Normes et Standards pour les systèmes d'information

UNIVERSITÉ PARIS DESCARTES

Plan

- Règlements, normes et standards: définition
- Notion de Processus
- Vue d'ensemble des principaux dispositifs
- Zoom sur quelques normes et standards
  - Qualité - ISO 9001
  - Sécurité - ISO 27001
  - Amélioration des processus - CMMI
  - Certification des personnes en informatique ITIL / ISO 20000
  - Gouvernance - COBIT
  - Management de projet -Prince 2 / PMBOK
  - Infogérance- eSCM
- Conclusion

Introduction

Règlements, normes et standards

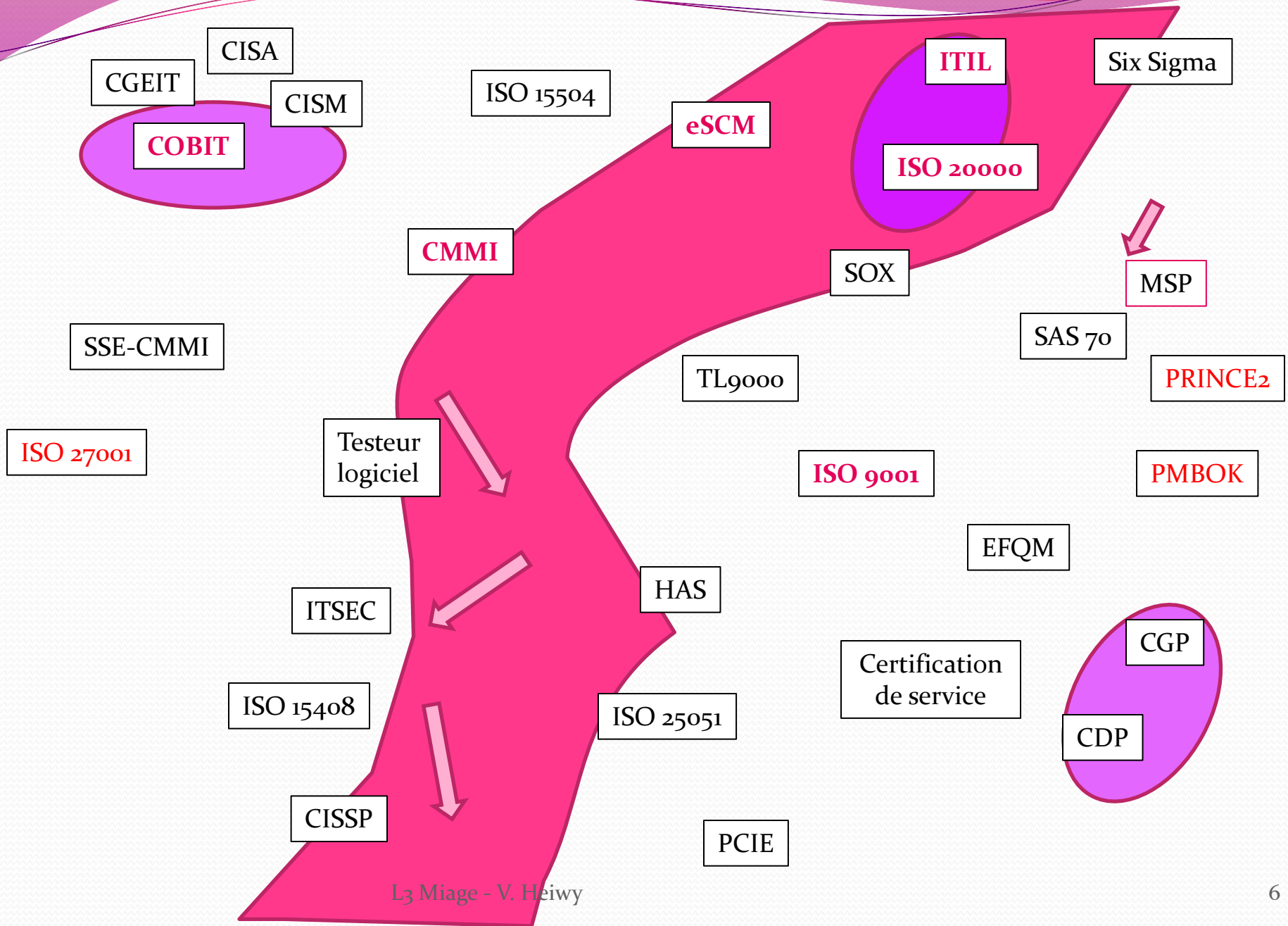
Processus

Règlements, Normes et standards

- Un **règlement** est une exigence légale à laquelle toute entreprise est tenue.
- Les **normes**, deviennent des exigences lorsqu'elles sont citées dans un marché public.
- Elles sont produites par des organismes de normalisation:
  - **Internationaux**, comme l'organisation International de normalisation (**ISO**) et le Comité électronique international (**CEI**)
  - **Régionaux**, comme le Comité européen de normalisation (**CEN**)
  - **Nationaux**, comme **Afnor** en France et les bureaux de normalisation, comme le Bureau de normalisation de l'aéronautique et de l'espace (BNAE)
- Les **standards** sont des documents rédigés par des entreprises ou des groupements d'entreprise afin de répondre rapidement à un problème souvent sectoriel. Ils sont souvent considérés comme des « **normes de fait** ».

Processus

- Terme parmi les plus utilisés en entreprise.
- Présent dans la majorité des référentiels:
  - Dans **ISO 9000**, « *ensemble d'activités corrélées ou interactives qui transforme des éléments d'entrée en éléments de sortie* ».
  - Dans **CMMI**, « *les descriptions fournies ne sont pas des processus, chaque entreprise doit adapter à son contexte les « domaines de processus » pour élaborer ses processus* ».
  - Dans **PMBOK**, « *une série d'actions qui produit un résultat* ».
  - Dans **PRINCE2**, « *ce qui doit être réalisé pour parvenir à un résultat particulier, en termes d'informations à réunir, de décisions à prendre et de résultats à produire*».
  - Dans **ITIL**, « *série organisée d'actions, d'activités, de changement exécutés par des acteurs avec l'intention de satisfaire et d'atteindre un objectif* ».


