



# Management Stratégique du SI (MSSI)

Cours N°3

Gouvernance d'entreprise et Gouvernance du SI (3)



# Position dans le programme



1- Rappels

**2- Gouvernance du Système d'Information**

3- Architecture d'entreprise & Urbanisation du Système d'Information

4 - Alignement du Système d'Information

# Sommaire

 COBIT, VAL IT et RISK IT

 ITIL

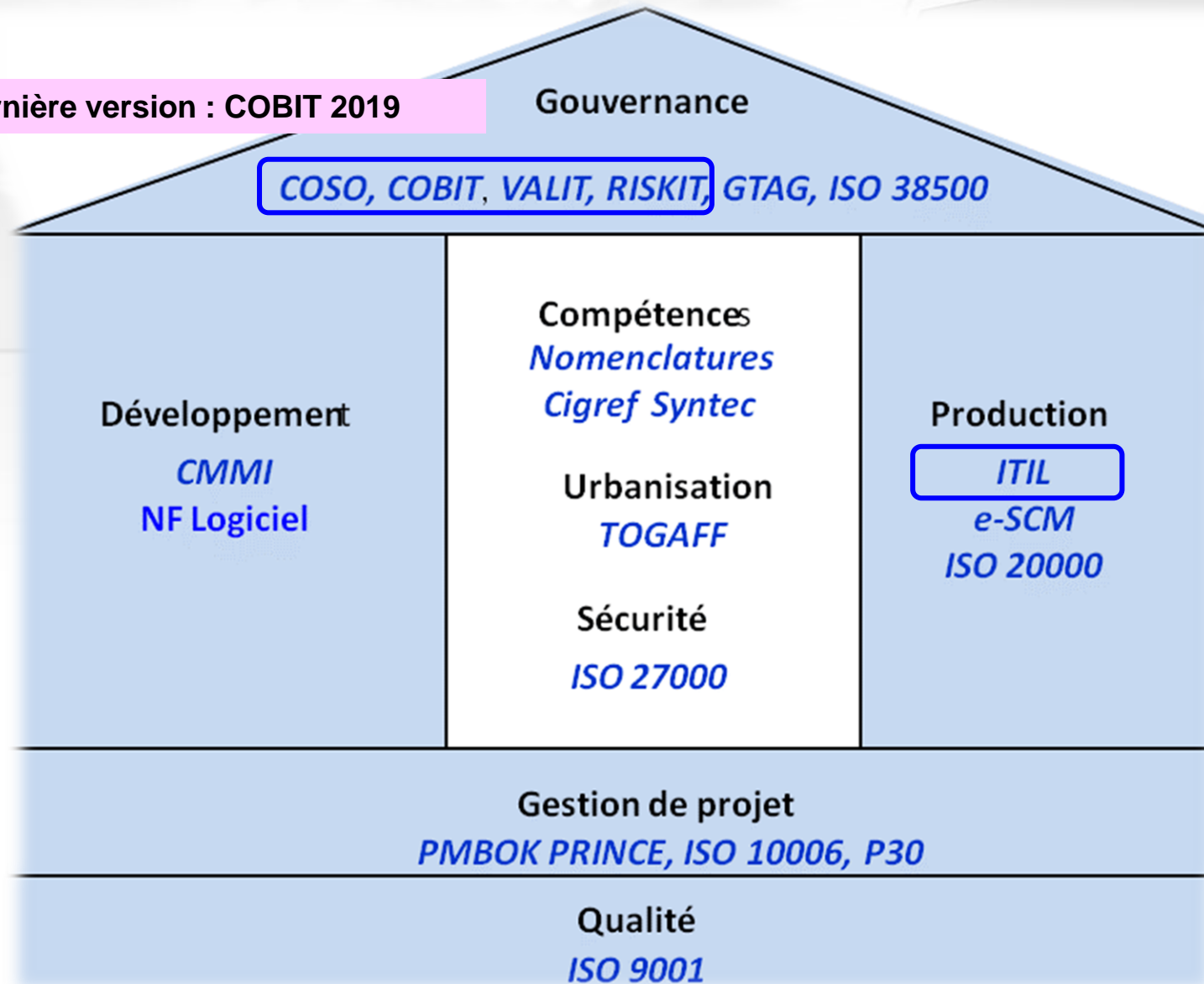
 Différence COBIT vs ITIL



# MSSI de l'entreprise

## Approche par « les référentiels institutionnels »

Dernière version : COBIT 2019



Référentiels = Bonnes pratiques

(Alban, 2012)

# Qu'est-ce que COBIT ?

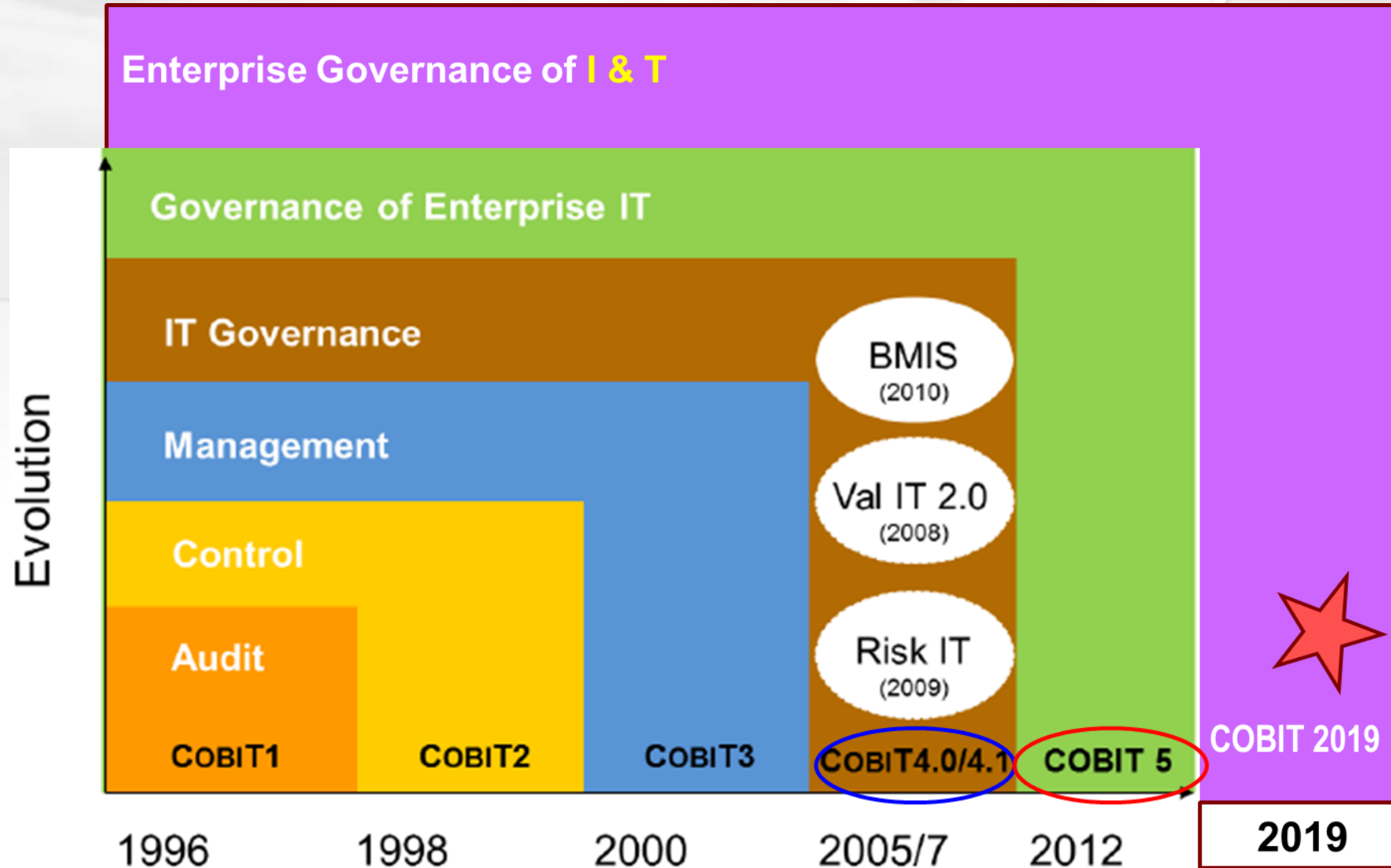
**COBIT** — *Control Objectives for Information and Technology* — est un cadre de gouvernance et de gestion des technologies de l'information reconnu à l'échelle mondiale, il constitue la référence incontournable pour les organisations souhaitant structurer leur gouvernance TI.

Son ambition centrale : **aligner les systèmes d'information sur les objectifs métiers** de l'entreprise, tout en garantissant sécurité, conformité et création de valeur.

