Pour une meilleure gouvernance des systèmes d'information

COBIT

GOVERNANCE, CONTROL *and* ASSURANCE *for* INFORMATION *and* RELATED TECHNOLOGY

VOTRE FOMATEUR

TOUR DE TABLE

QU'ATTENDEZ VOUS DE CETTE FORMATION ?

La Formation

COBIT
GOVERNANCE, CONTROL *and* ASSURANCE *for* INFORMATION *and* RELATED TECHNOLOGY

Participez

- Posez vos questions
- Partagez vos expériences,
  Bonnes ou mauvaises

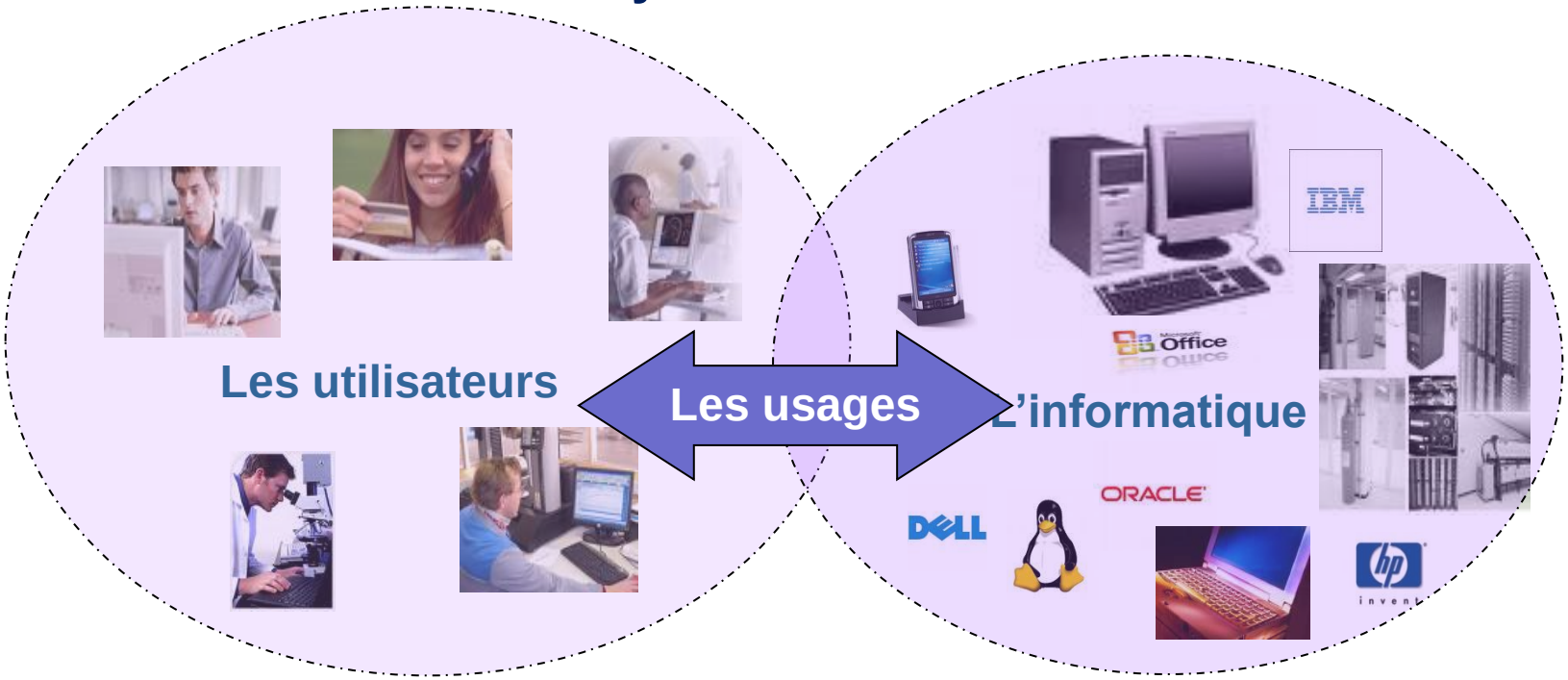
Présentation des concepts
COBIT®

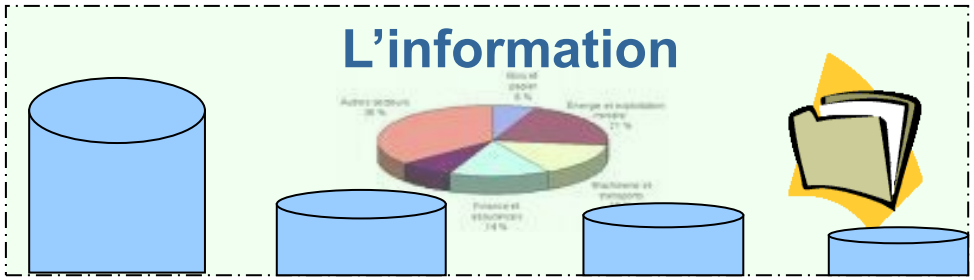
Prenez du plaisir !

NE PAS PERTURBER !

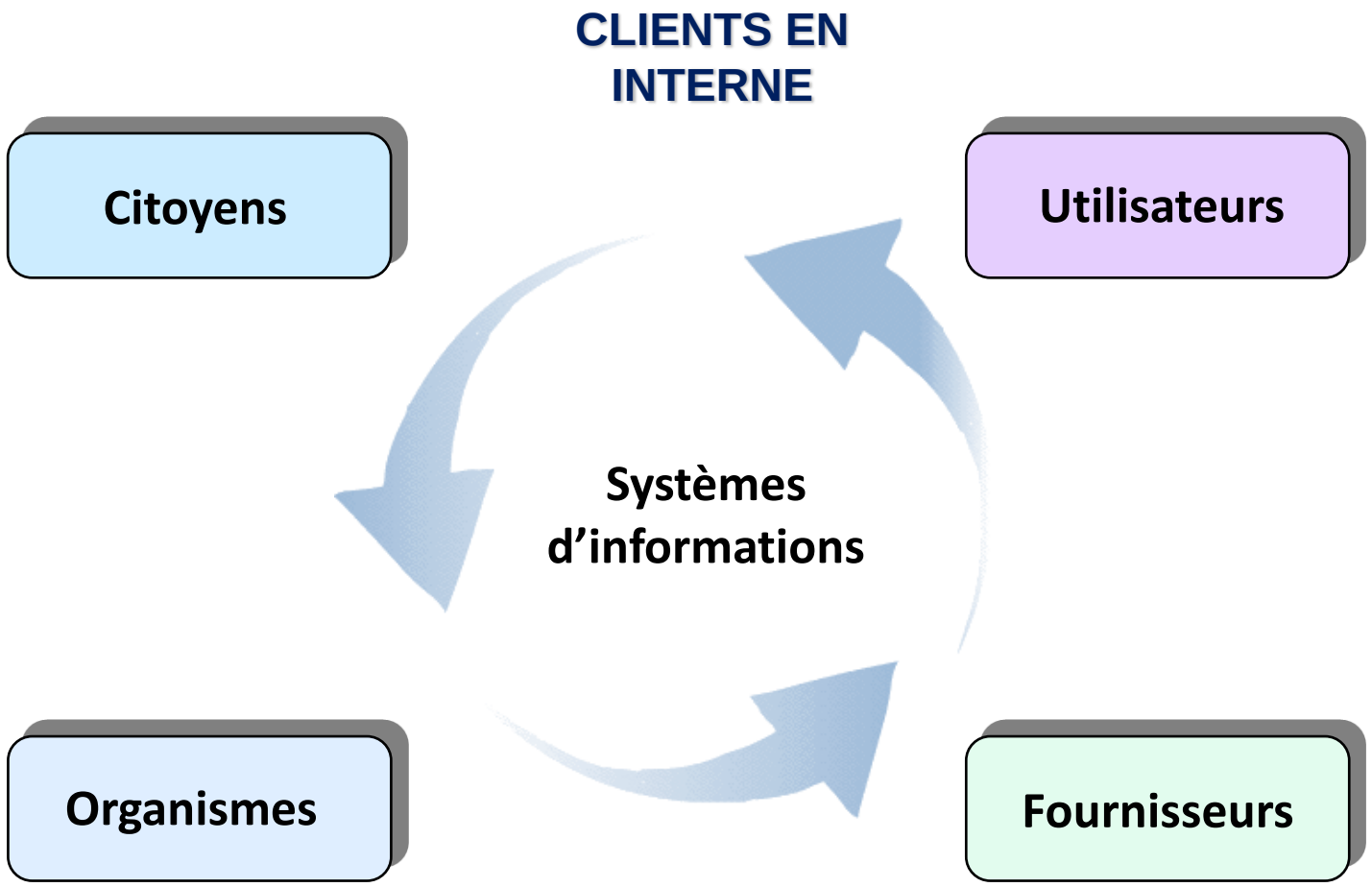
Que faut-il piloter?

Le système d'information





Importance des SI



Une fonction complexe à gérer

COBIT
GOVERNANCE, CONTROL *and* ASSURANCE *for* INFORMATION *and* RELATED TECHNOLOGY

Industrie informatique

Métiers de l'entreprise

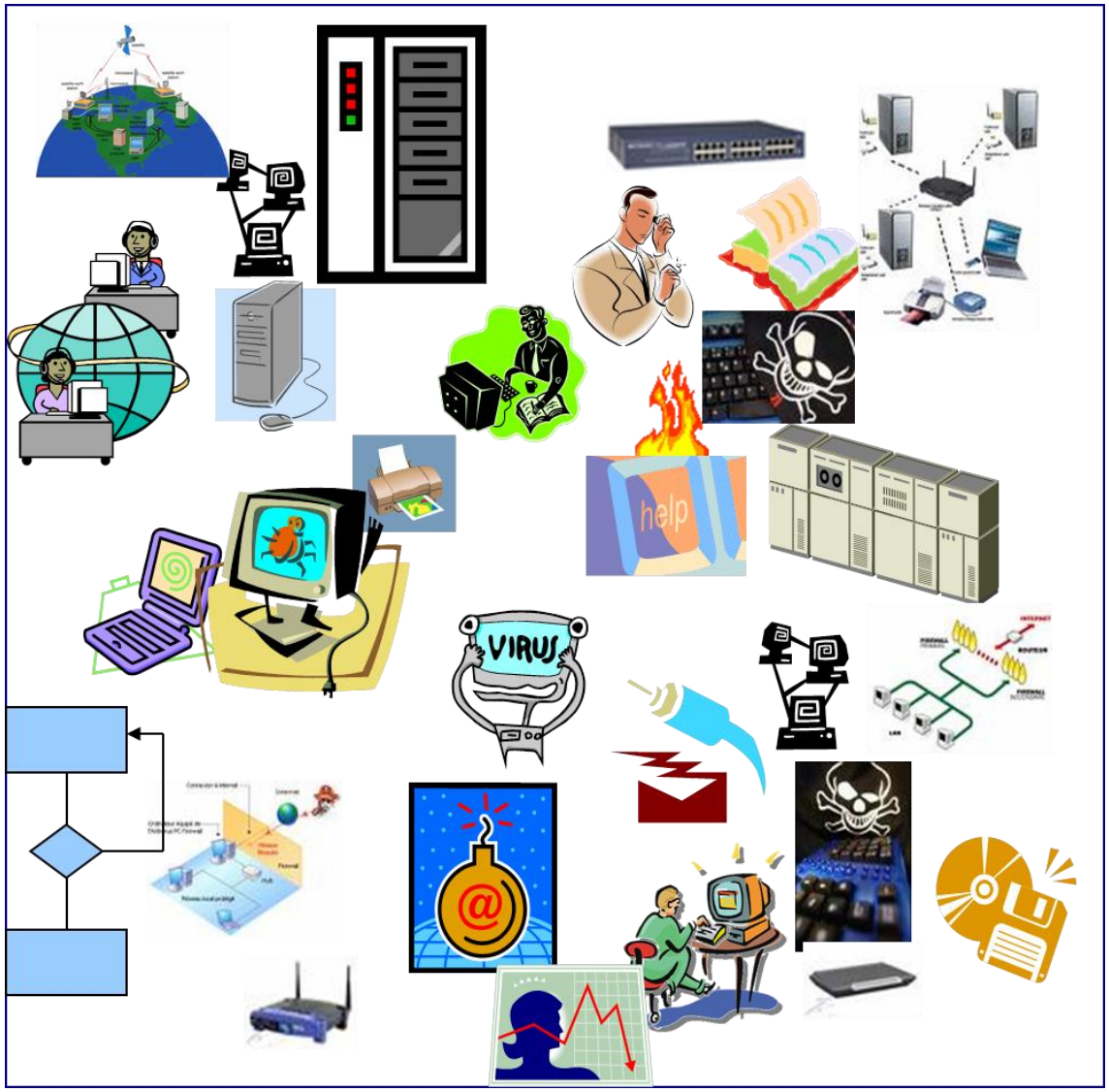
Aucune fonction de l'entreprise ne connaît l'arrivée d'autant de nouveaux produits/versions chaque année