CISA
CGEIT
CISM
COBIT
ISO 15504
eSCM
ITIL
Six Sigma
ISO 20000
CMMI
SOX
MSP
SSE-CMMI
SAS 70
TL9000
PRINCE2
ISO 27001
Testeur logiciel
ISO 9001
PMBOK
EFQM
HAS
ITSEC
CGP
Certification de service
ISO 15408
ISO 25051
CDP
CISSP
PCIE

Les principales Normes et Standard

Acronyme	Nom	Origine	Type
AFITEP-CDP	Certification en direction de projet	France	Projet
AFITEP-CGP	Certification en gestion de projet	France	Projet
Certification de services		France	Qualité de service
CISSP	Certified Information Systems Security Professional	USA	Sécurité des SI
CMMI	Capability Maturity Model Integration	USA	Ingénierie système, acquisition, service
COBIT		USA	audit, securité, gouvernance ces SI
EFQM	European Foundation for Quality Management	Europe	Excellence
eSCM	eSourcing Capability Model	USA	Service
HAS	Haute Autorité de Santé	France	Qualité et sécurité des systèmes de santé
ISO 15408	ou Critère commun	Europe	Developpement et sécurité des systèmes informatisés
ISO 15504		Europe	Tout type de processus
ISO 20000		Europe	Production Informatique
ISO 25051		Europe	Qualité du produit logiciel
ISO 27001		Europe	Sécurité des SI
ISO 9001		Europe	Qualité
ITIL	Information Technology Infrastucture Library	Royaume Uni	Production informatique
ITSEC	Information Technology Security Evaluation Criteria	Europe	Sécurité des SI
MSP	Managing Successful Programmes	Royaume Uni	Projet
PCIE	Passeport de compétences informatique européen	Europe	Poste de travail informatique
PMBOK	Project Management Body of Knowledge	USA	Projet
PRINCE2	Projects IN Controlled Environments	Royaume Uni	Projet
SAS 70	Statement on Auditing Standards N° 70	USA	Audit
Six Sigma		USA	Tout type de processus
SOX	Sarbanes-Oxley	USA	Finance
SSE-CMM	Systems-Security Engineering Capability Maturity Model	USA	Sécurité des SI
Testeur logiciel		Europe	Tests du locigiel

Les principales Normes et Standards abordés ici

- ISO 9001 - *Qualité*
- ISO 27001 – *Sécurité des SI*
- CMMI – Amélioration des Processus
- ITIL/ ISO 20000 (voir exposés 2010) – Certification des personnes
- *COBIT* (voir exposés 2010) - Gouvernance
- eSCM (voir exposés 2010) - Services

La qualité

ISO 9000, ISO 9001 et ISO 9004

ISO9000

- L'**ISO9000** décrit les principes essentiels des systèmes de **management de la qualité** et définit la terminologie.
- L'**ISO 9001** spécifie les exigences relatives aux systèmes de management de la qualité lorsqu'un organisme doit démontrer son aptitude à fournir des produits satisfaisant aux exigences des clients, à la réglementation applicable et qu'il vise à accroitre la satisfaction de ses clients

Famille des normes ISO9000

ISO 9001

- **ISO 9001** permet à une entreprise d'obtenir une **certification** pour son système de **management de la qualité**
- C'est le référentiel de certification **le plus connu**.
- Sa 4eme et **dernière version** date du 15 novembre **2008**
- Elle insiste sur l'importance de prendre en considération le **produit** ou **service** en plus du système de management de la **qualité.**
- Elle liste des **exigences** sur l'identification et la maitrise des **processus** dans la perspective **d'amélioration continue.** La présentation d'une **cartographie des processus** est **recommandée.**

ISO 9001

- **ISO 9000** se rapporte à la partie « principes »
- **ISO 9001** est le référentiel des exigences servant de support à la certification.
- **ISO 9004** énonce des recommandations de mise en œuvre et d'auto-évaluation

ISO 9001

- Exigences sur:
  - Le **produit** doit être **vérifié** et **validé.** Il est soumis à **des exigences** de **conformité** et de **traçabilité**
  - Les **personnes**, à propos de
    - l'attribution des **responsabilités**
    - des **compétences**
    - de la **formation**
  - Les **processus** et les **résultats de l'exécution** de ces processus

ISO 9001

- La démarche d'amélioration nécessite la mise en place:
  - d'indicateurs de management des processus
  - de mesures des caractéristiques du produit afin de vérifier que les exigences relatives au produit sont satisfaisantes, et
  - de mesures de la satisfaction du client
- Aucune directive précise donnée sur le choix de ces indicateurs qui dépendent des objectifs de l'entreprise.
- Le mot « sécurité » ne figure pas dans cette norme.

ISO 9001

- Documentation
  - La norme ISO 9001: 2008 est disponible en France après d'Afnor.
  - Sa compréhension nécessite la lecture préliminaire de la Norme ISO 9000:2005 (principe et vocabulaire)

ISO 9001

- Mise en œuvre
  - L'ISO 9001 est **applicable à toute activité**, quel que soit le type de produit ou service
  - ISO 9001 est mondialement reconnue
  - La **certification doit être renouvelée tous les 3 ans** et fait l'objet d'un **audit de suivi annuel** par l'organisme de certification
  - Le **délai de mise en œuvre** incompressible reste estimé à **18 mois** et elle doit s 'appuyer sur une volonté forte de la direction. « **responsable qualité** »
  - La désignation d'un rattaché à la direction est indispensable ainsi que la mise en place d'une fonction d'audit interne

ISO9001

- Conclusion
  - (+) Son atout essentiel est le caractère universel de la certification ISO9001
  - (-) ISO 9001, est très générale et doit être souvent complétée par des guides ou des exigences spécifiques au domaine d'application.
  - Dans le domaine du traitement de l'information, le référentiel plus spécialisé **ISO 20000** bénéficie de la culture d'amélioration permanente et de l'approche « processus » diffusée par l'ISO9001

La sécurité

ISO 27001 (pour les exigences)

ISO 17799 (pour les recommandations)

SSE-CMM (ISO 21827) indications sur les moyens d'améliorer les pratiques en matière de sécurité des systèmes d'information.

ISO 27001

- ISO 27001 permet à une entreprise d'obtenir une certification pour son système de management de la **sécurité des systèmes d'information**.
- ISO 27001 et ISO 27002 constituent un couple complémentaire en matière de sécurité .
- ISO 27001 spécifie **les processus** qui permettent à une entreprise de construire, de gérer et d'entretenir un système de gestion de sécurité de l'information.
- ISO 27001 intègre l'approche du processus et le cycle **PDCA** (Plan-Do-Check-Act) **d'amélioration continue** (ou de réduction continue des risques).

