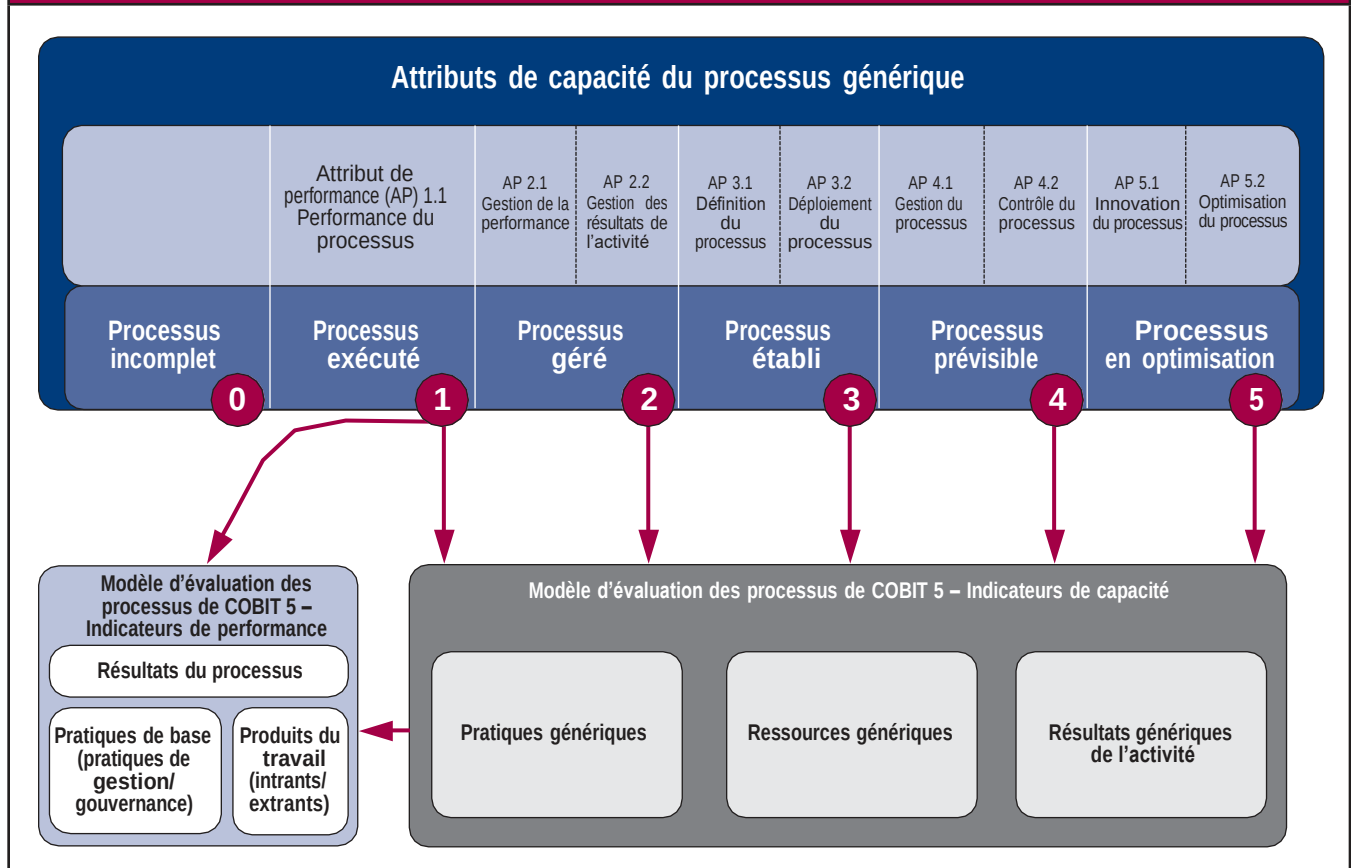


L'utilisation du modèle de maturité de COBIT 4.1 pour améliorer les processus (évaluation de la maturité du processus, définition de la cible de maturité et repérage des écarts) exigeait de recourir aux éléments de COBIT 4.1 suivants :

- Premièrement, évaluer si les objectifs de contrôle du processus étaient atteints.
- Ensuite, déterminer le profil de maturité du processus visé au moyen du modèle inclus dans les directives de gestion relatives à chaque processus.
- De plus, obtenir une perspective détaillée du niveau de maturité des processus en appliquant à chacun les six attributs distincts du modèle de maturité générique de COBIT 4.1.
- Enfin, puisque les contrôles de processus répondent aux objectifs de contrôle génériques, les passer en revue lors de chaque évaluation de processus. Soulignons que les contrôles des processus chevauchent partiellement les attributs du modèle de maturité générique.

L'approche de COBIT 5 quant à la capacité des processus peut être résumée de la façon illustrée à la **figure 19**.

Figure 19 – Résumé du modèle de capacité des processus de COBIT 5



Il existe six niveaux de capacité qu'un processus peut atteindre, y compris un niveau « processus incomplet » si les pratiques ne permettent pas de réaliser l'objectif désiré :

- **0 Processus incomplet** – Le processus n'est pas mis en œuvre ou ne parvient pas à réaliser la fonction désirée. À ce niveau, il y a peu de preuves, voire aucune, que l'objectif du processus est atteint systématiquement.
- **1 Processus exécuté** (un attribut) – Le processus mis en œuvre réalise la fonction désirée.
- **2 Processus géré** (deux attributs) – Le processus exécuté décrit précédemment est maintenant mis en œuvre et bien géré (planifié, surveillé et ajusté), et ses résultats sont adéquatement établis, contrôlés et maintenus.
- **3 Processus établi** (deux attributs) – Le processus géré décrit précédemment est maintenant mis en œuvre selon une procédure définie qui permet l'atteinte des résultats souhaités.
- **4 Processus prévisible** (deux attributs) – Le processus établi décrit précédemment fonctionne maintenant selon des limites définies qui assurent l'atteinte des résultats souhaités.
- **5 Processus en optimisation** (deux attributs) – Le processus prévisible décrit précédemment est amélioré continuellement afin d'atteindre les objectifs d'affaires pertinents actuels et projetés.

Chaque niveau de capacité ne peut être atteint que lorsque les critères du niveau précédent sont entièrement satisfaits. À titre d'exemple, une capacité de niveau 3 (processus établi) exige que les attributs de définition et de déploiement du processus soient satisfaits en grande partie, en plus de la satisfaction complète des attributs d'une capacité de niveau 2 (processus géré).

Il existe une distinction importante entre le niveau de capacité 1 et les niveaux supérieurs. L'atteinte du niveau 1 exige que les attributs de performance du processus soient satisfaits en grande partie, ce qui signifie concrètement que le processus est exécuté avec succès et que l'entreprise obtient les résultats souhaités. Quant aux niveaux de capacité supérieurs, différents attributs s'ajoutent. Selon ce modèle d'évaluation, l'atteinte du niveau de capacité 1, même sur une échelle de 5, constitue déjà une réalisation importante pour une entreprise. Mentionnons que par souci de rentabilité et de faisabilité, chaque entreprise décidera de son niveau cible ou désiré, lequel sera rarement l'un des plus élevés.

Les distinctions les plus importantes entre une évaluation des capacités fondées sur ISO/CEI 15504 et le modèle de maturité de COBIT 4.1 (ainsi que les modèles de maturité par domaine semblables Val IT et Risk IT) peuvent se résumer comme suit :

- Les noms et les significations des niveaux de capacité définis dans ISO/CEI 15504 sont assez différents des niveaux de maturité des processus de COBIT 4.1 actuels.

- Dans ISO/CEI 15504, les niveaux de capacité sont définis par un ensemble de neuf attributs. Ces attributs recoupent en partie les domaines couverts par les attributs de maturité ou processus de contrôle de COBIT 4.1, mais seulement dans une certaine mesure, et de façon différente.

Les exigences relatives à un modèle de référence des processus conforme à ISO/CEI 15504:2 prescrivent que pour tout processus à évaluer, c'est-à-dire tout processus de gouvernance ou de gestion de COBIT 5, la description doit :

- Énoncer clairement l'objectif et les résultats du processus.
- Ne contenir aucun aspect du référentiel de mesure au-delà du niveau 1, ce qui veut dire qu'aucune caractéristique d'un attribut au-delà du niveau 1 ne peut figurer dans une description de processus. Le fait qu'un processus soit mesuré et surveillé ou décrit formellement, etc., ne peut être inclus dans la description du processus ni dans les pratiques ou activités de gestion énoncées plus bas. Cela signifie que les descriptions – telles qu'elles sont présentées dans *COBIT 5 : Processus facilitants* – ne contiennent que les étapes nécessaires à la réalisation des buts et des objectifs du processus.
- En conséquence de ce qui précède, les attributs communs applicables à tous les processus d'entreprise, qui ont produit les objectifs de contrôle redondants dans la publication *COBIT[®] 3^e édition* et étaient regroupés sous les objectifs de processus de contrôle (PC) dans COBIT 4.1, sont maintenant définis dans les niveaux 2 à 5 du modèle d'évaluation.

Différences dans la pratique¹²

Les descriptions ci-dessus mettent en évidence les différences pratiques découlant des changements apportés aux modèles d'évaluation des processus. Les utilisateurs doivent être conscients de ces changements et être prêts à en tenir compte dans leurs plans d'action.

Les principaux changements à considérer sont les suivants :

- Même s'il est tentant de comparer les résultats d'évaluation entre COBIT 4.1 et COBIT 5, étant donné les ressemblances apparentes entre les échelles numériques et le vocabulaire qui sert à les décrire, il est difficile de faire une telle comparaison compte tenu des différences de portée, d'orientation et d'intention illustrées à la **figure 20**.
- En général, le modèle de capacité des processus de COBIT 5 donnera des notes plus basses, comme le montre la **figure 20**. Selon le modèle de maturité de COBIT 4.1, un processus peut atteindre le niveau 1 ou 2 sans avoir réalisé tous ses objectifs; selon l'échelle du modèle de capacité de COBIT 5, cela entraînerait une note plus faible, soit 0 ou 1.

Des correspondances approximatives entre les échelles de COBIT 4.1 et de COBIT 5 sont illustrées à la **figure 20**.

- Dans le contenu détaillé de COBIT 5, il n'y a plus de modèle de maturité spécifique par processus inclus, car l'approche d'évaluation des capacités des processus de la norme ISO/CEI 15504 ne l'exige pas; en fait, elle l'interdit. L'approche définit plutôt l'information requise dans le « modèle de référence du processus » (le modèle de processus à utiliser pour l'évaluation) :
 - Description du processus et énoncé de ses objectifs
 - Pratiques de base, soit l'équivalent des pratiques de gouvernance ou de gestion du processus selon les dispositions de COBIT 5
 - Les produits du travail, soit l'équivalent des intrants et des extrants selon les dispositions de COBIT 5
- Le modèle de maturité de COBIT 4.1 produisait un profil de maturité d'une entreprise. L'objectif principal de ce profil était de cerner les caractéristiques ou attributs présentant des faiblesses précises à corriger. Les entreprises avaient recours à cette approche lorsque leur priorité était l'amélioration plutôt que le besoin d'obtenir une cote de maturité aux fins d'établissement de rapports. Le modèle d'évaluation de COBIT 5 fournit une échelle de mesure pour chaque attribut de capacité, de même que des orientations sur la manière d'appliquer cette échelle. Ainsi, pour chaque processus, une évaluation peut être faite pour chacun des neuf attributs de capacité.
- Les attributs de maturité de COBIT 4.1 et les attributs de capacité des processus de COBIT 5 ne sont pas identiques. Ils se chevauchent et correspondent dans une certaine mesure, comme le montre la **figure 21**. Les entreprises qui ont utilisé les attributs du modèle de maturité de COBIT 4.1 peuvent réutiliser leurs données d'évaluation et les reclasser conformément aux attributs d'évaluation de COBIT 5, selon la **figure 21**.

¹² De plus amples renseignements sur le nouveau programme d'évaluation de COBIT fondé sur ISO/CEI 15504 se trouvent au www.isaca.org/cobit-assessment-programme.

Figure 20 – Tableau de comparaison entre les niveaux de maturité (COBIT 4.1) et les niveaux de capacité des processus (COBIT 5)

Niveau du modèle de maturité de COBIT 4.1	Capacité de processus en fonction de ISO/CEI 15504	Contexte
5 Optimisé – Les processus ont été perfectionnés de manière à constituer de bonnes pratiques, selon les résultats de l'amélioration continue et les modèles de maturité des autres entreprises. Les TI sont intégrées pour automatiser le flux des travaux, fournir des outils d'amélioration de la qualité et de l'efficacité, et faciliter la rapidité d'adaptation de l'entreprise.	Niveau 5 : Processus en optimisation – Le processus prévisible du niveau 4 est amélioré continuellement afin d'atteindre les objectifs d'affaires pertinents actuels et projetés.	Perspective d'entreprise – Connaissance organisationnelle
4 Géré et mesurable – La direction surveille et mesure la conformité aux procédures et prend des mesures lorsque les processus semblent ne pas fonctionner efficacement. Les processus font l'objet d'une amélioration continue et fournissent de bonnes pratiques. L'automatisation et les outils sont utilisés de manière limitée ou fragmentée.	Niveau 4 : Processus prévisible – Le processus établi au niveau 3 fonctionne maintenant selon des limites définies pour atteindre les résultats souhaités.	
3 Processus défini – Les procédures ont été normalisées, documentées et communiquées par de la formation. Le respect d'un tel processus est obligatoire; il est toutefois peu probable que les écarts soient détectés. Les procédures en soi sont peu complexes, mais servent à officialiser les pratiques existantes.	Niveau 3 : Processus établi – Le processus géré de niveau 2 est maintenant mis en œuvre selon une procédure définie qui permet l'atteinte des résultats souhaités.	
	Niveau 2 : Processus géré – Le processus exécuté de niveau 1 est maintenant mis en œuvre et bien géré (planifié, surveillé et ajusté). Ses produits sont adéquatement établis, contrôlés et maintenus.	Perspective particulière – Connaissance individuelle
2 Répétable mais intuitif – Les processus ont évolué au stade où des procédures semblables sont suivies par différentes personnes entreprenant la même tâche. Il n'y a aucune formation officielle ni communication des procédures normalisées, et la responsabilité est laissée à l'individu. Compte tenu du haut degré de dépendance sur la connaissance des individus, le risque d'erreur est élevé.	Niveau 1 : Processus exécuté – Le processus mis en œuvre réalise l'objectif. Remarque : Il est possible que certains éléments classés niveau 1 selon le modèle de maturité soient classés niveau 0 selon la norme 15504, si les résultats du processus ne sont pas atteints.	
1 Initial/Ponctuel – Des preuves existent indiquant que l'entreprise a reconnu que des problèmes sont présents et doivent être réglés. Il n'existe cependant pas de processus normalisés, mais plutôt des approches <i>ponctuelles</i> qui doivent être appliquées individuellement ou au cas par cas. L'approche générale de gestion est désorganisée.		
0 Inexistant – Absence totale de processus reconnaissables. L'entreprise n'a même pas reconnu qu'il y a un problème à corriger.	Niveau 0 : Processus incomplet – Le processus n'est pas mis en œuvre ou ne parvient pas à réaliser l'objectif désiré.	

Figure 21 – Tableau de comparaison des attributs de maturité (COBIT 4.1) et des attributs de processus (COBIT 5)

Attribut de maturité de COBIT 4.1	Attribut de capacité des processus de COBIT 5								
	Performance du processus	Gestion de la performance	Gestion des résultats d'activité	Définition du processus	Déploiement du processus	Gestion du processus	Contrôle du processus	Innovation du processus	Optimisation du processus
Sensibilisation et communication									
Politiques, plans et procédures									
Outils et automatisation									
Compétences et expertise									
Responsabilité et approbation									
Établissement et mesure des objectifs									

Avantages des changements

Voici les avantages du modèle de capacité des processus de COBIT 5, comparativement aux modèles de maturité de COBIT 4.1 :

- L'accent est mis sur l'amélioration du processus exécuté afin de confirmer qu'il réalise bien sa fonction et qu'il donne les résultats requis, comme prévu.
- Un contenu simplifié grâce à l'élimination des chevauchements. En effet, pour appuyer l'évaluation d'un processus, le modèle de maturité de COBIT 4.1 nécessitait l'utilisation de plusieurs composants précis, incluant le modèle de maturité générique, les modèles de maturité des processus, les objectifs de contrôle et les processus de contrôle.
- Une meilleure fiabilité et reproductibilité des activités d'évaluation de la capacité des processus, ce qui minimise les débats et désaccords entre parties prenantes quant aux résultats d'évaluation.
- Une facilité d'utilisation accrue des résultats des évaluations de la capacité des processus puisque le nouveau modèle établit une base pour l'exécution d'évaluations plus rigoureuses et formelles, aux fins d'une utilisation interne et potentiellement externe.
- Une conformité à une norme d'évaluation des processus généralement acceptée, entraînant un fort soutien envers l'approche d'évaluation des processus sur le marché.

Exécution des évaluations de la capacité des processus dans COBIT 5

La norme ISO/CEI 15504 précise que les évaluations de la capacité des processus peuvent être exécutées pour différentes fonctions et avec différents degrés de rigueur. Les fonctions peuvent être internes, c'est-à-dire concentrées sur la comparaison entre secteurs de l'entreprise ou sur l'amélioration des processus en vue d'obtenir des bénéfices internes, ou externes, si elles sont axées sur l'évaluation formelle, les rapports et la certification.

L'approche d'évaluation de COBIT 5, fondée sur ISO/CEI 15504, continue de favoriser les objectifs suivants qui ont été des éléments clés de l'approche de COBIT depuis 2000 :

- Permettre au groupe de gouvernance et à la direction d'établir des jalons quant à la capacité des processus.
- Permettre des vérifications de l'état actuel et désiré afin d'appuyer la prise de décisions quant aux investissements consentis par le groupe de gouvernance et la direction pour améliorer les processus.
- Fournir une analyse des écarts et l'information de planification des améliorations afin d'appuyer la définition de projets d'amélioration justifiables.
- Fournir au groupe de gouvernance et à la direction des notes d'évaluation permettant de mesurer et de contrôler les capacités actuelles.

La section qui suit décrit comment effectuer une évaluation de haut niveau, selon le modèle de capacité des processus de COBIT 5, afin d'atteindre ces objectifs.

L'évaluation fait la distinction entre le niveau de capacité 1 et les niveaux supérieurs. En effet, comme décrit précédemment, le niveau de capacité 1 indique si un processus atteint l'objectif désiré. Il s'agit donc d'un niveau crucial à atteindre, car il établit les bases de l'atteinte des niveaux supérieurs.

La vérification de la réalisation des objectifs – en d'autres termes, de l'atteinte du niveau 1 – peut se faire :

1. En vérifiant les résultats des processus, tels qu'ils figurent dans les descriptions détaillées de chaque processus. À l'aide de l'échelle de notation ISO/CEI 15504, pour affecter une cote indiquant à quel degré l'objectif est réalisé. L'échelle se compose des cotes suivantes :
 - **N** (Non réalisé) – Il existe peu de preuves, voire aucune, de la réalisation de l'attribut défini dans le processus évalué. (0 % à 15 % de réalisation)
 - **P** (Partiellement réalisé) – Il existe certaines preuves d'une approche quant à l'attribut défini dans le processus évalué ainsi que de la réalisation partielle de cet attribut. Certains aspects de la réalisation de l'attribut peuvent être imprévisibles. (15 % à 50 % de réalisation)
 - **G** (Grandement réalisé) – Il existe des preuves d'une approche systématique quant à l'attribut défini dans le processus évalué ainsi que de la réalisation significative de cet attribut. Certaines faiblesses liées à l'attribut peuvent exister dans le processus évalué. (50 % à 85 % de réalisation)
 - **C** (Complètement réalisé) – Il existe des preuves d'une approche complète et systématique quant à l'attribut défini dans le processus évalué ainsi que de la réalisation complète de cet attribut. Aucune faiblesse majeure liée à l'attribut n'existe dans le processus évalué. (85 % à 100 % de réalisation)
2. De plus, les pratiques (de gouvernance ou de gestion) liées au processus peuvent être évaluées selon la même échelle de notation, exprimant le degré auquel les pratiques de base sont appliquées.
3. Afin de préciser l'évaluation, les produits du travail peuvent aussi être pris en considération dans le but de déterminer à quel point un attribut d'évaluation donné a été réalisé.

Bien que les entreprises soient libres de décider des niveaux de capacité à atteindre, la plupart voudront voir tous leurs processus atteindre une capacité de niveau 1. (Autrement, quelle serait l'utilité de tous ces processus?) Si ce niveau n'est pas atteint, les raisons en sont tout à fait évidentes étant donné l'approche décrite plus haut, et un plan d'amélioration peut être défini :

1. Si un résultat de processus obligatoire n'est pas réalisé de façon constante, le processus n'atteint pas son objectif et doit être amélioré.
2. L'évaluation des pratiques liées au processus révélera lesquelles d'entre elles sont manquantes ou échouent, ce qui permettra d'appliquer ou d'améliorer ces pratiques à mettre en place et de réaliser tous les résultats du processus.

Pour des niveaux supérieurs de capacité des processus, on se réfère aux pratiques génériques tirées d'ISO/CEI 15504:2. Celles-ci fournissent des descriptions génériques pour chacun des niveaux de capacité.

ANNEXE A

RÉFÉRENCES

Les référentiels, les normes et les autres orientations ci-dessous ont servi de documentation de référence et ont contribué à l'élaboration de COBIT 5.