La DSI est la fonction la plus complexe à gérer de l'entreprise

Aucune fonction de l'entreprise ne doit connaître aussi bien les métiers et le fonctionnement d'entreprise

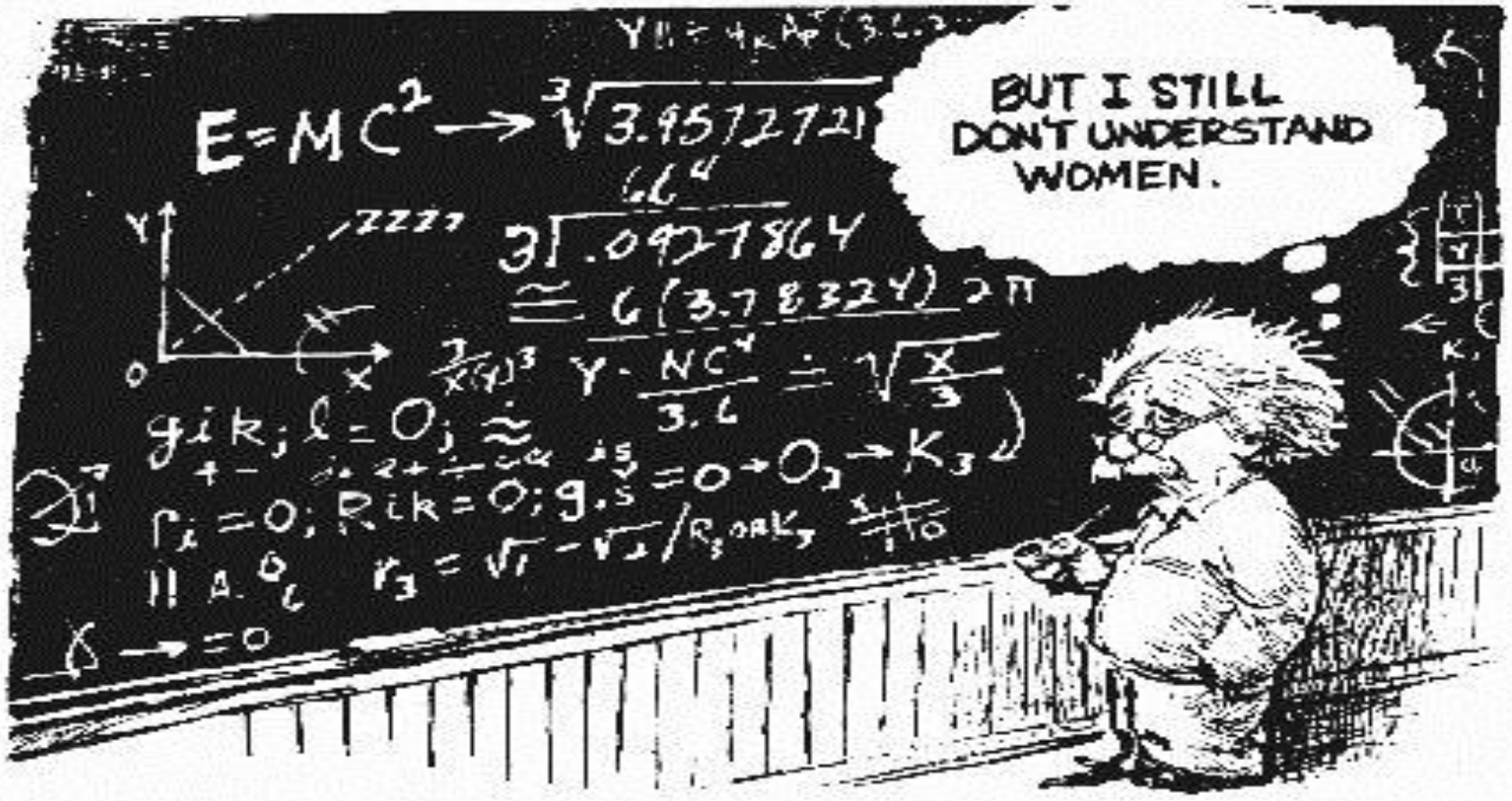
L'Infrastructure/L'opérationnel: un vrai casse tête

COBIT
GOVERNANCE, CONTROL *and* ASSURANCE *for* INFORMATION *and* RELATED TECHNOLOGY



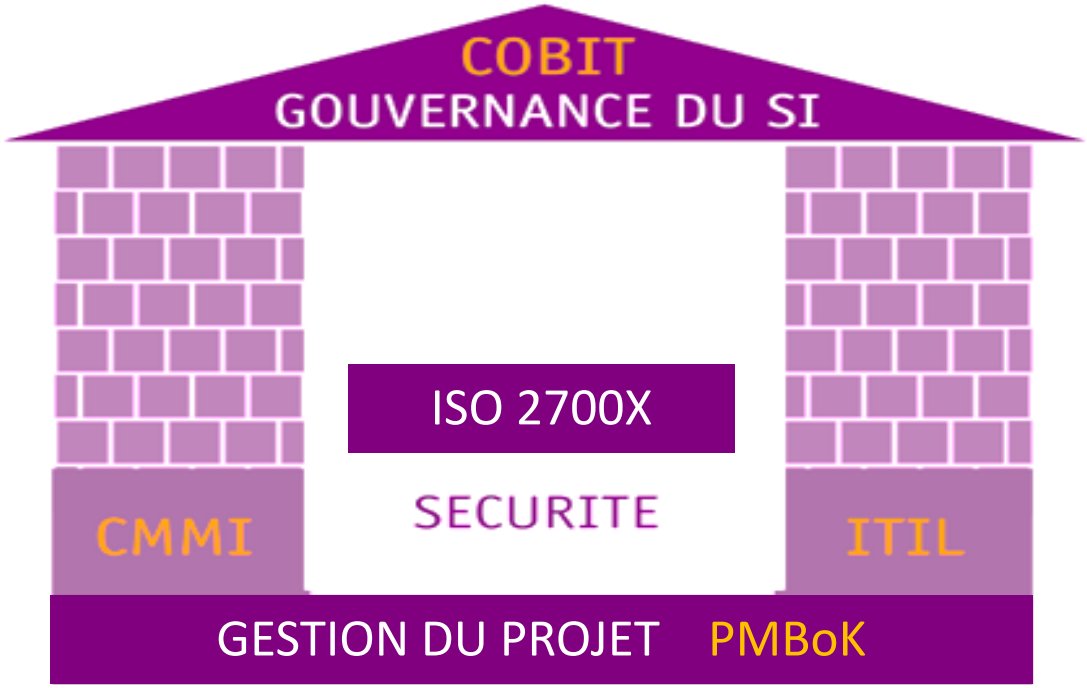
Les Maths, c'est pas tout !

COBIT
GOVERNANCE, CONTROL *and* ASSURANCE *for* INFORMATION *and* RELATED TECHNOLOGY



Solution……Bonnes pratiques SI

De nombreux référentiels ont été conçus pour aider les organisations à encadrer leur GTI et la rendre effective, dont les plus reconnus et utilisés sont:



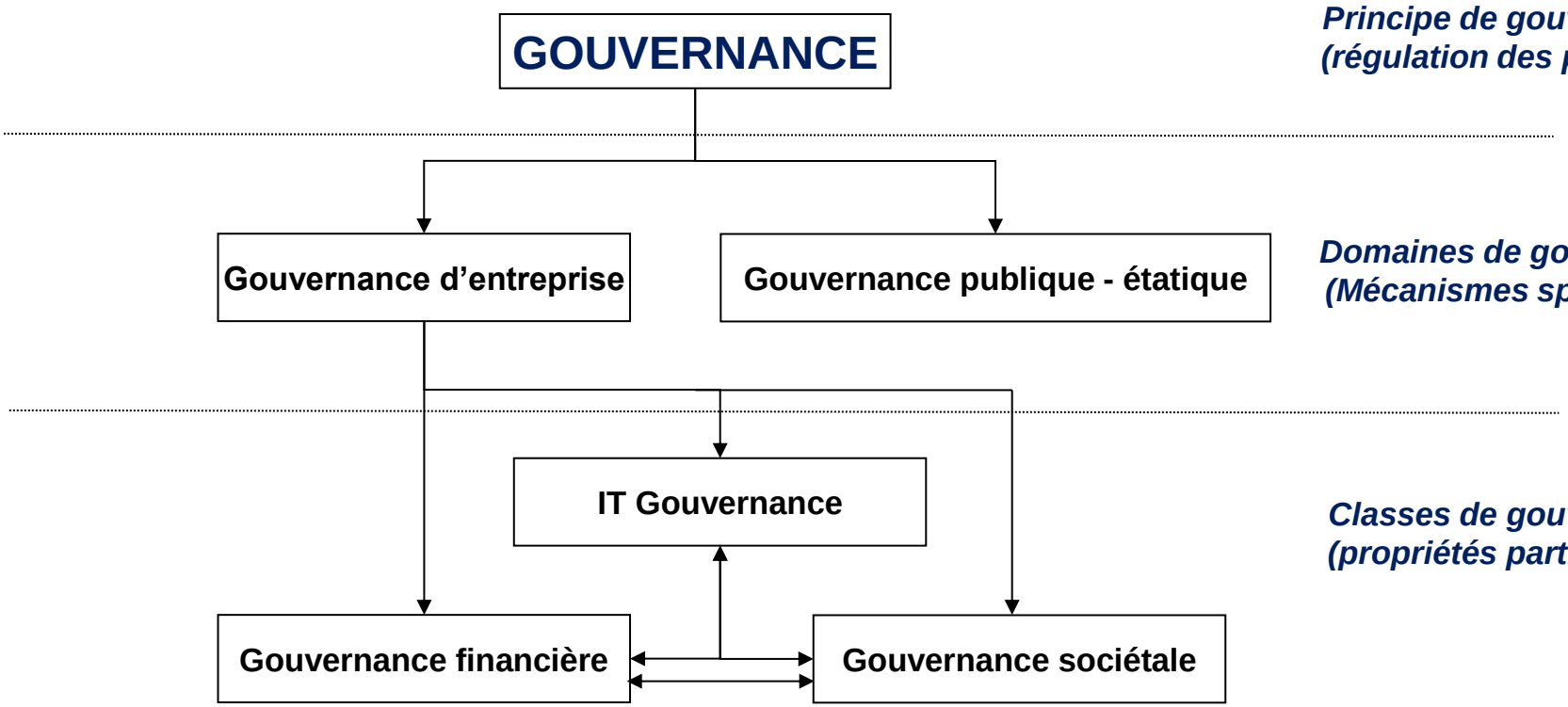
Problème: On ne vous dira jamais Comment !