Amélioration continue- PDCA: Roue de Deming

ISO 27001

- **Plan** : organiser la mise en place du système de gestion de sécurité de l'information
- **Do**: mettre en place et faire fonctionner le système
- **Check**: contrôler l'efficacité du système par des audits internes et des évaluations de risque
- **Act**: améliorer le système par des actions correctives et préventives appropriées, l'entretenir par des actions de communication et de formation.

ISO 27001

- En pratique, il convient de mettre en place des procédures pour:
  - **Détecter** rapidement **les erreurs** de traitement;
  - **Identifier** immédiatement toute **non-conformité** aux règles de sécurité et organiser la remontée immédiate des incidents;
  - **Vérifier** que toutes les tâches relatives à la sécurité sont réellement exécutées que ce soit par des hommes ou des automates;
  - Identifier les **actions à réaliser** pour corriger les non-conformités aux règles de sécurité

L’amélioration continue des processus

CMMI

CMMI

- Le **CMMI** (Capability Maturity Model Integration) concerne tous les **processus** liés aux affaires et aux projets, de l'acquisition au service rendu en passant par le développement et la présentation de la production en série.
- Il s'intéresse à la **qualité des processus de management et d'ingénierie d'une entreprise**, et donc globalement à sa maturité.
- Le CMMI est organisé sous forme de constellations, un ensemble de composants CMMI regroupant un modèle, sa formation et sa méthode d'évaluation.
- Il existe trois **constellations** (ou recueils de bonnes pratiques)
- La **particularité** des constellations est de proposer **un noyau commun.**
- **16 « domaines de processus » sont communs** à toutes les constellations.

CMMI : un référentiel qui évolue

- 1986 CMM, la 1ere version du référentiel
- 2002 La version CMMI (« I » pour Integrated)
- 2006 Les constellations CMMI

CMMI: structuration et organisation du modèle

- Le modèle CMMI s'articule autour de **six concepts** centraux
  1. Les **domaines de processus;**
  2. La **représentation** du modèle, **étagée** ou **continue;**
  3. Les **objectifs génériques**, qui s'appliquent à tous les processus pour un niveau donné;
  4. Les **objectifs spécifiques** à un domaine de processus;
  5. Les **pratiques génériques** liées à un objectif générique;
  6. Les **pratiques spécifiques** liées à un objectif spécifique.

CMMI: les domaines de processus *(process area);*

- Un **domaine de processus** (process area) regroupe un ensemble de « bonnes pratiques pour réussir » qui, mises en œuvre collectivement répondent à l'ensemble des objectifs à satisfaire pour apporter des améliorations dans un type donné d'activités.

	Gestion de processus	Gestion de projet	Ingénierie	Support
N2		* Planification de projet * surveillance et contrôle de projets * gestion des accords avec les fournisseurs	* Gestion des exigences	* Gestion de configuration * Assurance-qualité processus et produit * Mesure et analyse
N3	* Focalisation sur le processus organisationnel * Définition de processus organisationnel *Formation organisationnelle	* Gestion de projet intégrée * Gestion des risques	* Solution technique * Intégration de produit *Developpement des exigences * Vérification * Validation	* Analyse et prise de décision
N4	* Performance du processus organisationnel	* Gestion de projet quantitative		
N5	* Innovation et déploiement organisationnel			* Analyse causale et Résolution

Catégories de domaines et niveaux de maturité

Deux approches coexistent pour la représentation du modèle

CMMI

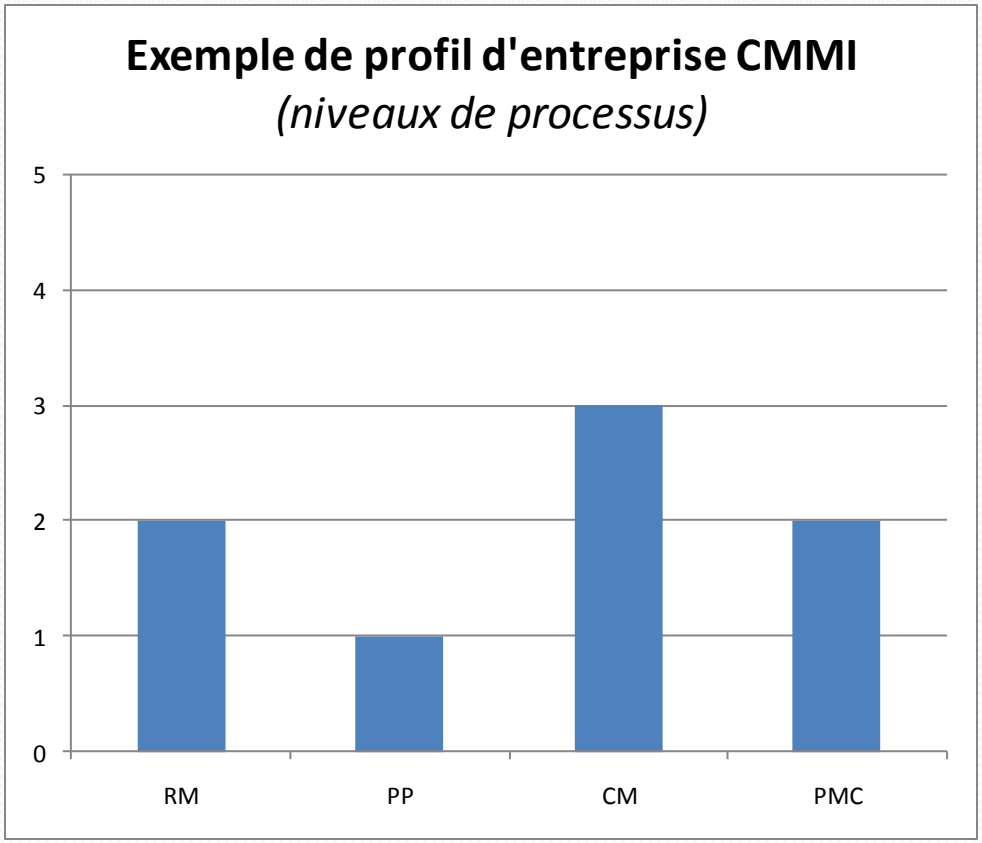
Première approche

- On retrouve un **modèle étagé** (staged representation):
  - Pour le niveau 1 **Initial**:
    - Organisation artisanale
    - Peu de processus existent
    - Les succès dépendent des efforts de chacun
    - L'efficacité repose sur les compétences et la motivation des individus
    - C'est le mode héroïque, le succès n'est pas reproductible
  - Pour le niveau 2 **Discipliné**:
    - Gestion des exigences
    - Planification de projet
    - Surveillance et contrôle de projet
    - Mesure et analyse
    - Assurance qualité processus et produit
    - Gestion de configuration
  - Pour le niveau 3 **Ajusté**:
    - Focalisation sur le processus organisationnel
    - Définition du processus organisationnel
    - Formation organisationnelle
    - Gestion de projet intégrée
    - Gestion des risques
    - Analyse et prise de décision
  - Pour le niveau 4 **Géré quantitativement**:
    - Performance du processus organisationnel
    - Gestion de projet quantitative
  - Pour le niveau 5 **En Optimisation**:
    - Innovation et déploiement organisationnels
    - Analyse causale et résolution de problèmes