Association for Project Management (APM); *APM Introduction to Programme Management*, Latimer, Trend and Co., R.-U., 2007

British Standards Institute (BSI), BS25999:2007 Business Continuity Management Standard, R.-U., 2007

CIO Council, *Federal Enterprise Architecture* (FEA), ver 1.0, É.-U., 2005

Commission européenne, *The Commission Enterprise IT Architecture Framework (CEAF)*, Belgique, 2006

Kotter, John; *Leading Change*, Harvard Business School Press, É.-U., 1996

HM Government, Best Management Practice Portfolio, *Managing Successful Programmes (MSP)*, R.-U., 2009

HM Government, Best Management Practice Portfolio, *PRINCE2[®]*, R.-U., 2009

HM Government, Best Management Practice Portfolio, *Information Technology Infrastructure Library (ITIL[®])*, 2011

Organisation internationale de normalisation (ISO), 9001:2008 Systèmes de management de la qualité, Suisse, 2008

ISO/Commission électrotechnique internationale (CEI), 20000:2006 Norme de gestion des services des TI, Suisse, 2006

ISO/CEI, 27005:2008, Norme sur la gestion des risques liés à la sécurité de l'information, Suisse, 2008

ISO/CEI, 38500:2008, Norme sur la gouvernance des technologies de l'information par l'entreprise, Suisse, 2008

King Code of Governance Principles (King III), Afrique du Sud, 2009

Organisation de coopération et de développement économiques (OCDE), *Principes du gouvernement d'entreprise de l'OCDE*, France, 2004

The Open Group, TOGAF[®] 9, R.-U., 2009

Project Management Institute, Project Management Body of Knowledge (PMBOK2[®]), É.-U., 2008

UK Financial Reporting Council, 'Combined Code on Corporate Governance', R.-U., 2009

ANNEXE B

CORRESPONDANCE DÉTAILLÉE ENTRE LES OBJECTIFS D'ENTREPRISE ET LES OBJECTIFS LIÉS AUX TI

La cascade d'objectifs de COBIT 5 est expliquée au chapitre 2.

Le tableau de correspondance à la **figure 22** a pour fonction de démontrer comment les objectifs d'entreprise sont soutenus par les objectifs liés aux TI ou se traduisent en ceux-ci. Pour cela, le tableau contient l'information suivante :

- Dans les colonnes, les 17 objectifs génériques d'entreprise définis dans COBIT 5, regroupés par caractéristiques de la carte de pointage équilibrée.
- Dans les rangées, les 17 objectifs liés aux TI, également groupés dans les dimensions du tableau de bord prospectif (TBP) des TI.
- Une correspondance de la façon dont chaque objectif d'entreprise est appuyé par des objectifs de TI. Cette correspondance est exprimée en utilisant l'échelle suivante :
 - « P » signifie primaire, lorsqu'il y a une relation importante, c'est-à-dire que l'objectif lié aux TI sert d'appui primaire à l'objectif d'entreprise.
 - « S » signifie secondaire, lorsqu'il y a une relation forte, mais d'importance moindre, c'est-à-dire que l'objectif lié aux TI sert d'appui secondaire à l'objectif d'entreprise.

EXEMPLE 7 – TABLEAU DE CORRESPONDANCE

Le tableau de correspondance suggère que l'on peut normalement avoir les attentes suivantes :

- L'objectif d'entreprise 7. Continuité et disponibilité des services d'entreprise :
 - Dépend principalement de la réalisation des objectifs liés aux TI ci-dessous :
 - 04 Gestion du risque d'affaires lié aux TI
 - 10 Sécurité de l'information, des infrastructures de traitement et des applications
 - 14 Disponibilité d'informations fiables et utiles pour la prise de décision
 - Dépend également, mais à un degré moindre, de la réalisation des objectifs liés aux TI ci-dessous :
 - 01 Alignement des TI et de la stratégie d'affaires
 - 07 Livraison de services des TI conformes aux exigences opérationnelles
 - 08 Utilisation adéquate des applications, de l'information et de solutions technologiques
- Si on utilise le tableau dans le sens inverse, on réalise que l'objectif lié aux TI « 09. Agilité des TI » contribuera à l'atteinte de plusieurs objectifs :
 - Principalement, les objectifs d'entreprise suivants :
 - 2. Portefeuille de produits et services concurrentiels
 - 8. Réponses agiles à un environnement d'affaires en évolution
 - 11. Optimisation de la fonctionnalité des processus d'affaires
 - 17. Culture d'innovation des produits et des affaires
 - À un degré moindre, les objectifs d'entreprise suivants :
 - 1. Valeur pour les parties prenantes des investissements d'affaires
 - 3. Gestion du risque d'affaires (protection des actifs)
 - 6. Culture de service orientée client
 - 13. Programmes de gestion du changement en entreprise
 - 14. Productivité opérationnelle et productivité du personnel
 - 16. Personnes qualifiées et motivées

Le tableau a été créé sur la base des intrants suivants :

- Recherches menées par la University of Antwerp Management School IT Alignment and Governance Research Institute
- Des examens complémentaires et des avis d'experts obtenus au cours du processus d'élaboration et d'examen de COBIT 5

Lors de l'utilisation du tableau de la figure 22, veuillez tenir compte des remarques formulées dans le chapitre 2 sur la façon d'utiliser la cascade d'objectifs de COBIT 5.

Figure 22 – Correspondance entre les objectifs d'entreprise de COBIT 5 et les objectifs liés aux TI																			
			Objectif d'entreprise																
			Valeur pour les parties prenantes des investissements d'affaires	Portefeuille de produits et services concurrentiels	Gestion du risque d'affaires (protection des actifs)	Conformité aux lois et aux réglementations	Transparence financière	Culture de service orientée client	Continuité et disponibilité des services d'affaires	Réponses agiles à un environnement d'affaires en évolution	Prise de décisions stratégiques basées sur l'information	Optimisation des coûts de livraison des services	Optimisation de la fonctionnalité des processus d'affaires	Optimisation des coûts des processus d'affaires	Programmes de gestion du changement en entreprise	Productivité opérationnelle et productivité du personnel	Conformité avec les politiques internes	Personnes qualifiées et motivées	Culture d'innovation des produits et des affaires
			1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.
Objectif lié aux TI			Financier				Client				Interne				Apprentissage et croissance				
Financier	01	Alignement des TI et de la stratégie d'affaires	P	P	S			P	S	P	P	S	P	S	P			S	S
	02	Conformité des TI et soutien à la conformité de l'entreprise aux lois et à la réglementation			S	P										P			
	03	Engagement de la haute direction dans la prise de décisions liées aux TI	P	S	S					S	S		S		P			S	S
	04	Gestion du risque d'affaires lié aux TI			P	S			P	S		P			S		S	S	
	05	Bénéfices réalisés sur les investissements en TI et sur le portefeuille de services	P	P				S		S		S	S	P		S			S
	06	Transparence des coûts, des bénéfices et des risques des TI	S		S		P				S	P		P					
Client	07	Livraison de services des TI conformes aux exigences opérationnelles	P	P	S	S		P	S	P	S		P	S	S			S	S
	08	Utilisation adéquate des applications, de l'information et de solutions technologiques	S	S	S			S	S		S	S	P	S		P		S	S
Interne	09	Agilité des TI	S	P	S			S		P			P		S	S		S	P
	10	Sécurité de l'information, des infrastructures de traitement et des applications			P	P			P								P		
	11	Optimisation des actifs, des ressources et des capacités des TI	P	S						S		P	S	P	S	S			S
	12	Mise en œuvre et soutien des processus d'affaires par leur intégration dans les applications et les technologies	S	P	S			S		S		S	P	S	S	S			S
	13	Livraison de programmes procurant des avantages, en temps opportun, en respectant le budget, les exigences et les normes de qualité	P	S	S			S				S		S	P				
	14	Disponibilité d'informations fiables et utiles pour la prise de décision	S	S	S	S			P		P		S						
	15	Conformité des TI aux politiques internes			S	S											P		
Apprentissage et croissance	16	Personnel des TI et des lignes d'affaires compétent et motivé	S	S	P			S		S						P		P	S
	17	Connaissances, compétences et initiatives pour l'innovation d'affaires	S	P				S		P	S		S		S			S	P

ANNEXE C

CORRESPONDANCE DÉTAILLÉE ENTRE LES OBJECTIFS ET LES PROCESSUS LIÉS AUX TI

Cette annexe présente le tableau de correspondance entre les objectifs liés aux TI et les processus qui les appuient, dans le contexte de la cascade d'objectifs expliquée au chapitre 2.

La **figure 23** contient :

- Dans les colonnes, les 17 objectifs génériques liés aux TI définis au chapitre 2, regroupés par caractéristiques du tableau de bord prospectif (TBP) des TI.
- Dans les lignes, les 37 processus de COBIT 5, regroupés par domaine
- Une correspondance illustrant comment chaque objectif lié aux TI est appuyé par un processus de COBIT 5. Cette correspondance est exprimée en utilisant l'échelle suivante :
 - « P » signifie primaire, lorsqu'il y a une relation importante, c'est-à-dire que le processus de COBIT 5 sert d'appui primaire à l'atteinte d'un objectif lié aux TI.
 - « S » signifie secondaire, lorsqu'il y a une relation forte, mais de moindre importance, c'est-à-dire que le processus de COBIT 5 sert d'appui secondaire à l'objectif lié aux TI.

EXEMPLE 8 – APO13 GÉRER LA SÉCURITÉ

Le processus APO13 *Gérer la sécurité* contribuera :

- Principalement, à la réalisation des objectifs liés aux TI :
 - 02 Conformité des TI et soutien à la conformité de l'entreprise aux lois et à la réglementation
 - 04 Gestion du risque d'affaires lié aux TI
 - 06 Transparence des coûts, des bénéfices et des risques des TI
 - 10 Sécurité de l'information, des infrastructures de traitement et des applications
 - 14 Disponibilité de renseignements fiables et utiles pour la prise de décision
- Dans une moindre mesure, à la réalisation des objectifs liés aux TI :
 - 07 Livraison de services des TI conformes aux exigences opérationnelles
 - 08 Utilisation adéquate des applications, de l'information et des solutions technologiques

Le tableau a été créé sur la base des intrants suivants :

- Recherches menées par la University of Antwerp Management School IT Alignment and Governance Research Institute
- Des examens complémentaires et des avis d'experts obtenus au cours du processus d'élaboration et de révision de COBIT 5

Lors de l'utilisation du tableau de la figure 23, veuillez prendre en considération les remarques formulées dans le chapitre 2 sur la façon d'utiliser la cascade d'objectifs de COBIT 5.

Figure 23 – Correspondance entre les objectifs liés aux TI de COBIT 5 et les processus

			Objectif lié aux TI																
			Alignement des TI et de la stratégie d' affaires	Conformité des TI et soutien à la conformité de l' entreprise aux lois et la réglementation	Engagement de la haute direction dans la prise de décisions liées aux TI	Gestion du risque d' affaires lié aux TI	Bénéfices réalisés sur les investissements en TI et sur le portefeuille de services	Transparence des coûts, des bénéfices et des risques des TI	Livraison de services des TI conformes aux exigences opérationnelles	Utilisation adéquate des applications, de l' information et des solutions technologiques	Agilité des TI	Sécurité de l' information, des infrastructures de traitement et des applications	Optimisation des actifs, des ressources et des capacités des TI	Mise en oeuvre et soutien des processus d' affaires par leur intégration dans les applications et les technologies	Livraison de programmes procurant des avantages, en temps opportun, en respectant le budget, les exigences et les normes de qualité	Disponibilité d' informations fiables et utiles pour la prise de décision	Conformité des TI aux politiques internes	Personnel des TI et des lignes d' affaires compétent et motivé	Connaissances, compétences et initiatives pour l' innovation d' affaires
			01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
Processus COBIT 5			Financier					Client			Interne					Apprentissage et croissance			
Évaluer, diriger et surveiller	EDS01	Assurer la définition et l'entretien d'un référentiel de gouvernance	P	S	P	S	S	S	P		S	S	S	S	S	S	S	S	S
	EDS02	Assurer la livraison des bénéfices	P		S		P	P	P	S			S	S	S	S		S	P
	EDS03	Assurer l'optimisation du risque	S	S	S	P		P	S	S		P			S	S	P	S	S
	EDS04	Assurer l'optimisation des ressources	S		S	S	S	S	S	S	P		P		S			P	S
	EDS05	Assurer aux parties prenantes la transparence	S	S	P			P	P						S	S	S		S
Aligner, planifier et organiser	APO01	Gérer le cadre de gestion des TI	P	P	S	S			S		P	S	P	S	S	S	P	P	P
	APO02	Gérer la stratégie	P		S	S	S		P	S	S		S	S	S	S	S	S	P
	APO03	Gérer l'architecture d'entreprise	P		S	S	S	S	S	S	P	S	P	S		S			S
	APO04	Gérer l'innovation	S			S	P			P	P		P	S		S			P
	APO05	Gérer le portefeuille	P		S	S	P	S	S	S	S		S		P				S
	APO06	Gérer le budget et les coûts	S		S	S	P	P	S	S			S		S				
	APO07	Gérer les ressources humaines	P	S	S	S			S		S	S	P		P		S	P	P
	APO08	Gérer les relations	P		S	S	S	S	P	S			S	P	S		S	S	P
	APO09	Gérer les accords de service	S			S	S	S	P	S	S	S	S		S	P	S		
	APO10	Gérer les fournisseurs		S		P	S	S	P	S	P	S	S		S	S	S		S
	APO11	Gérer la qualité	S	S		S	P		P	S	S		S		P	S	S	S	S
	APO12	Gérer le risque		P		P		P	S	S	S	P			P	S	S	S	S
	APO13	Gérer la sécurité		P		P		P	S	S		P				P			

ANNEXE C : CORRESPONDANCE DÉTAILLÉE ENTRE LES OBJECTIFS LIÉS AUX TI ET LES PROCESSUS LIÉS AUX TI

Figure 23 – Correspondance entre les objectifs liés aux TI de COBIT 5 et les processus (suite)

			Objectif lié aux TI																
			Alignement des TI et de la stratégie d' affaires	Conformité des TI et soutien à la conformité de l' entreprise aux lois et à la réglementation	Engagement de la haute direction dans la prise de décisions liées aux TI	Gestion du risque d' affaires lié aux TI	Bénéfices réalisés sur les investissements en TI et sur le portefeuille de services	Transparence des coûts, des bénéfices et des risques des TI	Livraison de services des TI conformes aux exigences opérationnelles	Utilisation adéquate des applications, de l' information et des solutions technologiques	Agilité des TI	Sécurité de l' information, des infrastructures de traitement et des applications	Optimisation des actifs, des ressources et des capacités des TI	Mise en oeuvre et soutien des processus d' affaires par leur intégration dans les applications et les technologies	Livraison de programmes procurant des avantages, en temps opportun, en respectant le budget, les exigences et les normes de qualité	Disponibilité d' informations fiables et utiles pour la prise de décision	Conformité des TI aux politiques internes	Personnel des TI et des lignes d' affaires compétent et motivé	Connaissances, compétences et initiatives pour l' innovation d' affaires
			01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
Processus COBIT 5			Financier					Client			Interne					Apprentissage et croissance			
Bâtir, acquérir et implanter	BAI01	Gérer les programmes et les projets	P		S	P	P	S	S			S		P			S	S	
	BAI02	Gérer la définition des exigences	P	S	S	S	S		P	S	S	S	S	P	S	S			S
	BAI03	Gérer l'identification et la conception des solutions	S			S	S		P	S			S	S	S	S			S
	BAI04	Gérer la disponibilité et la capacité				S	S		P	S	S		P		S	P			S
	BAI05	Gérer le changement organisationnel	S		S		S		S	P	S		S	S	P				P
	BAI06	Gérer les changements			S	P	S		P	S	S	P	S	S	S	S	S		S
	BAI07	Gérer l'acceptation du changement et de la transition				S	S		S	P	S			P	S	S	S		S
	BAI08	Gérer la connaissance	S				S		S	S	P	S	S			S		S	P
	BAI09	Gérer les actifs		S		S		P	S		S	S	P			S	S		
	BAI10	Gérer la configuration		P		S		S		S	S	S	P			P	S		
Livrer, servir et soutenir	LSS01	Gérer les opérations		S		P	S		P	S	S	S	P			S	S	S	S
	LSS02	Gérer les demandes de service et les incidents				P			P	S		S				S	S		S
	LSS03	Gérer les problèmes		S		P	S		P	S	S		P	S		P	S		S
	LSS04	Gérer la continuité	S	S		P	S		P	S	S	S	S	S		P	S	S	S
	LSS05	Gérer les services de sécurité	S	P		P			S	S		P	S	S		S	S		
	LSS06	Gérer les contrôles des processus d'affaires		S		P			P	S		S	S	S		S	S	S	S
Surveiller, évaluer et mesurer	SEM01	Surveiller, évaluer et mesurer la performance et la conformité	S	S	S	P	S	S	P	S	S	S	P		S	S	P	S	S
	SEM02	Surveiller, évaluer et mesurer le système de contrôles internes		P		P		S	S	S		S				S	P		S
	SEM03	Surveiller, évaluer et mesurer la conformité aux exigences externes		P		P	S		S			S					S		S

ANNEXE D

BESOINS DES PARTIES PRENANTES ET OBJECTIFS D'ENTREPRISE

Le chapitre 2 montrait les étapes individuelles de la cascade d'objectifs, des besoins des parties prenantes aux objectifs facilitateurs. Le chapitre 2 incluait un tableau montrant les questions de gouvernance et de gestion typiques relativement aux TI. Pour les parties prenantes, il est intéressant de connaître la relation entre ces questions et les objectifs d'entreprise. C'est pourquoi la **figure 24** est incluse : elle montre comment les besoins des parties prenantes peuvent être liés aux objectifs d'entreprise.

Ce tableau peut servir à établir et à prioriser des objectifs d'entreprise spécifiques ou des objectifs liés aux TI, en fonction des besoins spécifiques des parties prenantes. Les mêmes précautions devraient être prises lors de l'utilisation de ces tableaux qu'avec les autres tableaux de la cascade d'objectifs. En effet, comme la situation de chaque entreprise est différente, ces tableaux ne devraient pas être pris à la lettre, mais plutôt comme un ensemble de relations génériques suggérées. Dans la **figure 24**, l'intersection entre un besoin des parties prenantes et un objectif d'entreprise est remplie seulement si ce besoin doit être pris en considération pour cet objectif.

Figure 24 – Correspondance entre les objectifs d'entreprise de COBIT 5 et les questions de gouvernance et de gestion

	Valeur pour les parties prenantes des investissements d' affaires	Portefeuille de produits et services concurrentiels	Gestion du risque d' affaires(protection des affaires)	Conformité aux lois et à la réglementation	Transparence financière	Culture de service orientée client	Continuité et disponibilité des services d' affaires	Réponses agiles dans un contexte d' affaires en évolution	Prise de décisions stratégiques basées sur l' information	Optimisation des coûts de livraison des services	Optimisation de la fonctionnalité des processus d' affaires	Optimisation des coûts des processus d' affaires	Programmes de gestion du changement du contexte d' affaires	Productivité opérationnelle et productivité du personnel	Conformité aux politiques internes	Personnes qualifiées et motivées	Culture d' innovation des produits et des affaires
BESOINS DES PARTIES PRENANTES	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.
Comment puis-je tirer profit de l'utilisation des TI? Les utilisateurs finaux sont-ils satisfaits de la qualité du service des TI?																	
Comment puis-je gérer la performance des TI?																	
Comment puis-je exploiter au mieux les nouvelles technologies pour en tirer de nouvelles opportunités stratégiques?																	
Comment puis-je bâtir et structurer au mieux mon service des TI?																	
Dans quelle mesure suis-je dépendant des fournisseurs externes? Dans quelle mesure les accords d'impartition (externalisation) des TI sont-ils bien gérés? Comment puis-je obtenir une assurance envers les fournisseurs externes?																	
Quelles sont les exigences (de contrôle) en matière d'information?																	
Ai-je considéré tous les risques liés aux TI?																	
Mon exploitation des TI est-elle efficace et résiliente?																	
Comment puis-je contrôler le coût des TI? Comment puis-je utiliser les ressources TI de la manière la plus efficace? Quelles sont les options d'impartition (externalisation) les plus efficaces?																	

Figure 24 – Correspondance entre les objectifs d'entreprise de COBIT 5 et les questions de gouvernance et de gestion (suite)

	Valeur pour les parties prenantes des investissements d' affaires	Portefeuille de produits et services concurrentiels	Gestion du risque d' affaires(protection des d' affaires)	Conformité aux lois et à la réglementation	Transparence financière	Culture de service orientée client	Continuité et disponibilité des services d' affaires	Réponses agiles dans un contexte d' affaires en évolution	Prise de décisions stratégiques basées sur l' information	Optimisation des coûts de livraison des services	Optimisation de la fonctionnalité des processus d' affaires	Optimisation des coûts des processus d' affaires	Programmes de gestion du changement du contexte d' affaires	Productivité opérationnelle et productivité du personnel	Conformité aux politiques internes	Personnes qualifiées et motivées	Culture d' innovation des produits et des affaires
BESOINS DES PARTIES PRENANTES	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.
Ai-je suffisamment de personnel pour les TI? Comment puis-je développer et maintenir leurs compétences, et comment puis-je gérer leur performance?																	
Comment puis-je obtenir une assurance envers les TI?																	
L'information que je traite est-elle bien sécurisée?																	
Comment puis-je améliorer l'agilité de l'entreprise au moyen d'un environnement des TI plus flexible?																	
Les projets en TI ne réussissent pas à livrer ce qu'ils avaient promis, si oui, pourquoi? Les TI entravent-elles l'exécution de la stratégie d'entreprise?																	
Quelle est l'importance des TI pour soutenir l'entreprise? Que dois-je faire si les TI ne sont pas disponibles?																	
Quels processus critiques de l'entreprise sont dépendants des TI et quelles sont les exigences des processus d'affaires?																	
Quel a été le dépassement moyen des budgets opérationnels des TI? À quelle fréquence et de combien les projets des TI dépassent-ils leur budget?																	
Quelle fraction de l'effort en TI sera consacré à la résolution de problèmes plutôt qu'à l'amélioration des affaires?																	
Les ressources et l'infrastructure des TI disponibles sont-elles suffisantes pour répondre aux objectifs stratégiques de l'entreprise?																	
Combien de temps faut-il pour prendre des décisions importantes en matière de TI?																	
Les efforts et les investissements en TI sont-ils transparents?																	
Les TI aident-elles l'entreprise à respecter la réglementation et les niveaux de service? Comment puis-je savoir si l'entreprise est conforme à toute la réglementation en vigueur?																	

ANNEXE E

CORRESPONDANCE ENTRE COBIT 5 ET LES NORMES ET RÉFÉRENTIELS CONNEXES LES PLUS PERTINENTS

Introduction

Cette annexe compare COBIT 5 aux normes et référentiels les plus pertinents et les plus utilisés dans le domaine de la gouvernance. Pour ISO/CEI 38500, cette comparaison se fait au moyen de ses propres principes; pour les autres comparaisons, on utilise un tableau dans lequel les processus de COBIT 5 sont mis en correspondance avec le contenu équivalent de la norme ou du référentiel auquel on fait référence.