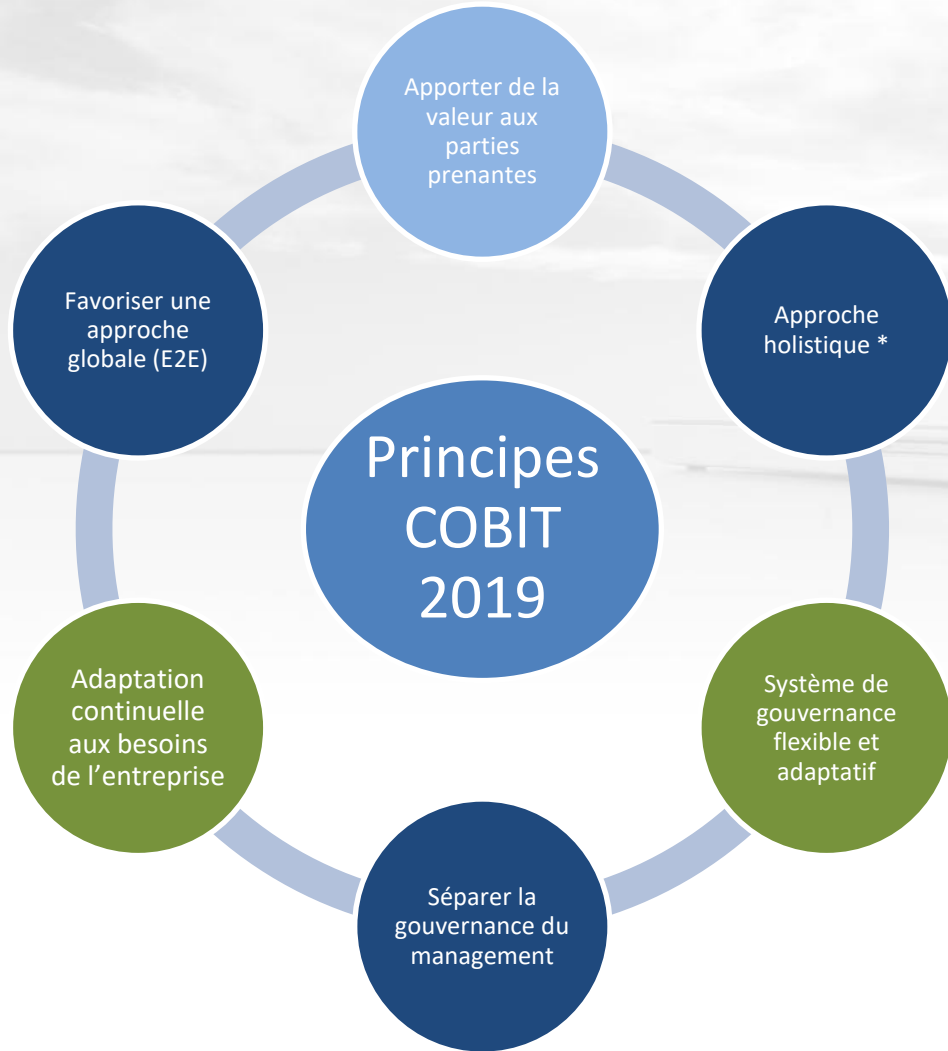
- Référentiel reconnu dans plus de 180 pays
- Adopté par des milliers d'organisations mondiales
- Développé et maintenu par l'ISACA (Information Systems Audit and Control Association)
- Apporte un langage commun
- Intègre gouvernance et SI
- Compatible avec d'autres normes internationales
- Répertoire de meilleures pratiques

# COBIT: Utilisation optimale & responsable des ressources

COBIT en quelques dates :



# COBIT: Utilisation optimale & responsable des ressources



COBIT 2019 a été mis à jour pour inclure :

- Plus de **clarté** sur la **création d'un système de gouvernance**
- Un **meilleur alignement avec les normes**, les **cadres** et les **meilleures pratiques**.
- Un modèle **open source** pour encourager des **mise à jour** et améliorations plus rapides.
- **Plus de conseils et d'outils** pour aider les entreprises **développer** un « **système de gouvernance mieux adapté. Ceci rend COBIT 2019 plus normatif** »
- Un **meilleur outil** pour mesurer les **performances de l'informatique** et l'**alignement** avec d'autres référentiels.
- **Plus d'aide à la prise de décision**, y compris de nouvelles **fonctionnalités collaboratives**.

An business framework from ISACA, at [www.isaca.org/cobit](http://www.isaca.org/cobit)

\* Une approche holistique est une méthode qui prend en compte l'ensemble des éléments d'un système, en considérant leurs interactions et leurs interdépendances.

# COBIT 2019

COBIT s'articule autour de **composants structurés et interdépendants** qui forment un système cohérent de gouvernance et de gestion des TI. Chaque composant joue un rôle précis dans l'atteinte des objectifs organisationnels.

Les **domaines principaux** regroupent les processus selon leurs fonctions :

- **Évaluer, Diriger et Surveiller (EDM)**
- **Aligner, Planifier et Organiser (APO)**
- **Construire, Acquérir et Implémenter (BAI)**
- **Délivrer, Servir et Soutenir (DSS)**
- **Surveiller, Évaluer et Mesurer (MEA)**

## Principes

Les fondations conceptuelles sur lesquelles repose l'ensemble du cadre COBIT.

## Cadre

La structure globale qui organise et articule tous les éléments du référentiel.

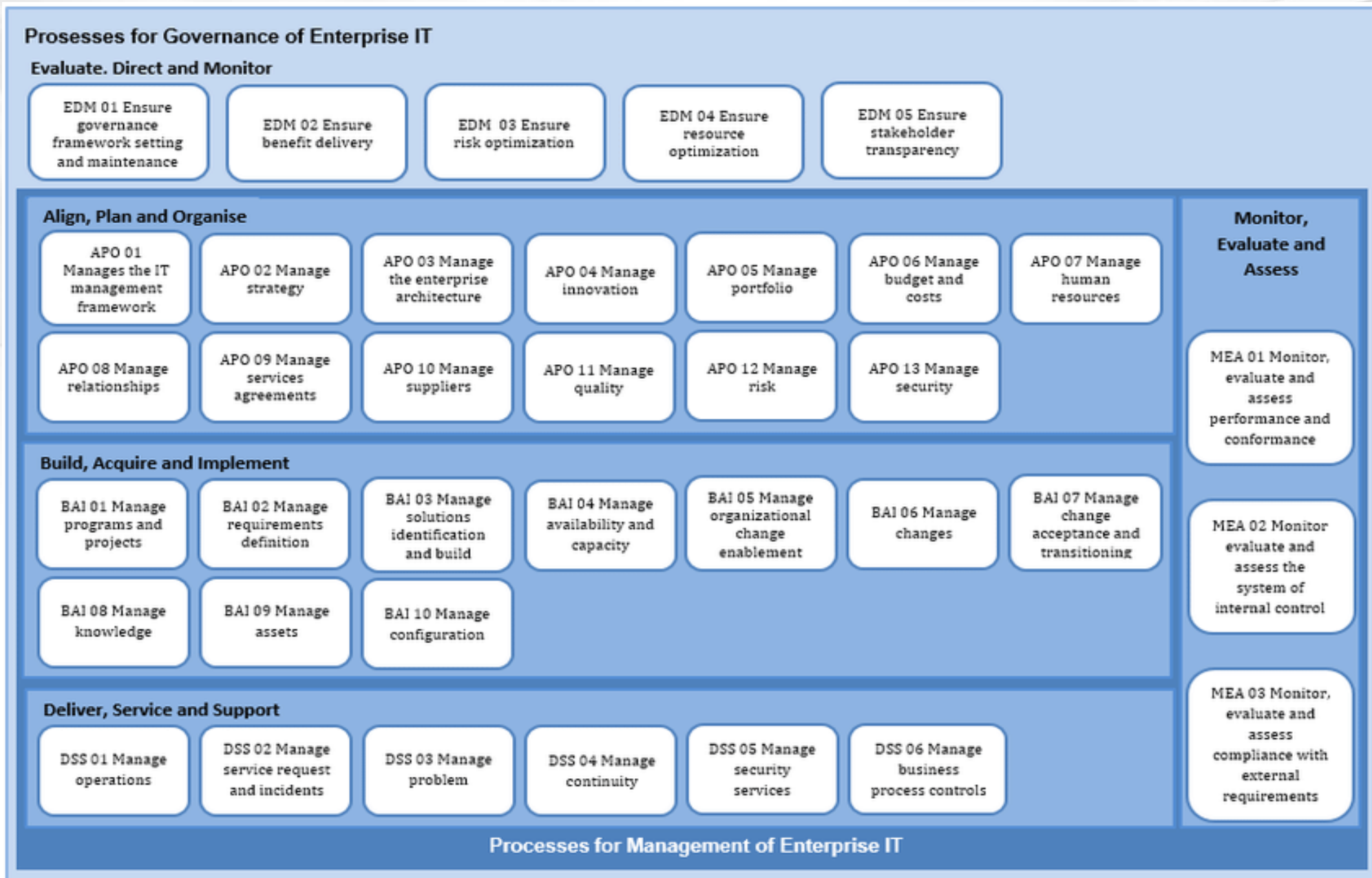
## Processus

Des ensembles d'activités définies et mesurables pour atteindre des objectifs spécifiques.

## Domaines

Regroupement logique des processus par grandes fonctions de gouvernance et de gestion.

# COBIT 2019



# COBIT: Utilisation optimale & responsable des ressources

Comment en piloter l'efficacité ?

## Facteurs Clés de Succès

- Les activités de gouvernance des TI sont intégrées dans le processus de gouvernance de l'entreprise et dans les comportements des responsables au plus haut niveau
- La gouvernance des TI se concentre sur les buts de l'entreprise, ses initiatives stratégiques, l'utilisation des technologies pour améliorer l'activité, et sur la disponibilité de ressources et de capacités suffisantes pour faire face aux demandes des métiers
- On a défini pour les activités de gouvernance des TI un objectif clair, documenté et implémenté, basé sur les besoins de l'entreprise, avec des responsabilités bien définies
- On a mis en place des pratiques de gestion pour augmenter l'utilisation efficiente et optimale des ressources ainsi que l'efficacité des processus informatiques
- On a établi des pratiques qui permettent : une surveillance fiable ; une culture et un environnement de contrôle ; l'évaluation des risques comme pratique standard ; un bon degré d'adhésion aux standards établis ; la surveillance et le suivi des risques et des défaillances des contrôles
- On a défini des pratiques de contrôle pour éviter les ruptures de contrôle interne et de surveillance
- Les processus informatiques les plus complexes comme la gestion des problèmes, la gestion des changements et celle de la configuration sont intégrés et interagissent entre eux facilement
- On a créé un comité d'audit qui a la charge de choisir un auditeur indépendant et de suivre son travail, qui est axé sur les TI lorsqu'il pilote les plans d'audit, et qui révise les résultats des audits ainsi que les revues faites par des tiers