CMMI

Deuxième approche

- La **représentation en continue** (**continuous representation**)
- Il permet à l'organisation de choisir un ou plusieurs domaines de processus prédéfinis pour déterminer la voie d'amélioration des pratiques qui lui sont liées.
- Cette représentation utilise des **niveaux d'aptitude** pour caractériser les progrès réalisés et déterminer son « profil d'entreprise»

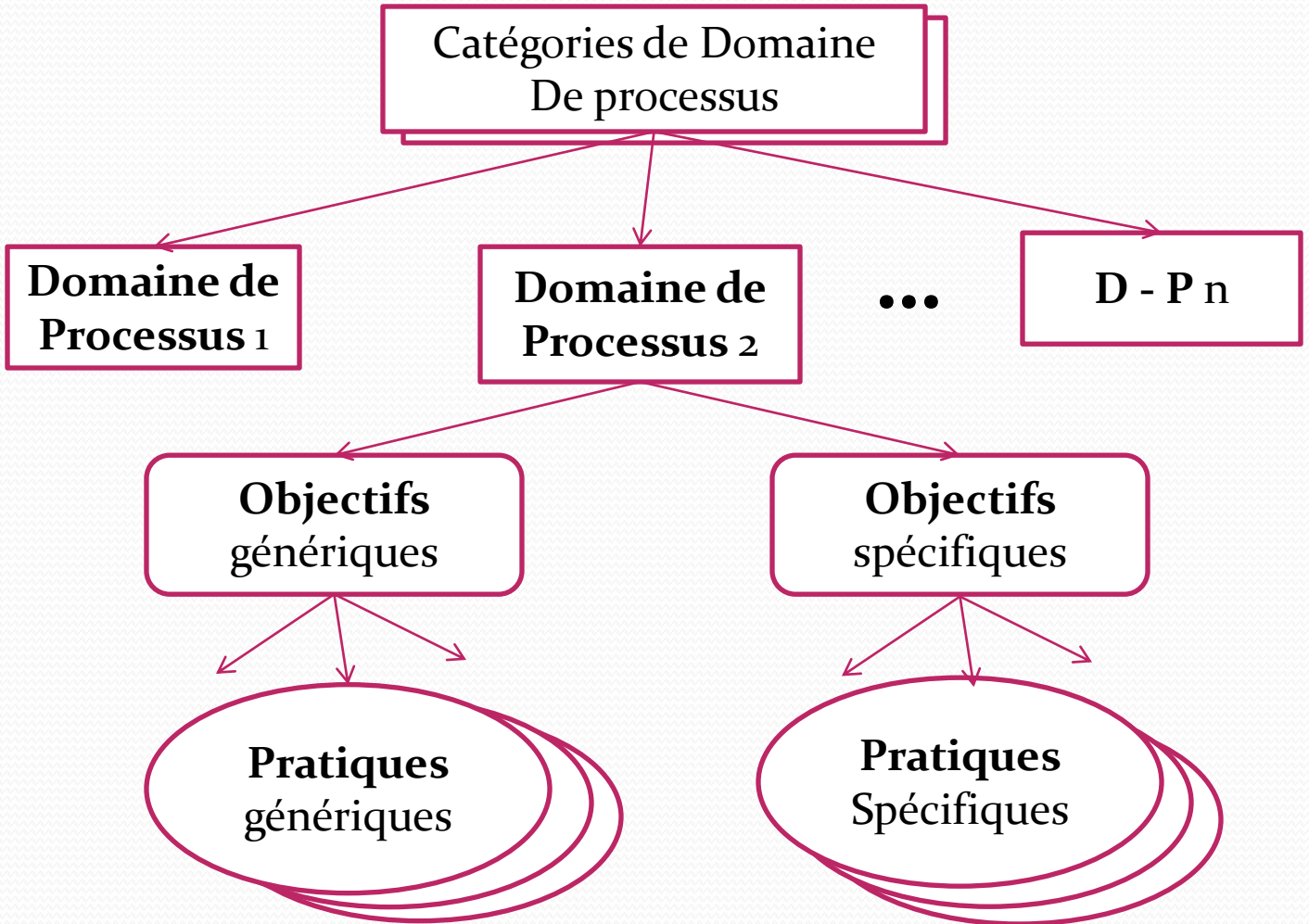


- Un niveau d'aptitude se compose de l'objectif générique et des pratiques qui sont liées.
- Ces **six niveaux d'aptitude** sont définis ainsi:
  - 0. incomplet
  - 1. basique
  - 2. discipliné
  - 3. ajusté
  - 4. géré quantitativement
  - 5. en optimisation

***RM** : Requirements management, **PP**: Project planning, **CM** : configuration management; **PMC**: Project monitoring and control*

CMMI: les objectifs génériques ou spécifiques à un niveau de maturité

- Chaque **domaine de processus** doit satisfaire des **objectifs** qui lui sont **spécifiques** (SG: Specific goal), et d'autres **génériques** (GG: Generic Goal)



CMMI: les pratiques génériques ou spécifiques à un niveau de maturité

- Seuls les objectifs sont exigés, la démarche de déploiement du référentiel dans l'organisation doit mettre en œuvre le juste nécessaire pour atteindre impérativement chaque objectif.
- Il peut appliquer des **pratiques** de terrain recommandées, dites « **spécifiques** » (SP: Specific practice), ou **génériques** (GP: Generic Practice)
- Les pratiques génériques sont applicables de façon identique à chacun des processus attachés à un niveau.
- Il y en a dix pour le niveau 2, liées à l'objectif générique « institutionnaliser le processus en tant que processus discipliné.
- Il faut ajouter deux pratiques génériques pour chacun des niveaux 3, 4 et 5.