COBIT 5 et ISO/CEI 38500

Ce qui suit résume en quoi COBIT 5 appuie l'adoption des principes standards et de l'approche de mise en œuvre. La norme ISO/CEI 38500:2008 – *Gouvernance des technologies de l'information par l'entreprise* est fondée sur six principes clés. Les implications pratiques de chacun de ces principes sont expliquées ici, tout comme les moyens par lesquels les orientations de COBIT 5 permettent une bonne pratique.

Principes ISO/CEI 38500

PRINCIPE 1 – RESPONSABILITÉ

Ce que cela signifie en pratique :

L'entreprise (le client) et les TI (le fournisseur) doivent collaborer selon un modèle de partenariat, privilégier les communications efficaces fondées sur une relation de confiance positive et identifier clairement la responsabilité et l'imputabilité de chacun. Dans les grandes entreprises, un comité exécutif des TI (aussi appelé comité stratégique des TI), agissant pour le compte du conseil d'administration et présidé par un membre de celui-ci, constitue un mécanisme efficace d'évaluation, de direction et de surveillance de l'utilisation des TI. Il s'agit également d'une excellente façon d'orienter le conseil face aux enjeux de TI cruciaux. Les dirigeants de petites et moyennes entreprises dotées d'une structure hiérarchique simple et de voies de communication brèves doivent adopter une approche plus directe quant à la supervision des activités des TI. Dans tous les cas, des structures organisationnelles de gouvernance, des rôles et des responsabilités doivent être attribués par le groupe de gouvernance afin d'établir la propriété et les approbation des décisions et des tâches importantes. Cela s'applique aussi aux relations avec les principaux fournisseurs de services de TI externes.

Comment les orientations de l'ISACA permettent une bonne pratique :

1. Le cadre de référence de COBIT 5 définit différents facilitateurs pour la gouvernance des TI en entreprise. Les facilitateurs des processus et des structures organisationnelles, combinés aux tableaux RACI¹³, sont particulièrement pertinents dans ce contexte. Ils encouragent fortement l'attribution de responsabilités et donnent des exemples de rôles et de responsabilités des membres du conseil et de la direction, et ce, pour tous les processus et activités clés.
2. Le document *COBIT 5 Mise en œuvre* explique les responsabilités des parties prenantes et autres parties concernées au moment de la mise en œuvre ou de l'amélioration des ententes de gouvernance des TI.
3. COBIT 5 propose deux niveaux de surveillance. Le premier est pertinent dans un contexte de gouvernance. Le processus EDS05 *Assurer aux parties prenantes la transparence* explique le rôle du directeur dans la surveillance et l'évaluation de la gouvernance et de la performance des TI à l'aide d'une méthode générique d'établissement des buts et objectifs ainsi que d'indicateurs connexes.

PRINCIPE 2 – STRATÉGIE

Ce que cela signifie en pratique :

La planification stratégique des TI constitue une activité complexe et critique qui exige une coordination étroite entre les unités d'affaires de toute l'entreprise et les plans stratégiques de TI. Il est également crucial d'accorder la priorité aux plans les plus susceptibles de procurer les bénéfices souhaités et d'attribuer les ressources efficacement. Les objectifs de haut niveau doivent se traduire en plans tactiques réalisables afin de minimiser les échecs et les surprises. Le but est de créer une valeur qui appuie les objectifs stratégiques tout en tenant compte des risques connexes, en fonction de la tolérance au risque du conseil d'administration. Bien qu'il soit important de définir des plans en cascade, de haut en bas, ceux-ci doivent également être souples et adaptables afin de satisfaire les exigences d'affaires et les opportunités en TI qui évoluent rapidement.

De plus, la présence ou l'absence de capacité en TI peut faciliter ou entraver les stratégies d'affaires; par conséquent, la planification stratégique des TI doit inclure une planification transparente et adéquate des capacités en TI. Cette

¹³ Les tableaux RACI décrivent qui est responsable, qui approuve, qui est consulté et qui est informé pour une tâche.

planification doit comprendre une évaluation de la capacité actuelle de l'infrastructure des TI et des ressources humaines à appuyer les exigences d'affaires futures, de même qu'une prise en considération des percées technologiques à venir qui pourraient procurer un avantage concurrentiel ou optimiser les coûts. Les ressources en TI comprennent des relations avec de nombreux fournisseurs externes de produits et de services, dont certains sont susceptibles de jouer un rôle crucial de soutien à l'entreprise. La gouvernance de l'approvisionnement stratégique est donc une activité de planification stratégique majeure exigeant une orientation et une surveillance de la part de la haute direction.

Comment les orientations de l'ISACA permettent une bonne pratique :

1. COBIT 5 fournit des orientations précises quant à la gestion des investissements en TI et (plus précisément, dans le processus EDS02 *Assurer la livraison des bénéfices* dans le domaine de gouvernance) la façon d'appuyer les objectifs stratégiques au moyen de dossiers d'affaires adéquats.
2. Le domaine APO de COBIT 5 explique les processus requis pour la planification et l'organisation efficaces des ressources en TI internes et externes, y compris la planification stratégique, la planification de la technologie et de l'architecture, la planification organisationnelle, la planification de l'innovation, la gestion du portefeuille, la gestion des investissements, la gestion du risque, la gestion des relations et la gestion de la qualité. L'alignement des objectifs d'entreprise et des TI y est également expliqué. Des exemples génériques montrent comment ces objectifs appuient les objectifs stratégiques de tous les processus liés aux TI, selon des recherches menées dans toute l'industrie.
3. L'identification et l'alignement des objectifs d'entreprise et des TI permettent une meilleure compréhension de la relation en cascade entre les objectifs d'entreprise, les objectifs des TI et les facilitateurs, ces derniers incluant les processus de TI. Il en résulte une liste fiable de 17 objectifs d'entreprise génériques et de 17 objectifs génériques liés aux TI, validés et priorisés entre différents secteurs. En plus d'établir une relation entre les deux types d'objectifs, la liste constitue une bonne base sur laquelle bâtir une cascade générique depuis les objectifs d'affaires et objectifs des TI.

PRINCIPE 3 – ACQUISITION

Ce que cela signifie en pratique :

Les solutions de TI sont là pour appuyer les processus d'affaires existants; par conséquent, il ne faut pas les considérer de façon isolée ou comme des projets ou des services strictement « technologiques ». D'autre part, le choix d'une architecture technologique inadéquate, l'incapacité à maintenir une infrastructure technique appropriée et à jour ou l'absence de ressources humaines compétentes peuvent entraîner l'échec du projet, l'impossibilité de maintenir les opérations d'affaires ou une perte de valeur pour l'entreprise. Les acquisitions de ressources en TI doivent être envisagées comme une partie des changements organisationnels globaux découlant des TI. La technologie acquise doit aussi appuyer et fonctionner avec les processus d'affaires et les infrastructures des TI existant et planifiés. La mise en œuvre n'est pas seulement un enjeu technologique : elle combine le changement organisationnel, la révision des processus d'affaires, la formation et l'autorisation au changement. Par conséquent, les projets de TI devraient être entrepris dans le cadre de programmes de changement globaux dans toute l'entreprise, incluant d'autres projets qui satisfont à toute la gamme d'activités requises pour assurer leur succès.

Comment les orientations de l'ISACA permettent une bonne pratique :

1. Le domaine EDS de COBIT 5 fournit des orientations sur la gouvernance et la gestion d'investissements d'affaires dépendant des TI tout au long du cycle de vie (acquisition, mise en œuvre, exploitation et déclasserment). Le processus APO05 *Gérer le portefeuille* présente les moyens d'appliquer une gestion de portefeuille et de programme efficace à de tels investissements afin d'assurer la réalisation des bénéfices et l'optimisation des coûts.
2. Le domaine APO de COBIT 5 fournit des orientations sur la planification des acquisitions, y compris la planification des investissements, la gestion des risques, la planification du programme et du projet et la planification de la qualité.
3. Le domaine BAI de COBIT 5 fournit des orientations quant aux processus nécessaires pour acquérir et mettre en œuvre des solutions de TI. Il couvre la définition des exigences, la détermination de solutions réalisables, la préparation des documents, la formation et permet aux utilisateurs et aux opérations l'exploitation des nouveaux systèmes. Des orientations supplémentaires visent à s'assurer que les solutions sont mises à l'essai et contrôlées adéquatement lorsque le changement est appliqué aux activités d'exploitation et à l'environnement des TI.
4. Le domaine SEM et le processus EDS05 de COBIT 5 comprennent des orientations à l'intention des directeurs sur la surveillance et l'évaluation du processus d'acquisition, ainsi que des mesures de contrôle interne qui contribuent à ce que les acquisitions soient bien gérées et réalisées.

PRINCIPE 4 – PERFORMANCE

Ce que cela signifie en pratique :

Deux aspects essentiels doivent être abordés pour que la mesure de la performance soit efficace : il faut définir clairement les objectifs de performance et établir des indicateurs efficaces visant à surveiller leur atteinte. Un processus de gestion de la performance est également nécessaire pour assurer une surveillance constante et fiable de la performance. Pour obtenir une gouvernance efficace, les buts doivent être fixés de façon hiérarchique et alignés sur des objectifs d'affaires de haut niveau et approuvés, alors que les indicateurs doivent être établis depuis la base vers le haut et harmonisés de manière à ce que l'atteinte des buts soit surveillée à tous les niveaux, par tous les paliers de direction. L'approbation des

but par les parties prenantes et l'acceptation de la responsabilité pour leur atteinte par les directeurs et gestionnaires sont deux facteurs essentiels au succès de la gouvernance. Comme les TI représentent un domaine technique complexe, il est important de faire preuve de transparence en employant des termes compréhensibles pour les parties prenantes dans les buts, les indicateurs et les rapports de performance, de sorte que des mesures appropriées puissent être prises.

Comment les orientations de l'ISACA permettent une bonne pratique :

1. Le référentiel COBIT 5 fournit des exemples génériques de buts et indicateurs pour tout l'éventail des processus liés aux TI et les autres facilitateurs, en plus de montrer les relations entre ceux-ci et les objectifs d'affaires, ce qui permet aux organisations de les adapter à leurs besoins particuliers.
2. COBIT 5 donne à la direction des orientations quant à la façon de fixer des objectifs de TI alignés avec les objectifs d'affaires et décrit comment surveiller la performance de ces objectifs à l'aide de buts et d'indicateurs. La capacité des processus peut être évaluée selon le modèle d'évaluation de la conformité de la capacité de la norme ISO/CEI 15504.
3. Deux processus clés de COBIT 5 fournissent des orientations spécifiques :
 - APO02 *Gérer la stratégie* se concentre sur l'établissement des objectifs.
 - APO09 *Gérer les accords de service* se concentre sur la définition de services et objectifs de services adéquats et sur la façon de les documenter dans les accords sur les niveaux de service.
4. Avec son processus SEM01 *Surveiller, évaluer et mesurer la performance et la conformité*, COBIT 5 fournit des orientations quant aux responsabilités de la haute direction pour cette activité.
5. Le guide *COBIT 5 pour l'assurance* explique comment les professionnels de l'audit peuvent fournir une assurance indépendante aux directeurs en matière de performance des TI.

PRINCIPE 5 – CONFORMITÉ

Ce que cela signifie en pratique :

Dans le marché mondial d'aujourd'hui, rendu possible par Internet et les percées technologiques, les entreprises doivent se plier à un nombre croissant d'exigences juridiques et réglementaires. Comme les dernières années ont été marquées par des scandales touchant le monde des affaires et des échecs financiers, les conseils d'administration sont de plus en plus conscients de l'existence et des implications de lois et de réglementations strictes. Les parties prenantes veulent avoir l'assurance que les entreprises respectent les lois et réglementations et se conforment aux bonnes pratiques de gouvernance dans leur contexte d'exploitation. De plus, comme les TI favorisent l'intégration des processus organisationnels entre les entreprises, il est de plus en plus nécessaire d'assurer que les contrats comprennent des exigences clés liées aux TI relatives à la protection de la vie privée, à la confidentialité, à la propriété intellectuelle et à la sécurité.

Les directeurs doivent veiller à ce que la conformité aux exigences externes fasse partie de la planification stratégique plutôt que de devenir une considération ultérieure coûteuse. Ils doivent aussi donner le ton et mettre en place des politiques et procédures qui seront suivies par la direction et le personnel, afin d'assurer la réalisation des objectifs de l'entreprise, la minimisation des risques et la conformité. La haute direction doit trouver l'équilibre entre la performance et la conformité, et faire en sorte que les objectifs de performance ne nuisent pas à la conformité. À l'inverse, elle doit faire en sorte que les règles de conformité soient adéquates et qu'elles n'entravent pas déraisonnablement les activités de l'entreprise.

Comment les orientations de l'ISACA permettent une bonne pratique :

1. Les pratiques de gouvernance et de gestion de COBIT 5 fournissent une base sur laquelle fonder un contexte de contrôle adéquat en entreprise. Les évaluations de la capacité des processus permettent à la direction d'évaluer la capacité des processus de TI et d'établir des références quant à ces derniers.
2. Le processus APO02 *Gérer la stratégie* de COBIT 5 contribue à l'alignement du plan de TI avec les objectifs d'affaires globaux, incluant les exigences de gouvernance.
3. Le processus SEM02 *Surveiller, évaluer et mesurer le système de contrôles internes* de COBIT 5 permet aux directeurs de juger si les contrôles sont adéquats pour satisfaire aux exigences de conformité.
4. Le processus SEM03 *Surveiller, évaluer et mesurer la conformité aux exigences externes* de COBIT 5 aide à assurer que les exigences externes de conformité sont identifiées, que les directeurs donnent l'orientation en matière de conformité et que la conformité des TI en soi est surveillée, évaluée et déclarée dans le contexte de la conformité générale aux exigences organisationnelles.
5. Le guide *COBIT 5 pour l'assurance* explique comment les auditeurs peuvent offrir une assurance indépendante de la conformité et du respect des politiques internes issues de directives internes ou d'exigences juridiques, réglementaires ou contractuelles externes, en confirmant que les mesures correctives nécessaires pour corriger les écarts de conformité ont été prises par le responsable du processus en temps opportun.

PRINCIPE 6 – COMPORTEMENT HUMAIN

Ce que cela signifie en pratique :

La mise en œuvre de tout changement induit par les TI, y compris la gouvernance des TI elle-même, requiert habituellement des changements culturels et comportementaux majeurs au sein des entreprises ainsi que chez les clients et partenaires d'affaires. Comme cela peut susciter des craintes et de l'incompréhension chez les membres du personnel,

la mise en œuvre doit être soigneusement gérée afin qu'ils demeurent motivés. Les directeurs doivent communiquer clairement les objectifs et appuyer ouvertement les changements proposés. La formation et le perfectionnement des compétences du personnel sont des aspects essentiels du changement – surtout compte tenu de l'évolution rapide de la technologie. Les personnes sont concernées par les TI à tous les paliers de l'entreprise, qu'il s'agisse des parties prenantes, des gestionnaires, des utilisateurs ou des spécialistes offrant à l'organisation des services et solutions liés aux TI. Au-delà de l'entreprise, les TI touchent les clients et les partenaires d'affaires et facilitent de plus en plus les transactions libre-service et automatisées entre entreprises, au pays comme à l'étranger. Bien que les processus d'affaires induits par les TI apportent de nouveaux bénéfices et de nouvelles opportunités, ils comportent aussi des risques accrus. Les problèmes de confidentialité et de fraude préoccupent de plus en plus les individus. Ces types de risques, tout comme d'autres, doivent être gérés afin que les personnes aient confiance envers les systèmes TI qu'ils utilisent. Les systèmes d'information peuvent aussi modifier radicalement les pratiques de travail en automatisant les procédures manuelles.

Comment les orientations de l'ISACA permettent une bonne pratique :

Les facilitateurs de COBIT 5 ci-dessous (qui incluent des processus) fournissent des orientations quant aux exigences liées au comportement humain :

1. Les facilitateurs de COBIT 5 concernent les personnes, les aptitudes et compétences, ainsi que la culture, l'éthique et le comportement. Un modèle illustré par des exemples présente la façon de composer avec chaque facilitateur.
2. Le processus APO07 *Gérer les ressources humaines* de COBIT 5 explique comment la performance des individus doit être alignée sur les objectifs d'entreprise, comment les compétences spécialisées en TI doivent être maintenues et comment les rôles et responsabilités doivent être définies.
3. Le processus BAI02 *Gérer la définition des exigences* contribue à assurer que la conception des applications est conforme aux opérations humaines et aux exigences d'utilisation.
4. Les processus BAI05 *Gérer le changement organisationnel* et BAI08 *Gérer la connaissance* de COBIT 5 contribuent à assurer que les utilisateurs sont en mesure d'utiliser efficacement des systèmes.

De plus, ISACA fournit quatre certifications aux professionnels qui jouent des rôles essentiels liés à la gouvernance des TI, et pour lesquels les connaissances sont couvertes en grande partie par le contenu de COBIT 5 :

- Certified in the Governance of Enterprise IT® (CGEIT®)
- Certified Information Systems Auditor® (CISA®)
- Certified Information Security Manager® (CISM®)
- Certified in Risk and Information Systems Control™ (CRISC™)

Les détenteurs de ces certifications ont démontré leur compétence et leur expérience dans l'exécution de tels rôles.

ISO/CEI 38500 Évaluer, diriger et surveiller

COMMENT LES ORIENTATIONS DE L'ISACA PERMETTENT UNE BONNE PRATIQUE :

Le domaine de gouvernance compris dans le modèle de processus de COBIT 5 comporte cinq processus. Des pratiques EDS sont définies pour chacun d'eux. Il s'agit de la principale section de COBIT 5 où les activités liées à la gouvernance sont définies.

Comparaison à d'autres normes

COBIT 5 a été élaboré en tenant compte d'un grand nombre d'autres normes et référentiels, dont la liste est dressée à l'annexe A.

COBIT 5 : Processus facilitateurs contient un tableau de correspondance générale entre chaque processus de COBIT 5 et les sections les plus pertinentes des normes et référentiels contenant des orientations supplémentaires.

La section ci-dessous comprend une brève discussion sur chaque référentiel ou norme et indique à quels secteurs ou domaines de COBIT 5 ils sont liés.

ITIL® V3 2011 et ISO/CEI 20000

Les secteurs et domaines de COBIT 5 qui suivent sont couverts par ITIL V3 2011 et ISO/CEI 20000 :

- Un sous-ensemble des processus du domaine LSS
- Un sous-ensemble des processus du domaine BAI
- Certains processus du domaine APO

Série de normes ISO/CEI 27000

Les secteurs et domaines de COBIT 5 qui suivent sont couverts par la norme ISO/CEI 27000 :

- Les processus liés à la sécurité et au risque des domaines EDS, APO et LSS

- Diverses activités liées à la sécurité au sein des processus d'autres domaines
- Les activités de surveillance et d'évaluation du domaine SEM

Série de normes ISO/CEI 31000

Les secteurs et domaines de COBIT 5 qui suivent sont couverts par la norme ISO/CEI 31000 :

- Les processus liés à la gestion du risque des domaines EDS et APO

TOGAF®

Les secteurs et domaines de COBIT 5 qui suivent sont couverts par le TOGAF :

- Les processus liés aux ressources du domaine EDS (gouvernance) – les composants de TOGAF concernant le comité d'architecture, la gouvernance de l'architecture et les modèles de maturité de l'architecture sont mis en correspondance avec l'optimisation des ressources.
- Le processus d'architecture d'entreprise du domaine APO. Le fondement de TOGAF est le cycle de la méthode de développement de l'architecture (MDA), qui correspond aux pratiques de COBIT 5 en matière d'élaboration d'une vision d'architecture (MDA étape A), de définition des architectures de référence (MDA étapes B, C et D), de sélection des possibilités et solutions (MDA étape E) et de définition de la mise en œuvre de l'architecture (MDA étapes F et G). Différents composants de TOGAF correspondent à la pratique de COBIT 5 en matière de fourniture de services d'architecture d'entreprise. Ils comprennent :
 - La gestion des exigences de la MDA
 - Les principes d'architecture
 - La gestion des parties prenantes
 - L'évaluation de l'état de préparation à la transformation organisationnelle
 - La gestion du risque
 - La planification fondée sur la capacité
 - La conformité de l'architecture
 - Les contrats d'architecture

Capability Maturity Model Integration (CMMI) (développement)

Les secteurs et domaines de COBIT 5 qui suivent sont couverts par le CMMI :

- Processus liés à la création et à l'acquisition d'applications du domaine BAI
- Certains processus liés à l'organisation et à la qualité du domaine APO

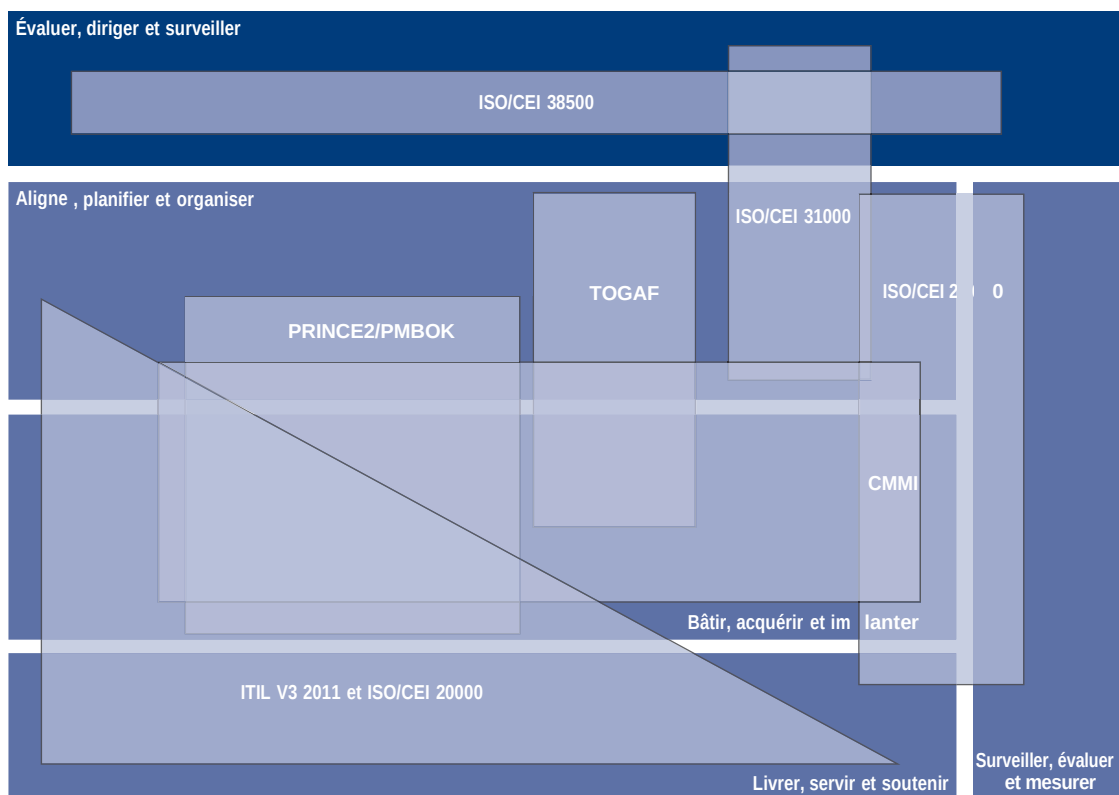
PRINCE2®

Les secteurs et domaines de COBIT 5 qui suivent sont couverts par PRINCE2 :

- Processus liés au portefeuille du domaine APO
- Processus de gestion de programme et de projet du domaine BAI

La **figure 25** illustre la correspondance de la couverture de COBIT 5 et des autres normes et référentiels.