COBIT
GOVERNANCE, CONTROL *and* ASSURANCE *for* INFORMATION *and* RELATED TECHNOLOGY

Gouvernance des SI

Les différentes dimensions de la gouvernance

La gouvernance d'entreprise découle directement des principes fondamentaux de la gouvernance. Par ailleurs, elle est constituée de **trois classes de gouvernances distinctes**. Chaque classe correspondant aux éléments fondamentaux de l'entreprise: le **capital**, les **ressources humaines** et l'**information**.



(Source : White Paper, ITBF, Frédéric Georgel)

Gouvernance SI

Aujourd'hui, la gouvernance informatique telle que définie par l'ITGI et l'ISACA se résume aux **5 problématiques** suivantes :

- Alignement stratégique (« IT Strategic Alignment »)
- Création de valeur (« IT Value Delivery »)
- Gestion du risque informatique (« IT Risk Management »)
- Mesure de performance (« Performance Measurement »)
- Gestion des ressources (« IT Resource Management »)

(Source : IT Governance Institute - ISACA)

CoBit
ISO 2700x…
ITIL

La gouvernance des Systèmes d'Information est définie comme la structure des relations et des processus visant à diriger et contrôler l'entreprise pour qu'elle atteigne ses objectifs en générant de la valeur, tout en trouvant le bon équilibre entre les risques et les avantages des TI et de leurs processus.

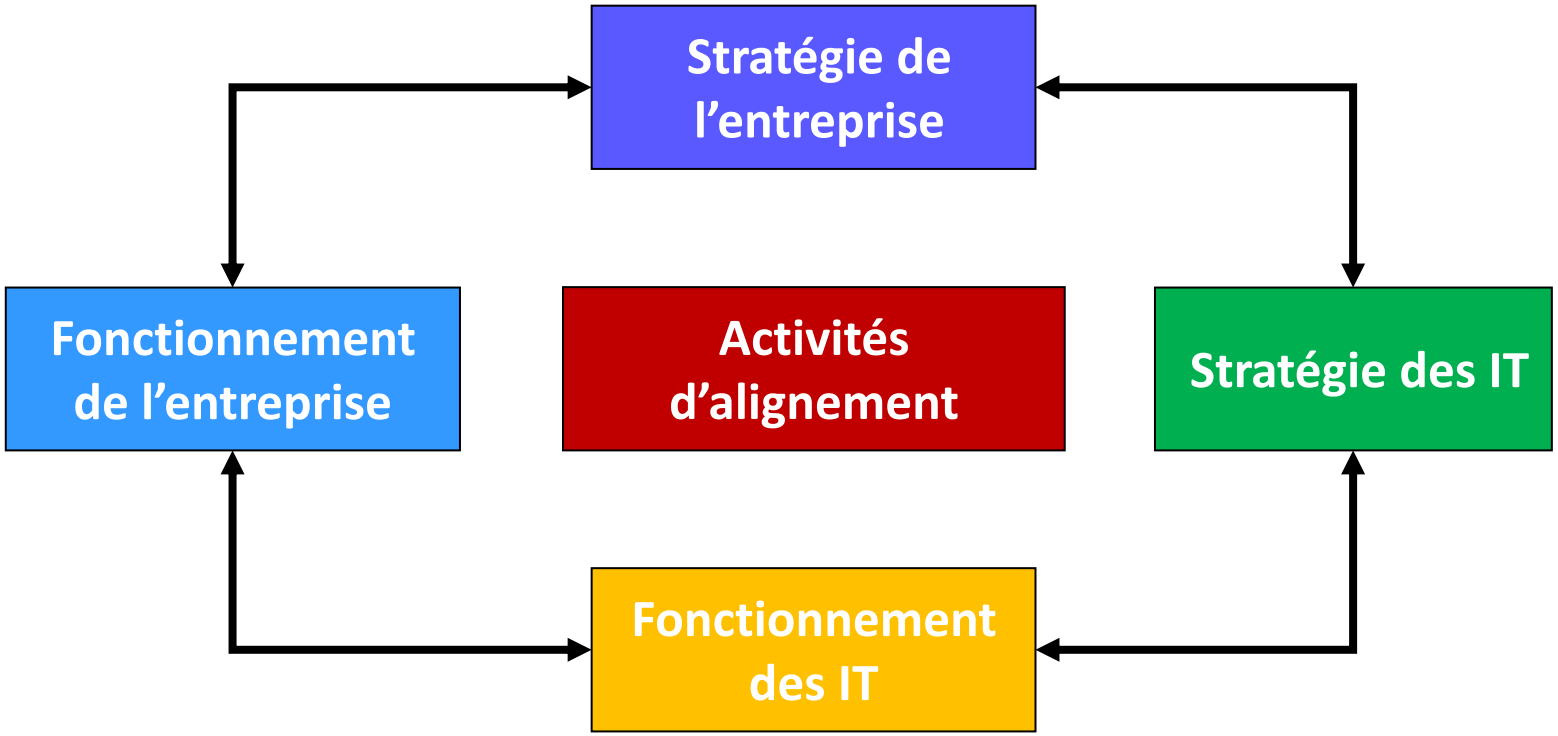
(Source : ITGI)

ALIGNEMENT STRATÉGIQUE

COBIT
GOVERNANCE, CONTROL *and* ASSURANCE *for* INFORMATION *and* RELATED TECHNOLOGY

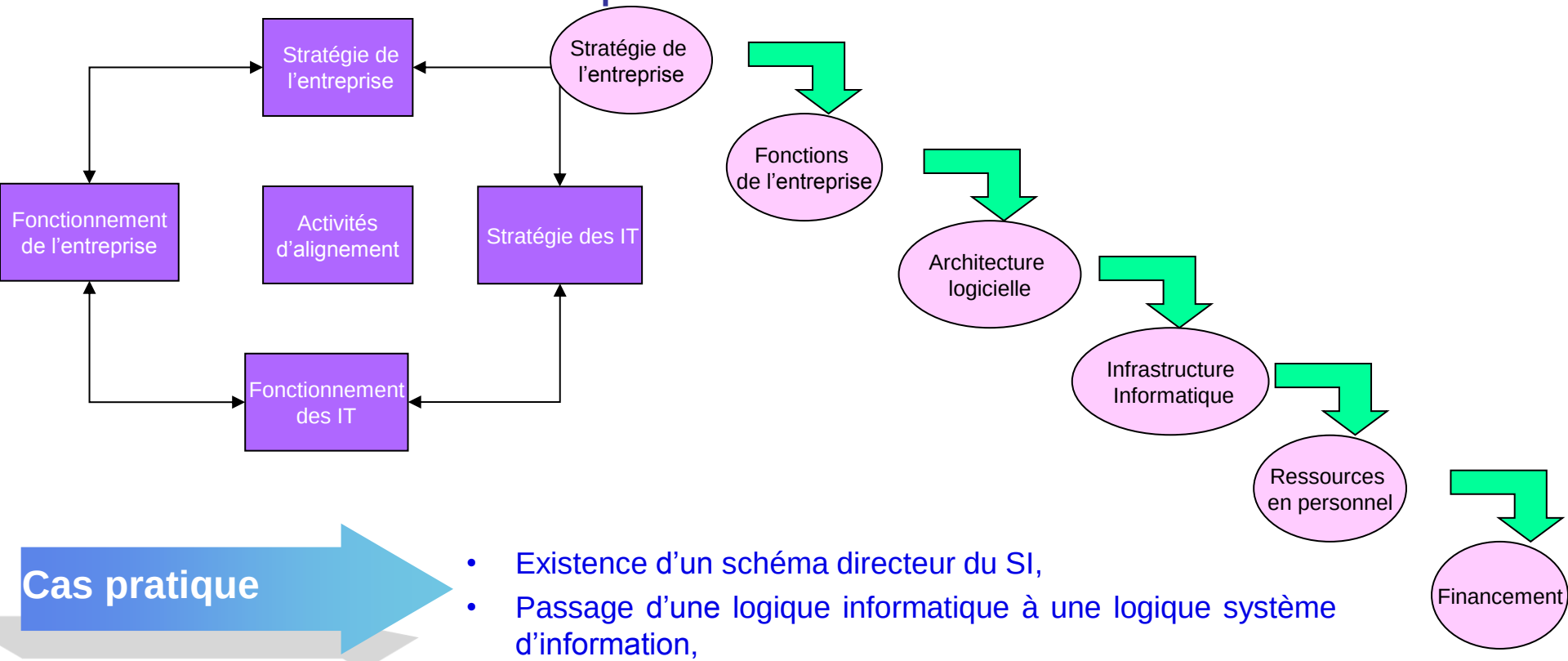
Alignement Stratégique

La question fondamentale est de savoir dans quelle mesure les investissements informatiques d'une entreprise sont en phase avec ses objectifs stratégiques et ainsi de construire les solutions qui fourniront la valeur attendue.



Alignement Stratégique

La question fondamentale est de savoir dans quelle mesure les investissements informatiques d'une entreprise sont en phase avec ses objectifs stratégiques et ainsi de construire les solutions qui fourniront la valeur attendue.



Cas pratique

- Existence d'un schéma directeur du SI,
- Passage d'une logique informatique à une logique système d'information,
- Stratégie SI est intégrée dans la stratégie globale de l'entreprise.

