DAUPHINE
UNIVERSITÉ PARIS

Capitalisation

CoBiT

RÉFÉRENCE DSI

UNE BREVE HISTOIRE …

- Une brève histoire de COBIT:

  - ISACA
    - Audit et contrôle SI
    - 50000 membres/ 140 Pays
  - En France AFAI
  - 1996 , 1998, 2000, 2005, 2007 4.1

  - V5 en 2012
    - V4.1
      - Are we doing them the right way?
      - Are we getting them done well?
    - ValIT
      - Frame work/ B Value
        - Processes
        - Best practices
        - Enterprise level
      - Are we doing the right things?
      - Are we getting the benefits?
    - Risk IT framework
    - BM for Information Security

Le modèle de maturité de COBIT

Le modèle de maturité permet d'évaluer le niveau de chaque processus de gestion. Le modèle contient 5 niveaux de maturité:

Niveau	Nom	Description
0	Non-existent	Les processus de gestion ne sont pas appliqués.
1	Initial	Les processus sont ad hoc et désorganisés.
2	Repeatable	Les processus suivent un modèle répétable.
3	Defined	Les processus sont formalisés et communiqués.
4	Managed	Les processus sont surveillés et mesurés.
5	Optimised	L'amélioration du processus est géré.

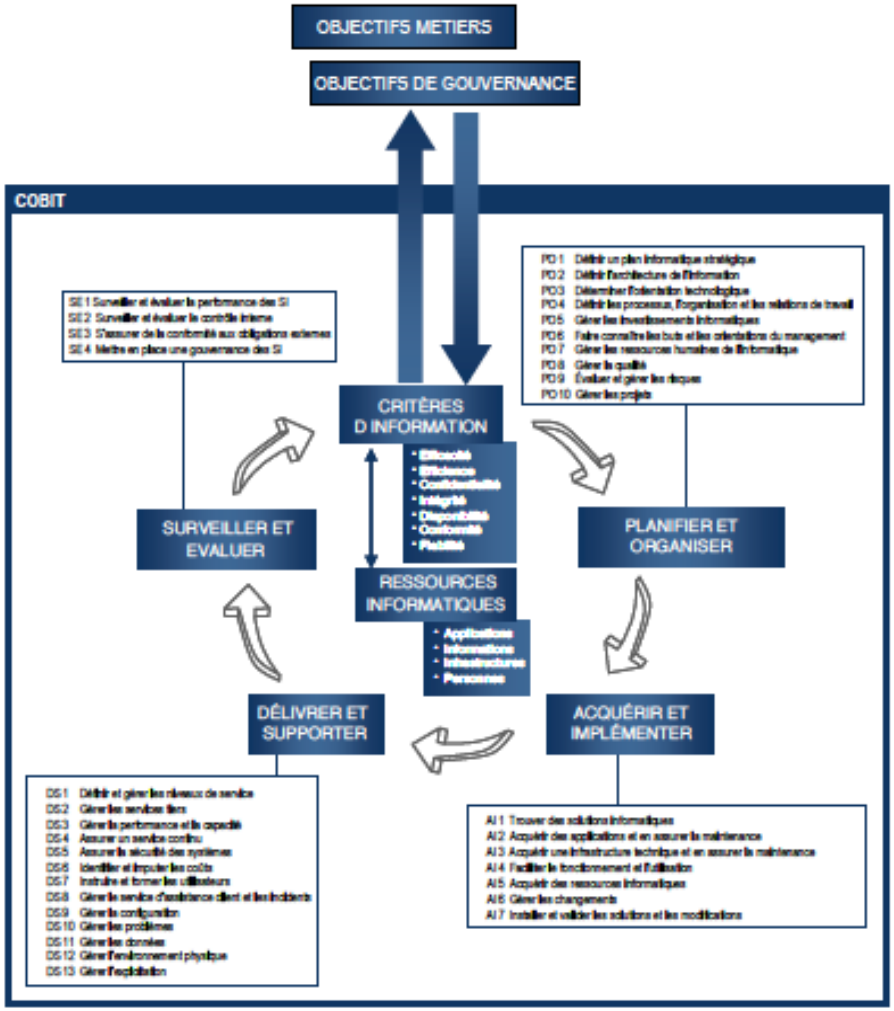
Le modèle de maturité permet de définir:

La situation actuelle de l'organisation.
La situation des entreprises dans un domaines métier équivalent.
Les standards internationaux.
La stratégie d'amélioration de l'entreprise, là où elle souhaite aller.