Figure 25 – Couverture des autres normes et référentiels par COBIT 5



ANNEXE F

COMPARAISON ENTRE LE MODÈLE D'INFORMATION DE COBIT 5 ET LES CRITÈRES D'INFORMATION DE COBIT 4.1

Quelle est la relation entre les sept critères d'information de COBIT 4.1 – efficacité, efficience, intégrité, fiabilité, disponibilité, confidentialité, conformité – et les catégories et caractéristiques des facilitateurs de COBIT 5 montrés à la **figure 32** de l'annexe G?

Le tableau ci-dessous présente deux listes pour faciliter la comparaison :

- La première comprend les sept critères d'information de COBIT 4.1.
- La seconde comporte les éléments correspondants de COBIT 5, c'est-à-dire les objectifs facilitants de l'information.

Figure 26 – Équivalents des critères d'information de COBIT 4.1 dans COBIT 5	
Critère d'information de COBIT 4.1	Équivalent de COBIT 5
Efficacité	L'information est efficace si elle répond aux besoins de la personne qui l'utilise pour une tâche donnée. Si l'information permet à l'utilisateur de réaliser sa tâche, alors elle est efficace. Ceci correspond aux objectifs de qualité de l'information suivants : quantité adéquate, pertinence, compréhensibilité, possibilité d'interprétation, objectivité.
Efficience	Alors que l'efficacité aborde l'information en tant que produit, l'efficience concerne plutôt le processus d'obtention et d'utilisation de l'information et correspond à une perspective « d'information en tant que service ». Si l'information qui répond aux besoins de l'utilisateur est facile à obtenir et à exploiter (autrement dit, si elle exige peu de ressources – effort physique ou cognitif, temps, argent), alors l'utilisation de cette information est efficiente. Ceci correspond aux objectifs de qualité de l'information suivants : crédibilité, accessibilité, facilité d'exploitation, réputation.
Intégrité	Si l'information est intègre, alors elle est exacte et complète. Cela correspond aux objectifs de qualité de l'information suivants : exhaustivité, exactitude.
Fiabilité	La fiabilité est souvent perçue comme synonyme d'exactitude; toutefois, on peut aussi dire que l'information est fiable si elle est juste et crédible. Comparativement à l'intégrité, la fiabilité est un critère plus subjectif, lié à la perception et non seulement aux faits. Cela correspond aux objectifs de qualité de l'information suivants : crédibilité, réputation, objectivité.
Disponibilité	La disponibilité est l'un des objectifs de qualité de l'information dans la catégorie accessibilité et sécurité.
Confidentialité	La confidentialité correspond à l'objectif de qualité de l'information « restriction d'accès ».
Conformité	La conformité, au sens où l'information doit se conformer aux spécifications, est couverte par tous les objectifs de qualité de l'information, selon les exigences. La conformité à la réglementation est généralement un objectif ou une exigence d'utilisation de l'information plutôt qu'une qualité intrinsèque de l'information.

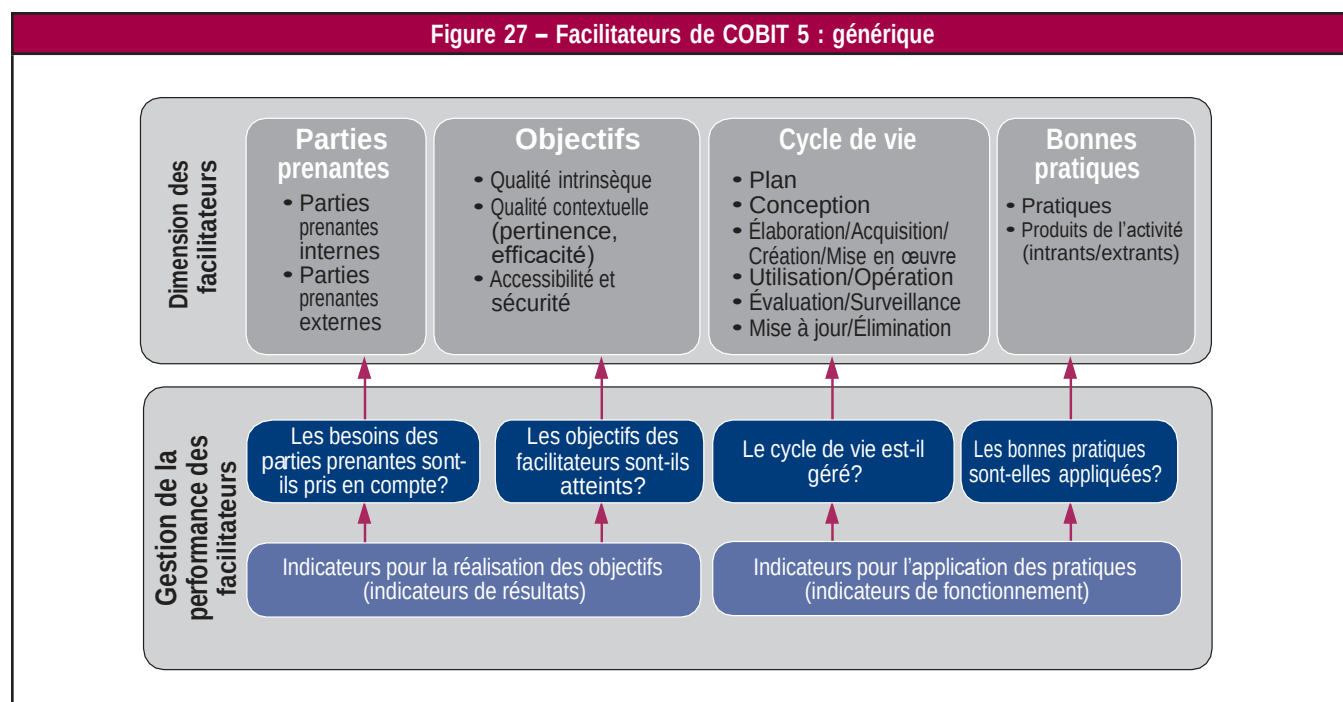
Ce tableau montre que tous les critères d'information de COBIT 4.1 sont couverts par COBIT 5; cependant, le modèle d'information de COBIT 5 permet la définition d'un ensemble de critères supplémentaires, ce qui enrichit la valeur des critères de COBIT 4.1.

ANNEXE G

DESCRIPTION DÉTAILLÉE DES FACILITATEURS DE COBIT 5

Introduction

La section qui suit contient une description détaillée des sept catégories de facilitateurs du cadre de COBIT 5, décrits initialement au chapitre 5 et répétés à la **figure 27**.



Dimensions des facilitateurs

Les quatre dimensions communes des facilitateurs sont :

- **Parties prenantes** – Chaque facilitateur est associé à des parties prenantes, c'est-à-dire des parties qui jouent un rôle actif ou ont un intérêt envers le facilitateur. À titre d'exemple, différentes parties exécutent les activités des processus ou ont un intérêt quant aux résultats des processus. Les structures organisationnelles sont également constituées de parties prenantes, chacune ayant ses propres rôles et intérêts. Les parties prenantes peuvent être internes ou externes à l'entreprise et toutes ont leurs propres intérêts et besoins parfois contradictoires. Les besoins des parties prenantes se traduisent par des objectifs d'entreprise, qui à leur tour se traduisent par des objectifs liés aux TI pour l'entreprise. La liste des parties prenantes est indiquée à la **figure 7**.
- **Objectifs** – Chaque facilitateur a un certain nombre d'objectifs, et tous ces facilitateurs fournissent de la valeur par la réalisation de ces objectifs. Les objectifs peuvent être définis sous l'angle de :
 - Résultats attendus du facilitateur
 - Application ou exploitation du facilitateur comme tel

Les objectifs facilitants constituent la dernière étape de la cascade d'objectifs de COBIT 5. Ces objectifs peuvent être de nouveau divisés en différentes catégories :

- **Qualité intrinsèque** – La mesure dans laquelle les facilitateurs fonctionnent de façon exacte et objective pour donner des résultats précis, neutres et fiables.
- **Qualité contextuelle** – La mesure dans laquelle les facilitateurs et leurs résultats sont adaptés à la fonction, compte tenu du contexte d'utilisation. Par exemple, les résultats doivent être pertinents, complets, à jour, appropriés, cohérents, compréhensibles et faciles à utiliser.
- **Accès et sécurité** – La mesure dans laquelle les facilitateurs et leurs résultats sont accessibles et sécurisés :
 - Les facilitateurs sont disponibles au besoin, au moment opportun.
 - Les résultats sont sécurisés, c'est-à-dire que l'accès est restreint à ceux qui y ont droit et en ont besoin.
- **Cycle de vie** – Chaque facilitateur a un cycle de vie, depuis sa création en passant par sa vie opérationnelle et utile jusqu'à son élimination. Ceci s'applique à l'information, aux structures, aux processus, aux politiques, etc. Les étapes du cycle de vie se composent des éléments suivants :
 - Planifier (inclut l'élaboration et la sélection des concepts)

- Concevoir
- Bâtir/acquérir/créer/implanter
- Utiliser/exploiter
- Évaluer/surveiller
- Mettre à jour/éliminer

• **Bonnes pratiques** – Pour chacun des facilitateurs, de bonnes pratiques peuvent être définies afin de contribuer à la réalisation des objectifs facilitants. Elles fournissent des exemples ou des suggestions sur la meilleure façon de mettre en œuvre les facilitateurs, et quels produits de l'activité ou intrants et extrants sont nécessaires. COBIT 5 fournit des exemples de bonnes pratiques relatives à certains de ses facilitateurs (p. ex., les processus) alors que pour les autres, des orientations provenant d'autres normes, référentiels, etc., peuvent être utilisées.

Gestion de la performance des facilitateurs

Les entreprises s'attendent à ce que la mise en œuvre et l'utilisation des facilitateurs donnent des résultats positifs. Afin de gérer la performance des facilitateurs, les réponses aux questions qui suivent doivent être obtenues – selon les indicateurs – de façon régulière :

- Les besoins des parties prenantes sont-ils pris en compte?
- Les objectifs facilitants sont-ils atteints?
- Le cycle de vie des facilitateurs est-il géré?
- Les bonnes pratiques sont-elles appliquées?

Les deux premiers points concernent le résultat concret du facilitateur. Les indicateurs utilisés pour évaluer dans quelle mesure les objectifs sont atteints peuvent être appelés « indicateurs de résultats ».

Les deux derniers points traitent du fonctionnement réel du facilitateur lui-même et les indicateurs qui y sont associés peuvent être appelés « indicateurs de fonctionnement ».

Pour chaque facilitateur, il existe une section distincte qui commence par une illustration semblable à celle de la **figure 27**, mais qui inclut différents éléments propres au facilitateur concerné, mis en évidence en **rouge** et en **gras**.

Ensuite, chacun des quatre éléments est décrit en détail. Les éléments précis et leurs relations avec d'autres facilitateurs sont abordés.

Divers exemples ont aussi été inclus afin d'illustrer la signification et l'utilisation des facilitateurs.

L'objet de cette section consiste à mieux faire connaître le cadre de COBIT 5 et à démontrer comment le concept de facilitateurs peut être appliqué pour mettre en œuvre et améliorer la gouvernance et la gestion des TI en entreprise.

Facilitateur de COBIT 5 : principes, politiques et cadres

Les principes et les politiques font référence aux mécanismes de communication mis en place pour transmettre l'orientation et les consignes du groupe de gouvernance et de la haute direction. Les spécificités du facilitateur des principes, des politiques et des cadres, comparativement à la description générique des facilitateurs, sont présentées à la **figure 28**.

Le modèle des principes, des politiques et des cadres présente :

- **Les parties prenantes** – Les parties prenantes des principes et des politiques peuvent être internes et externes à l'entreprise. Elles incluent le conseil d'administration et la haute direction, les responsables de la conformité, les gestionnaires de risque, les auditeurs internes et externes, les fournisseurs de services, les clients et les agences de réglementation. Il existe deux types de parties prenantes : les unes définissent et établissent les politiques, les autres doivent s'y conformer.
- **Les objectifs et les indicateurs** – Les principes, les politiques et les cadres sont des instruments qui énoncent les règles de l'entreprise, de manière à appuyer les objectifs de gouvernance et les valeurs organisationnelles définis par le conseil d'administration et la haute direction. Les principes doivent être :
 - Limités en nombre
 - Rédigés en termes simples qui expriment aussi clairement que possible les valeurs fondamentales de l'entreprise

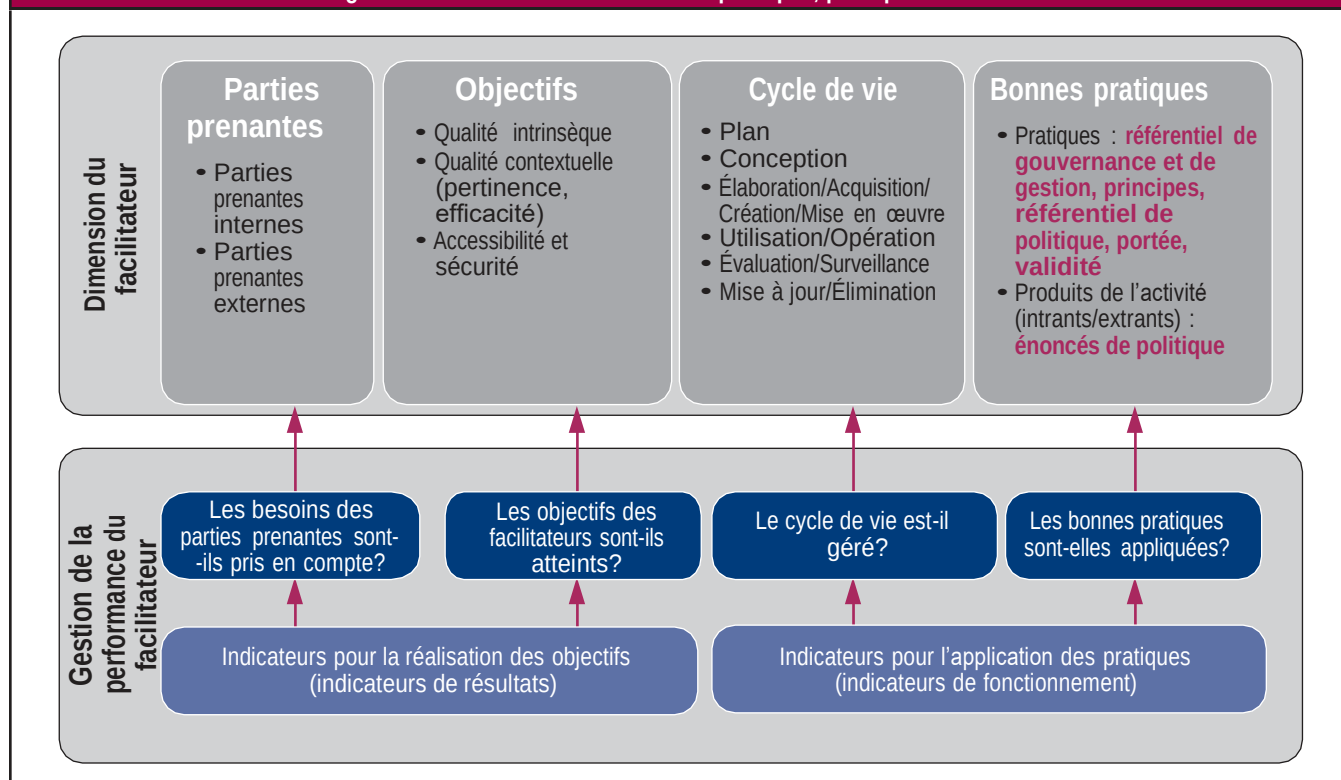
Les politiques fournissent des orientations détaillées sur la manière d'appliquer les principes et influencent l'alignement de la prise de décision avec ceux-ci. Les bonnes politiques sont :

- Efficaces – Elles réalisent la fonction annoncée.
- Efficaces – Elles garantissent la mise en œuvre des principes de la façon la plus efficace possible.

– Non intrusives – Elles semblent logiques pour ceux qui doivent les respecter. Autrement dit, elles n’entraînent pas de résistance indue.

Accès aux politiques – Y a-t-il un mécanisme en place qui permette un accès facile aux politiques pour toutes les parties prenantes? En d’autres termes, les parties prenantes savent-elles où trouver les politiques?

Figure 28 – Facilitateur de COBIT 5 : principes, politiques et cadres



Les référentiels de gouvernance et de gestion doivent fournir à la direction une structure, des orientations, des outils, etc., qui permettent de bien gouverner et de bien gérer les TI de l’entreprise. Les référentiels doivent être :

- Exhaustifs, couvrant tous les secteurs requis
- Ouverts et souples, permettant une adaptation à la situation particulière de chaque entreprise
- À jour, c’est-à-dire représentatifs de l’orientation et des objectifs de gouvernance actuels de l’entreprise
- Disponibles et accessibles pour toutes les parties prenantes
- **Le cycle de vie** – Le cycle de vie des politiques doit appuyer l’atteinte des objectifs définis. Les référentiels sont essentiels puisqu’ils fournissent une structure qui détermine des orientations uniformes. Par exemple, un référentiel de politique fournit une structure qui permet la création et le maintien d’un ensemble cohérent de politiques, en plus d’aider à la navigation entre les différentes politiques.

Selon le contexte externe dans lequel l’entreprise exerce ses activités, il peut exister divers degrés d’exigences réglementaires qui demandent des contrôles internes forts et par conséquent, un cadre de politique robuste. Un point crucial à prendre en considération relativement aux référentiels et aux politiques est l’actualisation des politiques; sont-elles examinées et mises à jour? Si oui, à quelle fréquence? Existe-t-il des mécanismes solides assurant que les personnes sont au courant des mises à jour, que les dernières versions sont facilement accessibles (voir le point précédent) et que l’information désuète est archivée ou éliminée correctement?

• Les bonnes pratiques :

- Les bonnes pratiques exigent que les politiques s’inscrivent dans un référentiel global de gouvernance et de gestion, fournissant une structure (hiérarchique) au sein de laquelle toutes les politiques ont leur place et où les liens avec les principes sous-jacents sont évidents.
- Le référentiel de politique doit décrire les éléments suivants :
 - La portée et la validité
 - Les conséquences de la non-conformité à la politique
 - Les moyens de gérer les exceptions
 - La méthode utilisée pour vérifier et évaluer la conformité à la politique
- Les référentiels de gouvernance et de gestion généralement reconnus peuvent fournir de précieuses orientations quant aux énoncés concrets à inclure dans les politiques.

- Les politiques doivent être harmonisées avec la tolérance au risque de l’entreprise. Ces politiques constituent un élément clé du système de contrôle interne d’une entreprise, dont la fonction est de gérer et de contenir le risque. La tolérance au risque de l’entreprise, définie dans le cadre des activités de gouvernance du risque, devrait se refléter dans les politiques. Une entreprise qui redoute les risques se dote de politiques plus strictes qu’une entreprise tolérante aux risques.
- Les politiques doivent être revalidées ou mises à jour à intervalles réguliers.
- **Les relations avec les autres facilitateurs** – Les liens avec les autres facilitateurs comprennent :
 - Les principes, les politiques et les cadres doivent être représentatifs de la culture et des valeurs éthiques de l’entreprise, ainsi qu’encourager le comportement souhaité; il existe donc un lien fort avec les facilitateurs de la culture, de l’éthique et du comportement.
 - Les pratiques et les activités liées aux processus constituent le véhicule le plus important pour l’exécution des politiques.
 - Les structures organisationnelles peuvent définir et mettre en œuvre des politiques qui dépendent de leur contrôle; les politiques déterminent aussi leurs activités.
 - Puisque les politiques constituent également de l’information, toutes les bonnes pratiques applicables à l’information s’appliquent aux politiques.

EXEMPLE 9 – MÉDIAS SOCIAUX

Une entreprise se demande comment composer avec l'utilisation croissante des médias sociaux et les pressions de son personnel qui veut y avoir un accès complet. Jusqu'à présent, l'organisation s'est montrée prudente ou restrictive en matière d'accès à ce genre de service, principalement pour des raisons de sécurité.

Différents intervenants insistent pour que l'on adopte une nouvelle position relativement aux médias sociaux. Les membres du personnel veulent profiter d'un accès comparable à celui dont ils jouissent à la maison, alors que l'organisation veut exploiter les avantages des médias sociaux aux fins de marketing et de sensibilisation auprès du public.