Création de la valeur

COBIT
GOVERNANCE, CONTROL *and* ASSURANCE *for* INFORMATION *and* RELATED TECHNOLOGY

Création de la valeur

COBIT
GOVERNANCE, CONTROL *and* ASSURANCE *for* INFORMATION *and* RELATED TECHNOLOGY

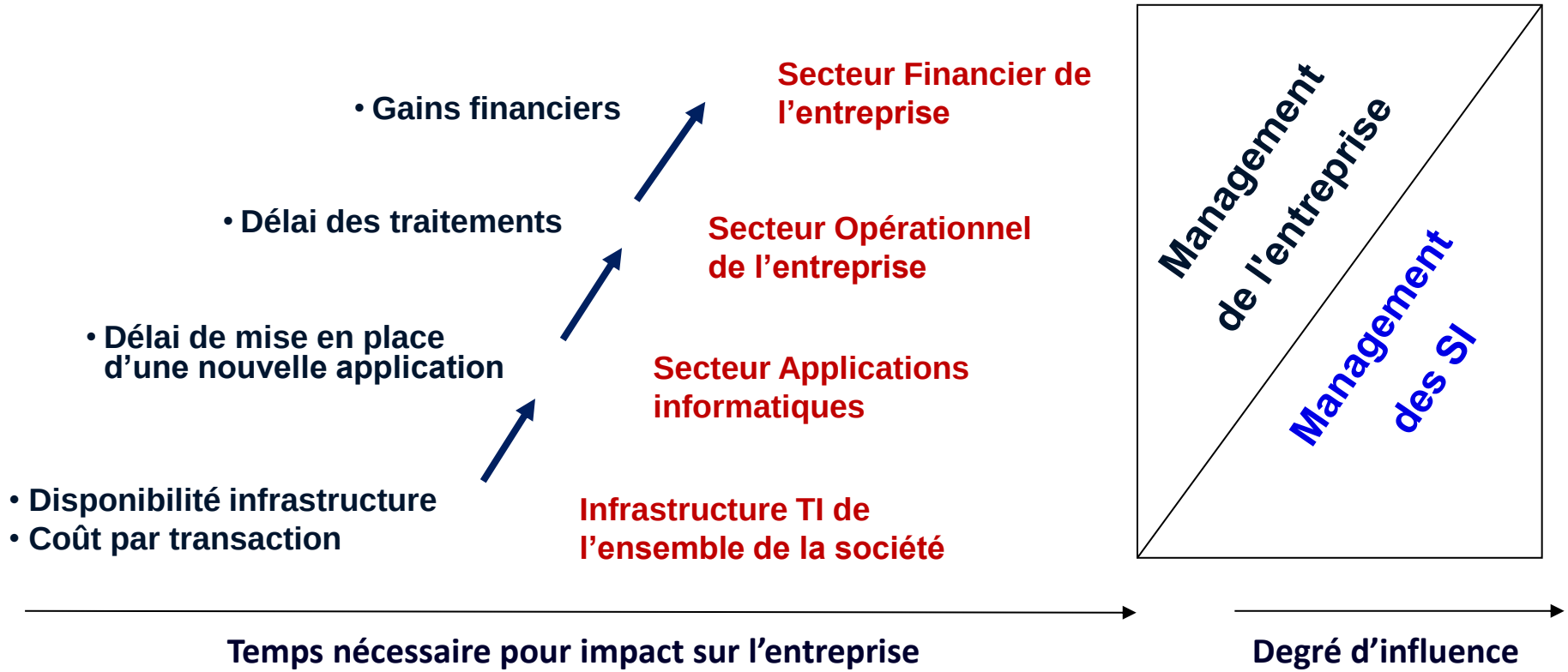
Les principes de base générateurs de valeur par l'informatique sont :

- **Avantages concurrentiels:** Délai entre les commandes et fourniture du service, satisfaction client, délai de livraison, productivité et rentabilité du personnel…
- **Fourniture**: Dans les délais et sans dépassement de budget, de la qualité voulue, qui apporte les bénéfices promis.

Création de la valeur

COBIT
GOVERNANCE, CONTROL *and* ASSURANCE *for* INFORMATION *and* RELATED TECHNOLOGY

Cas Pratique



Gestion des risques informatiques

COBIT
GOVERNANCE, CONTROL *and* ASSURANCE *for* INFORMATION *and* RELATED TECHNOLOGY

Gestion des risques informatiques

COBIT
GOVERNANCE, CONTROL *and* ASSURANCE *for* INFORMATION *and* RELATED TECHNOLOGY

La gestion des risques informatiques permet de :

- ☑ S'assurer que le système de contrôle interne mis en place pour gérer les risques a souvent la capacité de générer de la rentabilité,
- ☑ S'assurer qu'une approche transparente et proactive de la gestion du risque peut créer un avantage concurrentiel exploitable,
- ☑ S'assurer que le fait de gérer les risques doit faire partie du fonctionnement de l'entreprise.

« Je n'imagine aucune circonstance qui puisse provoquer le naufrage de ce navire. Je ne peux imaginer une catastrophe vitale qui puisse affecter ce navire »

Capitaine du TITANIC, 1912

Gestion des risques informatiques

COBIT
GOVERNANCE, CONTROL *and* ASSURANCE *for* INFORMATION *and* RELATED TECHNOLOGY

Cas Pratique

- Sensibilisation des collaborateurs sur les risques potentiels des systèmes d'information (Guide sécurité de l'information, politique sécurité de l'information, politique de mots de passe…),
- Démarche proactive d'analyse des risques,
- La classification des actifs informationnels de l'entreprise,
- Passage d'une analyse des risques informatiques à une évaluation des risques informationnels.

Mesure de performance

COBIT
GOVERNANCE, CONTROL *and* ASSURANCE *for* INFORMATION *and* RELATED TECHNOLOGY

Les TDB comportent des informations de gestion apportées par les parties concernées, informations rendues efficaces par un bon système de Reporting.

Cas Pratique

- Proposition d'objectifs et d'indicateurs concrets,
- Intégration des logiques de pilotage stratégique et de pilotage opérationnel.

La Gestion des Ressources Informatiques

COBIT
GOVERNANCE, CONTROL *and* ASSURANCE *for* INFORMATION *and* RELATED TECHNOLOGY

Un critère essentiel de la performance informatique est l'investissement optimal, l'utilisation et l'allocation des ressources informatiques (HW, SW, RH) au service des besoins de l'entreprise.

La plupart des entreprises échoue dans l'optimisation de leurs actifs informatiques.

De plus, récemment, un challenge important est de savoir quoi, où et comment gérer l'externalisation de certains services tout en générant la valeur ajoutée promise à un prix acceptable.

La Gestion des Ressources Informatiques

COBIT
GOVERNANCE, CONTROL *and* ASSURANCE *for* INFORMATION *and* RELATED TECHNOLOGY

Cas Pratique

- Les responsabilités sont clairement identifiées et appliquées,
- Les méthodes et les compétences pour gérer les projets et systèmes informatiques sont présentes,
- Existence d'une planification et d'une gestion des RH,
- Les besoins en formation sont clairement identifiés,
- **Considération des ressources humaines et réflexion en matière d'externalisation, de sous-traitance ou d'internalisation**

COBIT

GOVERNANCE, CONTROL *and* ASSURANCE *for* INFORMATION *and* RELATED TECHNOLOGY

COBIT

un référentiel d'audit des SI

Définition

CobiT (Control Objectives for Information and Related Technology) est le résultat des travaux collectifs réalisés par les principaux acteurs de la profession, auditeurs internes ou externes, fédérés au sein de l'ISACA (Information System Audit and Control Association).

www.isaca.org

À propos de l' ISACA

COBIT
GOVERNANCE, CONTROL *and* ASSURANCE *for* INFORMATION *and* RELATED TECHNOLOGY

- Actuellement, avec plus de 100.000 membres dans 180 pays
- Un des leaders mondiaux dans les domaines de la connaissance, de la certification, des communautés, de la promotion et de la formation en sécurité et assurance des systèmes d'information (SI), de la gouvernance et du management des SI de l'entreprise, ainsi que de la maîtrise des risques et de la conformité des SI.
- Créée en 1969, l'ISACA, organisme indépendant et sans but lucratif, organise des conférences internationales, publie la revue *ISACA Journal*®, et développe des normes internationales en audit et contrôle des systèmes d'information afin d'aider ses membres à promouvoir des systèmes d'information de confiance et créateurs de valeur.
- L'ISACA Atteste des connaissances et de l'expertise en matière de SI par le biais des certifications mondialement reconnues du CISA® (Certified Information Systems Auditor®), du CISM® (Certified Information Security Manager™), du CGEIT® (Certified in the Governance of Enterprise IT®) et du CRISC™ (Certified in Risk and Information Systems Control™).

1967	Association d'auditeurs dans le domaine des ordinateurs
1969	EDP Auditors Association
1976	ISACA Information Systems Audit and Control Association
1998	Fondation de l'institut de recherche ITGI Information Technology Governance Institute
2011	95,000 membres répartis en 190 chapitres dans 75 pays

ITGI

En 1998, l'ITGI (Information Technology Governance Institute) a été créé sur l'initiative de l'ISACA, en réponse à la place de plus en plus importante occupée par les technologies de l'information.

Depuis une dizaine d'années, l'ITGI a mené de nombreuses recherches au travers de groupes de travail répartis dans le monde entier. Le résultat de ces recherches a notamment donné lieu en 2000 à la publication de la version V3 du référentiel CobiT proposant, parallèlement à un « guide d'audit », un « guide de management » préfigurant les versions ultérieures.

Un référentiel...Un standard

COBIT
GOVERNANCE, CONTROL *and* ASSURANCE *for* INFORMATION *and* RELATED TECHNOLOGY

Ensemble de règles et d'usages que les professionnels reconnaissent comme vrais et qui devraient être appliquées. On parle aussi de modèle ou de cadre (framework)

Un standard est un référentiel publié par une entité non officielle, ou un groupe représentatif d'utilisateurs.

Nous ne parlons de standard qu'à partir du moment où le référentiel a une diffusion large : c'est un standard de facto (standard de fait).

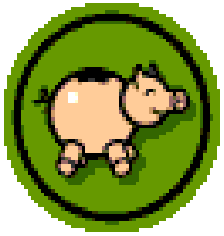
La vision de l'entreprise évolue …

COBIT
GOVERNANCE, CONTROL *and* ASSURANCE *for* INFORMATION *and* RELATED TECHNOLOGY

Un mal nécessaire

Un centre de coûts

Un créateur d'économies



Un facilitateur de la stratégie

Une partie intégrante de la stratégie

«L'informatique» → **«Système d'information»**

CoBiT

- Conçu et géré par l'IT Governance Institute.
  - http://itgi-france.com/
  - http://www.afai.fr/
- Indépendant et libre de droits.
- Très utilisée dans les SI.
- Diffusion mondiale.
- Très nombreuses traductions.
- L'AFAI a publié la version française de COBIT V4.1
- Utilisation importante et en croissance forte.
- Utilisé dans les cadres Sarbanes Oxley, IFRS, LSF.

Histoire du cadre CobiT

1996	First Edition	Le cadre CobiT a été défini dans la première édition, en Avril par l' IT Gouvernance Institute.
1998	Deuxième Edition	Cette version comprend un ensemble d'outils de mise en œuvre et la révision des objectifs de contrôle de haut niveau.
2000	Troisième Edition	Cette version contient un examen des versions précédentes. Cette édition est incrémenté pour soutenir le contrôle de gestion, contrôle des performances et ajouter des concepts de gouvernance.
2005	Quatrième Edition	Cette version est conforme aux COSO, ITIL et ISSO/IEC17799 modèles, avec un accent gouvernance IT.
2007	4.1 Edition	Les définitions des mesures et des concepts clés ont été améliorées.

Cadre de référence COBIT: Pourquoi?

Les dirigeants ont de plus en plus conscience de l'impact significatif de l'information sur le succès de l'entreprise. Ils s'attendent à ce que l'on comprenne de mieux en mieux comment sont utilisées les technologies de l'information et la probabilité qu'elles contribuent avec succès à donner un avantage concurrentiel à l'entreprise.

Ils veulent savoir en particulier si la gestion des SI peut leur permettre:

- d'atteindre leurs objectifs ;
- d'avoir assez de résilience pour apprendre et s'adapter ;
- de gérer judicieusement les risques auxquels ils doivent faire face ;
- de savoir bien identifier les opportunités et d'agir pour en tirer parti.

Cadre de référence COBIT: Pourquoi?