## Indicateurs Clés d'Objectif

- Amélioration de la gestion des performances et des coûts
- Amélioration du retour sur les investissements informatiques majeurs
- Réduction du délai de mise sur le marché
- Amélioration de la gestion de la qualité, de l'innovation et des risques
- Élargissement de la clientèle, et satisfaction de la clientèle existante
- Amélioration de la disponibilité de la bande passante, de la puissance de traitement et des mécanismes de fournitures de services informatiques
- Exigences et attentes du client du processus satisfaites dans le respect des délais et des coûts
- Respect des lois, règlements, standards professionnels et engagement contractuels
- Transparence dans la prise de risques et respect du cadre convenu de profil de risque de l'entreprise
- Tests comparatifs appliqués à la maturité de la gouvernance des TI
- Création de nouveaux canaux de distribution de services

## Indicateurs Clés de Performance

- Meilleure rentabilité des processus informatiques (coûts versus livrables)
- Plus grand nombre de plans d'actions informatiques d'initiatives d'amélioration des processus
- Plus grande utilisation des infrastructures informatiques
- Plus grande satisfaction des parties concernées (sondages, nombre de plaintes)
- Plus grande productivité (nombre de livrables) et motivation (sondages) des personnels
- Plus grande disponibilité des connaissances et des informations nécessaires à la gestion de l'entreprise
- Plus grand nombre de liens entre l'informatique et la gouvernance d'entreprise
- Amélioration de la performance mesurée par les tableaux de bord équilibrés des TI

# Val IT - Création et gestion de la valeur

- 🏠 **VAL IT** (Enterprise Value : Governance of IT investments) est un **cadre de référence** pour la gouvernance des investissements informatiques.
- 🏠 Les **projets de transformation organisationnel** et de ses processus comportent de plus en plus souvent une composante **informatique significative**.
- 🏠 A l'échelle d'une entreprise ou d'une organisation, il n'est pas rare qu'une multitude de projets soient menés en parallèle, à des stades de développement divers.
- 🏠 Les dirigeants exigent **de plus en plus de transparence** sur les apports des projets et souhaitent pouvoir **étayer leurs décisions** et **arbitrer** ou **réviser les choix effectués**.
- 🏠 Cette situation implique un questionnement de la part de l'organisation.

# Val IT - Création et gestion de la valeur

Est-ce que les investissements informatiques sont réellement gérés de sorte à :

- **Obtenir la contribution maximale à la création de valeur et des résultats ?**
- **Obtenir un coût optimal ?**
- **Réduire le risque au niveau acceptable ?**

QUOI ?

**Val IT complète COBIT et traite :**

- **Investissements à forte composante TI pour des projets business**
- **Gestion d'un "Portefeuille" de projets et de programmes**

POURQUOI ?

**L'objectif est de :**

- **Accroître la transparence des coûts, risques et bénéfices**
- **Accroître la probabilité d'identifier les options gagnantes**
- **Accroître la probabilité de réussite de ces options gagnantes**
- **Réduire les coûts en ne faisant pas ce qu'il n'est pas utile de faire**
- **Réduire les risques d'échecs à fort impact négatif pour le business**
- **Réduire les incertitudes relatives aux coûts, délais et qualité des projets IT**

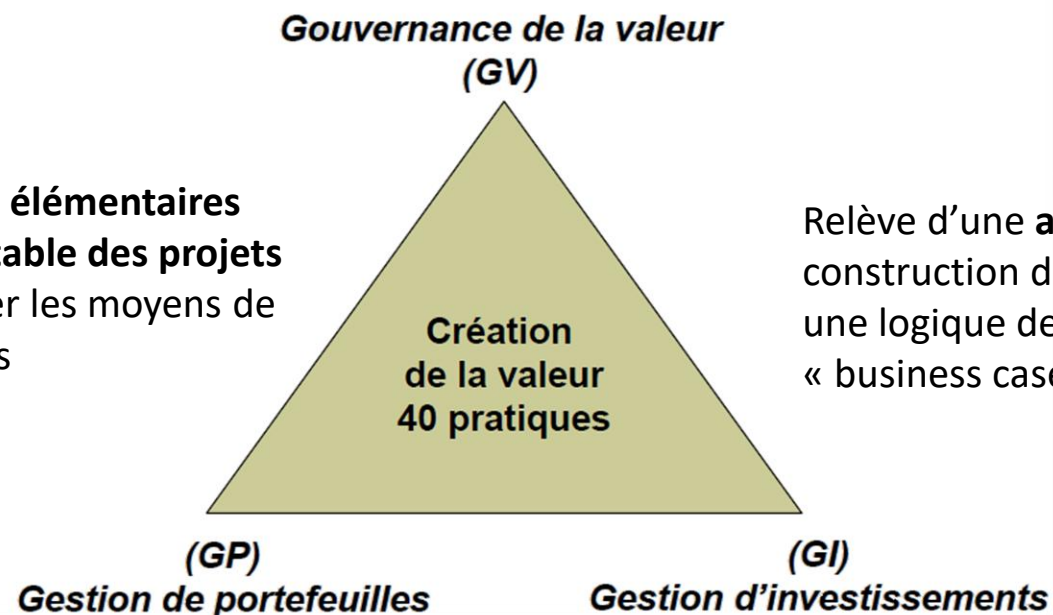
# Val IT - Création et gestion de la valeur

Val IT comprend 3 parties:

- Un **cadre de référence** pour obtenir une **réelle valeur des investissements informatiques**;
- La **description** du rôle clé du « plan d'affaires »;
- Un **retour d'expérience** réel.

Comment s'organiser pour **piloter, maîtriser** les projets, **décider** de la **poursuite des projets** et savoir, en toute connaissance d'où vient la valeur pour l'entreprise et les moyens pour la valoriser

Comment **organiser les projets élémentaires** pour obtenir une **vision exploitable des projets** lancés ou en cours, et se donner les moyens de piloter le portefeuille de projets



Relève d'une **analyse des projets élémentaires** et de construction de **programmes qui les englobent**, et s'appuie sur une logique de **démonstration de la valeur créée**, au travers de « business case ».

# Val IT - Création et gestion de la valeur

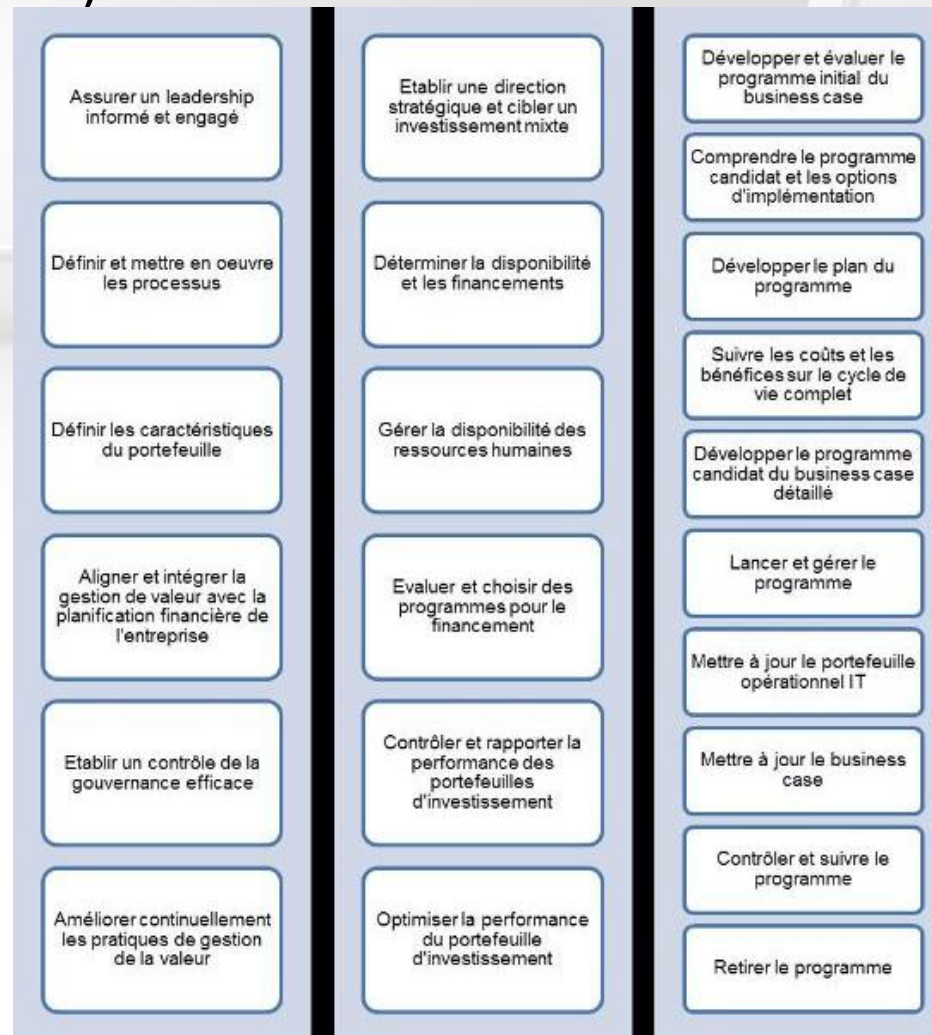
Quels sont les principes de VAL IT ?

🏠 Basé sur les processus (3 domaines, 22 processus, 69 activités)

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

🏠 Val IT/COBIT traite des questions :

- Faisons-nous ce qu'il faut (question stratégique)?
- En obtenons-nous les bénéfices (question de la valeur) ?
- Le faisons-nous comme il faut (question architecture)?
- Le faisons-nous faire comme il faut (question de la réalisation)?



# Val IT - Création et gestion de la valeur

Quels sont bénéfices constatés par profil métier ?