Le Management Guideline COBIT décrit les 5 niveaux de maturité pour chacun des 34 processus de gestion, permettant la définition précise du niveau de maturité d'une organisation informatique.

- Huit Guides/ Thèmes:
  - Executive overview
  - Framework
  - Control objectives
  - Control practices
  - Management guide lines
  - IT assurance Guide
  - IT Governance implementation guide
  - IT Control objectives for SOX.
- Organisation générale:
  - 4 Domaines
  - 34 Processus
  - 220 Activités

Figure 23 Le Cadre de référence général de COBIT



CONTENU FRAMEWORK

- CONTENU FRAMEWORK
  - ✓ **Planifier et Organiser.**
  - ✓ Acquérir et Implémenter.
  - ✓ Délivrer et Supporter.
  - ✓ Surveiller et Evaluer.

...

- PO1 Définir un plan stratégique:
  - PO1.1 Gestion de la valeur des SI
  - PO1.2 Alignement métiers-informatique
  - PO1.3 Évaluation de la capacité et de la performance actuelle
  - PO1.4 Plan informatique stratégique
  - PO1.5 Plans informatiques tactiques
  - PO1.6 Gestion du portefeuille informatique

- PO2 Définir l'architecture de l'information:
  - PO2.1 Modèle d'architecture de l'information de l'entreprise
  - PO2.2 Dictionnaire et règles de syntaxe des données de l'entreprise
  - PO2.3 Système de classification des données
  - PO2.4 Gestion de l'intégrité

- PO3 Déterminer l'orientation technologique:
  - PO3.1 Planification de l'orientation technologique
  - PO3.2 Plan d'infrastructure technologique
  - PO3.3 Surveillance de l'évolution des tendances et de la réglementation
  - PO3.4 Standards informatiques
  - PO3.5 Comité d'architecture technologique

- PO4 Définir les processus, l'organisation et les relations de travail
  - PO4.1 Cadre de référence des processus informatiques
  - PO4.2 Comité stratégique informatique
  - PO4.3 Comité de pilotage informatique
  - PO4.4 Position de la fonction informatique au sein de l'entreprise
  - PO4.5 Structure du service informatique
  - PO4.6 Établissement des rôles et responsabilités
  - PO4.7 Responsabilité de l'assurance qualité informatique
  - PO4.8 Responsabilité des risques, de la sécurité et de la conformité
  - PO4.9 Propriété des données et du système
  - PO4.10 Supervision
  - PO4.11 Séparation des tâches
  - PO4.12 Recrutement informatique
  - PO4.13 Personnel informatique clé
  - PO4.14 Procédures et règles applicables au personnel sous contrat
  - PO4.15 Relations

- PO5 Gérer les investissements informatiques
  - PO5.1 Référentiel de gestion financière
  - PO5.2 Définition des priorités dans le budget informatique
  - PO5.3 Budget informatique
  - PO5.4 Gestion des coûts
  - PO5.5 Gestion des bénéfices

- PO6 Faire connaitre les buts et les orientations du Management:
  - PO6.1 Politique informatique et environnement de contrôle
  - PO6.2 Risque informatique pour l'entreprise et cadre de contrôle
  - PO6.3 Gestion des politiques informatiques
  - PO6.4 Déploiement des politiques, des standards et des procédures
  - PO6.5 Communication des objectifs et des orientations informatiques