CMMI

- **<u>Trois recueils de bonnes pratiques</u>** pour l'amélioration continue de processus
  - **CMMI-DEV** pour les processus de développement et de maintenance des produits
  - **CMMI-SVC** pour les processus de service
  - **CMMI-ACQ** pour les processus d'acquisition
- Permet à une entreprise **d'obtenir un diagnostic d'aptitude ou de maturité de ses processus**

Evaluation du CMMI

- L'évaluation CMMI est effectuée par des equipes formées à la méthode d'évaluation SCAMPI *(Standard Appraisal Method for Process Improvement)*du SEI, et conduite par un évaluateur (Lead Appraiser) formé et autorisé par SEI
- Le résultat de l'évaluation est une **cotation**, déterminant un **profil de niveau d'aptitude** ou de maturité selon la représentation adoptée par l'organisation

Certification de personne physique en informatique

ITIL

ISO 20000

ITIL

- Le dispositif ITIL permet à une **personne physique** d'obtenir une certification en matière de **production informatique.**
- L'ITIL (*Information Technology Infrastructure Library*) est **un référentiel de bonnes pratiques pour la fourniture de services informatiques**; ce référentiel aide les entreprises à atteindre leurs objectifs de **qualité** et de **maitrise des coûts**
- Il existe 2 versions de ITIL, la V2 et la V3.

ITIL v2: une approche par processus

- ITIL V2, toujours d'actualité malgré la v3, repose sur 8 modules:
  - ITIL – The Business Perspective, présente les avantages pour l'entreprise d'une gestion des services afin de mieux comprendre l'ITIL,
  - **ITIL – Service Delivery**, couvre les processus nécessaires à la conception et à la fourniture de services,
  - **ITIL – Service Support**, couvre la fonction *Service-Desk* et les processus nécessaires à la maintenance et au support des services,

Certification

  - ITIL – Security Management, couvre les aspect de mise en œuvre et de gestion de la sécurité des systèmes d'information
  - ITIL – ICT Infrastructure Management, couvre les processus de conception et de gestion des infrasctructures informatiques
  - ITIL – Application Management, couvre les interactions de la gestion des applications avec la gestion des services
  - ITIL – Software Asset Management, couvre la gestion des objets logiciels sur l'ensemble de leur cycle de vie
  - ITIL – Planning to implement service Management, couvre le plan de mise en œuvre de la gestion des services et les conseils à suivre

ITIL v2: une approche par processus

- Chaque **module** décrit un **domaine** constitué de plusieurs **processus**.
- Chaque **Processus** établit des **règles de bonnes pratiques** en matière de service délivré et s'assure du bon fonctionnement grâce à la **certification des individus**.
- La **certification** porte sur deux modules « Soutien des services » et « fourniture des services »
- **ITIL décrit le service à rendre** et non pas la façon de s'y prendre.
- **Documentation** en anglais ou en Français. La version anglaise est disponible sous forme de **CD-ROM**. Il existe aussi un *Guide de poche sur la gestion des services des TI*

ITIL v2: une formation structurée en trois niveaux

- Les examens sont structurés en trois niveaux
  - Fondamentaux-ITIL / **ITIL Professionals for ITIL** Foundation
  - Practicien-ITIL / **ITIL Practitioner**
  - Managérial-ITIL / **ITIL Service Manager**

ITIL v3: une approche fondée sur le cycle de vie du service rendu

- ITIL v3 repose sur la notion de cycle de vie du service, chaque étape faisant l'objet d'une publication:

Certification sur les 5 domaines

- **ITIL – SS** (Service Strategy) fournit des conseils sur les modèles d'organisation definissant les relations entre entreprise et fournisseur de service.
- **ITIL-SD** (Service Design) fournit des conseils sur la conception et la maintenance des services
- **ITIL – ST** (Service Transition) fournit des conseils sur la gestion des changements le maitrise des risques et les mises en production. Elle cherche à améliorer l'aptitude aux changements.
- **ITIL-SO** (Service Operation) fournit des conseils d'afficacité et d'efficience dans l'exploitation et le support des services.
- **ITIL-CSI** (Continual Service Improvement) traite du suivi de l'amélioration du service sur toutes les etapes du cycle de vie. Il fournit des conseils pour maintenir et créer de la valeur au client.

ITIL v3: une approche fondée sur le cycle de vie du service rendu

- ITIL v3 insiste sur le fait que les composants du systèmes sont en contact les uns avec les autres à la façon d'un mikado. Dès que l'un d'eux est modifié, il y a implicitement répercussion de la modification sur les autres composants.
- *La V3 est plus complexe car vue à travers les étapes du cycle de vie du service rendu. Cela explique peut être la difficulté de certains utilisateurs à adopter la V3.*
- ***La documentation** en anglais peut être acquise sur un site dédié à ITIL géré par l'OGC, celle en français à partir de celui de l'itSMF France. En anglais, l' «Official ITIL Website » propose, en plus des **5 publications centrales** des titres dérivés intitulés « Key element Guide » fournissant des **modèles**, des **études de cas** et des **aides**, ainsi qu'une **introduction à ITIL v3** sous forme de guide de poche.*

ITIL: mise en œuvre

- L'ITIL connait un succès croissant.
- En France il devient incontournable
- C'est un « **standard de fait** » dans plus de 50 pays
- La documentation existe en 10 langues
- ITIL est devenu une norme internationale : **l'ISO 20000**

ISO 20000

Découle de ITIL

- **ISO20000** permet à une **entreprise** d'obtenir une certification de son système de management de la qualité de service, en matière de **production informatique.**

Les détails vous seront présentés lors d'un exposé

Découle de ITIL

ISO20000 se présente en 2 parties:

- Partie 1 – Spécifications (ISO-20000-1), norme d'exigences.
  - S'appuie sur **l'approche processus** et la **boucle d'amélioration continue** ou PDCA
    - Processus de fourniture de services
    - Processus de gestion des relations
    - Processus de résolution
    - Processus de contrôle
    - Processus de mise en production
- Partie 2 – Code de bonnes pratiques (ISO- 20000-2), norme de recommandations.