## Pour les Chefs de projet(s)

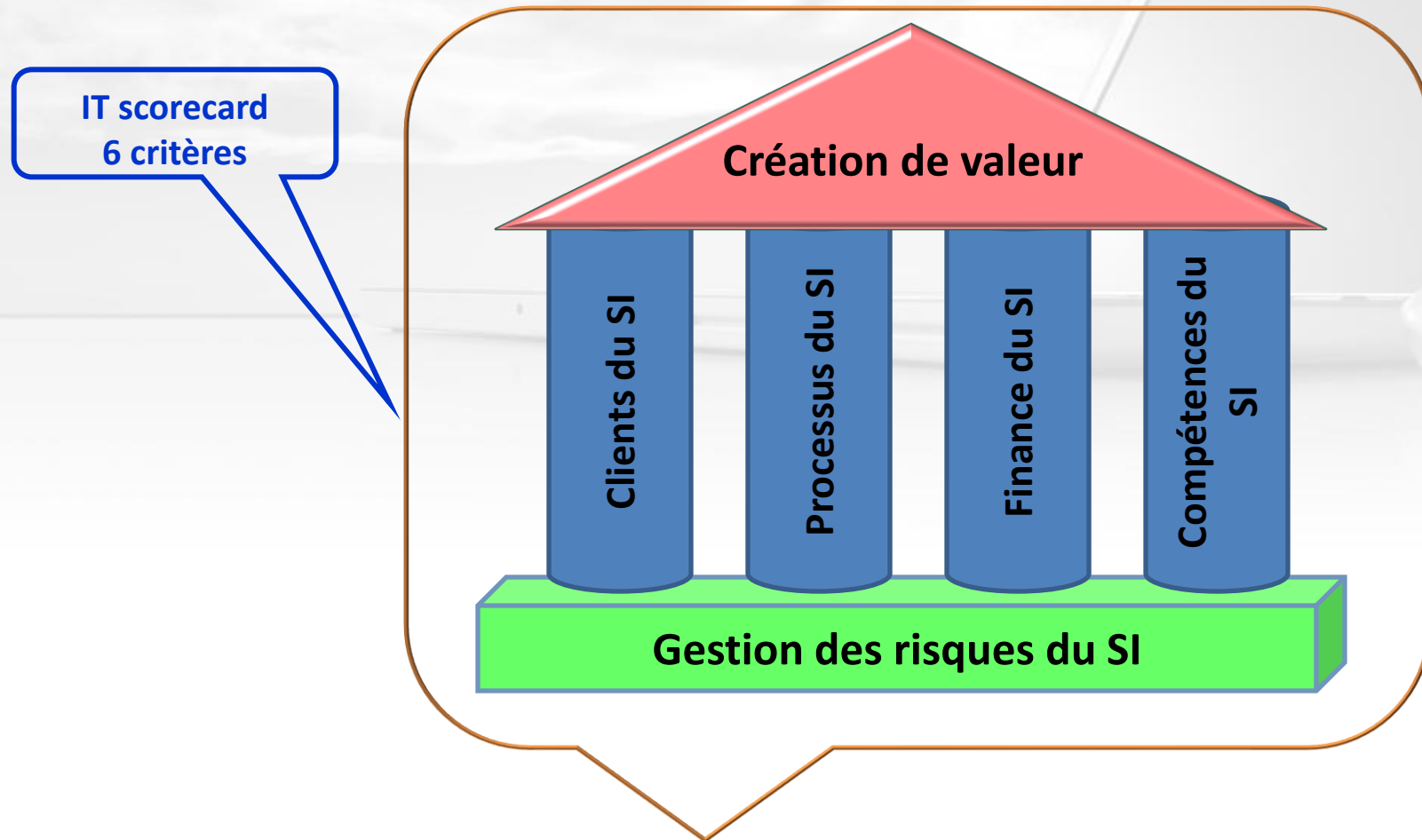
- **Identification amont des points durs du projet** → réalisation d'arbitrages
- **Support d'échange et de dialogue** avec les décideurs (MOA métier, DSI...) et la MOE à chaque étape du projet sur la base d'éléments factuels
- **Mise en valeur de la rentabilité et des bénéfices qualitatifs** du projet

## Pour les Décideurs (DSI, R Prog)

- **Méthode commune d'évaluation des projets** → arbitrages
- **Engagement de la Direction projet sur des résultats**
- **Engagement de la MOA métier sur des objectifs de gain**
- **Suivi de l'évolution de la valeur du projet** au fil du temps
- **Identification des éléments qualitatifs du projet**

# IT Governance: Approche par les objectifs (IT Scorecard)

IT Scorecard & transparence



+ Transparence et relations

# IT Governance: Approche par les objectifs (IT Scorecard)

Diagnostic du niveau de maturité de l'entreprise

Développement de  
La transparence

Création de valeur

Orientation  
client

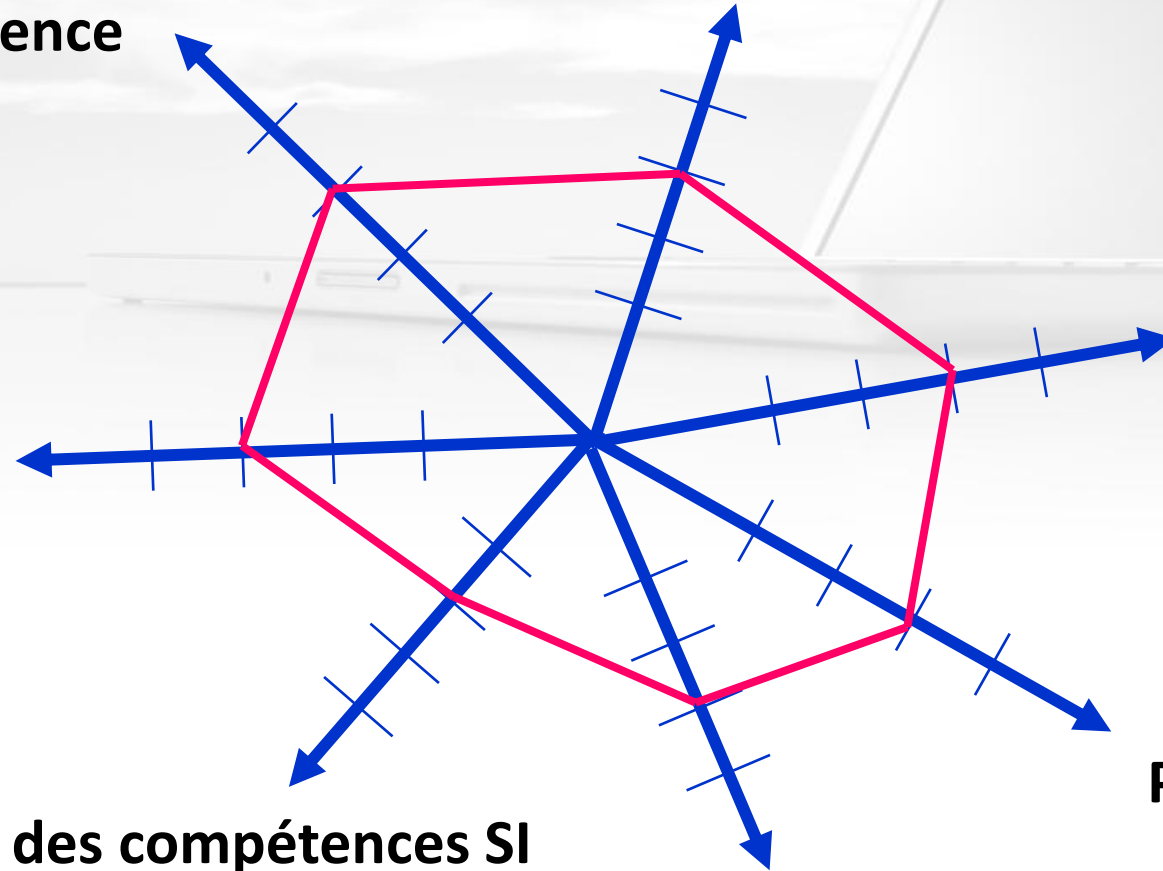
Gestion des  
risques SI

Performance des  
processus SI

Gestion des compétences SI

Maîtrise des aspects  
financiers du SI

Niveau de maturité d'un objectif



# Risk IT - Maîtrise du niveau de risque

- 🏠 Complémentaire à CobiT et VALIT, basé sur les mêmes principes
- 🏠 CobiT identifie les bonnes pratiques pour les « moyens » de la maîtrise des risques
- 🏠 Risk IT identifie les **bonnes pratiques** pour les « fins » de la maîtrise des risques
- 🏠 Basé sur les processus (3 domaines , 9 processus, 47 activités)

## Gouvernance des risques

- Etablir et maintenir une vision commune des risques
- Intégrer les risques SI à la démarche de risque au niveau de l'entreprise
- Prendre des décisions business qui tiennent compte des risques

## Evaluation des risques

- Collecter des données
- Analyser les risques
- Maintenir un profil de risque

## Réponses aux risques

- Articuler la situation relative aux risques
- Gérer les risques SI
- Réagir aux évènements

# Risk IT - Maîtrise du niveau de risque

3 types de risques identifiés

## 🏠 Fourniture de **services informatiques**

- Associé à la performance et la disponibilité des services informatiques qui peut conduire à la perte ou à la réduction de valeur
  - Interruptions de services, problèmes de sécurité, problèmes de conformité,...

## 🏠 Fourniture de **solutions informatiques**

- Associé à la contribution du SI aux nouvelles solutions business ou aux solutions améliorées sous forme de programmes et de projets
  - Qualité des projets, Pertinence des projets, Dépassements,...