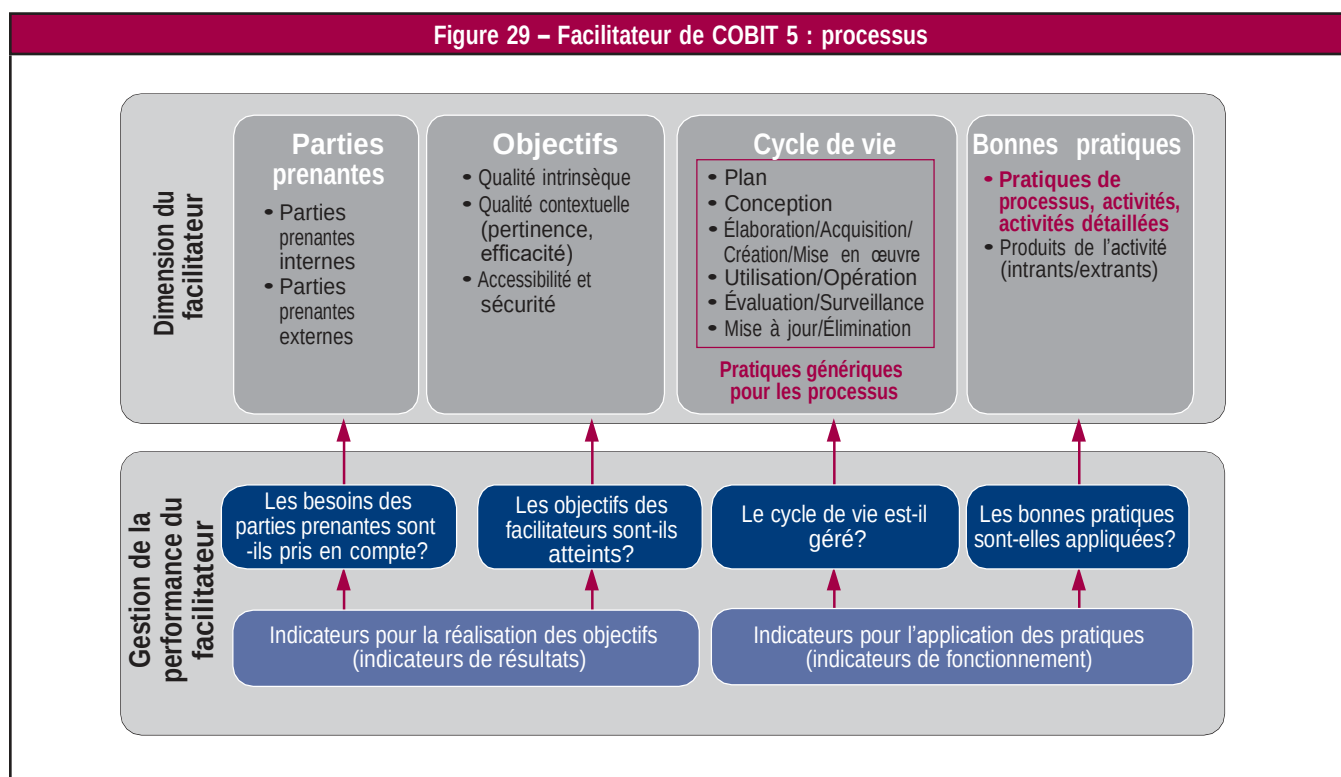
On décide de définir une politique d'utilisation des médias sociaux sur les réseaux et les systèmes de l'entreprise, y compris les ordinateurs portables fournis au personnel. La nouvelle politique s'inscrit dans le cadre existant, sous la catégorie « politiques d'utilisation acceptable », et est plus permissive que les précédentes. On élabore donc une communication expliquant les motifs de la nouvelle politique. Par la même occasion, cette décision a des répercussions sur certains autres facilitateurs :

- Le personnel doit apprendre à utiliser les nouveaux médias de manière à éviter de créer une situation gênante pour l'entreprise. Il doit apprendre les comportements appropriés à la nouvelle orientation de l'entreprise et acquérir les compétences adéquates.
- Divers processus de sécurité doivent être modifiés. Comme on permet désormais l'accès aux médias sociaux, les paramètres et configurations de sécurité doivent être modifiés. Il pourrait également être nécessaire de définir certaines mesures compensatoires.

Remarque : COBIT 5 est un exemple de cadre selon la description de ce facilitateur.

Facilitateur de COBIT 5 : processus

Les spécificités du facilitateur des processus, comparativement à la description générique d'un facilitateur, sont montrées à la **figure 29**.



Un processus est défini comme « **un ensemble de pratiques, influencées par les politiques et procédures de l'entreprise, qui prend des intrants de différentes sources (incluant d'autres processus), les utilise et en tire des extrants (p. ex., produits, services)** ».

Le modèle des processus présente les éléments suivants :

- **Les parties prenantes** – Les processus ont des parties prenantes internes et externes, chacune ayant ses propres rôles; les parties prenantes et leurs niveaux de responsabilité sont documentés dans les tableaux RACI. Les parties prenantes externes comprennent les clients, les partenaires d'affaires, les actionnaires et les organismes de réglementation. Les parties prenantes internes comprennent le conseil d'administration, la direction, le personnel et les bénévoles.
- **Les objectifs** – Les objectifs des processus sont définis comme étant « des énoncés décrivant le résultat désiré d'un processus. Le résultat peut être un objet, un changement d'état significatif ou une amélioration majeure à la capacité d'autres processus. » Ils font partie de la cascade d'objectifs. Autrement dit, les objectifs des processus appuient les objectifs liés aux TI, qui appuient à leur tour les objectifs d'entreprise.

Les objectifs des processus peuvent être catégorisés comme suit :

- **Objectifs intrinsèques** – Le processus a-t-il une qualité intrinsèque? Est-il précis et aligné aux bonnes pratiques? Est-il conforme aux règles internes et externes?
- **Objectifs contextuels** – Le processus est-il adapté et personnalisé à la situation propre à l'entreprise? Le processus est-il pertinent, compréhensible et facile à appliquer?
- **Objectifs d'accessibilité et de sécurité** – Le processus demeure confidentiel, si nécessaire, est connu et est accessible pour ceux qui en ont besoin.

À chaque niveau de la cascade d'objectifs, et par conséquent pour les processus, des indicateurs sont définis pour mesurer à quel point les objectifs sont atteints. Ces indicateurs sont définis comme « des entités quantifiables qui permettent de mesurer l'atteinte d'un objectif de processus. Ils devraient être SMART – spécifiques, mesurables, atteignables, réalistes et en temps opportun. »

Afin de gérer le facilitateur de façon efficace et efficiente, les indicateurs doivent être définis de manière à mesurer à quel point les résultats attendus sont atteints. De plus, un second aspect de la gestion de la performance du facilitateur décrit dans quelle mesure les bonnes pratiques sont appliquées. Ici aussi, des indicateurs connexes peuvent être définis pour faciliter la gestion du facilitateur.

- **Cycle de vie** – Chaque processus a un cycle de vie. Il est défini, créé, exploité, surveillé, ajusté, mis à jour ou retiré. Les pratiques génériques liées aux processus, comme celles décrites dans le modèle d'évaluation de COBIT fondé sur la norme ISO/CEI 15504, peuvent contribuer à définir, exploiter, surveiller et optimiser les processus.
- **Bonnes pratiques** – *COBIT 5 : Processus facilitants* contient un modèle de référence dans lequel les bonnes pratiques internes liées aux processus sont décrites de façon de plus en plus précise : pratiques, activités et activités détaillées :¹⁴

Pratiques :

- Pour chaque processus de COBIT 5, les pratiques de gouvernance et de gestion fournissent un ensemble complet d'exigences de haut niveau pour une gouvernance et une gestion efficaces et pratiques des TI de l'entreprise. Ces processus :
 - Sont des énoncés proposant des mesures visant à réaliser les bénéfices, à minimiser le risque et à optimiser l'utilisation des ressources.
 - Sont alignés sur les normes généralement acceptées et sur les bonnes pratiques.
 - Sont génériques et doivent donc être adaptés à chaque entreprise.
 - Couvrent les acteurs des lignes d'affaires et des TI qui participent au processus (du début à la fin).
- Le groupe de gouvernance et la direction de l'entreprise doivent faire des choix relatifs aux pratiques de gouvernance et de gestion en :
 - Choissant celles qui s'appliquent et en décidant lesquelles mettre en œuvre.
 - Adaptant les pratiques ou en ajoutant au besoin.
 - Définissant et ajoutant des pratiques non liées aux TI pour les intégrer aux processus d'affaires.
 - Choissant comment les mettre en œuvre (fréquence, portée, automatisation, etc.).
 - Acceptant le risque pouvant survenir si une pratique applicable n'est pas mise en œuvre.

Activités – Dans COBIT, les activités sont les principales mesures prises pour l'exploitation du processus

- Elles sont définies comme étant « des orientations pour mettre en œuvre des pratiques organisationnelles assurant la réussite de la gouvernance et de la gestion des TI de l'entreprise ». Les activités de COBIT 5 précisent le quoi, le comment et le pourquoi des mesures à appliquer pour chaque pratique de gouvernance ou de gestion afin d'améliorer la performance des TI ou d'aborder le risque lié aux solutions TI et à la livraison de services. Ce contenu est utile pour :
 - La haute direction, les fournisseurs de services, les utilisateurs finaux et les professionnels des TI qui doivent planifier, créer, exploiter ou surveiller les TI de l'entreprise.
 - Les professionnels de l'audit qui peuvent être appelés à donner leur opinion concernant les mises en œuvre actuelles ou proposées, ou les améliorations nécessaires.
- Réunir en une seule approche un ensemble d'activités génériques et spécifiques qui consistent en toutes les étapes nécessaires et suffisantes pour la réalisation des pratiques de gouvernance et de gestion essentielles. Elles fournissent des orientations de haut niveau, à un niveau inférieur aux pratiques de gouvernance et de gestion, pour l'évaluation de la performance et l'étude d'améliorations potentielles. Les activités :
 - Décrivent un ensemble d'étapes de mise en œuvre axées sur l'action, nécessaires et suffisantes pour la réalisation des pratiques de gouvernance et de gestion.
 - Tiennent compte des intrants et des extrants du processus.
 - Sont fondées sur des normes généralement acceptées et sur de bonnes pratiques.
 - Soutiennent l'établissement de rôles et de responsabilités clairs.
 - Ne sont pas normatives et doivent être adaptées et élaborées afin d'en faire des procédures appropriées à l'entreprise.

Activités détaillées – Les activités ne sont pas nécessairement détaillées de manière suffisante pour leur mise en œuvre; des orientations supplémentaires peuvent être :

- Obtenues à partir de normes et de bonnes pratiques spécifiques et précises comme ITIL, la série ISO/CEI 27000 et PRINCE2.
- Développées dans le cadre d'activités plus précises ou détaillées en tant qu'ajouts à la famille de produits de COBIT 5 comme telle.

Intrants et extrants – Les intrants et les extrants de COBIT 5 sont les produits et les objets issus de l'activité jugés nécessaires pour appuyer l'exploitation d'un processus donné. Ils aident la prise de décisions cruciales, fournissent des registres et des pistes d'audit quant aux activités du processus et permettent un suivi en cas d'incident. Ils sont définis au niveau des pratiques clés de gouvernance et de gestion, peuvent inclure certains produits de l'activité qui servent uniquement au processus et sont souvent des intrants essentiels pour d'autres processus.¹⁵

¹⁴ Seules les pratiques et les activités sont élaborées dans le cadre du projet en cours. Les niveaux plus détaillés sont sujets à une élaboration supplémentaire; par exemple, les différents guides professionnels peuvent fournir des orientations plus détaillées sur leurs domaines. En outre, d'autres orientations peuvent être obtenues grâce à des normes et des référentiels connexes, comme cela est indiqué dans les descriptions détaillées des processus.

¹⁵ Les exemples d'intrants et d'extrants de COBIT 5 ne doivent pas être considérés comme une liste exhaustive, car des flux d'information supplémentaires pourraient être définis en fonction du contexte particulier d'une entreprise et du référentiel de processus.

Les bonnes pratiques externes peuvent exister sous toute forme ou tout degré de détail, et font principalement référence à d'autres normes et référentiels. Les utilisateurs peuvent consulter ces bonnes pratiques externes en tout temps, en sachant que COBIT y est aligné lorsque cela est pertinent, et que des informations de correspondance seront disponibles.

Gestion de la performance des facilitateurs

Les entreprises s'attendent à des résultats positifs de la mise en œuvre et de l'utilisation des facilitateurs. Afin de gérer la performance des facilitateurs, les réponses aux questions suivantes doivent être obtenues – selon les indicateurs – de façon régulière :

- Les besoins des parties prenantes sont-ils pris en compte?
- Les objectifs facilitants sont-ils atteints?
- Le cycle de vie des facilitateurs est-il géré?
- Les bonnes pratiques sont-elles appliquées?

Dans le cadre du facilitateur des processus, les deux premiers points concernent le résultat concret du processus. Les indicateurs utilisés pour mesurer à quel point les objectifs sont atteints peuvent être appelés « indicateurs de résultats ». Dans *COBIT 5 : Processus facilitants*, différents indicateurs sont définis pour chaque objectif lié à un processus.

Les deux derniers points traitent du fonctionnement réel du facilitateur lui-même, et les indicateurs qui y sont associés peuvent être appelés « indicateurs de fonctionnement ».

Niveau de capacité des processus – COBIT 5 inclut un modèle d'évaluation de la capacité des processus fondé sur ISO/CEI 15504. Le chapitre 8 de COBIT 5 l'aborde et des orientations supplémentaires se trouvent dans d'autres publications sur COBIT 5 de l'ISACA. En bref, le niveau de capacité des processus mesure tant l'atteinte des objectifs que la mise en œuvre des bonnes pratiques.

Relations avec d'autres facilitateurs – Des liens existent entre les processus et les autres catégories de facilitateurs en fonction des relations suivantes :

- Les processus ont besoin d'information (comme un des types d'intrants) et peuvent produire de l'information (en tant que produit de l'activité).
- Les processus ont besoin de structures et de rôles organisationnels pour fonctionner, par exemple : comité directeur des TI, comité du risque d'entreprise, conseil d'administration, audit, directeur de l'information, chef de la direction, comme le montrent les tableaux RACI.
- Les processus produisent et exigent des capacités de service (infrastructure, applications, etc.).
- Les processus peuvent dépendre d'autres processus, et c'est généralement le cas.
- Les processus donnent lieu à, ou nécessitent, des politiques et procédures assurant une mise en œuvre et une exécution constantes.
- Des aspects culturels et comportementaux déterminent la bonne exécution des processus.

Exemple pratique de processus facilitant

L'exemple 10 illustre le processus facilitant, ses interconnexions et ses caractéristiques. Cet exemple se base sur l'exemple 7, présenté plus haut dans le document.

Modèle de référence du processus COBIT 5

PROCESSUS DE GOUVERNANCE ET DE GESTION

Un des principes directeurs de COBIT est la distinction faite entre la gouvernance et la gestion. Conformément à ce principe, chaque entreprise doit mettre en place certains processus de gouvernance et de gestion afin d'assurer une gouvernance et une gestion exhaustives des TI de l'entreprise.

Lorsque la gouvernance et la gestion sont prises en considération dans le contexte de l'entreprise, les différences entre les types de processus se trouvent dans les objectifs propres à ceux-ci :

- **Processus de gouvernance** – Les processus de gouvernance traitent des objectifs de gouvernance des parties prenantes – création de valeur, minimisation du risque et optimisation des ressources – et incluent des pratiques et activités qui visent à évaluer les options stratégiques, à fournir des orientations aux TI et à surveiller les résultats (EDS – aligné sur les concepts de la norme ISO/CEI 38500).
- **Processus de gestion** – Conformément à la définition de la gestion, des pratiques et des activités liées aux processus de gestion couvrent les domaines de responsabilité PCES des TI en entreprise et doivent fournir une couverture de bout en bout des TI.

EXEMPLE 10 – INTERCONNEXIONS DU FACILITATEUR DE PROCESSUS

Une organisation a nommé des « gestionnaires de processus » pour les processus liés aux TI. Ces gestionnaires sont chargés de les définir et de les exploiter de manière efficace et efficiente, dans le cadre de la bonne gouvernance et de la bonne gestion des TI de l'entreprise.

Initialement, les gestionnaires de processus mettront l'accent sur les facilitateurs des processus, en tenant compte des dimensions des facilitateurs :

- **Parties prenantes** : Les parties prenantes du processus incluent tous les acteurs du processus, c'est-à-dire toutes les parties qui sont responsables des activités du processus ou qui les approuvent, qui sont consultées ou qui sont informées (RACI) pendant les activités. Pour cela, il est possible d'utiliser un tableau RACI comme celui décrit dans *COBIT 5 : Processus facilitateurs*.
- **Objectifs** : Pour chaque processus, des objectifs adéquats ainsi que leurs indicateurs connexes doivent être définis. À titre d'exemple, pour le processus APO08 *Gérer les relations* (dans *COBIT 5 : Processus facilitateurs*), on peut trouver un ensemble d'objectifs de processus et d'indicateurs tels que :
 - **Objectif** : Les stratégies, les plans et les exigences d'affaires sont bien compris, documentés et approuvés.
 - **Indicateurs** : Pourcentage des programmes alignés sur les exigences et priorités d'affaires de l'entreprise
 - **Objectif** : De bonnes relations existent entre l'entreprise et le service des TI.
 - **Indicateurs** : Évaluations des utilisateurs et sondages de la satisfaction du personnel des TI
- **Cycle de vie** : Chaque processus dispose d'un cycle de vie, c'est-à-dire qu'il doit être créé, exécuté et surveillé, ainsi qu'ajusté si nécessaire. Enfin, les processus cesseront d'exister. Dans ce cas, les gestionnaires de processus devront concevoir et définir le processus en premier. Ils peuvent utiliser plusieurs éléments de *COBIT 5 : Processus facilitateurs* pour concevoir les processus, c'est-à-dire pour définir les responsabilités et pour scinder le processus en pratiques et en activités, ainsi que pour définir les produits des activités du processus (intrants et extrants). Dans un stade ultérieur, le processus doit être plus robuste et plus efficace. Pour cela, les gestionnaires de processus peuvent élever le niveau de capacité du processus. Le modèle de capacité des processus de COBIT 5, inspiré d'ISO/CEI 15504, ainsi que les attributs de capacité peuvent servir à cette fin. À titre d'exemple :
 - Une capacité de processus de niveau 2 exige l'atteinte de deux attributs : La gestion de la performance et la gestion des produits du travail. Le premier attribut exige différentes activités liées à l'étape de planification :
 - Les objectifs de performance du processus sont définis.
 - La performance du processus est planifiée.
 - Les responsabilités relatives à la performance du processus sont définies.
 - Les ressources sont identifiées.
 - Etc.
 Le même niveau de capacité prescrit la réalisation de différentes activités pour l'étape de « surveillance » du cycle de vie du processus, par exemple :
 - Surveillance de la performance du processus.
 - Adaptation de la performance du processus en fonction des plans.
 - Etc.
 - La même approche peut servir à obtenir des orientations quant aux différentes étapes du cycle de vie des divers attributs de capacité de performance à des niveaux croissants de capacité des processus.
- **Bonnes pratiques** : COBIT 5 décrit en détail les bonnes pratiques liées aux processus dans *COBIT 5 : Processus facilitateurs*, comme mentionnés au point précédent. Elles sont une source d'inspiration et d'exemples de processus couvrant toute la gamme des activités requises pour le succès de la gouvernance et de la gestion des TI de l'entreprise.

En plus des orientations sur les processus facilitateurs, les gestionnaires de processus peuvent décider de prendre connaissance d'un certain nombre d'autres facilitateurs comme :

- Le tableau RACI décrit les rôles et responsabilités. D'autres facilitateurs permettent de cibler cette dimension, dont :
 - Dans le facilitateur des aptitudes et compétences, les aptitudes et les compétences requises pour chaque rôle sont définies; des objectifs appropriés (p. ex., niveau de compétence technique et comportementale) et indicateurs connexes peuvent également être définis.
 - Le tableau RACI contient par ailleurs différentes structures organisationnelles. Ces structures peuvent être consolidées par le facilitateur des structures organisationnelles, qui fournit une description plus détaillée des structures et définit les résultats attendus, indicateurs connexes (p. ex., décisions) et bonnes pratiques (portée du contrôle, principes de fonctionnement de la structure, niveau d'autorité).
- Des principes et des politiques officialiseront les processus et expliqueront pourquoi un processus donné existe, à qui il s'applique et comment il doit être utilisé. Il s'agit de la zone de concentration des facilitateurs des principes et des politiques.

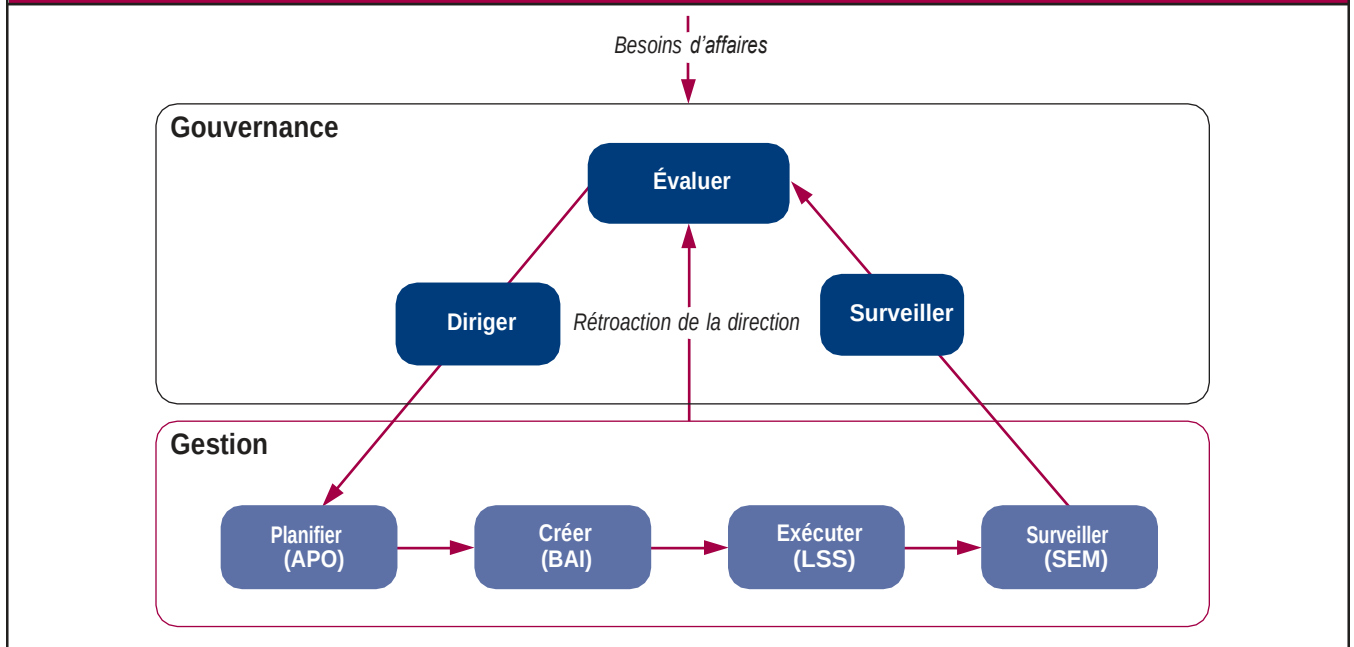
Bien que les résultats des deux types de processus soient différents et visent un public différent, à l'interne, depuis le contexte des processus mêmes, tous les processus doivent comporter des activités de « planification », de « création ou de mise en œuvre », d'« exécution » et de « surveillance ».