ISO 20000

Découle de ITIL

- **Processus de fourniture de services**
  - Gestion des niveaux de service,
  - Reporting
  - Gestion de la continuité de service et gestion de la disponibilité
  - Budgétisation et comptabilisation des services informatiques
  - Gestion de la capacité
  - Gestion de la sécurité de l'information

Retour

ISO 20000

Découle de ITIL

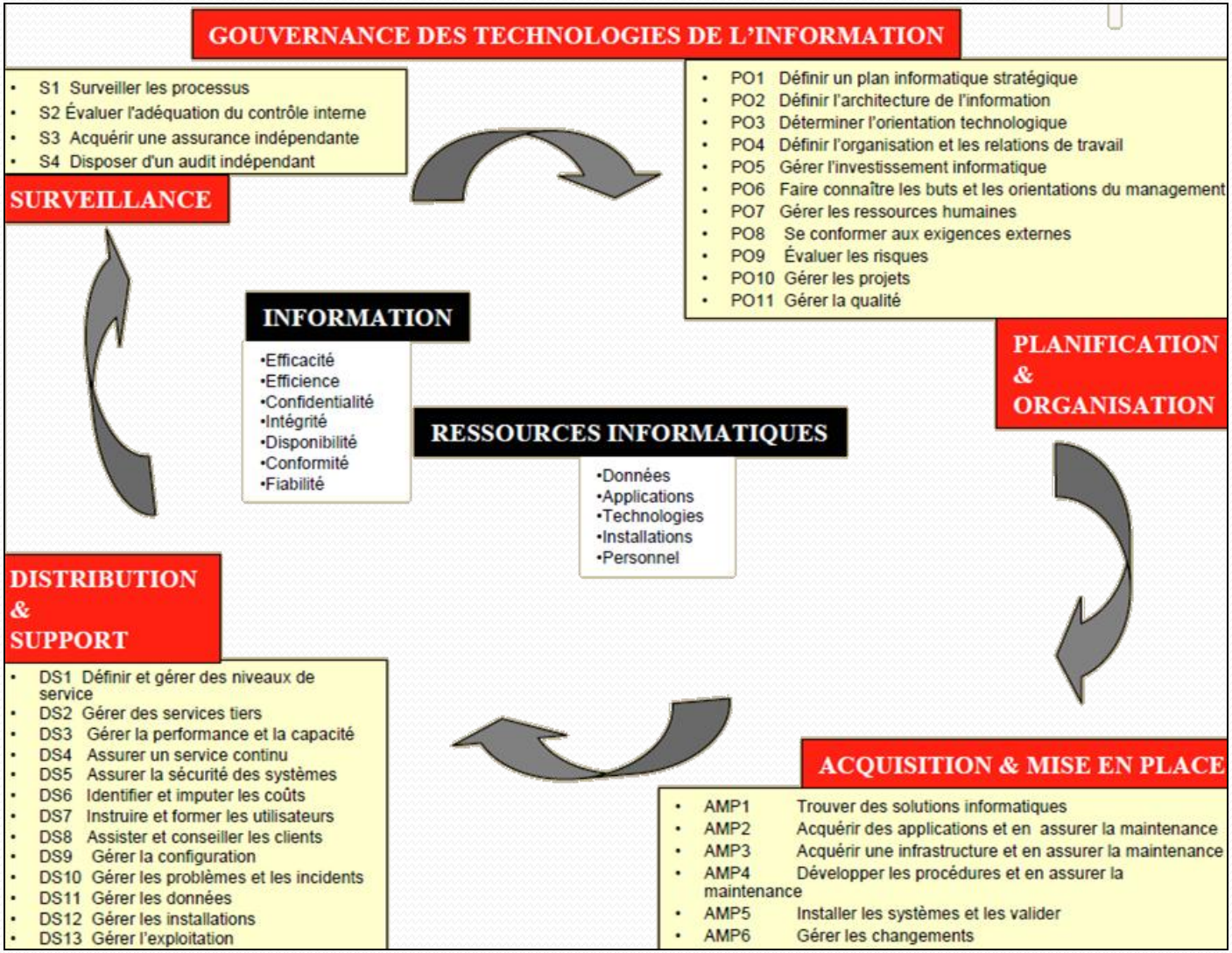
- **Processus de gestion des relations**
  - Gestion de la relation commerciale
  - Gestion des fournisseurs
- **Processus de résolution**
  - Gestion des incidents ou comment s'attaquer aux conséquences des dysfonctionnements,
  - Gestion des problèmes ou comment s'attaquer à leurs causes.
- **Processus de contrôle**
  - Gestion de configuration
  - Gestion des changements
- **Processus de mise en production**

Gouvernance des SI

CobiT

CobiT

Référentiel intégrant ISO 27000 ,CMMI et ITIL



CobiT

- Le **référentiel CobiT** sert de cadre pour la certification d'une personne physique en matière d'audit, de sécurité ou de gouvernance des systèmes d'information.
- L'ISACA (Information Systems Audit and Control Association) a développé le CobiT (**Objectifs de contrôle pour l'information et les technologies associées**) à partir de 1994 en tant que modèle de référence pour l'audit des systèmes d'information.
- **Les bonnes pratiques de CobiT** sont le fruit d'un consensus d'experts mondiaux.
- Elles sont très orientées vers le contrôle, au sens de maîtrise pour la réalisation des objectifs et moins vers l'exécution.
- Leur but:
  - Aider à optimiser les investissements informatiques
  - Assurer la fourniture des services
  - Fournir des métriques auxquelles se référer pour assurer le bon fonctionnement des systèmes.
- CobiT est en permanence tenu à jour et harmonisé avec d'autres cadres de référence faisant autorité.

CobiT

- **CobiT répond à plusieurs préoccupations** concernant les systèmes d'information:
  - Offrir un référentiel unique au contrôle interne, aux auditeurs internes ainsi qu'à l'inspection en relation avec la DSI et les tiers externes;
  - Offrir un cadre d'investigation pour les auditeurs externes, les actionnaires , les commissaires aux comptes;
  - Couvrir la préoccupation de la gouvernance des systèmes d'information et de management des risques;
  - **Intégrer les référentiels de la DSI (ISO27001, CMMI, ITIL)** dans un souci de gouvernance des systèmes d'information.
- **CobiT aide les dirigeants**
  - à évaluer les risques,
  - à contrôler les investissements dans un environnement informatique souvent imprévisible et
  - À vérifier que la gouvernance des SI est cohérente avec celle de l'entreprise (alignement stratégique)

CobiT

- **CobiT fournit aux directions opérationnels**, utilisatrices de l'informatique, des garanties sur la sécurité et les contrôles des services informatiques internes ou sous-traités.
- **Les auditeurs peuvent l'utiliser pour** justifier leur opinion et conseiller les dirigeants sur les contrôles internes à mettre en œuvre.
- **Auditeurs et informaticiens** peuvent utiliser CobiT pour évaluer le niveau de gouvernance des systèmes d'information de l'entreprise.