## 🏠 Réalisation de **bénéfices**

- Associé aux opportunités ratées pour utiliser la technologie pour améliorer l'efficacité et l'efficience des processus business ou comme levier à de nouvelles initiatives business
  - Levier pour de nouvelles opportunités business, Levier pour des opérations efficientes

# Risk IT - Maîtrise du niveau de risque

**Tous les risques doivent être analysés** à l'aune des bénéfices et des pertes potentielles

- Impacts liés à un risque non traité versus les bénéfices associés au fait d'être traité
- Bénéfices potentiels liés à la saisie d'une opportunité versus les bénéfices manqués liés à la non saisie d'une opportunité

Risk IT explicite les risques SI et va permettre aux acteurs de s'assurer que :

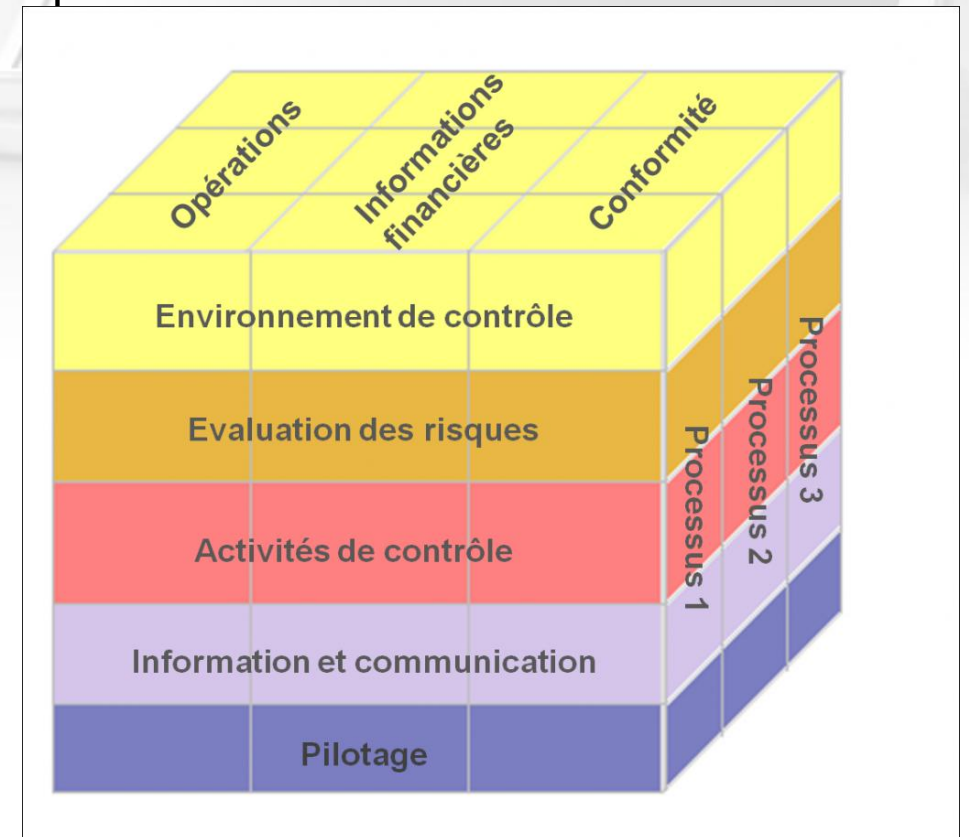
- La gestion des risques SI soit intégrée à la gestion des risques d'entreprise
- La démarche permet de prendre des décisions en étant « informées » sur les risques acceptables, tolérables, ou devant être traités immédiatement.
- La démarche permet de comprendre comment répondre aux risques identifiés

# COSO : Un référentiel international

Le Committee Of Sponsoring Organization de la Commission Treadway est un groupe de réflexion constitué aux Etats-Unis. Ce groupe a développé **un référentiel méthodologique** d'analyse du contrôle interne, dénommé "le COSO" publié en 1992.

**Le C.O.S.O.** structure l'analyse du contrôle interne selon cinq composantes :

- 🏠 L'environnement de contrôle
- 🏠 L'évaluation des risques
- 🏠 Les activités de contrôle, c'est-à-dire la définition des mesures de contrôle interne
- 🏠 L'information et la communication
- 🏠 Le pilotage (du contrôle interne).



# COSO : Un exemple avec l'organisation des tâches

- 🏠 La **séparation des tâches, le contrôle mutuel, la supervision, des règles de rotation** sur les fonctions sensibles sont des mesures de contrôle d'ordre organisationnel souvent utilisées pour garantir la sécurité dans le maniement des fonds publics.
- 🏠 Elles sont **intégrées aux procédures par tous les collaborateurs** (du manager aux opérationnel)
- 🏠 Le risque "0" n'existe pas. L'enjeu de cette démarche est donc de **trouver un équilibre entre le besoin de sécurité et une gestion efficiente des moyens** dont disposent les managers.

# COSO : Le champ d'intervention de l'audit

Les natures d'audits internes :

- régularité (ou de conformité)
- système (efficacité du contrôle interne)
- performance (appréciation des résultats, efficacité, efficience)

Plusieurs champs audités : informatique, budgétaire, comptable, gestion des RH, sécurité, etc...

Un audit très spécifique : l'audit financier (qui est un audit de régularité) = certification des comptes : AUDIT EXTERNE

# COSO : En résumé les trois types de contrôle

	Inspection	Audit	Contrôle interne
1. Périodicité	Ponctuelle, voire improvisée (secret)	Périodique et systématique (plan accepté)	Permanente
2. Position	Extérieure au service, voire supérieure	Interne	Intégrée
3. Objet	Opérations Personnes	Système Résultats	Gestion Risques
4. Buts / Préoccupation	La régularité (voir découvrir des irrégularités)	Efficacité	Maîtrise
5. Méthodologie	Guides	Standards	Référentiels de CI (piste d'audit)
6. Conséquences	Sanctions	Recommandations	Régularisations (plan d'action)
7. Responsabilité	Garantie	Opinion Assurance raisonnable	<i>Accountability</i>
8. Métiers	« Policier »	Consultant	Manager

# COSO : Les 17 principes

Domaines	Principes
Environnement de contrôle	<ol style="list-style-type: none"><li>1. L'organisation démontre son engagement en faveur de <b>l'intégrité</b> et de <b>valeurs éthiques</b>.</li><li>2. Le <b>conseil d'administration</b> fait preuve <b>d'indépendance</b> vis-à-vis du <b>management</b>. Il surveille la mise en place et le bon fonctionnement du système de contrôle interne.</li><li>3. La <b>direction</b>, agissant sous la surveillance du conseil d'administration, <b>définit</b> les <b>structures</b>, les <b>rattachements</b>, ainsi que les <b>pouvoirs</b> et les <b>responsabilités</b> appropriés pour atteindre les objectifs.</li><li>4. L'organisation démontre son <b>engagement</b> à <b>attirer, former et fidéliser des collaborateurs compétents</b> conformément aux objectifs.</li><li>5. L'organisation <b>instaure</b> pour chacun un <b>devoir de rendre compte</b> de ses responsabilités en matière de contrôle interne.</li></ol>
Evaluation des risques	<ol style="list-style-type: none"><li>6. L'organisation spécifie les <b>objectifs</b> de façon suffisamment <b>claire</b> pour permettre l'identification et l'évaluation des risques associés aux objectifs.</li><li>7. L'organisation identifie les <b>risques associés</b> à la réalisation de ses <b>objectifs</b> dans l'ensemble de son périmètre de responsabilité et elle procède à leur analyse de façon à déterminer les modalités de gestion des risques appropriées.</li><li>8. L'organisation <b>intègre</b> le <b>risque de fraude</b> dans son <b>évaluation</b> des <b>risques</b> susceptibles de compromettre la réalisation des objectifs.</li><li>9. L'organisation <b>identifie</b> et <b>évalue</b> les <b>changements</b> qui pourraient avoir un <b>impact significatif</b> sur le système de <b>contrôle interne</b>.</li></ol>

# COSO : Les 17 principes

Domaines	Principes
Activités de contrôle	<p>10. L'organisation <b>sélectionne</b> et <b>développe</b> les <b>activités de contrôle</b> qui contribuent à <b>ramener</b> à des <b>niveaux acceptables</b> les risques associés à la réalisation des objectifs.</p> <p>11. L'organisation <b>sélectionne</b> et <b>développe</b> des activités <b>de contrôle général</b> en matière de <b>système d'information</b> pour faciliter la réalisation des objectifs.</p> <p>12. L'organisation met en <b>place les activités de contrôle par</b> le biais de directives qui précisent les objectifs poursuivis, et de procédures qui mettent en œuvre ces directives.</p>
Information et communication	<p>13. L'organisation obtient ou génère puis <b>utilise des informations pertinentes</b> et de <b>qualité</b> pour <b>faciliter</b> le fonctionnement des autres composantes du contrôle interne.</p> <p>14. L'organisation <b>communique</b> en <b>interne les informations nécessaires</b> au bon <b>fonctionnement</b> des autres composantes du <b>contrôle interne</b>, notamment en ce qui concerne les objectifs et les responsabilités associés au contrôle interne.</p> <p>15. L'organisation <b>communique</b> avec les <b>tiers</b> au <b>sujet des facteurs</b> qui <b>affectent</b> le bon <b>fonctionnement</b> des autres composantes du contrôle interne.</p>
Pilotage	<p>16. L'organisation <b>sélectionne</b>, met au point et réalise des <b>évaluations continues</b> et/ou <b>ponctuelles</b> afin de <b>vérifier</b> si les composantes du <b>contrôle interne</b> sont bien mises en place et fonctionnent.</p> <p>17. L'organisation évalue et <b>communique</b> les <b>faiblesses de contrôle interne</b> en <b>temps voulu</b> aux responsables des mesures correctrices, notamment à la direction générale et au conseil d'administration.</p>

# ITIL : Les meilleurs pratiques dans la fourniture de service SI



- **Information Technology Infrastructure Library**
- **Collection de livres** sur les différents aspects de la gestion de la **production informatique**.
- Code de **bonnes pratiques** pour la **fourniture de services informatiques**.
- **Adoptée** et reconnue par les **grandes entreprises internationales**.
- Adoptée comme **standard** dans certains pays : ex : Pays-Bas ou Grande-Bretagne.
- Bibliothèque **ouverte** et **publique**

# ITIL : un peu d'histoire

- 1980** UK → IBM externalisation services IT  
IBM → UK avec un refus : trop hétérogènes, trop disparates, différents niveaux de maturité du SI
- 1986-90** CCTA (Central Computer and Telecom Agency) est mandatée pour **amener cohérence dans les services IT**  
Une équipe de 11 consultants fut constituée et travailla sur le sujet.
- Objectifs** Définir une **méthode** pour **recenser et cataloguer les meilleures pratiques** en matière de gestion de la production Informatique
- Principes** « méthode » et non d'une « méthodologie » :  
Méthode : ensemble de procédés (pratique)  
Méthodologie : étude des méthodes dans un domaine particulier (théorique)
- Conséquences** Tous les **départements IT** utilisent depuis le **même vocabulaire** et les mêmes processus quel que soit le service informatique.
- Deux exemples** Objectifs des organisations est le même : Créer de la valeur (Netflix vs VideoMax /Amazon vs La redoute)

# ITIL : C'est quoi ?

- 🏠 Ensemble de **bonnes pratiques** pour la gestion des services TI d'une organisation.
- 🏠 **Indépendant** du fournisseur et **immatérielle**
- 🏠 Offres des pratiques **testées et applicables** dans toutes les organisations.
- 🏠 Représente **l'expérience des plus grands fournisseurs IT** du monde
- 🏠 Pas vraiment un standard, mais plutôt des **directives** (guidances)
- 🏠 **Valeur** pour le consommateur et le fournisseur.
- 🏠 Condition d'utilisation **prédéfinie**

# ITIL : C'est quoi ?

Un **Service** est constitué d'une **combinaison de personnes**, de **processus**, de **produits** et **partenaires** et doit être défini dans un accord de niveau de service (SLA).