MODÈLE DE RÉFÉRENCE DES PROCESSUS DE COBIT 5

COBIT 5 n'est pas normatif, mais ce qui a été écrit précédemment démontre clairement que les entreprises mettent en œuvre des processus de gouvernance et de gestion faisant en sorte que les principaux domaines soient couverts, comme l'illustre la **figure 30**.

En théorie, une entreprise peut organiser ses processus comme bon lui semble, tant que les objectifs de gouvernance et de gestion de base soient couverts. Les petites entreprises peuvent mettre en place moins de processus, tandis que les entreprises plus grandes et plus complexes peuvent en implanter plusieurs, couvrant tous les mêmes objectifs.

Figure 30 – Zones clés de gouvernance et de gestion de COBIT 5



Indépendamment de ce qui précède, COBIT 5 inclut un modèle de référence de processus qui définit et décrit en détail un certain nombre de processus de gouvernance et de gestion. Ce modèle de référence représente tous les processus liés aux activités des TI que l'on trouve habituellement dans une entreprise. Il s'agit donc d'un modèle commun, compréhensible des gestionnaires responsables tant de l'exploitation des TI que des lignes d'affaires. Le modèle de processus proposé est global et complet, mais il ne s'agit pas du seul possible. Chaque entreprise doit définir son propre ensemble de processus en tenant compte de sa situation.

L'intégration d'un modèle opérationnel et d'un langage commun pour toutes les parties de l'entreprise impliquées dans les activités des TI est l'une des étapes les plus importantes et critiques vers une bonne gouvernance. Cela fournit aussi un cadre pour mesurer et surveiller la performance des TI, communiquer avec les fournisseurs de service et intégrer les meilleures pratiques de gestion.

Le modèle de référence des processus de COBIT 5 sous-divise les processus de gouvernance et de gestion des TI de l'entreprise en deux grands secteurs d'activité : la gouvernance et la gestion, elles-mêmes divisées en domaines de processus :

- **Gouvernance** – Ce domaine contient cinq processus de gouvernance; les pratiques EDS sont définies au sein de chaque processus.
- **Gestion** – Ces quatre domaines sont alignés avec les zones de responsabilité des PCES (une évolution des domaines de COBIT 4.1) et ils fournissent une couverture complète des TI. Chaque domaine contient un certain nombre de processus, comme dans COBIT 4.1 et les versions antérieures. Bien que, comme indiqué précédemment, la plupart des processus nécessitent une « planification », une « mise en œuvre », une « exécution » et des activités de « suivi » dans le cadre du processus ou de la question particulière (par exemple : la qualité, la sécurité), ils se trouvent dans des domaines alignés avec ce qui représente généralement la zone la plus pertinente de l'activité, du point de vue des TI au niveau de l'entreprise.

Dans COBIT 5, les processus couvrent également toute la portée de l'entreprise et les activités des TI liées à la gouvernance et à la gestion des TI de l'entreprise. Le modèle de processus devient ainsi utilisable à l'échelle de l'entreprise.

Le modèle de référence du processus de COBIT 5 constitue le successeur du modèle de processus de COBIT 4.1. Il intègre les modèles de processus de Risk IT et de Val IT. La **figure 31** affiche l'ensemble des 37 processus de gouvernance et de gestion de COBIT 5. Les détails de tous les processus, selon le modèle de processus décrit précédemment, sont inclus dans *COBIT 5: Processus facilitateurs*.

Figure 31 – Modèle de référence du processus COBIT 5

Processus de gouvernance des TI de l'entreprise

Évaluer, diriger et surveiller

EDS01 Assurer la définition et l'entretien d'un référentiel de gouvernance

EDS02 Assurer la livraison des bénéfices

EDS03 Assurer l'optimisation du risque

EDS04 Assurer l'optimisation des ressources

EDS05 Assurer aux parties prenantes la transparence

Aligner, planifier et organiser

APO01 Gérer le cadre de gestion des TI

AP002 Gérer la stratégie

AP003 Gérer l'architecture d'entreprise

AP004 Gérer l'innovation

AP005 Gérer le portefeuille

AP006 Gérer le budget et les coûts

AP007 Gérer les ressources humaines

AP008 Gérer les relations

AP009 Gérer les accords de service

AP010 Gérer les fournisseurs

AP011 Gérer la qualité

AP012 Gérer le risque

AP013 Gérer la sécurité

Surveiller, évaluer et mesurer

SEM01 Surveiller, évaluer et mesurer la performance et la conformité

Bâtir, acquérir et implanter

BAI01 Gérer les programmes et les projets

BAI02 Gérer la définition des exigences

BAI03 Gérer l'identification et la conception des solutions

BAI04 Gérer la disponibilité et la capacité

BAI05 Gérer le changement organisationnel

BAI06 Gérer les changements

BAI07 Gérer l'acceptation du changement et de la transition

BAI08 Gérer la connaissance

BAI09 Gérer les actifs

BAI10 Gérer la configuration

SEM02 Surveiller, évaluer et mesurer le système de contrôles internes

Livrer, servir et soutenir

LSS01 Gérer les opérations

LSS02 Gérer les demandes de service et les incidents

LSS03 Gérer les problèmes

LSS04 Gérer la continuité

LSS05 Gérer les services de sécurité

LSS06 Gérer les contrôles des processus d'affaires

SEM03 Surveiller, évaluer et mesurer la conformité aux exigences externes

Processus de gestion des TI de l'entreprise

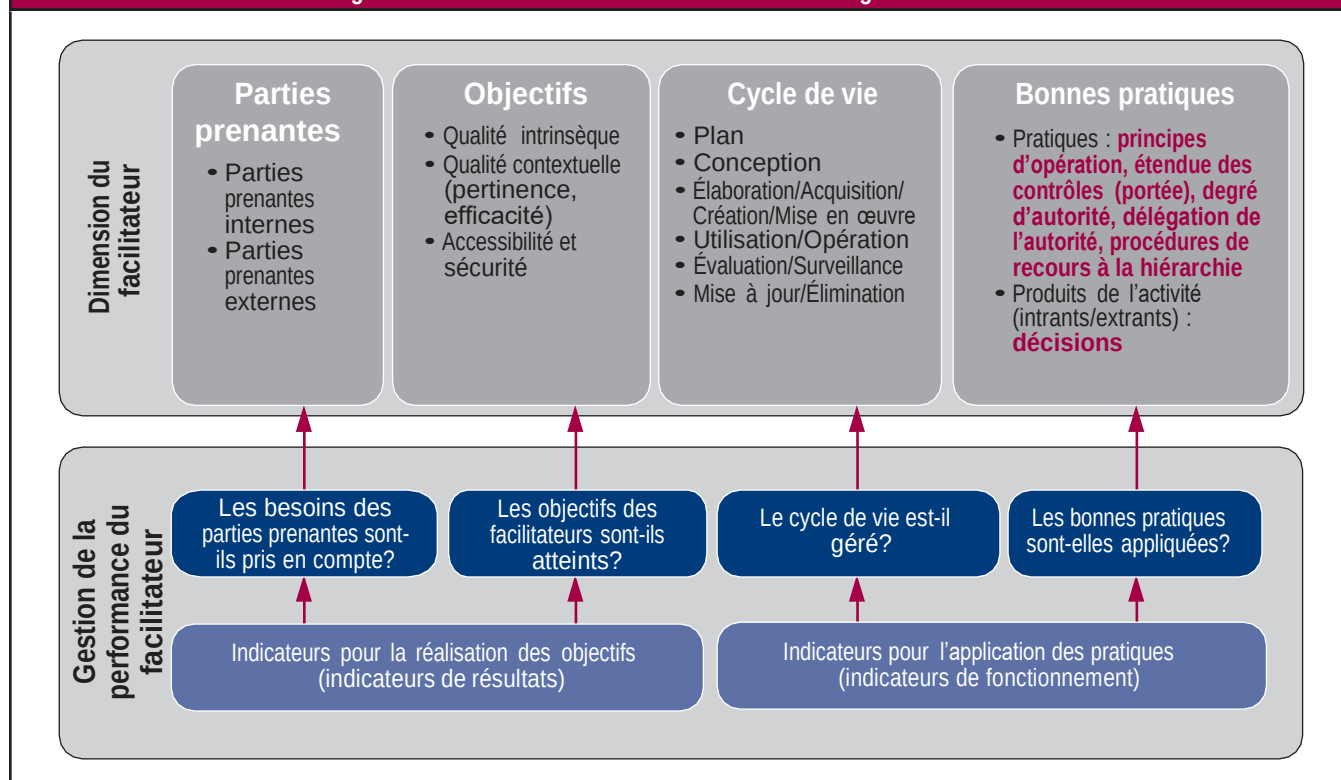
Facilitateur de COBIT 5 : structures organisationnelles

Les particularités du facilitateur des structures organisationnelles comparativement à la description générique d'un facilitateur sont présentées à la **figure 32**.

Le modèle des structures organisationnelles présente les éléments suivants :

- **Parties prenantes** – Les parties prenantes des structures organisationnelles peuvent être internes et externes à l'entreprise, et elles comprennent les membres de la structure, les autres structures, les entités organisationnelles, les clients, les fournisseurs et les organismes de réglementation. Leurs rôles varient et consistent entre autres à prendre des décisions, à influencer et à conseiller. Les enjeux de chacune des parties prenantes varient également, c'est-à-dire qu'elles ont peut-être des intérêts dans les décisions prises par la structure.
- **Objectifs** – Les objectifs pour le facilitateur des structures organisationnelles comprennent un mandat approprié, des principes de fonctionnement bien définis et la mise en œuvre d'autres bonnes pratiques. Le résultat du facilitateur des structures organisationnelles doit inclure un certain nombre d'activités pertinentes et de décisions éclairées.
- **Cycle de vie** – Une structure organisationnelle possède un cycle de vie. Elle est créée, existe et est ajustée, et finalement peut être dissoute. Au moment de sa création, un mandat (une raison et un but pour son existence) doit être défini.
- **Bonnes pratiques** – Il est possible d'énumérer un certain nombre de bonnes pratiques pour les structures organisationnelles. Par exemple :
 - Les principes de fonctionnement – Les dispositions pratiques sur le fonctionnement de la structure, comme la fréquence des réunions, la documentation et les règles de base.
 - La composition – Les structures regroupent des membres, qui constituent des parties prenantes internes ou externes.
 - L'étendue du contrôle – Les limites des droits de décision de la structure organisationnelle.
 - Le niveau d'autorité et les droits de décision – Les décisions que la structure est autorisée à prendre.
 - La délégation d'autorité – La structure peut déléguer en tout ou partie ses droits de décision à d'autres structures qui relèvent d'elle.
 - Les procédures de recours à la hiérarchie – La voie de recours à la hiérarchie pour une structure décrit les actions à réaliser en cas de problèmes dans la prise de décisions.

Figure 32 – Facilitateur de COBIT 5 : structures organisationnelles



Relations avec les autres facilitateurs – Les liens avec les autres facilitateurs sont les suivants :

- Des tableaux RACI relient les activités des processus aux structures organisationnelles et aux différents rôles dans l'entreprise. Ils décrivent le niveau de participation de chaque rôle pour chaque pratique de processus : responsable, approuvateur, personne consultée ou informée.

- La culture, l'éthique et le comportement déterminent l'efficacité et l'efficience des structures organisationnelles et de leurs décisions.
- La composition des structures organisationnelles doit prendre en compte les compétences de ses membres et exiger les compétences appropriées.
- Le cadre des politiques en place doit guider le mandat et les principes de fonctionnement des structures organisationnelles.
- Les intrants et les extrants – Une structure nécessite des intrants (généralement de l'information) avant de pouvoir prendre des décisions éclairées et elle produit des résultats, par exemple des décisions, d'autres informations ou des demandes d'intrants supplémentaires.

STRUCTURES ORGANISATIONNELLES ILLUSTRATIVES DE COBIT 5

Comme mentionné à la section sur le modèle de processus de COBIT 5, un modèle de référence de processus illustratif de COBIT 5 a été créé et est décrit en détail dans *COBIT 5: Processus facilitateurs*. Le modèle comprend des tableaux RACI, qui utilisent un certain nombre de rôles et de structures. Ces rôles et structures prédéfinis sont décrits à la **figure 33**.

Remarques :

- Ceux-ci ne doivent pas nécessairement correspondre aux fonctions réelles que les entreprises ont mises en place. Ils génèrent néanmoins de la valeur, car l'objectif décrit de la structure ou du rôle demeure valable pour la plupart des entreprises.
- L'objectif de ce tableau n'est pas de fournir un organigramme universel pour toutes les entreprises. Il doit plutôt être considéré comme un exemple.

Figure 33 – Rôles et structures organisationnelles de COBIT 5

Rôle / structure	Définition / description
Conseil d'administration	Le groupe des plus hauts dirigeants ou administrateurs non dirigeants de l'entreprise qui ont la responsabilité de la gouvernance de l'entreprise et ont le contrôle de ses ressources.
Chef de la direction	Le dirigeant le plus haut placé qui est en charge de la gestion globale de l'entreprise.
Directeur financier	Le plus haut responsable de l'entreprise en charge de tous les aspects de la gestion financière, y compris les risques et les contrôles financiers ainsi que la fiabilité et la précision des comptes.
Directeur de l'exploitation	Le plus haut responsable de l'entreprise en charge de l'exploitation de l'entreprise.
Directeur de la gestion des risques	Le plus haut responsable de l'entreprise en charge de tous les aspects de la gestion des risques dans l'entreprise. Une fonction de gestionnaire des risques TI pourrait être créée pour superviser les risques liés aux TI.
Dirigeant principal de l'information	Le plus haut dirigeant de l'entreprise en charge de l'alignement des stratégies des TI et des stratégies d'affaires. Il est également responsable de la planification, des ressources et de la gestion de la livraison des services des TI ainsi que des solutions pour soutenir les objectifs de l'entreprise.
Officier principal de la sécurité de l'information	Le plus haut dirigeant de l'entreprise responsable de la sécurité de l'information d'entreprise sous toutes ses formes.
Dirigeant d'entreprise	Un haut dirigeant responsable du fonctionnement d'une division ou d'une filiale particulière.
Détenteur des processus d'affaires	Une personne responsable de la performance d'un processus et de la réalisation de ses objectifs, de l'amélioration des processus et de l'approbation des changements aux processus.
Comité stratégique (dirigeants des TI)	Un groupe de hauts dirigeants nommés par le conseil d'administration afin de s'assurer que ce dernier participe aux grands dossiers et décisions liés aux TI, et qu'il en est tenu informé. Le comité est responsable de gérer les portefeuilles d'investissements en TI, les services des TI et les actifs des TI, en veillant à la création de valeur et que le risque soit géré. Le comité est généralement présidé par un membre du conseil d'administration et non par le dirigeant principal de l'information.
Comités directeurs (projets et programmes)	Un groupe de parties prenantes et d'experts responsables des orientations des programmes et des projets, incluant la gestion et le suivi des plans, l'affectation des ressources, la création de bénéfices et de valeur ainsi que la gestion du programme et des risques du projet.
Comité d'architecture	Un groupe de parties prenantes et d'experts responsable de fournir des orientations sur les questions et les décisions liées à l'architecture d'entreprise, et qui établissent des politiques architecturales et des standards.
Comité des risques d'entreprise	Le groupe de dirigeants de l'entreprise responsable de la collaboration à l'échelle de l'entreprise et du consensus requis pour soutenir les activités et les décisions liées à la gestion des risques d'entreprise. Il est possible de constituer un conseil des risques TI pour examiner les risques détaillés propres aux TI et pour conseiller le comité des risques d'entreprise.
Directeur des ressources humaines	Le plus haut dirigeant de l'entreprise qui est responsable de la planification et des politiques à l'égard de toutes les ressources humaines de l'entreprise.
Conformité	La fonction de l'entreprise responsable de fournir des orientations en matière de conformité juridique, réglementaire et contractuelle.
Audit	La fonction de l'entreprise responsable de réaliser des audits internes.

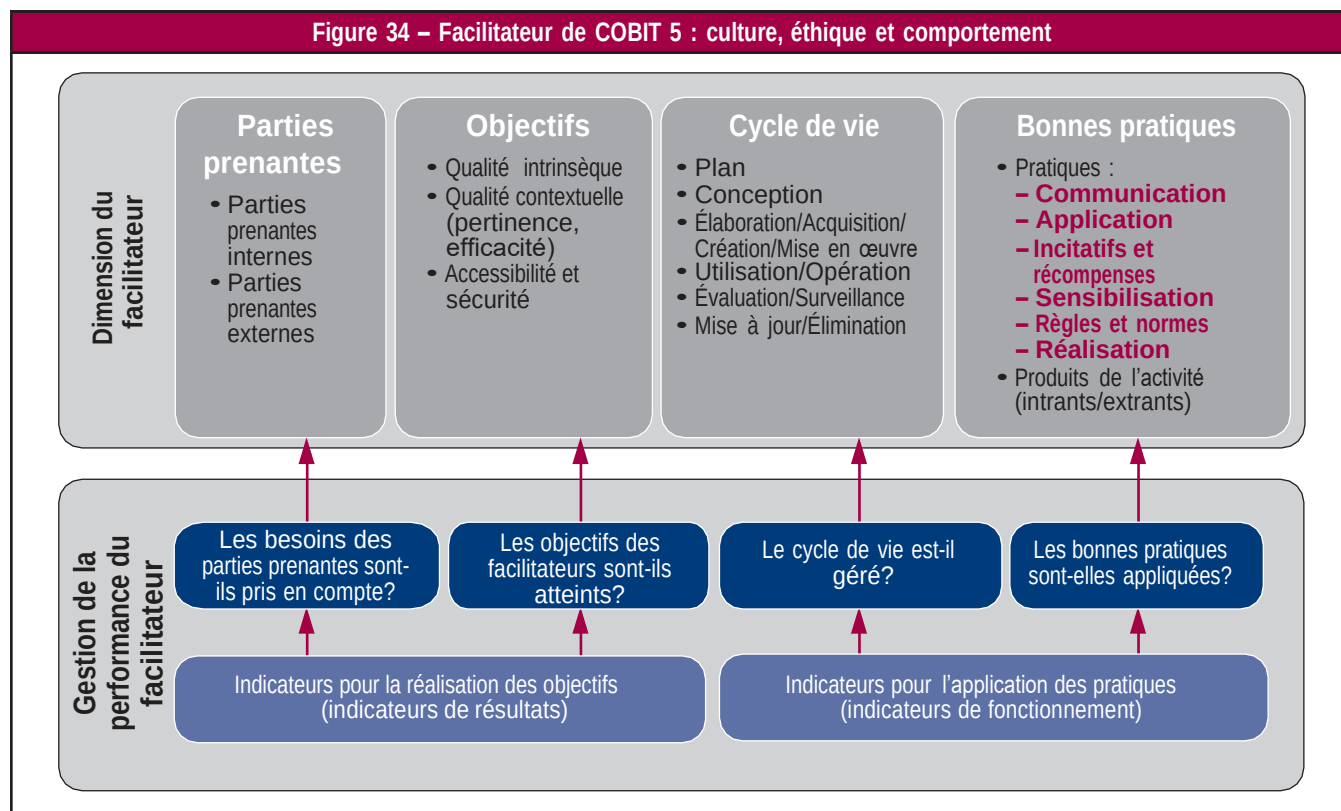
Figure 33 – Rôles et structures organisationnelles de COBIT 5 (suite)

Rôle / structure	Définition / description
Directeur de l'architecture	Un cadre supérieur responsable du processus d'architecture d'entreprise.
Directeur du développement	Un cadre supérieur responsable des processus de développement de solution liée aux TI.
Directeur de l'exploitation des TI	Un cadre supérieur responsable des milieux opérationnels et de l'infrastructure des TI.
Directeur de l'administration des TI	Un cadre supérieur responsable des dossiers liés aux TI et de soutenir les questions administratives liées aux TI.
Bureau de gestion des programmes et projets	La fonction responsable de soutenir le programme et les gestionnaires de projets, ainsi que la collecte, l'évaluation et la communication de l'information au sujet de la conduite de leurs programmes et projets constitutifs
Bureau de gestion de la valeur	La fonction qui fait office de secrétariat pour la gestion des portefeuilles d'investissements et de services, incluant l'évaluation et les conseils sur les opportunités d'investissement et les dossiers d'affaires, en recommandant des méthodes et des contrôles de gouvernance ou de gestion de la valeur, et en faisant rapport des progrès accomplis en matière de maintien et de création de valeur par des investissements et des services.
Gestionnaire de services	Une personne qui gère l'élaboration, la mise en œuvre, l'évaluation et la gestion continue des produits et services nouveaux et existants pour un client particulier (utilisateur) ou un groupe de clients (utilisateurs).
Responsable de la sécurité de l'information	Une personne qui gère, conçoit, supervise ou évalue la sécurité de l'information d'une entreprise.
Directeur de la continuité des opérations	Une personne qui gère, conçoit, supervise ou évalue la capacité de continuité des opérations d'une entreprise, afin d'assurer que les fonctions essentielles de l'entreprise se poursuivent en cas d'événements perturbateurs.
Responsable de la protection de la vie privée	Une personne qui est chargée de surveiller l'impact des lois de protection de la vie privée sur les risques et les affaires ainsi que de conseiller et de coordonner la mise en œuvre de politiques et d'activités qui feront en sorte que les directives de confidentialité soient respectées. Aussi nommé officier de la protection des données.