COBIT
GOVERNANCE, CONTROL *and* ASSURANCE *for* INFORMATION *and* RELATED TECHNOLOGY

Les entreprises qui réussissent comprennent les risques, exploitent les avantages des SI et trouvent comment :

- Aligner la stratégie de l'informatique sur celle de l'entreprise ;
- Assurer aux investisseurs et aux actionnaires que l'entreprise respecte une "norme de prudence et de diligence" relative à la réduction des risques informatiques ;
- Répercuter la stratégie et les objectifs de l'informatique dans l'entreprise ;
- Faire en sorte que l'investissement informatique produise de la valeur ;
- Apporter les structures qui faciliteront la mise en oeuvre de cette stratégie et de ces objectifs ;
- Susciter des relations constructives entre les métiers et l'informatique, et avec les partenaires externes
- Mesurer la performance des SI.

Cadre de référence COBIT: Qui?

COBIT
GOVERNANCE, CONTROL *and* ASSURANCE *for* INFORMATION *and* RELATED TECHNOLOGY

Un référentiel de gouvernance et de contrôle sert les intérêts de diverses parties prenantes internes et externes dont chacune a des besoins spécifiques :

1. Les parties prenantes internes à l'entreprise qui ont intérêt à voir les investissements informatiques générer de la valeur sont :
   - celles qui prennent les décisions d'investissements,
   - celles qui définissent les exigences,
   - celles qui utilisent les services informatiques.
2. Les parties prenantes internes et externes qui fournissent les services informatiques sont:
   - celles qui gèrent l'organisation et les processus informatiques,
   - celles qui en développent les capacités,
   - celles qui exploitent les systèmes d'information au quotidien.
3. Les parties prenantes internes et externes qui ont des responsabilités dans le contrôle et le risque sont :
   - celles qui sont en charge de la sécurité, du respect de la vie privée et/ou des risques,
   - celles qui sont en charge des questions de conformité,
   - celles qui fournissent des services d'assurance ou qui en ont besoin.

Cadre de référence COBIT: Quoi?

COBIT
GOVERNANCE, CONTROL *and* ASSURANCE *for* INFORMATION *and* RELATED TECHNOLOGY

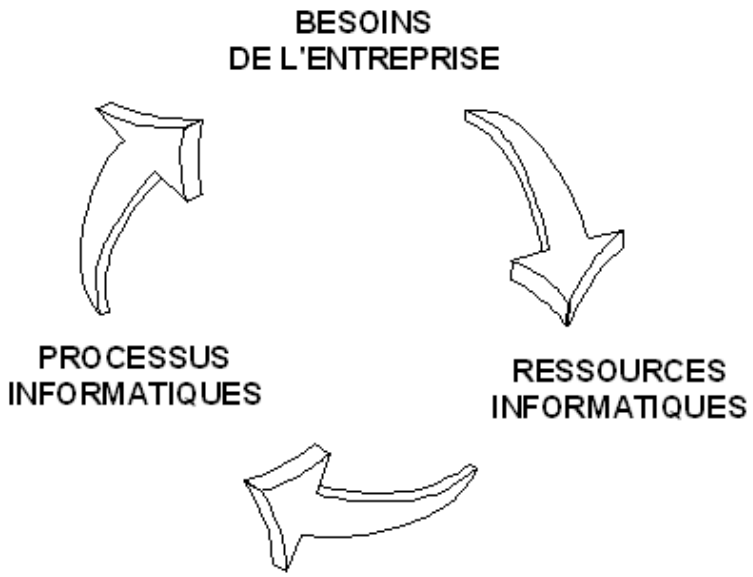
Pour faire face à ces exigences, un cadre de référence pour la gouvernance et le contrôle des SI doivent respecter les spécifications générales suivantes :

- Fournir une vision métiers qui permette d'aligner les objectifs de l'informatique sur ceux de l'entreprise.
- Établir un schéma par processus qui définisse ce que chacun d'eux recouvre, avec une structure précise qui permette de s'y retrouver facilement.
- Faire en sorte que l'ensemble puisse être généralement accepté, en se conformant aux meilleures pratiques et aux standards informatiques, et en restant indépendant des technologies spécifiques.
- Fournir un langage commun, avec son glossaire, qui puisse être généralement compris par toutes les parties prenantes.
- Aider à remplir les obligations réglementaires en se conformant aux standards généralement acceptés

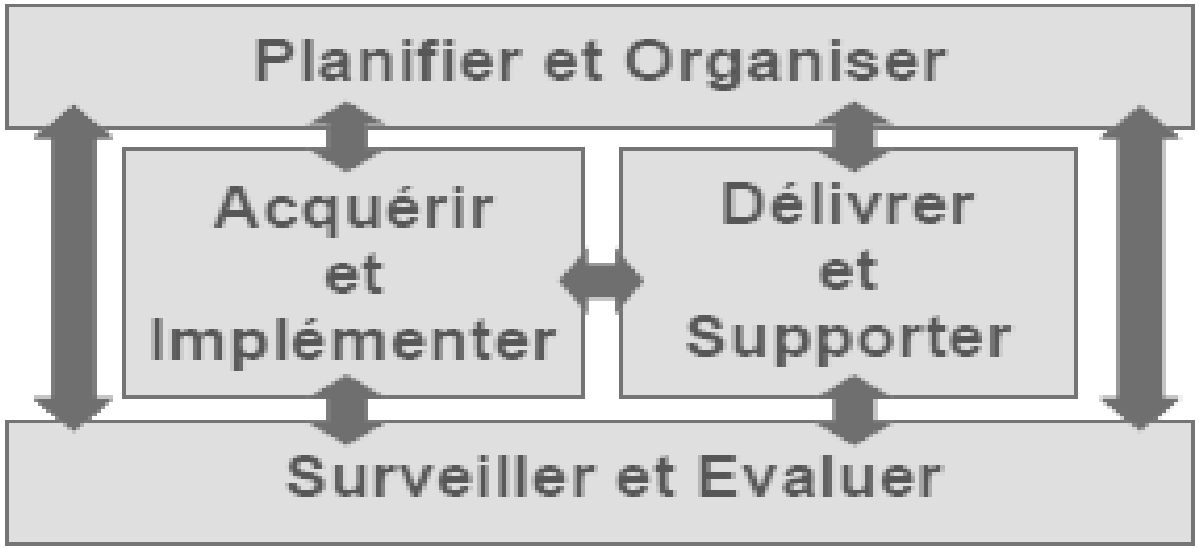
COBIT et les processus

COBIT
GOVERNANCE, CONTROL *and* ASSURANCE *for* INFORMATION *and* RELATED TECHNOLOGY

Structure de relations et de **processus** visant à diriger et contrôler **l'entreprise** pour qu'elle atteigne ses objectifs en générant de la valeur, tout en trouvant le bon équilibre entre les risques et les avantages des TI et de leurs processus.



Les composants de CobiT



PLANIFIER ET ORGANISER (PO)

Ce domaine recouvre la stratégie et la tactique et vise à identifier la meilleure manière pour les SI de contribuer à atteindre les objectifs métiers de l'entreprise. La mise en oeuvre de la vision stratégique doit être planifiée, communiquée et gérée selon différentes perspectives. Il faut mettre en place une organisation adéquate ainsi qu'une infrastructure technologique. Ce domaine s'intéresse généralement aux problématiques de management suivantes :

- Les stratégies de l'entreprise et de l'informatique sont-elles alignées ?
- L'entreprise fait-elle un usage optimum de ses ressources ?
- Est-ce que tout le monde dans l'entreprise comprend les objectifs de l'informatique ?
- Les risques informatiques sont-ils compris et gérés ?
- La qualité des systèmes informatiques est-elle adaptée aux besoins métiers ?

ACQUÉRIR ET IMPLÉMENTER (AI)

Le succès de la stratégie informatique nécessite d'identifier, de développer ou d'acquérir des solutions informatiques, de les mettre en œuvre et de les intégrer aux processus métiers. Ce domaine recouvre aussi la modification des systèmes existants ainsi que leur maintenance afin d'être sûr que les solutions continuent d'être en adéquation avec les objectifs métiers.

Ce domaine s'intéresse généralement aux problématiques de management suivantes :

- Est-on sûr que les nouveaux projets vont fournir des solutions qui correspondent aux besoins métiers ?
- Est-on sûr que les nouveaux projets aboutiront en temps voulu et dans les limites budgétaires ?
- Les nouveaux systèmes fonctionneront-ils correctement lorsqu'ils seront mis en oeuvre ?
- Les changements pourront-ils avoir lieu sans perturber les opérations en cours ?

DÉLIVRER ET SUPPORTER (DS)

Ce domaine s'intéresse à la livraison effective des services demandés, ce qui comprend l'exploitation informatique, la gestion de la sécurité et de la continuité, le service d'assistance aux utilisateurs et la gestion des données et des équipements. Il s'agit généralement des problématiques de management suivantes :

- Les services informatiques sont-ils fournis en tenant compte des priorités métiers ?
- Les coûts informatiques sont-ils optimisés ?
- Les employés sont-ils capables d'utiliser les systèmes informatiques de façon productive et sûre ?
- La confidentialité, l'intégrité et la disponibilité sont-elles mises en œuvre pour la sécurité de l'information ?

SURVEILLER ET ÉVALUER (SE)

Tous les processus informatiques doivent être régulièrement évalués pour vérifier leur qualité et leur conformité par rapport aux spécifications de contrôle. Ce domaine s'intéresse à la gestion de la performance, à la surveillance du contrôle interne, au respect des normes réglementaires et à la gouvernance. Il s'agit généralement des problématiques de management suivantes :

- La performance de l'informatique est-elle mesurée de façon à ce que les problèmes soient mis en évidence avant qu'il ne soit trop tard ?
- Le management s'assure-t-il que les contrôles internes sont efficaces et efficients ?
- La performance de l'informatique peut-elle être reliée aux objectifs métiers ?
- Des contrôles de confidentialité, d'intégrité et de disponibilité appropriés sont-ils mis en place pour la sécurité de l'information ?

À qui s’adresse Cobit?

COBIT
GOVERNANCE, CONTROL *and* ASSURANCE *for* INFORMATION *and* RELATED TECHNOLOGY

Aux trois intervenants principaux de l’organisation:

1. La direction
2. Les utilisateurs des TI
3. Les auditeurs (internes et externes).

À qui s'adresse Cobit?

1. CobiT permet à **la direction:**

- ✓ de disposer d'un modèle structuré pour maîtriser les risques (financiers, organisationnels et technologiques), reliés à l'alignement des TI sur les objectifs de l'entité
- ✓ de mieux définir les besoins en matière de contrôle TI et d'intégrité de l'information
- ✓ de sensibiliser tous les intervenants à l'importance des contrôles TI
- ✓ de réaliser efficacement des diagnostics des contrôles TI (listes détaillée des contrôles).

À qui s'adresse Cobit?

2. Les utilisateurs (des TI)

CobiT permet de fournir des garanties quant à la sécurité et aux contrôles des services informatiques fournis à l'interne ou par des tiers

3. Les auditeurs

CobiT offre aux auditeurs la possibilité:

- de mieux comprendre les contrôles TI
- de mieux formuler leurs recommandations sur les contrôles TI
- de mieux réaliser les tests d'efficacité des contrôles TI
- de mieux justifier leurs évaluations des contrôles TI.

Besoins de l'organisation en information

Pour atteindre ses objectifs **(stratégiques, financiers, opérationnels),** l'organisation doit disposer d'information pertinente.

Cette pertinence est déterminée dans CobiT à partir de sept critères, regroupés dans deux catégories d'impératifs:

- des impératifs économiques et fiduciaires
- des impératifs de sécurité.