Un service est **indissociable** de son **utilisation**.

Exemple : messagerie, support aux utilisateurs, ordinateur ( un service a toujours un propriétaire : Matrice RACI

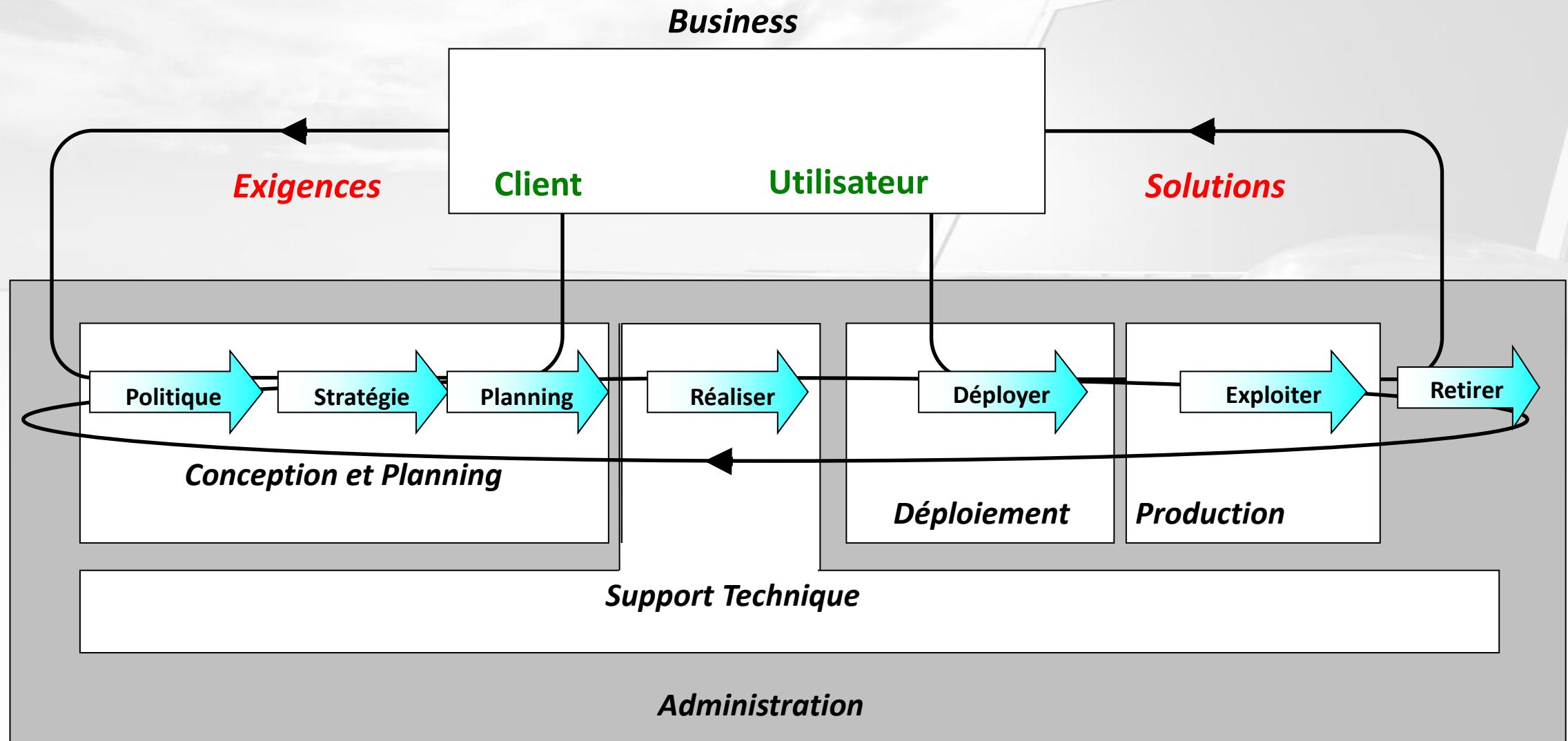
Un service est défini par:

- 🏠 Son utilité → Apport client : « Quoi » (Toujours adapté au besoin)
- 🏠 Sa garantie → Manière de fournir le service : « Comment » (Toujours adapté à l'utilisation)
- 🏠 Valeur du service → Niveau d'attente du client envers le service

# ITIL : Pour quoi faire ?

- 🏠 **Améliorer des services** informatiques
- 🏠 **Réduire** des coûts
- 🏠 **Améliorer de la satisfaction de la clientèle** grâce à une approche plus professionnelle de la prestation de services
- 🏠 **Accroître de la productivité**
- 🏠 **Développer l'utilisation des compétences** et de **l'expérience**

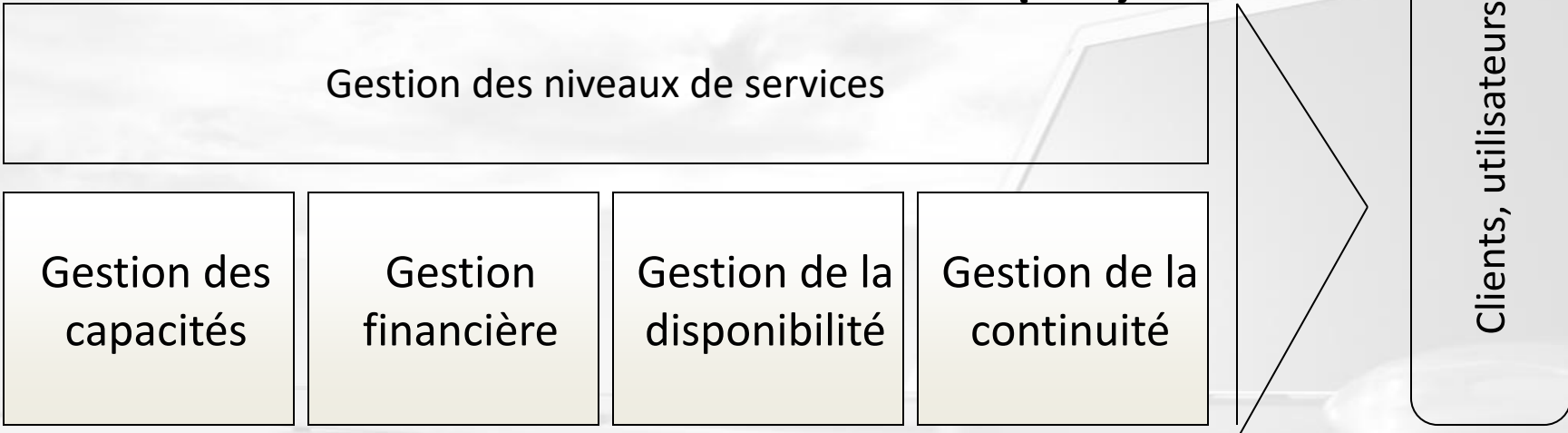
# ITIL : Le cycle de vie du service



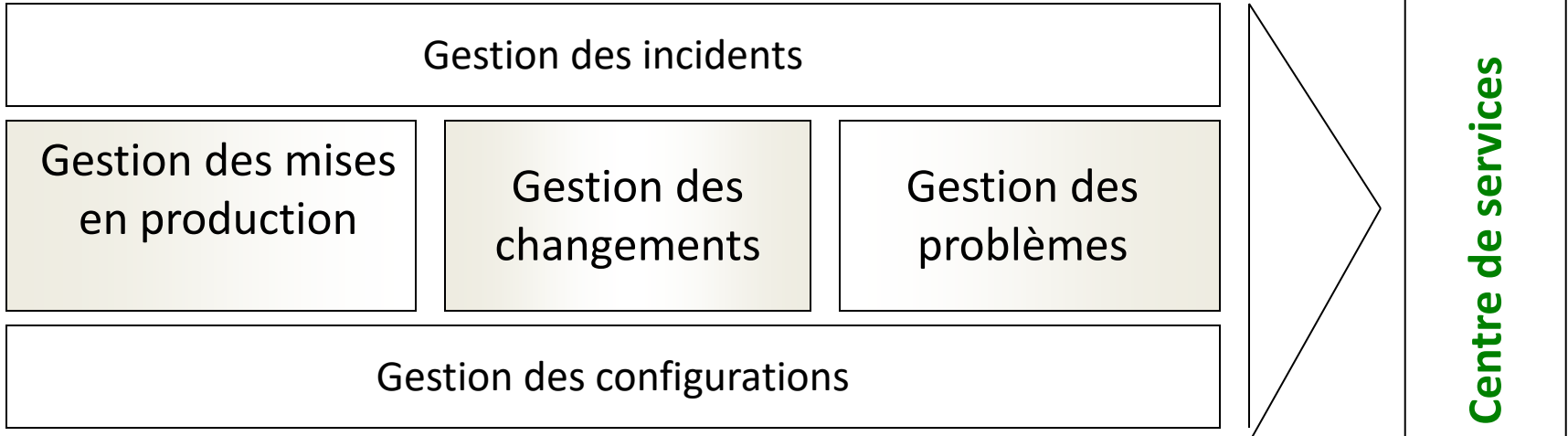
# ITIL : Comment gérer les services SI

## *Fourniture de services (BO)*

Les 10  
processus  
clés ITIL



## *Soutien des services (FO)*



# ITIL : 4 concepts principaux

1

- **Orientation client** : « client » = « utilisateur ». Le client et son métier doivent être au centre des préoccupations de la direction informatique.