Facilitateur de COBIT 5 : culture, éthique et comportement

L'expression « culture, éthique et comportement » fait référence à l'ensemble des comportements individuels et collectifs au sein d'une entreprise.

Les particularités du facilitateur en matière de culture, d'éthique et de comportement comparativement à la description générique d'un facilitateur sont présentées à la **figure 34**.



Le modèle culture, éthique et comportement illustre :

- **Parties prenantes** – Les parties prenantes en matière de culture, d'éthique et de comportement peuvent être internes et externes à l'entreprise. Les parties prenantes internes comprennent l'ensemble de l'entreprise, tandis que les parties prenantes externes comprennent les organismes de réglementation, par exemple les auditeurs externes ou les organismes de surveillance. Les enjeux sont de deux ordres : certaines parties prenantes, par exemple, les juristes, les gestionnaires de risques, les gestionnaires des ressources humaines, le comité de la rémunération et ses administrateurs, définissent et appliquent les comportements souhaités, tandis que d'autres doivent s'aligner sur les règles et les normes définies.
- **Objectifs** – Les objectifs facilitants de la culture, de l'éthique et du comportement concernent :
 - L'éthique organisationnelle, déterminée par les valeurs de l'entreprise.
 - L'éthique individuelle, déterminée par les valeurs personnelles de chaque individu de l'entreprise et dans une large mesure, en fonction de facteurs externes comme la religion, l'origine ethnique, les antécédents socioéconomiques, la géographie et les expériences personnelles.
 - Les comportements individuels, qui déterminent collectivement la culture d'une entreprise. De nombreux facteurs, comme les facteurs externes mentionnés ci-dessus, mais aussi les relations interpersonnelles au sein de l'entreprise, les objectifs et les ambitions personnelles, dictent les comportements. Voici certains types de comportements qui peuvent être pertinents dans ce contexte :
 - Comportement face à la prise de risque – Quel niveau de risque l'entreprise pense-t-elle pouvoir absorber et quels risques est-elle prête à prendre?
 - Comportement face au respect des politiques – Dans quelle mesure les personnes vont-elles adopter la politique ou s'y conformer?
 - Comportement face aux résultats négatifs – Comment l'entreprise gère-t-elle les résultats négatifs, c'est-à-dire les pertes ou les occasions manquées? Tire-t-elle des enseignements de ces comportements et essaie-t-elle de s'ajuster, ou distribuera-t-elle les blâmes sans s'attaquer à la cause profonde?
- **Cycle de vie** – Une culture organisationnelle, une position éthique et des comportements individuels, etc., ont tous leur cycle de vie. À partir d'une culture existante, une entreprise peut définir les changements requis et travailler à leur mise en œuvre. Plusieurs outils décrits dans les bonnes pratiques peuvent être utilisés.

- **Bonnes pratiques** – Parmi les bonnes pratiques pour créer, encourager et maintenir un comportement désiré dans toute l'entreprise, on compte :
 - La communication à l'échelle de l'entreprise des comportements souhaités et des valeurs d'entreprise sous-jacentes.
 - La conscience du comportement désiré, renforcée par l'exemple donné par la haute direction et autres champions.
 - Les mesures incitatives pour encourager le comportement souhaité et mesures de dissuasion pour le faire respecter. Il existe un lien clair entre les comportements individuels et le système de récompenses des ressources humaines mis en place par l'entreprise.
 - Les règles et normes, afin de donner des orientations sur les comportements organisationnels désirés. Cet aspect lie très clairement les principes et les politiques mis en place par l'entreprise.
- **Relations avec les autres facilitateurs** – Les liens avec les autres facilitateurs comprennent ce qui suit :
 - Les processus peuvent être élaborés jusqu'à un certain degré de perfection, mais si les parties prenantes du processus n'exécutent pas les activités comme prévu, par exemple si leur comportement en est un de non-respect, les résultats ne seront pas atteints.
 - De même, les structures organisationnelles peuvent être conçues et élaborées en respectant la théorie, mais si leurs décisions ne sont pas mises en œuvre (en raison de différentes motivations personnelles, de manque d'incitatifs, etc.), elles ne donneront pas lieu à une gouvernance et à une gestion convenables des TI de l'entreprise.
 - Les principes et les politiques constituent un mécanisme très important pour communiquer les valeurs de l'entreprise et le comportement désiré.

EXEMPLE 11 – AMÉLIORATION DE LA QUALITÉ

À plusieurs reprises, une entreprise est confrontée à de graves problèmes de qualité pour de nouvelles applications. Malgré le fait qu'une bonne méthodologie de conception de projet logiciel soit en place, des problèmes logiciels causent trop souvent des problèmes opérationnels dans les opérations quotidiennes.

Une enquête démontre que les membres de l'équipe de développement et de gestion sont évalués et récompensés en fonction du respect du délai de livraison et des budgets de leurs projets. Ils ne sont pas évalués en fonction de critères de qualité ou de critères de bénéfices d'affaire. Par conséquent, pendant le développement, ils se concentrent assidûment sur le temps de livraison et sur la réduction des coûts, par exemple la période consacrée aux essais. L'enquête montre également que le respect de la méthodologie et des procédures établies est pratiquement inexistant, car cela exigerait davantage de temps et affecterait le budget de développement (en faveur de la qualité). En outre, la structure organisationnelle fait en sorte que la participation officielle de l'équipe de développement cesse lorsque le développement est transféré à l'équipe des opérations. Dès lors, la participation de l'équipe de développement est seulement indirecte et se fait au moyen de processus établis de gestion des incidents et des problèmes.

La leçon à tirer de cette situation est qu'il faut recourir à de meilleurs incitatifs pour encourager la direction et les équipes de développement de solutions à réaliser un travail de qualité.

EXEMPLE 12 – RISQUE LIÉ AUX TI

Certains symptômes d'une culture inadéquate ou problématique en matière de risques liés aux TI comprennent :

- Désalignement entre la tolérance au risque réelle et ce qui est transmis dans les politiques. Les valeurs réelles de la direction face au risque peuvent être raisonnablement audacieuses et tolérantes au risque, alors que les politiques qui sont créées correspondent à une attitude beaucoup plus prudente. Par conséquent, il existe un décalage entre les valeurs et les moyens de les réaliser, ce qui conduit inévitablement à des conflits. Ceux-ci peuvent survenir, par exemple, entre les incitatifs prévus pour la direction et l'exécution des politiques désalignées.
- L'existence d'une « culture de blâme ». Il faut par tous les moyens éviter ce type de culture; c'est l'inhibiteur le plus efficace d'une communication pertinente et efficace. Dans une culture de blâme, les unités d'affaires ont tendance à pointer les TI du doigt lorsque les projets ne sont pas livrés à temps ou ne répondent pas aux attentes. Ce faisant, elles ne parviennent pas à comprendre à quel point la participation de l'unité d'affaires affecte la réussite du projet. Dans les cas extrêmes, l'unité d'affaires peut être blâmée pour ne pas avoir répondu aux attentes qu'elle n'a jamais clairement communiquées. Le « jeu du blâme » ne fait que porter atteinte à une communication efficace entre les unités d'affaires, ce qui crée de nouveaux retards. Les membres de la direction doivent cerner et maîtriser rapidement une culture de blâme afin de favoriser la collaboration dans toute l'entreprise.

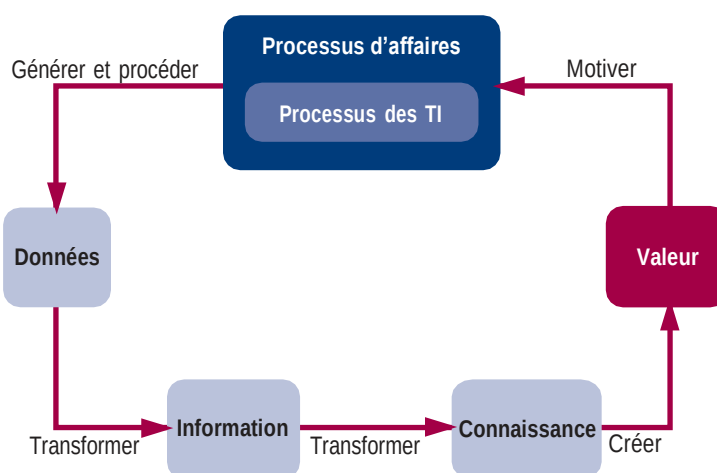
Facilitateur de COBIT 5 : information

Introduction – Le cycle de l'information

Le facilitateur de l'information traite toute l'information pertinente pour l'entreprise, et non uniquement l'information automatisée. L'information peut être structurée ou non structurée, formelle ou informelle.

L'information peut être considérée comme une étape du « cycle de l'information » de l'entreprise. Dans le cycle de l'information (**figure 35**), les processus d'affaires génèrent et traitent les données, les transformant en information et connaissance, et générant à terme la valeur pour l'entreprise. La portée du facilitateur de l'information concerne principalement l'étape « information » du cycle de l'information, mais les aspects des données et des connaissances sont également couverts dans COBIT 5.

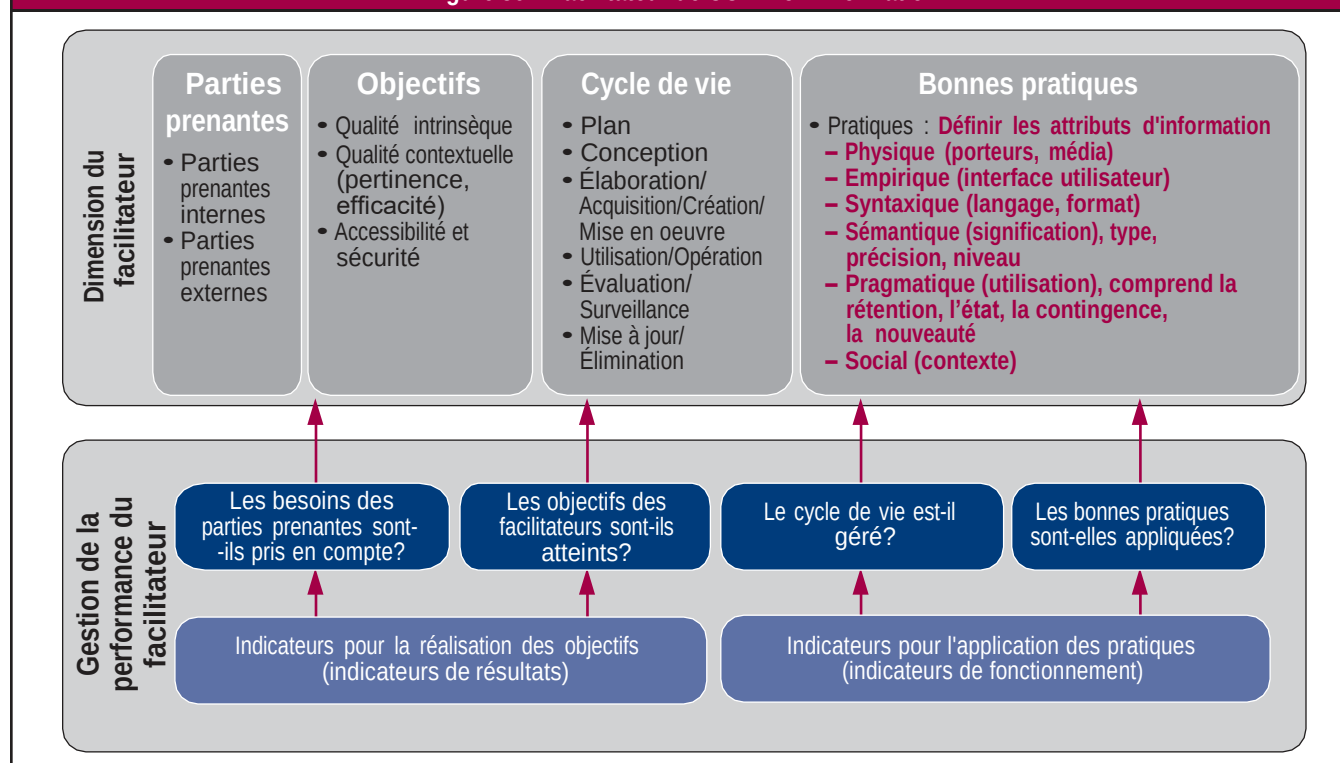
Figure 35 – Métadonnées de COBIT 5 – Cycle de l'information



Facilitateur de l'information de COBIT 5

Les particularités du facilitateur de l'information comparativement à la description générique d'un facilitateur sont présentées à la **figure 36**.

Figure 36 – Facilitateur de COBIT 5 : information



Le modèle d'information (MI) présente les éléments suivants :

- **Les parties prenantes** – Peuvent être internes ou externes à l'entreprise. Le modèle générique suggère également que, mis à part l'identification des parties prenantes, leurs enjeux doivent être définis, c'est-à-dire pourquoi elles se soucient de l'information ou pourquoi elles s'y intéressent.

En ce qui concerne les parties prenantes et l'information qui leur est liée, différents rôles sont possibles dans le traitement de l'information, allant de propositions détaillées (par exemple : suggérer des données précises ou des rôles d'information comme un architecte, un propriétaire, un administrateur, un fiduciaire, un fournisseur, un bénéficiaire, un modélisateur, un responsable de la qualité, un gestionnaire de la sécurité) jusqu'aux propositions plus générales (par exemple : établir une distinction entre les producteurs de l'information, les dépositaires de l'information et les consommateurs de l'information) :

- Le producteur de l'information, responsable de la création de l'information.
- Le dépositaire de l'information, responsable de la conservation et du maintien de l'information.
- Le consommateur de l'information, responsable de l'utilisation de l'information.

Ces catégories se rapportent à des activités particulières à l'égard de la ressource « d'information ». Les activités dépendent de l'étape du cycle de vie de l'information; par conséquent, pour trouver une catégorie de rôles qui possède un degré de granularité approprié au modèle d'information, on peut recourir à la caractéristique du cycle de vie de l'information du modèle d'information. Cela signifie que les rôles des parties prenantes de l'information peuvent être définis en termes d'étapes du cycle de vie de l'information. Par exemple, des planificateurs d'information, des collecteurs d'information, des utilisateurs d'information. Du coup, cela signifie que la dimension des parties prenantes de l'information n'est pas une dimension indépendante; différentes étapes du cycle de vie ont différentes parties prenantes.

Alors que les rôles pertinents dépendent de l'étape du cycle de vie de l'information, les enjeux peuvent être liés à des objectifs d'information.

- **Objectifs** – Les objectifs de l'information sont divisés en trois sous-dimensions de la qualité :

Qualité intrinsèque – La mesure selon laquelle les valeurs de données sont en conformité avec les valeurs réelles.

Cela comprend :

- Précision – La mesure selon laquelle l'information est correcte et fiable.
- Objectivité – La mesure selon laquelle l'information est non biaisée, sans préjugés et impartiale.
- Crédibilité – La mesure selon laquelle l'information est considérée comme vraie et crédible.
- Réputation – La mesure selon laquelle l'information est hautement considérée en matière de source ou de contenu.

Qualité contextuelle et de représentation – La mesure selon laquelle l'information est applicable à la tâche de l'utilisateur de l'information et est présentée d'une manière intelligible et claire, tout en reconnaissant que la qualité de l'information dépend du contexte d'utilisation. Cela comprend :

- Pertinence – La mesure selon laquelle l'information est applicable et utile pour la tâche à accomplir.
- Intégralité – La mesure selon laquelle aucune information ne manque et est de profondeur et d'ampleur suffisantes pour la tâche à accomplir.
- Actualisation – La mesure selon laquelle l'information est suffisamment actuelle pour la tâche à accomplir.
- Quantité appropriée d'information – La mesure selon laquelle le volume d'information est adéquat pour la tâche à accomplir.
- Représentation concise – La mesure selon laquelle l'information est représentée de façon condensée.
- Représentation constante – La mesure selon laquelle l'information est présentée dans le même format.
- Intelligibilité – La mesure selon laquelle l'information est fournie dans la langue appropriée en utilisant les symboles et les unités appropriées, avec des définitions claires.
- Compréhensibilité – La mesure selon laquelle l'information est facilement comprise.
- Facilité d'usage – La mesure selon laquelle l'information est facile à manipuler et à appliquer aux différentes tâches.

Qualité de sécurité et d'accessibilité – La mesure selon laquelle l'information est disponible ou peut être obtenue. Cela comprend :

- Disponibilité et rapidité – La mesure selon laquelle l'information est disponible en cas de besoin, ou facilement et rapidement accessible.
- Accès restreint – La mesure selon laquelle l'accès à l'information est limité de manière appropriée aux parties autorisées.

L'annexe F fournit une description détaillée de la façon dont le critère de qualité de l'information de COBIT 5 se compare au critère d'information de COBIT 4.1. Par exemple, l'intégrité (définie dans COBIT 4.1) est couverte par les objectifs d'information de l'exhaustivité et de l'exactitude.

- **Cycle de vie** – Le cycle de vie complet de l'information doit être pris en considération et différentes approches peuvent être nécessaires pour l'information lors des différentes étapes du cycle de vie. Le facilitateur de l'information de COBIT 5 distingue les étapes suivantes :

- **Plan** – L'étape au cours de laquelle la création et l'utilisation de la ressource d'information sont préparées. Les activités de cette étape peuvent comprendre la définition d'objectifs, la planification de l'architecture de l'information et l'élaboration de normes et de définitions, par exemple, les définitions des données ou les procédures de collecte des données.
- **Conception**
- **Bâtir / acquérir** – L'étape au cours de laquelle l'information est obtenue. Les activités de cette étape peuvent comprendre la création d'enregistrements de données, l'achat de données et le chargement de fichiers externes.
- **Utiliser / exploiter**, qui comprennent :
 - **Stocker** – L'étape au cours de laquelle l'information est conservée de façon électronique ou sur papier (ou simplement dans la mémoire humaine). Les activités de cette étape peuvent comprendre le stockage d'information sous forme électronique (par exemple, fichiers électroniques, bases de données, entrepôts de données) ou en version papier.
 - **Partager** – L'étape au cours de laquelle l'information est mise à la disposition des utilisateurs grâce à une méthode de distribution. Les activités de cette étape peuvent comprendre des processus inclus dans la livraison de l'information à des endroits où elle peut être consultée et utilisée, par exemple, la distribution de documents par courriel. Pour l'information conservée sur support électronique, cette étape du cycle de vie peut largement chevaucher l'étape de stockage, par exemple, le partage de l'information grâce à un accès à une base de données, à des serveurs de fichiers ou de documents.
 - **Utiliser** – L'étape au cours de laquelle l'information est utilisée pour atteindre les objectifs. Les activités de cette étape peuvent comprendre tous les types d'utilisation de l'information (par exemple, la prise de décision de gestion, l'exécution de processus automatisés), et peuvent également inclure des activités comme la recherche d'information et la conversion d'information d'une forme à une autre.

D'après « Taking Governance Forward », l'information constitue un facilitateur pour la gouvernance d'entreprise; ainsi, l'utilisation de l'information telle que définie dans le modèle d'information peut être prévue en fonction des besoins des parties prenantes en matière de gouvernance d'entreprise lorsqu'elles accomplissent leurs rôles et leurs activités, et lorsqu'elles interagissent les unes avec les autres.

Ces rôles, activités et relations sont illustrés à la **figure 9**. Les interactions entre les parties prenantes exigent des flux d'information dont les objectifs sont indiqués dans le schéma : approbation, délégation, suivi, établissement de l'orientation, alignement, exécution et contrôle.

- **Surveiller** – L'étape au cours de laquelle on veille à ce que la source d'information continue d'opérer correctement, par exemple afin d'être utile. Les activités de cette étape peuvent comprendre le fait de garder l'information à jour ainsi que d'autres types d'activités de gestion de l'information; par exemple, l'amélioration, le nettoyage, l'appariement, la suppression des doublons dans les entrepôts de données.
- **Éliminer** – L'étape au cours de laquelle l'information est supprimée quand elle n'est plus utile. Les activités de cette étape peuvent comprendre l'archivage ou la destruction de l'information.
- **Bonne pratique** – La notion d'information est comprise différemment dans différentes disciplines telles que l'économie, la théorie de la communication, la science de l'information, la gestion des connaissances et les systèmes d'information. Par conséquent, il n'existe pas de définition universellement acceptée de ce qu'est l'information. La nature de l'information peut toutefois être précisée par la définition et la description de ses propriétés.

Le schéma qui suit est proposé pour structurer les différentes propriétés de l'information : il se compose de six niveaux ou couches afin de définir et de décrire les propriétés de l'information. Ces six niveaux présentent un continuum d'attributs, allant du monde physique de l'information, où les attributs sont liés aux technologies de l'information et aux médias pour l'obtention, le stockage, le traitement, la distribution et la présentation de l'information, jusqu'au monde social de l'utilisation, de la compréhension et de l'action de l'information.

Les descriptions qui suivent peuvent être associées aux couches et aux attributs de l'information :

- **Couche du monde physique** – Le monde où ont lieu tous les phénomènes qui peuvent être observés de façon empirique.
 - Support de l'information et média – L'attribut qui définit le support physique de l'information, par exemple, papier, signaux électriques, ondes sonores.
- **Couche empirique** – L'observation empirique des signes utilisés pour coder l'information et leur distinction les uns des autres et du bruit de fond.
 - Canal d'accès à l'information – L'attribut qui identifie le canal d'accès de l'information, par exemple, des interfaces utilisateur.
- **Couche syntaxique** – Les règles et principes de construction des phrases dans les langues naturelles ou artificielles. La syntaxe fait référence à la forme de l'information.
 - Code / langage – Attribut qui définit le langage figuratif ou le format utilisé pour encoder l'information ainsi que les règles pour combiner les symboles de la langue pour former des structures syntaxiques.