Objectifs de la gouvernance des SI selon COBIT

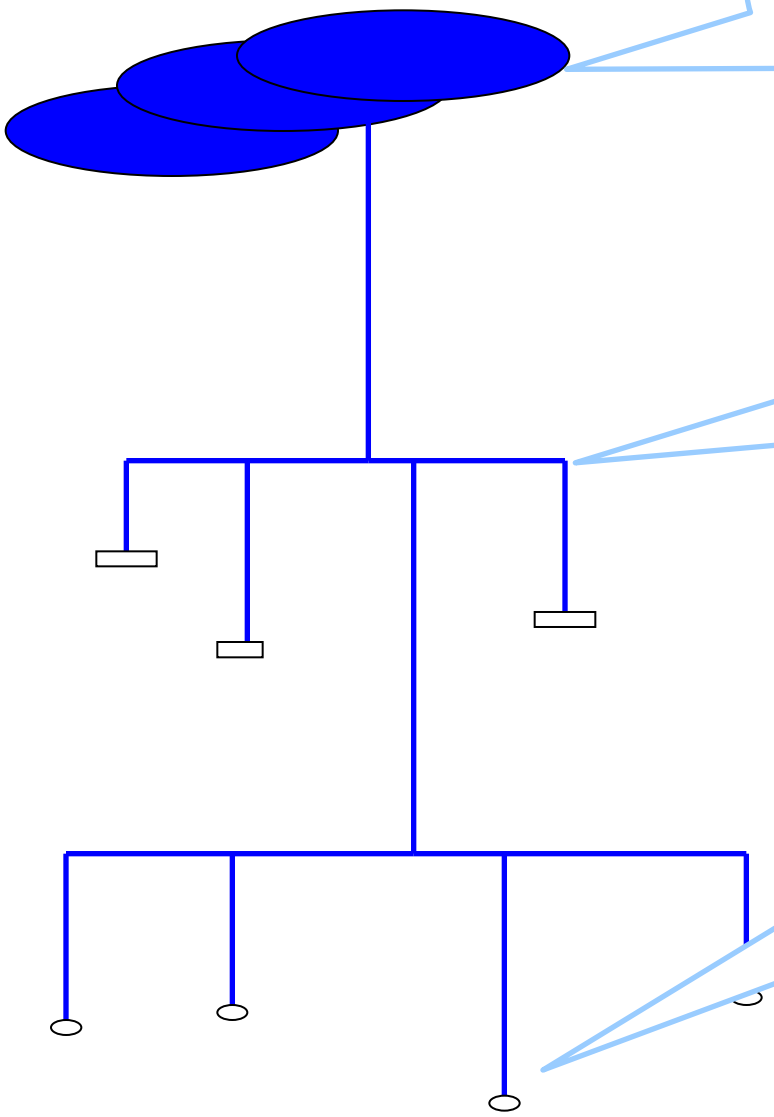
COBIT
GOVERNANCE, CONTROL *and* ASSURANCE *for* INFORMATION *and* RELATED TECHNOLOGY

Efficacité	**La mesure par laquelle l'information contribue au résultat des processus métier par rapport aux objectifs fixés ;**
Efficience	**La mesure par laquelle l'information contribue au résultat des processus métier au meilleur coût**
Confidentialité	**Protection de l'information sensible** contre toute communication non autorisée
Intégrité	Fait référence à l'**exactitude et à l'intégralité** de l'information
Disponibilité	**Information rendue disponible lorsque requise par le processus d'affaires, maintenant et à l'avenir;** se rapporte également à la sauvegarde des ressources nécessaires et aux fonctionnalités connexes
Conformité	**Respect des lois, de la réglementation et des dispositions contractuelles** auxquelles les processus d'affaires sont assujettis, c.-à-d. des critères dictés par des autorités externes ou par des politiques internes
Fiabilité	**La mesure par laquelle l'information de pilotage est pertinente**.

Les ressources TI

Cobit répartit les ressources TI en quatre segments, afin d'en atténuer la complexité:

- **Les informations**: les données relatives à une activité, insérées ou fournies par le système d'information
- **Les applications :** ensemble des procédures manuelles et programmées de traitement des données. Exemple:
- **Les infrastructures :** équipement, système d'exploitation, bases de données, réseau,…
- **Le personnel :** Le personnes (à l'interne et à l'externe) en charge de la gestion du système d'information



4 domaines: regroupement naturel de processus correspondant souvent à un domaine de responsabilité organisationnel;

4 Domaines

34 processus: série d'activités et de tâches groupées et qui constituent les objectifs de contrôles généraux;

34 Processus

220 activités: tâches nécessaires à l'obtention d'un résultat mesurable et qui forment les objectifs des contrôles détaillés.

220 Activités

Processus informatiques et domaines

Objectifs de l'entreprise

COBIT

Information

- efficacité
- efficience
- confidentialité
- intégrité
- disponibilité
- conformité
- fiabilité

Ressources informatiques

- données
- systèmes d'application
- technologie
- installations
- personnel

PO1 Définir un plan informatique stratégique
PO2 Définir l'architecture de l'information
PO3 Déterminer l'orientation technologique
PO4 Définir les processus, l'organisation et les relations de travail
PO5 Gérer les investissements informatiques
PO6 Faire connaître les buts et les orientations du management
PO7 Gérer les ressources humaines de l'informatique
PO8 Gérer la qualité
PO9 Évaluer et gérer les risques
PO10 Gérer les projets

Planification et Organisation

Acquisition et Mise en Place

AI1 Trouver des solutions informatiques
AI2 Acquérir des applications et en assurer la maintenance
AI3 Acquérir une infrastructure technique et en assurer la maintenance
AI4 Faciliter le fonctionnement et l'utilisation
AI5 Acquérir des ressources informatiques
AI6 Gérer les changements
AI7 Installer et valider les solutions et les modifications

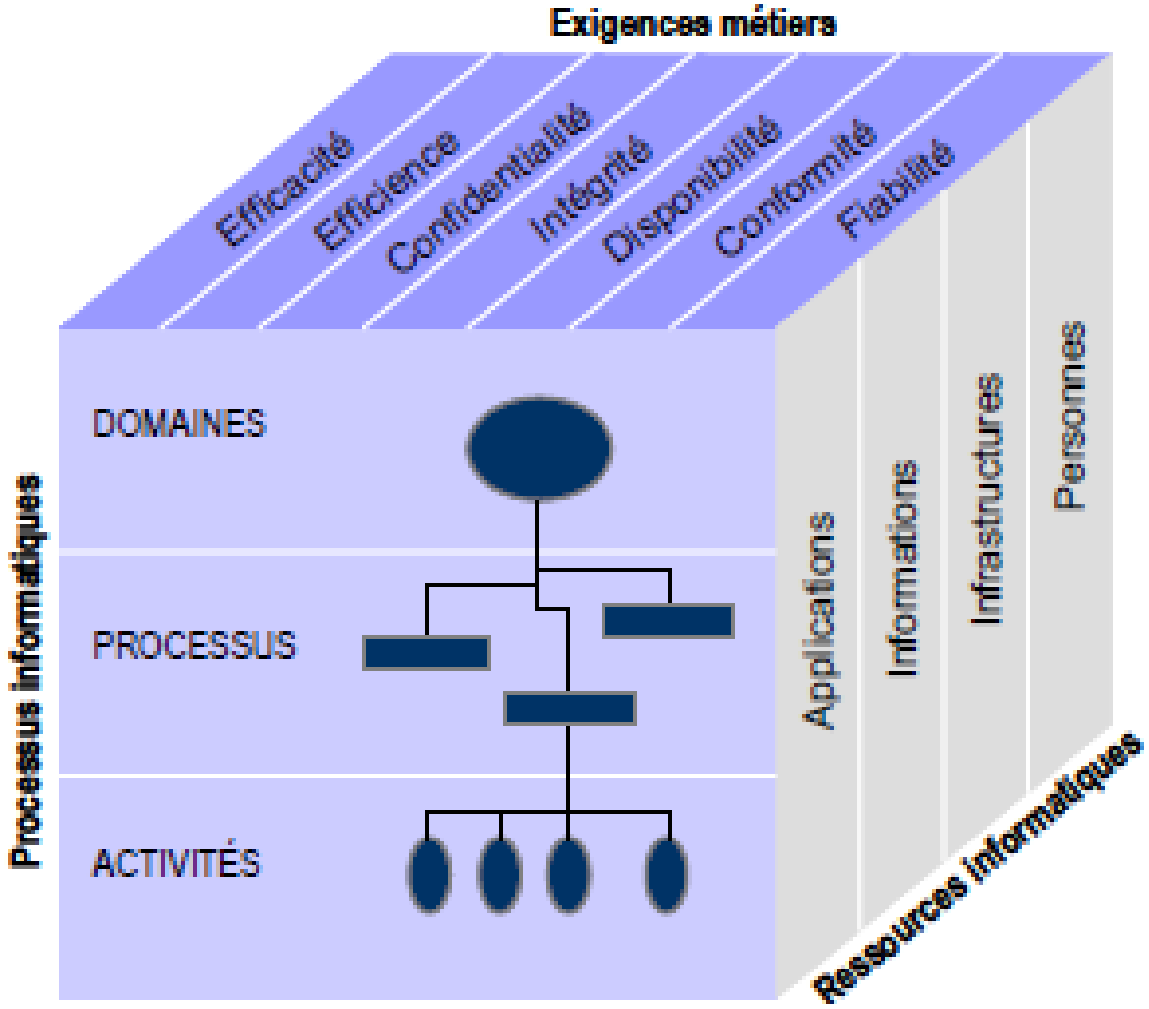
Distribution et Support

DS1 Définir et gérer les niveaux de services
DS2 Gérer les services tiers
DS3 Gérer la performance et la capacité
DS4 Assurer un service continu
DS5 Assurer la sécurité des systèmes
DS6 Identifier et imputer les coûts
DS7 Instruire et former les utilisateurs
DS8 Gérer le service d'assistance client et les incidents
DS9 Gérer la configuration
DS10 Gérer les problèmes
DS11 Gérer les données
DS12 Gérer l'environnement physique
DS13 Gérer l'exploitation

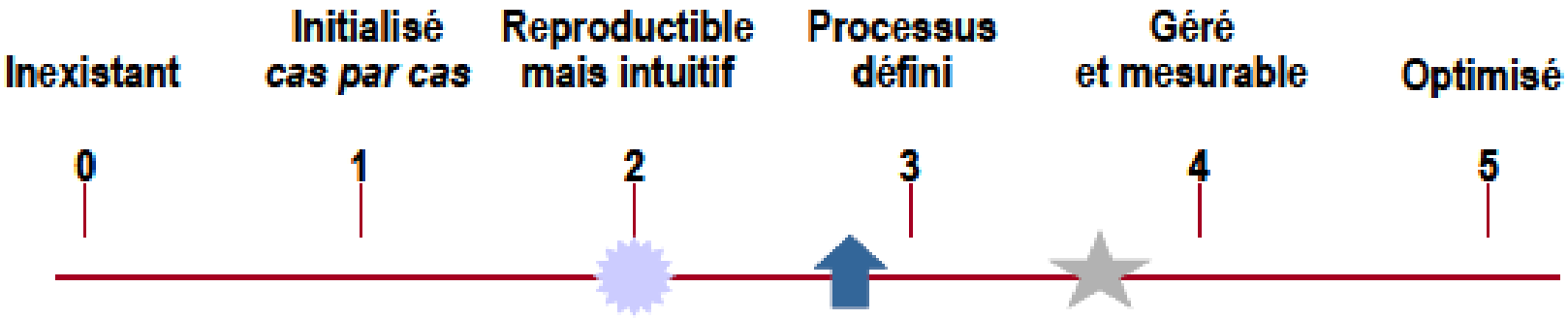
Surveillance

SE1 Surveiller et évaluer la performance des SI
SE2 Surveiller et évaluer le contrôle interne
SE3 S'assurer de la conformité aux obligations externes
SE4 Mettre en place une gouvernance des SI

Le cube de COBIT



COBIT :Modèle de maturité



LÉGENDE DES SYMBOLES UTILISÉS

- État actuel de l'entreprise
- Meilleure pratique du marché
- Stratégie de l'entreprise

LÉGENDE UTILISÉE POUR LE CLASSEMENT

0—Les processus de management ne sont pas appliqués du tout
1—Les processus sont mis en œuvre *au cas par cas* et sans méthode
2—Les processus suivent un même modèle
3—Les processus sont documentés et communiqués
4—Les processus sont surveillés et mesurés
5—Les bonnes pratiques sont suivies et automatisées

Source AFAI

COBIT :Modèle de maturité

COBIT
GOVERNANCE, CONTROL *and* ASSURANCE *for* INFORMATION *and* RELATED TECHNOLOGY

0 Inexistant : Absence totale de processus identifiables. L'entreprise n'a même pas pris conscience qu'il s'agissait d'un problème à étudier.