2

- **Cycle de vie** : la gestion des services doit être prise en considération en amont des projets informatiques, dès la phase d'étude et de conception.

3

- **Processus** : la qualité de service se fonde sur une approche par les processus.

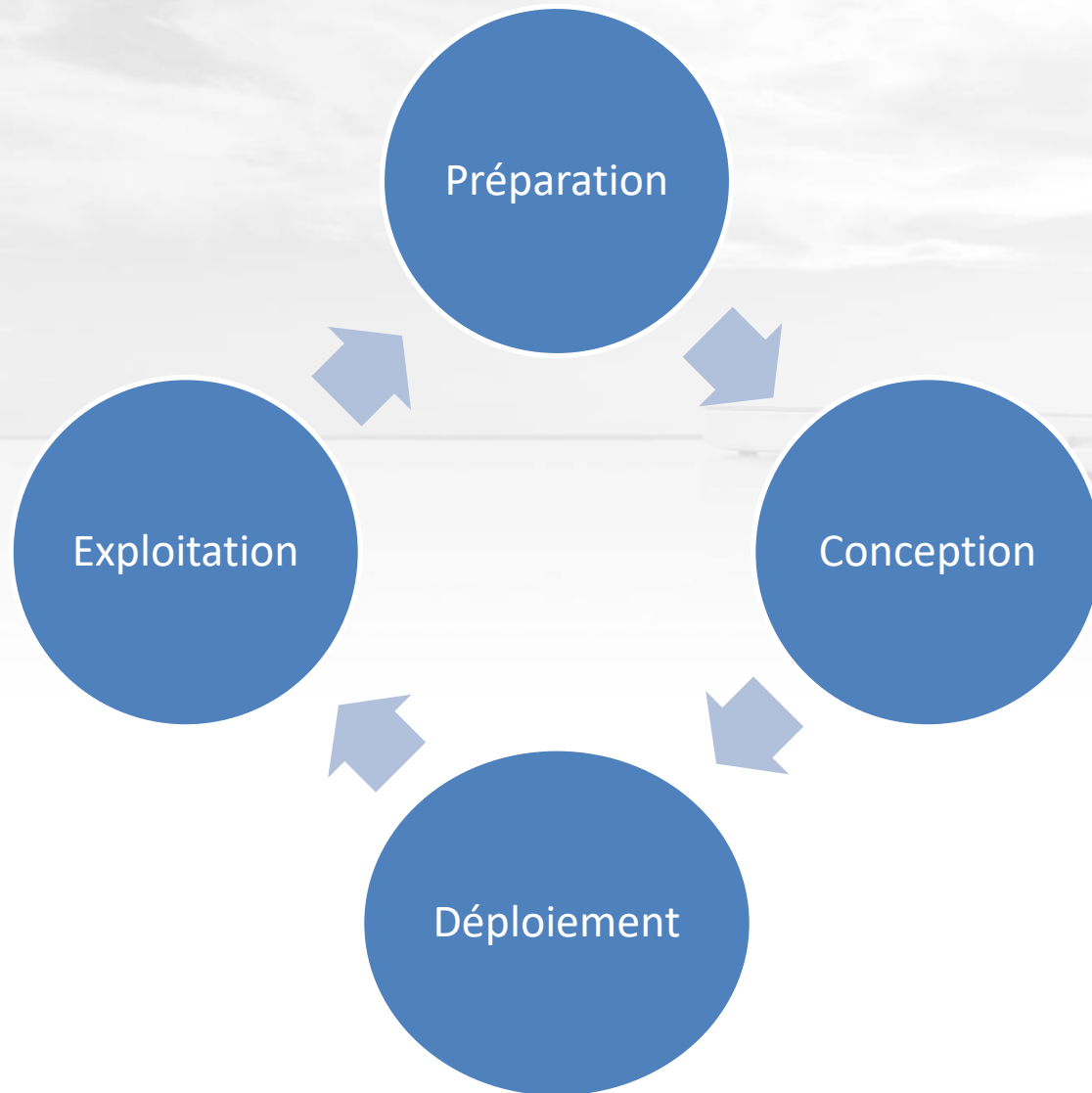
4

- **Amélioration continue** : La mesure de l'excellence. La capacité à répondre aux attentes des clients en matière de produits et services en relation avec la pratique de leur métier et ce à un coût justifiable

# ITIL – Orientation clients

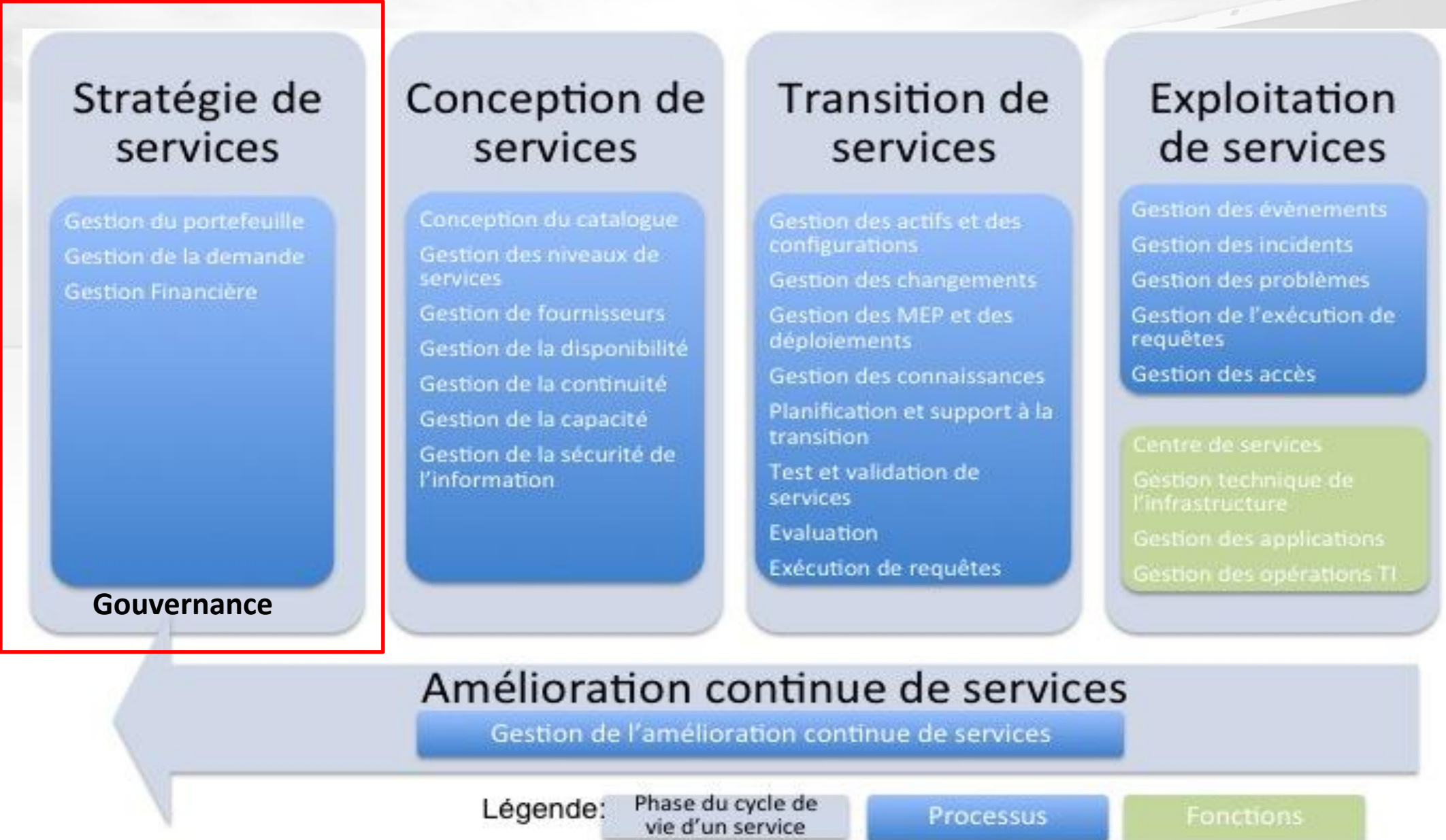
- **S'assurer** que les points de vue des clients sont pris en compte et justifiés par leur métier.
- **Mettre en place** une organisation de support et de conseil pour une meilleure utilisation des services informatiques.
- **Assurer** un suivi personnalisé des « plaintes » des clients.
- **Mesurer** la satisfaction des clients
- **Encourager** les "user groups" internes.
- **Fournir** un feedback au personnel informatique.
- **Être à l'écoute** de l'évolution des besoins des clients pour anticiper sur l'adaptation des services.