- **La version 4** (de 2005), traduite en français par l'AFAI **comprend 6 fascicules:**
  - Synthèse;
  - Cadre de référence (les 34 processus)
  - Noyau
    - Les objectifs du contrôle,
    - Le guide de management
  - Annexes;
  - Guide de mise en œuvre de la gouvernance des TI
  - Guide d'audit des systèmes d'information

CobiT

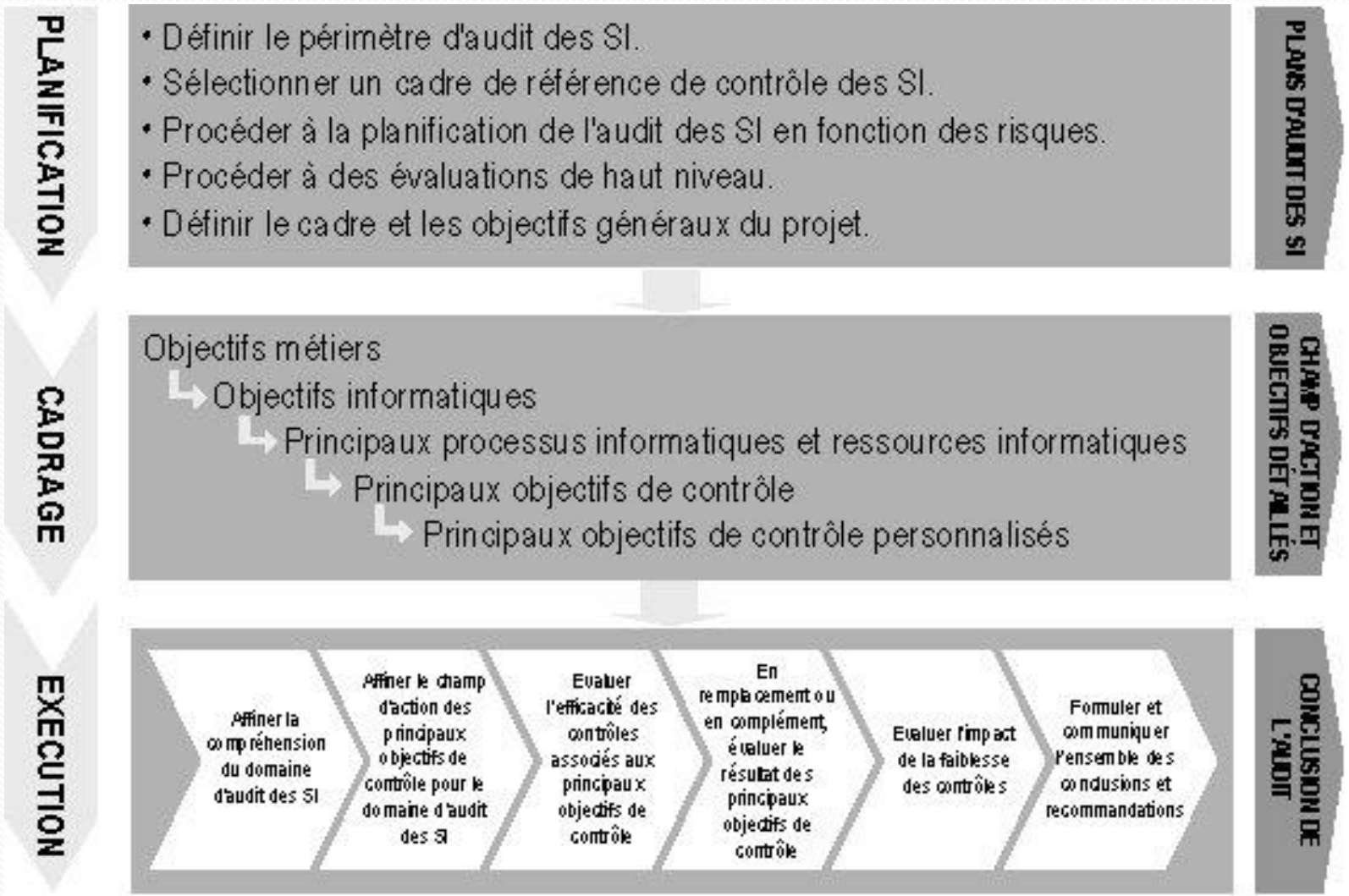
- **Le guide du management de CobiT** comprend:
  - **une description de chacun des 34 processus** , précisant les entrées/sorties et les liens avec les autres processus;
  - **Une matrice de responsabilité détaillée** pour les activités de chacun des processus
  - **Des objectifs et des métriques** revus dans le perspective orientée métier comprenant des indicateurs de management pour vérifier que les objectifs sont atteints, ainsi que **des indicateurs de performance** pour s'assurer que la qualité des dispositifs en place y contribuent;
  - Un **dispositif d'évaluation** des processus par rapport aux pratiques clés de gestion;
  - Un **modèle de maturité** de chaque processus permettant d'en apprécier le niveau sur une échelle de 0 (inexistant) à 5 (optimisé), sur la base de six critères de maturité:
    - Conscience et communication,
    - Règles, standards et procédures,
    - Outils et automatisation,
    - Compétences et expertises,
    - Responsabilité et charge,
    - Fixation et mesure des objectifs.

CobiT

- **Indicateurs et métriques** sont au cœur de **CobiT** :
  - dans la V4, ils sont **plus orientés métier** et **font mieux apparaitre la relation entre les objectifs d'un processus et les résultats obtenus**.
  - **L'utilisation d'indicateurs identiques pour les sociétés différentes utilisant CobiT** devrait permettre à chacun de se situer dans l'échelle des bonnes pratiques.
  - **Le modèle de maturité** fournit une mesure synthétique,

    mais pas forcément comparable à celle d'autres entreprises si elle est réalisée sous forme d'auto-évaluation.

CobiT



« **Guide d'audit des systèmes d'information: Utilisation de Cobit** » http://www.afai.asso.fr/index.php?m=347

L' AFAI (Association française de l'audit et du conseil informatique) est le volet français de l'ISACA

Certification de services

eSCM

eSCM

- Développé dans un institut de Carnegie Mellon University
- **eSCM-SP** (for Service Providers)
- **eSCM-CL** (for client organizations)
- L'association française chargée de sa diffusion en France est l'AeSCM

Les détails vous seront présentés lors d'un exposé

Management de projet

Certification pour personne physique:

PMBOK

PRINCE2

MSP

PMBOK

- Ce dispositif (Project Management Body of Knowledge) d'origine américaine, permet à une **personne physique** d'obtenir une **certification** en matière de **management de projet**.
- PMBOK définit le management de projet comme la ***mise en œuvre de connaissances, de compétences, d'outils et de techniques dans une large gamme d'activités*** nécessaire au déroulement de tout projet.
- Son originalité est de décrire la mission du chef de projet selon une **approche orientée processus** et **domaines de connaissances**.
- Il existe 9 domaines de connaissances: l'intégration du projet, son contenu, les délais, les coûts, la qualité, les ressources humaines, la communication, les risques et l'approvisionnement.
- Les groupes de processus définissent **la structure de base**: le **démarrage**, la **planification**, la **réalisation**, la **maîtrise** et la **clôture**.
- Il aborde les **aspects techniques** (Gantt, méthodes d'estimation, métriques, …), des **connaissances générales** comme la communication, le management ou la qualité.