- **Couche sémantique** – Les règles et principes de construction d'un sens à partir des structures syntaxiques. La sémantique fait référence à la signification de l'information.
 - Type d'information – L'attribut qui définit le type d'information. Par exemple, l'information financière ou non financière, l'origine interne ou externe de l'information, les valeurs prévues ou observées, les valeurs prévues ou réalisées.
 - Information à jour – L'attribut qui définit l'horizon temporel visé par l'information, c'est-à-dire de l'information sur le passé, le présent ou l'avenir.
 - Niveau d'information – L'attribut qui définit le degré de précision de l'information, par exemple, les ventes par année, trimestre, mois.
- **Couche pragmatique** – Les règles et les structures de construction de grandes structures linguistiques qui répondent à des fins précises dans la communication humaine. Le pragmatisme fait référence à l'utilisation de l'information.
 - Période de rétention – L'attribut qui définit pendant combien de temps l'information peut être conservée avant d'être détruite.
 - Statut de l'information – L'attribut qui définit si l'information est opérationnelle ou historique.
 - Nouveauté – L'attribut qui définit si l'information crée de nouvelles connaissances ou confirme les connaissances existantes, c'est-à-dire l'information ou la confirmation.
 - Contingence – L'attribut qui définit l'information qui doit précéder cette information (pour qu'elle soit considérée comme une information).
- **Couche du monde social** – Le monde qui est socialement construit grâce à l'utilisation des structures de la langue au niveau pragmatique de la sémiotique; par exemple, des contrats, le droit, la culture.
 - Contexte – L'attribut qui définit la situation dans laquelle l'information a un sens, est utilisée, a une valeur, etc. Par exemple, le contexte culturel, le contexte du domaine.

Autres considérations relatives à l'information – Les investissements dans l'information et les technologies connexes sont fondés sur des dossiers d'affaires, qui comprennent l'analyse coûts-bénéfices. Les coûts et bénéfices concernent non seulement des facteurs tangibles et mesurables, mais ils prennent également en considération des facteurs intangibles comme l'avantage concurrentiel, la satisfaction du client et l'incertitude technologique. Ce n'est que lorsque la ressource d'information est appliquée ou utilisée qu'une entreprise en retire des avantages, de sorte que la valeur de l'information est déterminée uniquement par son utilisation (à l'interne ou en la vendant); l'information n'a pas de valeur intrinsèque. Cette valeur peut-être générée uniquement grâce à la mise en action de l'information.

Le modèle d'information constitue un nouveau modèle très riche en terme de composants. Il en sera question dans une publication distincte. Pour le rendre plus tangible pour l'utilisateur de COBIT 5 et pour rendre sa pertinence plus évidente dans le contexte du référentiel global de COBIT 5, nous vous fournissons les exemples 13, 14 et 15, qui abordent l'utilisation possible du modèle d'information.

EXEMPLE 13 – MODÈLE D'INFORMATION UTILISÉ POUR LES SPÉCIFICATIONS DE L'INFORMATION

Au moment de concevoir une nouvelle application, il est possible d'utiliser le modèle de l'information pour aider à l'élaboration des spécifications de l'application et de l'information ou des modèles de données associés.

Les attributs d'information du modèle d'information peuvent être utilisés pour définir les spécifications de l'application et des processus d'affaires qui utiliseront l'information.

Par exemple, la conception et les spécifications du nouveau système doivent préciser ce qui suit :

- **Couche physique** – Où l'information sera-t-elle stockée?
- **Couche empirique** – Comment l'information peut-elle être consultée?
- **Couche syntaxique** – Comment l'information sera-t-elle structurée et codée?
- **Couche sémantique** – De quelle sorte d'information s'agit-il? Quel est le niveau d'information?
- **Couche pragmatique** – Quelles sont les exigences de conservation? Quelle autre information est nécessaire pour que cette information soit utile et utilisable?

En regardant la caractéristique des parties prenantes combinée au cycle de vie de l'information, on peut définir qui aura besoin de quel type d'accès aux données au cours de quelle étape du cycle de vie de l'information.

Lorsque l'application est testée, les testeurs peuvent considérer le critère de qualité de l'information pour élaborer un ensemble complet de cas d'essai.

EXEMPLE 14 – MODÈLE D'INFORMATION UTILISÉ POUR DÉTERMINER LA PROTECTION REQUISE

Les groupes de sécurité au sein de l'entreprise peuvent profiter de la dimension des attributs du modèle d'information. En effet, pour assurer la protection de l'information, ils doivent se pencher sur les éléments suivants :

- **Couche physique** – Comment et où l'information est-elle stockée physiquement?
- **Couche empirique** – Quels sont les canaux d'accès à l'information?
- **Couche sémantique** – De quel type d'information s'agit-il? L'information est-elle à jour ou en rapport avec le passé ou l'avenir?
- **Couche pragmatique** – Quelles sont les exigences de conservation? L'information est-elle historique ou opérationnelle?

L'utilisation de ces attributs permet à l'utilisateur de déterminer le niveau et les mécanismes de protection nécessaires.

En considérant une autre dimension du modèle d'information, les professionnels de la sécurité peuvent également envisager les étapes du cycle de vie de l'information, car l'information doit être protégée pendant toutes les étapes du cycle de vie. En effet, la sécurité commence à l'étape de planification de l'information et englobe différents mécanismes de protection pour le stockage, le partage et l'élimination de l'information. Le modèle d'information garantit que l'information est protégée pendant l'ensemble de son cycle de vie.

EXEMPLE 15 – MODÈLE D'INFORMATION UTILISÉ POUR DÉTERMINER LA FACILITÉ DE L'UTILISATION DES DONNÉES

Au cours de la révision d'un processus d'affaires (ou d'une application), le modèle d'information peut être utilisé pour aider à réaliser une revue générale de l'information traitée et livrée par le processus ainsi que des systèmes d'information sous-jacents. Le critère de qualité peut être utilisé pour évaluer dans quelle mesure l'information est disponible, c'est-à-dire si l'information est complète, exacte, pertinente, disponible en quantité appropriée et en temps opportun. On peut également envisager le critère d'accessibilité, c'est-à-dire si l'information est accessible lorsque cela est nécessaire et si elle est suffisamment protégée.

La révision peut être approfondie davantage pour inclure le critère de représentation, par exemple, la facilité avec laquelle l'information peut être comprise, interprétée, utilisée et manipulée.

Une révision qui utilise le critère de qualité de l'information du modèle d'information fournit à l'entreprise une vision globale et complète de la qualité de l'information actuelle au sein d'un processus d'affaires.

Facilitateur de COBIT 5 : services, infrastructures et applications

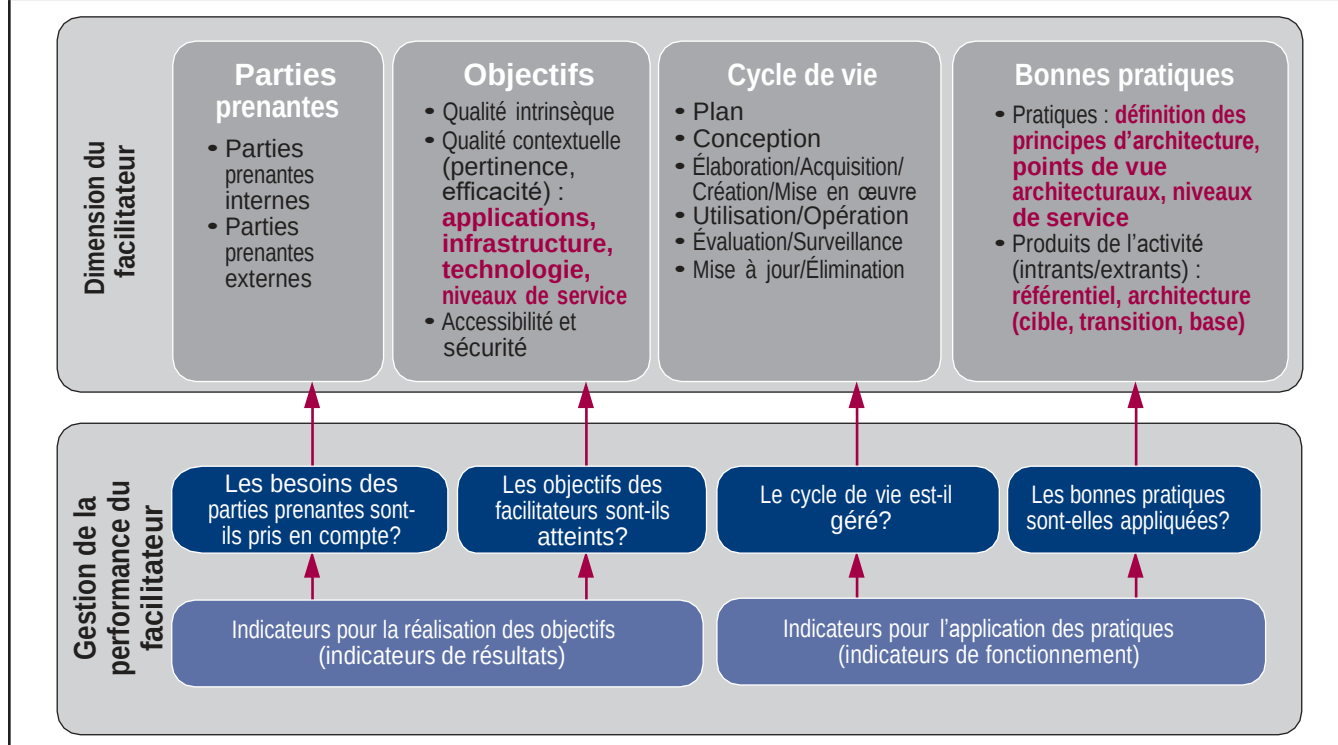
Les capacités de service font référence à des ressources telles que des applications et des infrastructures qui sont mises à profit dans la livraison des services liés aux TI.

Les particularités du facilitateur des capacités de service comparativement à la description générique d'un facilitateur sont présentées à la **figure 37**.

Le modèle de services, d'infrastructures et d'applications présente :

- **Les parties prenantes** – Les parties prenantes des capacités de service (les modalités combinées des services, de l'infrastructure et des applications) peuvent être internes ou externes. Les services peuvent être fournis par des parties prenantes internes ou externes (services des TI internes, directeurs des opérations, fournisseurs de services externes). Les utilisateurs de services peuvent aussi être internes (utilisateurs professionnels) ou externes (partenaires, clients, fournisseurs). Les enjeux de chacune des parties prenantes doivent être définis et seront axés sur la livraison de services adéquats ou sur la réception des services demandés par les fournisseurs.
- **Les objectifs** – Les objectifs de la capacité de niveau de service seront exprimés en matière de services (applications, infrastructures, technologie) et de niveaux de service, en tenant compte des services et des niveaux de service les plus économiques pour l'entreprise. Encore une fois, les objectifs porteront sur les services et la façon dont ils sont fournis, ainsi que leurs résultats, à savoir la contribution vers la prise en charge réussie des processus d'affaires.
- **Le cycle de vie** – Les capacités de service ont un cycle de vie. Les capacités de service futures ou planifiées sont généralement décrites dans une architecture cible. Cette dernière couvre les éléments constitutifs, comme les applications futures et le modèle d'infrastructure cible et décrit également les liens et les relations entre eux.

Figure 37 – Facilitateur de COBIT 5 : services, infrastructures et applications



Les capacités de service actuelles qui sont utilisées ou exploitées de manière à fournir des services de TI courants sont décrites dans une architecture de base. Selon le calendrier de l'architecture cible, une architecture de transition peut également être définie, ce qui montre l'entreprise dans différents états progressifs entre l'architecture cible et l'architecture de base.

- **Bonnes pratiques** – Les bonnes pratiques en matière de capacité de service comprennent ce qui suit :
 - Définition des principes d'architecture – Les principes d'architecture constituent des lignes directrices générales qui régissent la mise en œuvre et l'utilisation des ressources liées aux TI au sein de l'entreprise. Voici des exemples de principes d'architecture potentiels :
 - **Réutilisation** – Des composantes communes de l'architecture doivent être utilisées au moment de la conception et de la mise en œuvre des solutions dans le cadre d'architectures cibles ou de transition.
 - **Achat ou conception** – Les solutions doivent être achetées à moins qu'il existe une justification approuvée pour les concevoir à l'interne.
 - **SimPLICITÉ** – L'architecture d'entreprise doit être conçue et maintenue de telle sorte qu'elle soit aussi simple que possible, tout en respectant les exigences de l'entreprise.
 - **Agilité** – L'architecture d'entreprise doit intégrer l'agilité pour répondre d'une manière efficace aux besoins changeants de l'entreprise.
 - **Ouverture** – L'architecture d'entreprise doit tirer parti des normes ouvertes de l'industrie.
 - La définition de l'entreprise du point de vue architectural le plus approprié pour répondre aux besoins des différentes parties prenantes. Ce sont les modèles, les catalogues et les matrices utilisés pour décrire les architectures de base, cibles ou de transition; par exemple, une architecture d'application pourrait être décrite au moyen d'un diagramme d'interface de l'application, qui montre les applications en cours d'utilisation (ou prévues) et les interfaces entre elles.
 - Avoir un référentiel d'architecture, qui peut être utilisé pour contenir différents types de produits architecturaux, y compris les principes et les normes, les modèles de référence et les autres éléments livrables, et qui définit les éléments constitutifs des services, par exemple:
 - Applications qui fournissent des fonctionnalités d'affaires.
 - Infrastructure technologique, incluant le matériel, les logiciels et l'infrastructure réseau.
 - Infrastructure physique.
 - Les niveaux de service qui doivent être définis et réalisés par les fournisseurs de services.

Il existe de bonnes pratiques externes pour les référentiels d'architecture et les capacités de service. Ce sont des lignes directrices, des modèles ou des normes qui peuvent être utilisés pour accélérer la création des livrables d'architecture. Voici quelques exemples :

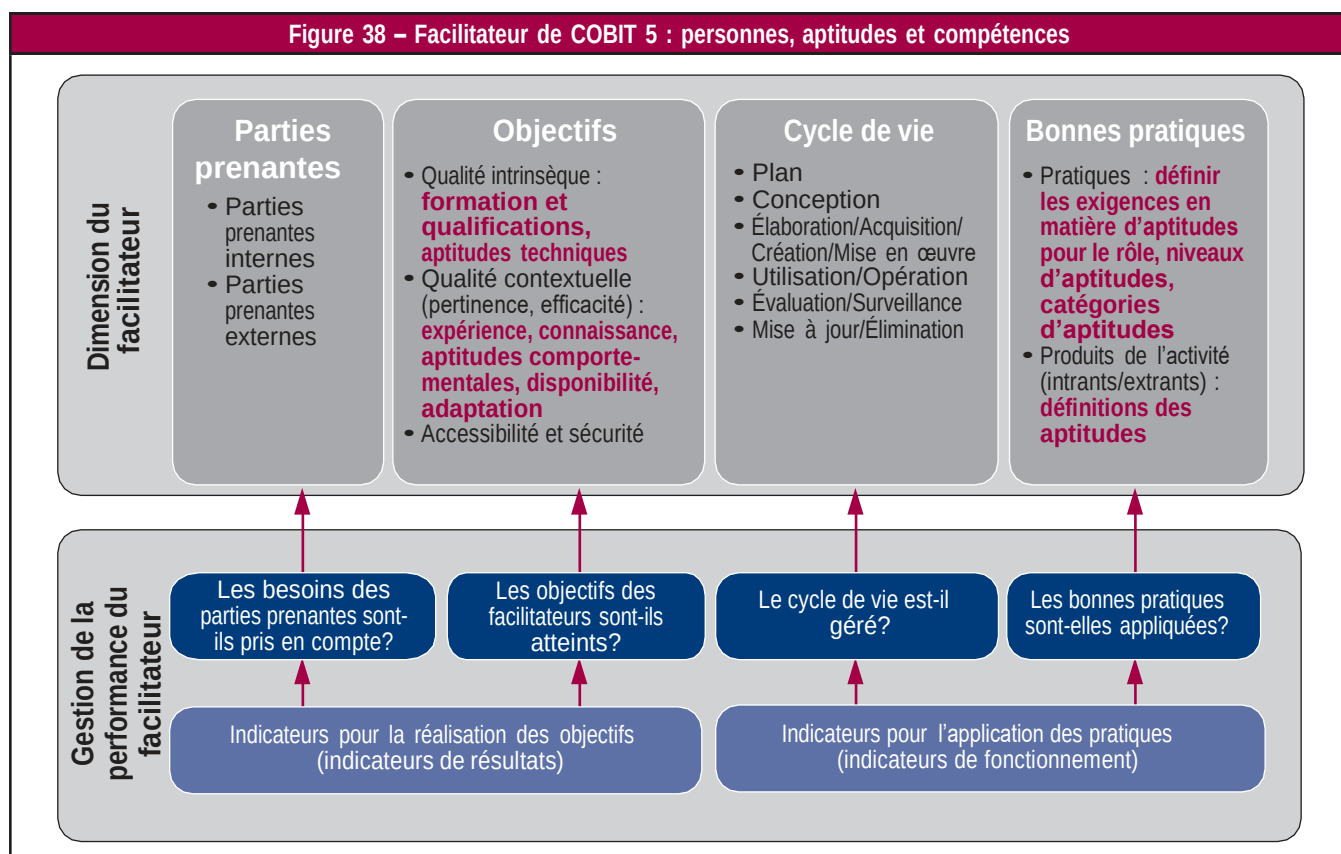
- TOGAF¹⁶ fournit un modèle de référence technique et un modèle intégré de référence d'infrastructure d'information.
- ITIL fournit des orientations détaillées sur la manière de concevoir et d'exploiter des services.

¹⁶ www.opengroup.org/togaf

- **Relations avec les autres facilitateurs** – Les liens avec les autres facilitateurs comprennent :
 - L’information est l’une des capacités de service, et les capacités de service sont exploitées au moyen de processus de livraison de services internes et externes.
 - Les aspects culturels et comportementaux sont aussi pertinents lorsqu’une culture axée sur le service doit être bâtie.
 - Dans COBIT 5, les intrants et les extrants des pratiques et des activités de gestion pourraient inclure des capacités de service, qui sont nécessaires à titre d’intrants ou livrées à titre d’extrants.

Facilitateur de COBIT 5 : personnes, aptitudes et compétences

Les particularités du facilitateur en matière de personnes, d’aptitudes et de compétences comparativement à la description générique d’un facilitateur sont présentées à la **figure 38**.



Le modèle de personnes, d’aptitudes et de compétences présente les éléments suivants :

- **Les parties prenantes** – Les parties prenantes détentrices d’aptitudes et de compétences sont internes et externes à l’entreprise. Différentes parties prenantes assument des rôles différents (gestionnaires d’affaires, gestionnaires de projets, partenaires, concurrents, recruteurs, formateurs, développeurs, spécialistes techniques en TI, etc.) et chaque rôle nécessite un ensemble de compétences distinctes.
- **Les objectifs** – Les objectifs en matière d’aptitudes et de compétences se rapportent à des niveaux de formation et de qualification, à des compétences techniques, à l’expérience, aux connaissances et aux compétences comportementales nécessaires pour exécuter avec succès les activités de processus, les rôles organisationnels, etc. Les objectifs pour les personnes comprennent les niveaux adéquats de disponibilité du personnel et le taux de roulement.
- **Le cycle de vie** :
 - Les aptitudes et les compétences ont un cycle de vie. Une entreprise doit savoir quelle est sa base de compétences actuelle et planifier ce qu’elle doit être. Cette base est entre autres influencée par la stratégie et les objectifs de l’entreprise. Les aptitudes doivent être perfectionnées (par exemple, grâce à la formation) ou acquises (par exemple, grâce au recrutement) et déployées dans les différents rôles au sein de la structure organisationnelle. Il faudra peut-être délaisser des aptitudes, par exemple, si une activité est automatisée ou confiée à l’externe.
 - Périodiquement, par exemple sur une base annuelle, l’entreprise doit évaluer les aptitudes de base pour comprendre l’évolution qui a eu lieu. Ce résultat sera intégré au processus de planification pour la prochaine période.
 - Cette évaluation peut également alimenter le processus de récompense et de reconnaissance des ressources humaines.
- **Les bonnes pratiques** :
 - Les bonnes pratiques en matière d’aptitudes et de compétences comprennent la définition des besoins en matière d’aptitudes pour chaque rôle joué par les différentes parties prenantes. Il est possible de décrire cet aspect grâce à divers

niveaux de qualification dans différentes catégories d'aptitudes. Pour chaque niveau d'aptitude approprié dans chaque catégorie d'aptitudes, une définition doit être disponible. Les catégories d'aptitudes correspondent aux activités liées aux TI, par exemple, la gestion de l'information, l'analyse d'affaires.

– Autre bonne pratique :

- Il existe des sources externes de bonnes pratiques, comme le référentiel de compétences pour l'ère de l'information (Skills Framework for the Information Age, SFIA),¹⁷ qui fournissent des définitions complètes de compétences.
- Des exemples de catégories de compétences possibles, mises en correspondance avec les domaines de processus de COBIT 5, sont présentés à la **figure 39**.

Figure 39 – Catégories de compétences de COBIT 5	
Domaine de processus	Exemples de catégories de compétences
Évaluer, diriger et surveiller (EDS)	• Gouvernance des TI de l'entreprise
Aligner, planifier et organiser (APO)	• Élaboration des politiques en TI • Stratégie des TI • Architecture d'entreprise • Innovation • Gestion financière • Gestion de portefeuille
Bâtir, acquérir et implanter (BAI)	• Analyse d'affaires • Gestion de projet • Évaluation de la convivialité • Définition et gestion des besoins • Programmation • Ergonomie du système • Déclassement de logiciel • Gestion de la capacité
Livrer, servir et soutenir (LSS)	• Gestion de la disponibilité • Gestion des problèmes • Bureau de service et gestion des incidents • Administration de la sécurité • Exploitation des TI • Administration de bases de données
Surveiller, évaluer et analyser (SEA)	• Examen de la conformité • Suivi de la performance • Audit des contrôles

• **Relations avec d'autres facilitateurs** – Les liens avec d'autres facilitateurs contiennent ce qui suit :

- Des aptitudes et des compétences sont nécessaires pour réaliser les activités des processus et pour prendre des décisions au sein des structures organisationnelles. Inversement, certains processus visent à soutenir le cycle de vie des aptitudes et des compétences.
- Il existe aussi un lien avec la culture, l'éthique et le comportement par le biais des compétences comportementales, qui entraînent des comportements individuels et sont influencées par l'éthique individuelle et l'éthique de l'organisation.
- Les définitions des aptitudes constituent également de l'information, pour lesquelles les bonnes pratiques du facilitateur de l'information doivent être prises en considération.