# ITIL – Cycle de vie

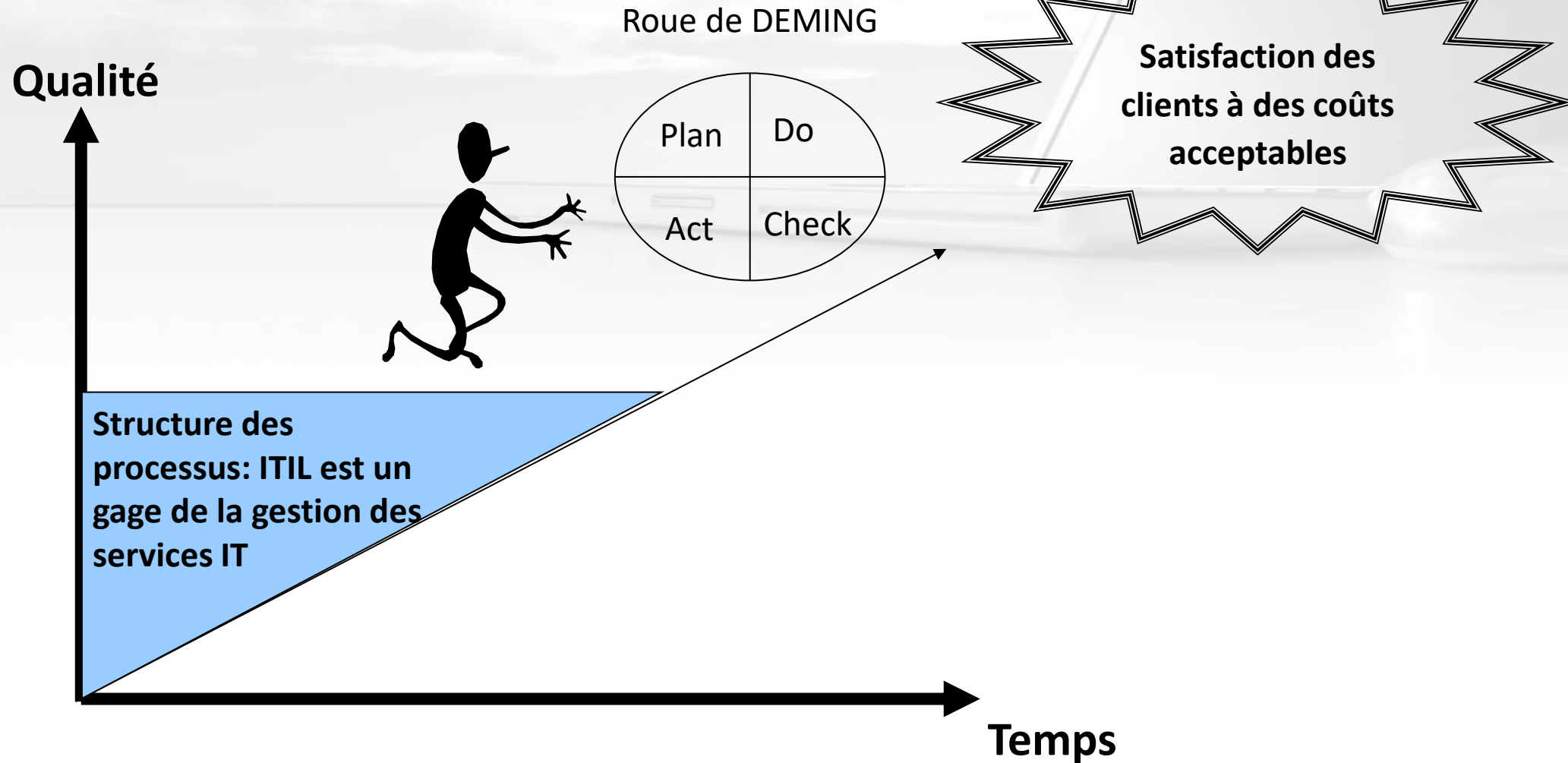


- Ne pas aborder la notion de service management (***gestion des services***) uniquement dans la phase d'exploitation
- Prendre en compte les besoins en termes de service dès la phase de préparation des projets
- Évaluer l'impact des nouveaux projets sur l'infrastructure existante
- Définir les conditions d'exploitabilité des nouveaux systèmes

# ITIL – Processus



# ITIL – Amélioration continue



# ITIL - Une évolution de la culture DSI

## Hier

- > Utilisateurs
- > Tourné vers l'intérieur
- > Centré sur les technologies
- > "Faire son possible"
- > Spécifique, interne
- > Réactif
- > Cloisonnement des compétences
- > Exploitation des "machines"

## Aujourd'hui

- > Clients
- > Tourné vers l'extérieur
- > Centré sur les processus
- > Contrats, résultats
- > Standard, externalisation
- > Proactif
- > Support de "bout en bout"
- > Gestion des services

# ITIL – Les apports

- **Facilite le dialogue** grâce à un langage commun : Compréhension des demandes clients et de notre capacité à répondre efficacement
- **Efforts fournis vers le client**, plutôt que vers la technologie
- **Amélioration** du ratio coût / service rendu : Meilleure efficacité et réduction des activités répétitives

→ En résumé, complémentaire à COBIT :

- COBIT, pratique pour le top management et quelles approches mettre en place pour la gestion de l'IT dans l'organisation
- ITIL, une roadmap sur ce qu'il faudrait faire exactement pour gérer le travail des collaborateurs IT

# COBIT vs ITIL

<i>Problèmes généraux</i>	<i>L'aide de COBIT</i>
1. L'organisation informatique est inefficace, ne remplit pas les objectifs de l'entreprise et semble obsolète.	1. La possibilité pour les chefs d'entreprise de hiérarchiser leurs besoins informatiques et d'élaborer les plans correspondants
2. L'entreprise échoue fréquemment aux audits effectués par des partenaires potentiels.	2. Un système clair de points de repère
3. Les partenaires à long terme ont tendance à ne plus utiliser les services de la société et préfèrent travailler avec leurs rivaux.	3. Stabilité et nouveau logiciel.
<i>Problèmes informatiques spécifiques</i>	<i>L'aide d'ITIL</i>
1. Les équipes informatiques sont constamment surchargées	1. Des processus ITIL spécifiques pour organiser et normaliser le travail des services informatiques.
2. Il est impossible de surveiller les performances du personnel informatique.	2. Un système de responsabilité.
3. Des pannes similaires continuent de se produire	3. Différencier les problèmes .
4. Les changements dans l'infrastructure informatique de l'entreprise sont chaotiques.	4. Gestion du changement et CMDB.

# Bibliographie

- « Gouvernance de l'information pour l'entreprise numérique », G. Balantzian, Hermès, 2013
- « Les tableaux de bord de la DSI, Pilotage, performance et benchmarking du système d'information », Christophe Legrenzi, Philippe Rosé, Dunod, 2012
- « Master SI », collectif, Eska, 2011
- « La transformation stratégique du SI », B. Le Roux, Hermès, 2009
- « IT gouvernance », F. Georgel, Dunod, 2009
- « Le plan de gouvernance du SI », G. Balantzian, Dunod, 2006
- « Urbanisme des SI et gouvernance », Club Urba, Dunod, 2010
- « Place de la gouvernance du SI dans la gouvernance générale de l'entreprise », AFAI\_CIGREF, 2005
- « Gouvernance du SI », CIGREF, 2002
- « La modélisation des systèmes complexes », J. L. Le Moigne, Dunod, 1990
- « Systémique et cognition » E. Andreewsky, Dunod, 1991

# Synthèse du cours (1)

MSSI de l'entreprise approche par « les référentiels institutionnels »

## **1/ COBIT : Répertoire de bonnes pratiques qui couvrent le cycle complet informatique, processus opérationnels, de management & de gouvernance**

Langage commun pour opérationnels, management, organes de gouvernance, auditeurs internes, auditeurs externes, ...

4 domaines : Planification et organisation (11 processus), Acquisition et mise en place (6 processus), distribution et supports (13 Processus) et Surveillance (4 processus)

## **2/ VAL IT est un cadre de référence pour la gouvernance des investissements informatiques.**

- Val IT complète COBIT et traite des investissements à forte composante IT pour des projets business & Gestion d'un "Portefeuille" de projets et de programmes,
- VAL IT est composé de 3 domaines : Gouvernance de la valeur, la gestion de portefeuille & la gestion de l'investissement

## **3/ RISK IT un cadre de référence pour la gestion des risques (identification, traitement et gestion)**

- Risk IT complète COBIT pour toute la gestion des risques. Risk IT explicite les risques SI et va permettre aux acteurs de s'assurer que de la prise en compte des risques IT, la démarche qui permet de prendre des décisions, la démarche qui permet de comprendre comment répondre aux risques identifiés
- 3 domaines : Gouvernance des risques, Evaluation des risques & Réponses aux risques
- 3 types de risques identifiés : Fourniture de services informatiques & Fourniture de solutions informatiques & Réalisation de bénéfices
- Risk IT peut s'appuyer sur C.O.S.O. qui structure l'analyse du contrôle interne selon cinq composantes : l'environnement de contrôle (5 principes), l'évaluation des risques (4 principes), les activités de contrôle (3 principes), l'information & la communication (3 principes) et le pilotage du contrôle interne (2 principes).

# Synthèse du cours (2)

## 4/ ITIL est un code de bonnes pratiques pour la fourniture de services informatiques.

- Facilite le dialogue grâce à un langage commun & efforts fournis vers le client, plutôt que vers la technologie & Amélioration du ratio coût / service rendu
- Un Service est constitué d'une combinaison de personnes, de processus et produits et partenaires et doit être défini dans un accord de niveau de service (SLA, Service Level Agreement).
- Objectifs principaux : Amélioration des services informatiques, réduction des coûts, amélioration de la satisfaction de la clientèle grâce à une approche plus professionnelle de la prestation de services, amélioration de la productivité, amélioration de l'utilisation des compétences et de l'expérience & amélioration de la prestation des services de tiers.
- 4 concepts principaux : Orientation client, Cycle de vie, Processus , Amélioration continue
- COBIT → pratique pour le top management et définition des approches à mettre en place pour la gestion de l'IT dans l'organisation
- ITIL → roadmap sur ce qu'il faudrait faire exactement pour gérer le travail des collaborateurs IT

## 5/ SDSI : C'est un plan stratégique prospectif qui permet d'anticiper et de prévoir les évolutions du SI.

- Il est destiné à piloter le développement de SI et à donner les axes stratégiques du futur technologique de l'organisation.
- Le Schéma Directeur SI= 1ère étape de la formalisation d'un SI : choix de stratégies & planification des objectifs relatifs à des scénarios de développement.
- Le SDSI donne : une vue globale de l'état actuel du système, une spécification des besoins & la définition des orientations;