1 Initialisé/Cas par cas : On constate que l'entreprise a pris conscience de l'existence du problème et de la nécessité de l'étudier. Il n'existe toutefois aucun processus standardisé, mais des démarches dans ce sens tendent à être entreprises individuellement ou cas par cas. L'approche globale du management n'est pas organisée.

2 Reproductible mais intuitif : Des processus se sont développés jusqu'au stade où des personnes différentes exécutant la même tâche utilisent des procédures similaires. Il n'y a pas de formation organisée ni de communication des procédures standard et la responsabilité et laissée à l'individu. On se repose beaucoup sur les connaissances individuelles, d'où un risque d'erreurs.

3 Processus défini : On a standardisé, documenté et communiqué des processus *via* des séances de formation. Ces processus doivent impérativement être suivis ; toutefois, des écarts seront probablement constatés. Concernant les procédures elles-mêmes, elles ne sont pas sophistiquées mais formalisent des pratiques existantes.

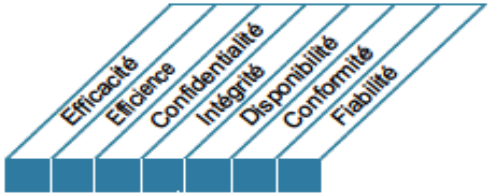
4 Géré et mesurable : La direction contrôle et mesure la conformité aux procédures et agit lorsque certains processus semblent ne pas fonctionner correctement. Les processus sont en constante amélioration et correspondent à une bonne pratique. L'automatisation et les outils sont utilisés d'une manière limitée ou partielle.

5 Optimisé : Les processus ont atteint le niveau des bonnes pratiques, suite à une amélioration constante et à la comparaison avec d'autres entreprises (Modèles de Maturité). L'informatique est utilisée comme moyen intégré d'automatiser le flux des tâches, offrant des outils qui permettent d'améliorer la qualité et l'efficacité et de rendre l'entreprise rapidement adaptable.

Source AFAI

Navigation dans COBIT

On trouvera une description de chacun des processus informatiques de COBIT, ainsi que des objectifs clés et des métriques, dans cette présentation en cascade.



Le contrôle du processus informatique

nom du processus

qui répond à l'exigence des métiers vis-à-vis de l'informatique

liste des principaux objectifs métiers

en se concentrant sur

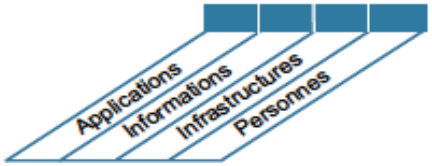
liste des principaux objectifs du processus

atteint son objectif grâce à

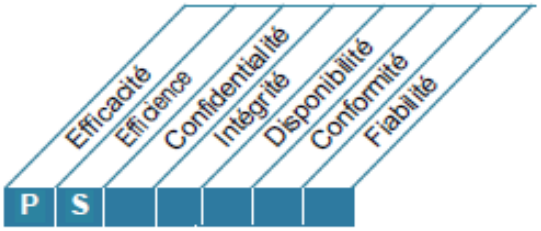
des objectifs liés à l'activité

et est mesuré par

des métriques clés



Navigation dans COBIT (exemple1/2)



Le contrôle du processus informatique

Définir un plan informatique stratégique

qui répond à l'exigence des métiers vis-à-vis de l'informatique

soutenir ou étendre les exigences de stratégie et de gouvernance de l'entreprise tout en maintenant la transparence des bénéfices, des coûts et des risques

en se concentrant sur

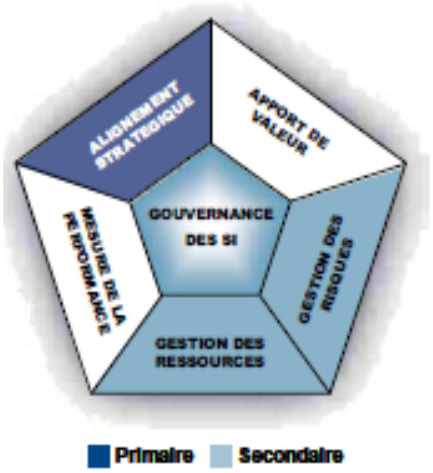
la convergence du management de l'entreprise et du management de l'informatique dans la traduction des exigences des métiers en offres de services, et sur le développement de stratégies pour fournir ces services en toute transparence et efficacité

atteint son objectif en

- travaillant avec les métiers et la direction générale pour aligner la planification stratégique des SI avec les besoins actuels et futurs de l'entreprise
- ayant un bonne connaissance des capacités actuelles des technologies de l'information
- fournissant un schéma des priorités à appliquer aux objectifs des métiers qui quantifie les exigences des métiers

Navigation dans COBIT (exemple2/2)

COBIT
GOVERNANCE, CONTROL *and* ASSURANCE *for* INFORMATION *and* RELATED TECHNOLOGY



et est mesuré par

- le pourcentage des objectifs informatiques du plan informatique stratégique qui apporte un soutien au plan stratégique des métiers
- le pourcentage de projets informatiques dans le portefeuille de projets qui découle directement du plan tactique des SI
- le délai entre les mises à jour du plan stratégique des SI et celles du plan tactique

IT BALANCED SCORECARD

COBIT
GOVERNANCE, CONTROL *and* ASSURANCE *for* INFORMATION *and* RELATED TECHNOLOGY

Axe Utilisateur

Comment les Utilisateurs perçoivent-ils le département IT ?

Mission : Etre le fournisseur préféré de SI

Stratégies : Fournisseur préféré d'application et de traitement ; Proposer la meilleure solution quelque soit la source; Partenariat avec les Utilisateurs ; Satisfaction des Utilisateurs

Contribution au Business

Comment la Direction perçoit-elle la DSI ?

Mission : Obtenir des investissements IT une contribution raisonnable au Business de l'entreprise

Stratégies : Contrôle des dépenses IT; Valeur Business des projets IT; Apporter des capacités nouvelles en terme de Business

Excellence Opérationnelle

Quelle est l'efficacité et l'efficience des Processus IT ?

Mission : Livrer des applications et des services efficaces et efficients

Stratégies :

Efficacité et Efficience des développements
Efficacité et Efficience des traitements

Orientation Future

Les TI sont-elles bien positionnées pour répondre aux besoins futurs ?

Mission : Développer des opportunités pour répondre aux besoins futurs

Stratégies : Formation générale et professionnelle du personnel IT; Expertise du personnel IT; recherche de technologies émergentes, ancienneté du portefeuille d'applications.

COBIT
GOVERNANCE, CONTROL *and* ASSURANCE *for* INFORMATION *and* RELATED TECHNOLOGY

L'Axe « Contribution au Business » peut s'analyser sous l'angle de 5 Objectifs Stratégiques :

- La DSI apporte sa contribution aux initiatives stratégiques de l'Entreprise.
- La DSI propose des initiatives basées sur sa maîtrise des Nouvelles Technologies et ouvre de nouveaux horizons stratégiques.
- Contrôle et Compétitivité des coûts informatiques.
- Évaluation et Contrôle financier des projets IT.
- Évolution de la productivité informatique.

IT BALANCED SCORECARD

COBIT
GOVERNANCE, CONTROL *and* ASSURANCE *for* INFORMATION *and* RELATED TECHNOLOGY

L'Axe « Utilisateur» peut s'analyser sous l'angle de 2 Objectifs Stratégiques

- **Qualité et Efficacité de la relation Informatique / Utilisateurs,**

- **Satisfaction des Utilisateurs (« clients » internes de l'Informatique).**

IT BALANCED SCORECARD

COBIT
GOVERNANCE, CONTROL *and* ASSURANCE *for* INFORMATION *and* RELATED TECHNOLOGY

L'Axe « Performance Opérationnelle» peut s'analyser sous l'angle de 5 Objectifs Stratégiques :

- **Efficacité du développement d'applications,**
- **Efficacité de la Production,**
- **Efficacité du Help-Desk / Service-Desk,**
- **Efficacité / Réactivité du Support Utilisateur,**
- **Adéquation du niveau de Sécurité aux besoins et aux enjeux.**

IT BALANCED SCORECARD

COBIT
GOVERNANCE, CONTROL *and* ASSURANCE *for* INFORMATION *and* RELATED TECHNOLOGY

L'Axe « Orientation Future » peut s'analyser sous l'angle de 5 Objectifs Stratégiques :

- **Amélioration des processus,**
- **Efficacité de la Gestion du Personnel,**
- **Amélioration de l'architecture technique et fonctionnelle des SI,**
- **Innovation et Leadership Technologique,**
- **Amélioration de la Gestion des Compétences.**

COBIT
GOVERNANCE, CONTROL *and* ASSURANCE *for* INFORMATION *and* RELATED TECHNOLOGY

Présentation de la famille COBIT

Depuis sa création, le contenu de base de COBIT n'a cessé d'évoluer au fil des ans et le nombre de produits dérivés de COBIT n'a cessé d'augmenter.