PMBOK

- Des métriques sont définies dans le cadre du Rappoort d'avancement traité dans le domaine des connaissances Communication du projet.
- Les mesures reposent sur trois types d'analyses
  - Analyse des écarts qui exprime le rapport entre le prévu et le réalisé
  - L'analyse de la tendance qui permet d'anticiper sur une éventuelle détérioration future,
  - L'analyse de la valeur acquise qui repose sur des indicateurs précis définis dans le référentiel.
- PMBOK guide 4e Edition a été publié fin 2008.
- Ce dispositif est très utilisé aux Etats-Unis.
- Il est largement diffusé dans le reste du monde.
- Il a servi de base à la norme ISO 10006 sur le management de projet.

PRINCE2

- Projects IN Controlled Environments *(projets en environnements contrôlés)* est un référenciel fondé sur des modèles de processus liés à une direction de projet.
- Ce dispositif permet à une **personne physique** d'obtenir une **certification** en matière de **management de projet**.
- PRINCE2 est une approche du management de projet, **à base de processus** fournissant une **méthode facilement personnalisable** et adaptable à tous types de projets.
- PRINCE2 repose sur les notions de **rôles**, **composants**, **processus** et **techniques**.
- Le manuel PRINCE2 a été **traduit en français**.
- C'est un standard **largement utilisé en Grande-Bretagne**. Il est également utilisé dans l'Europe du Nord.
- Des certificats PRINCE2 ont été délivrés à des candidats provenant de 50 pays.

PRINCE2

- Le **référentiel PRINCE2** est composé de **huit processus**:
  - La direction de projet (DP);
  - L'élaboration du projet (EP);
  - L'initialisation du projet (IP);
  - Le contrôle des séquences (CS);
  - La gestion des limites de séquences (LS);
  - La gestion des livraisons des produits (LP);
  - La clôture du projet (CP);
  - La planification (PL).
- Chaque **processus** est défini par ses **entrées**, ses **sorties**, des **objectifs** pour les **produits** à créer et aussi des **tâches** à accomplir.

Conclusion

Tableaux de synthèse pour:
règlements, normes et standards
Périmètre des dispositifs
Certification des personnes

Règlements, Normes et standards

Type de referentiel	Référentiels
Lois ou règlements	Lois et décrets relatifs à la certification des services Loi Sarbanes-Oxley Code des marchés publics
Normes	ISO 9001 ISO 15408 ISO 21827 (SSE-CMM) ISO 15504 ISO 25051 ISO 20000 ISO 27001 Certains référentiels de certification de services comme NF 13816
Standards	CMMI ITSEC CobiT SAS 70 EFQM TickIT eSCM TL 9000 HAS Certains référentiels de certification de sevices. Les référentiels de certification de personnes: AFITEP-CDP, AFITEP-CGP, CISSP, ITIL, PCIE, PMP, PRINCE2, Six Sigma.

Périmètre des dispositifs

Secteur d'activité	Activitées concernées	Entitée évaluée	Dispositif
Tous secteurs	Toutes	Entreprise ou entité	EFQM ISO 9001 Sarbanes-Oxley SAS 70
		Processus	ISO 15504
		Personne	Six Sigma
		Service	Certification de services
	Gouvernance	Personne	CobiT-CGEIT
	Sécurité des systèmes d'information	Entreprise ou entité	ISO 27001
		Processus	SSE-CCM
		Personne	CobiT-CISM CISSP
		Produit	ISO 15408 Critères communs ITSEC
	Management de projet	Personne	AFITEP-CDP AFITEP-CGP MSP PMBOK PRINCE2
	Informatique	Entreprise ou entité	ISO 20000 eSCM
		Processus	CMMI
		Produit	ISO 25051
		Personne	ITIL PCIE Testeur logiciel CobiT-CISA
Santé	Toutes	Entreprise ou entité	HAS
Télécommunications			TL 9000

La certification des personnes

Dispositif	Organisme d'accréditation	Présence de l'organisme d'accréditation dans	Organisme certificateur pour la France	Centres d'examen en France
AFITEP-CDP	IPMA	45 pays	AFITEP	Oui
AFITEP-CGP	ICEC	41 pays	AFITEP	Oui
CISSP	ISC	104 pays	ISC	Oui
CobiT CGEIT	ISACA	160 pays	AFAI	Oui
CobiT-CISA	ISACA	160 pays	AFAI	Oui
CobiT-CISM	ISACA	160 pays	AFAI	Oui
ITIL	APMG	33 pays (ceux des membres de l'itSMF)	APMG-international BCS-ISEB DANSK-IT DF Certifiering AB EXIN LCS TÜV SÜD Akademie	Oui
MSP	APMG	Plus de 50 pays	APMG au nom de l'OGC	Oui
PCIE	ECDL	140 pays	Euro-Aptitudes	Oui
PMBOK	PMI	68 pays	PMI France	Oui
PRINCE2	APMG	Plus de 50 pays	APMG au nom de l'OGC	Oui
Testeur logiciel	CFTL-ISTBQ	40 pays	CFTL	Oui

Bibliographie / Webgraphie

- **Bibliographie**
  - Guide des certifications SI –comparatif, analyse et tendances ITIL, CobiT, ISO27001, eSCM; M. Otter, J. Sidi, L. Hanaud; 2eme édition; 2009; DUNOD
  - Management et gouvernance des SI, C. Rosenthal-Sabroux et A. Carvalho, Octobre 2009, HERmès – Lavoisier
- **Webgraphie**
  - www.adeli.org *(Association ADELI)*
  - eSCM
    - Itsqc.cs.cmu.edu *(Itsqc et CarnegieMellon University)*
    - www.ae_scm.com *(association AeSCM France)*
  - CMMI
    - www.sei.cmu.edu/cmmi/models
  - ITIL
    - www.itil_officialsite.com/Qualifications/ITILV3QualificationScheme.asp