Les publications dérivées de COBIT sont aujourd'hui les suivantes :

Quickstart V2

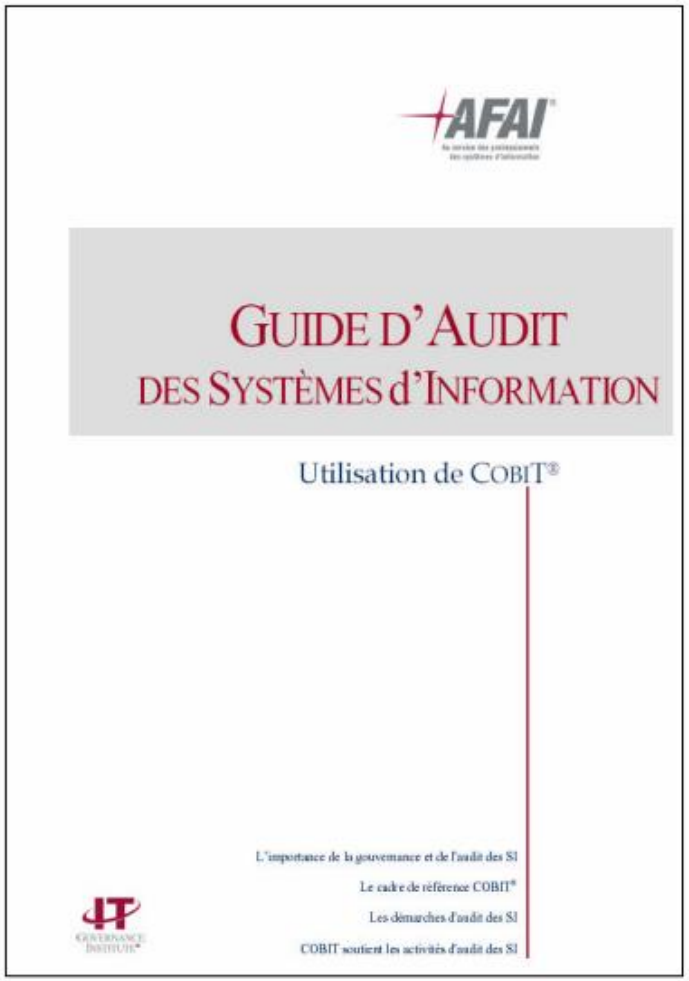
COBIT Quickstart propose une première approche aux nombreuses PME et autres entités pour lesquelles les TI ne sont ni un enjeu stratégique ni un élément clé de leur survie ; pour d'autres entreprises il constitue un point de départ dans leur évolution vers un niveau de contrôle et de gouvernance des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

- ☞ Version allégée de COBIT V4.1
- ☞ Bonnes pratiques de gestion revues et référencée par rapport aux activités COBIT V4.1
- ☞ Intègre les tableaux RACI et une révision complète des objectifs et métriques

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

- ❑ 30 processus sur les 34,
- ❑ 62 objectifs de contrôle détaillés sur les 220 habituels.

Guide d'audit de COBIT



- **Basé sur COBIT V4.1 et entièrement refondu**
- **Guide d'audit détaillé des 34 processus COBIT et des applications**
- **Intègre une présentation détaillée des concepts d'audit des SI**

Le référentiel **Val IT** est un ensemble structuré de pratiques clés de management se rapportant à la gouvernance des systèmes d'information.

Cette dernière comporte deux volets : un aspect **risques**, qui conduit à des pratiques d'audit et à des référentiels de bonnes pratiques comme CobiT. Et un aspect **performance**, insuffisamment outillé au début des années 2000.

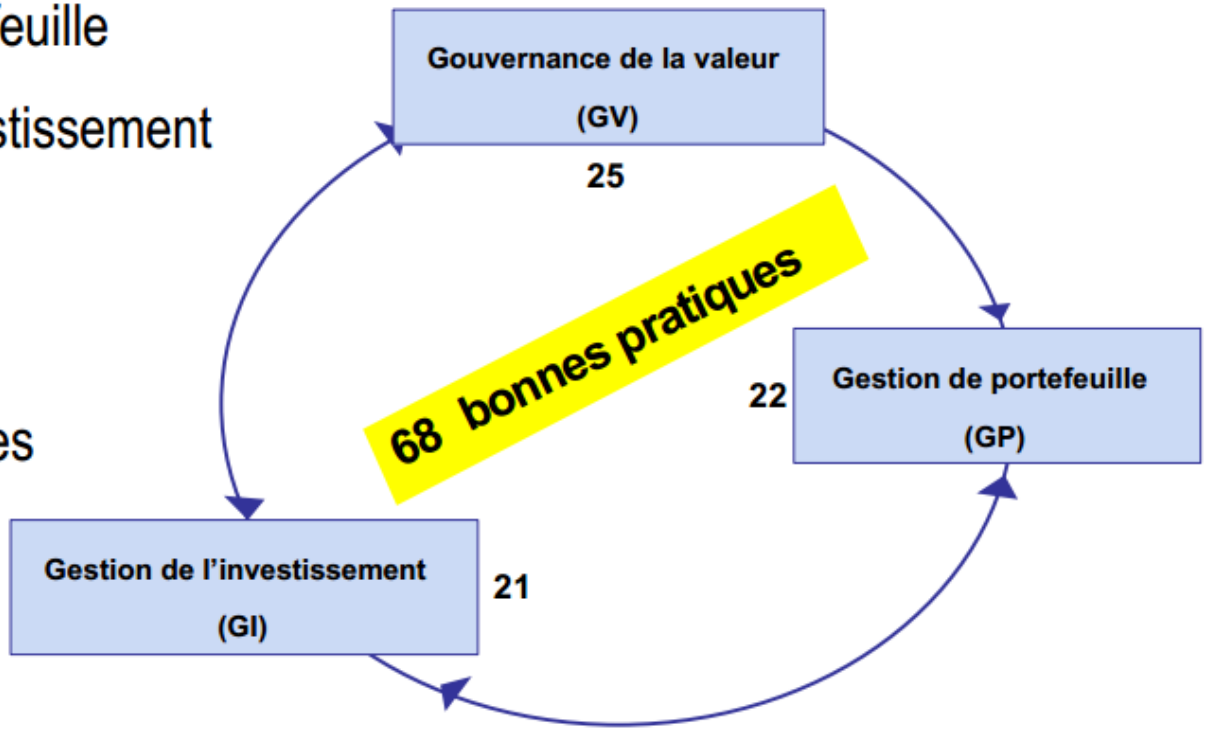
Val IT offre à la Direction de l'organisation un ensemble de préconisations lui permettant d'évaluer et sélectionner les projets de développement du système d'information en fonction de leur valeur, d'une part, d'anticiper puis de suivre leur cycle de vie du point de vue économique ensuite et, par retour d'expérience, d'améliorer les méthodes employées pour l'évaluation a priori des nouveaux projets, dénommées dans ce référentiel business cases.

3 domaines :

- Gouvernance de la valeur
- Gestion de portefeuille
- Gestion de l'investissement

22 processus

68 bonnes pratiques



Quatre questions guident la construction du *business case* (*4 Ares* en anglais):

- Faisons-nous les choses appropriées ? Quels objectifs métier, et le projet y contribue-t-il ?
- Faisons-nous les choses de façon appropriée? Prise en compte les capacités de la firme.
- Les tâches sont-elles effectuées correctement? Planification, budgets...
- En tirons-nous les bénéfices attendus ?

RISK IT est le référentiel de management du système d'information et des technologies par les risques. C'est un guide de principes directeurs et de bonnes pratiques. Il aide les entreprises à mettre en place une gouvernance ad hoc, à identifier et à gérer efficacement les risques informatiques. Il a été réalisé par une centaine d'experts internationaux de l'ISACA et adapté en langue française par l'AFAI, chapitre français de l'ISACA, en coopération étroite avec d'autres chapitres francophones.

RISK IT considère le risque informatique comme un risque d'affaire/métier alors qu'il est trop souvent vu comme un risque technique réservé aux experts de l'informatique.

3 domaines :

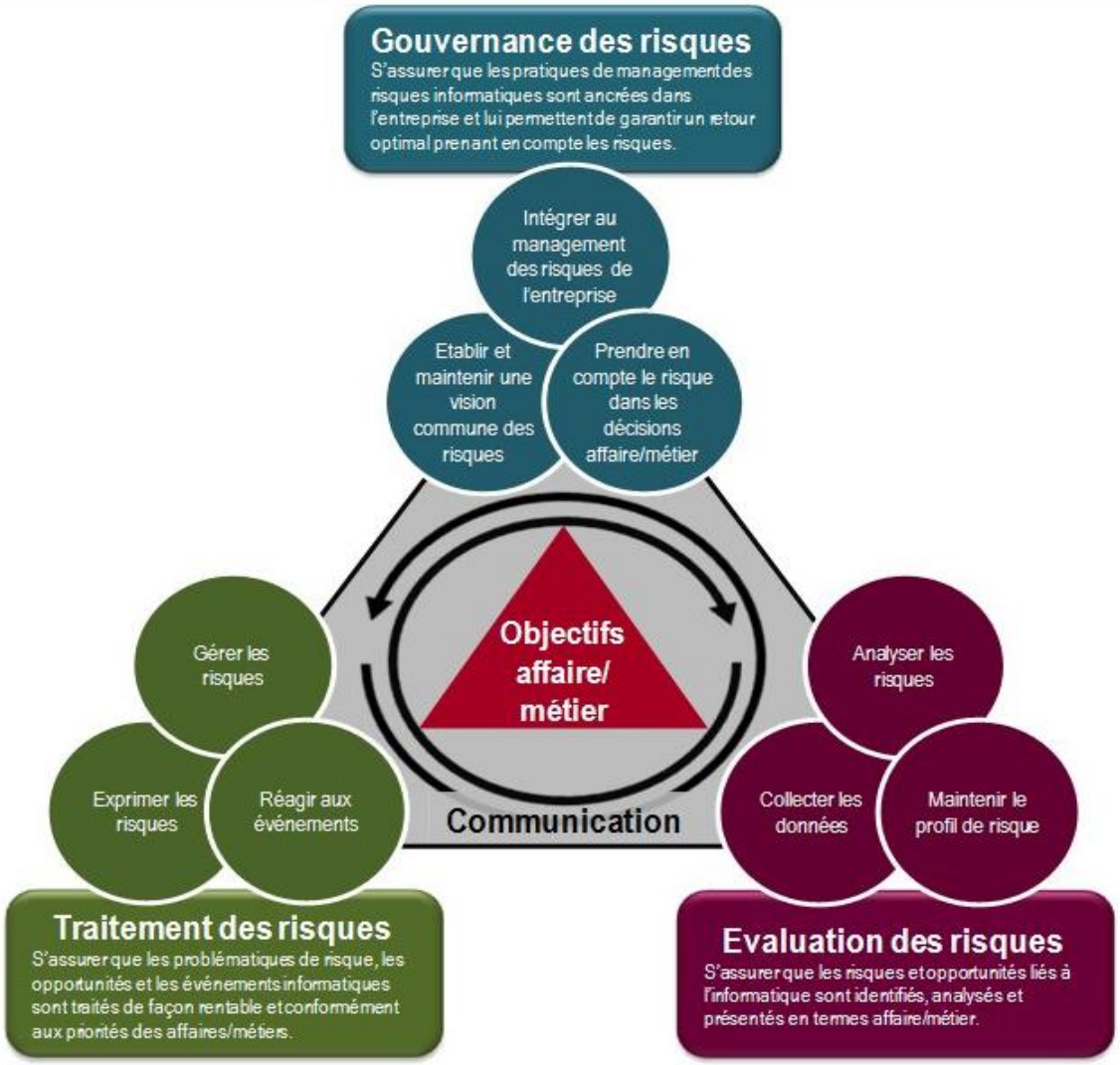
- Gouvernance des risques (GR)
- GR1 Établir et maintenir une vision commune des risques
- GR2 Intégrer le management des risques informatiques au management des risques de l'entreprise (MRE)
- GR3 Prendre en compte les risques dans les décisions affaire/métier

- Evaluation des risques (ER)
- ER1 Collecter les données
- ER2 Analyser les risques
- ER3 Maintenir le profil de risque

- Traitement des risques
- TR1 Exprimer les risques

- TR2 Gérer les risques
- TR3 Réagir aux événements.

Référentiel Risk IT



MERCI
POUR VOTRE ATTENTION

COBIT®
GOVERNANCE, CONTROL *and* ASSURANCE *for* INFORMATION *and* RELATED TECHNOLOGY

Pour une meilleure gouvernance des systèmes d'information