- PO7 Gérer les ressources humaines de l'informatique:
  - PO7.1 Recrutement et maintien du personnel
  - PO7.2 Compétences du personnel
  - PO7.3 Affectation des rôles
  - PO7.4 Formation
  - PO7.5 Dépendance à l'égard d'individus
  - PO7.6 Procédures de sécurité concernant le personnel
  - PO7.7 Évaluation des performances
  - PO7. 8 Changements de postes et départs

- PO8 Gérer la qualité:
  - PO8.1 Système de gestion de la qualité (SGQ)
  - PO8.2 Standards informatiques et pratiques qualité
  - PO8.3 Standards de développement et d'acquisition
  - PO8.4 Orientation client
  - PO8.5 Amélioration continue
  - PO8.6 Mesure, surveillance et revue qualité

- P09 Evaluer et gérer les risques:
  - PO9.1 Référentiel de gestion des risques informatiques
  - PO9.2 Établissement du contexte du risque
  - PO9.3 Identification des événements
  - PO9.4 Évaluation du risque
  - PO9.5 Réponse au risque
  - PO9.6 Maintenance et surveillance d'un plan d'action vis-à-vis des risques

- PO10 Gérer les projets:
  - PO10.1 Référentiel de gestion de programme
  - PO10.2 Référentiel de gestion de projet
  - PO10.3 Approche gestion de projet
  - PO10.4 Implication des parties prenantes
  - PO10.5 Énoncé du périmètre du projet
  - PO10.6 Démarrage d'une phase du projet
  - PO10.7 Plan projet intégré
  - PO10.8 Ressources du projet
  - PO10.9 Gestion des risques du projet
  - PO10.10 Plan qualité du projet
  - PO10.11 Contrôle des changements du projet
  - PO10.12 Planification du projet et méthodes d'assurance
  - PO10.13 Métrique, reporting et surveillance de la performance du projet
  - PO10.14 Clôture du projet

CONTENU FRAMEWORK

- CONTENU FRAMEWORK
  - ✓ Planifier et Organiser.
  - ✓ **Acquérir et Implémenter.**
  - ✓ Délivrer et Supporter.
  - ✓ Surveiller et Evaluer.

- AI1 Trouver des solutions informatiques:
  - AI1.1 Définition et actualisation des exigences métiers, techniques et fonctionnelles
  - AI1.2 Rapport d'analyse de risques
  - AI1.3 Étude de faisabilité et formulation d'alternatives
  - AI.4 Décision et approbation concernant les exigences et la faisabilité

- AI2 Acquérir des applications et en assurer la maintenance:
  - AI2.1 Conception générale
  - AI2.2 Conception détaillée
  - AI2.3 Contrôles applicatifs et auditabilité
  - AI2.4 Sécurité et disponibilité des applications
  - AI2.5 Configuration et implémentation des logiciels applicatifs acquis
  - AI2.6 Mises à jour majeures des systèmes existants
  - AI2.7 Développement d'applications
  - AI2.8 Assurance qualité des logiciels
  - AI2.9 Gestion des exigences des applications
  - AI2.10 Maintenance des applications

- AI3 Acquérir une infra technique et en assurer la maintenance:
  - AI3.1 Plan d'acquisition d'une infrastructure technique
  - AI3.2 Protection et disponibilité des ressources de l'infrastructure
  - AI3.3 Maintenance de l'infrastructure
  - AI3.4 Environnement de test de faisabilité

- AI4 Faciliter le fonctionnement et l'utilisation:
  - AI4.1 Planification pour rendre les solutions exploitables
  - AI4.2 Transfert de connaissances aux métiers
  - AI4.3 Transfert de connaissances aux utilisateurs finaux
  - AI4.4 Transfert de connaissances aux équipes d'exploitation et de support

- AI5 Acquérir des ressources informatiques:
  - AI5.1 Contrôle des achats
  - AI5.2 Gestion des contrats fournisseurs
  - AI5.3 Choix des fournisseurs
  - AI5.4 Acquisition de ressources informatiques

- AI6 Gérer les changements:
  - AI6.1 Standards et procédures de changement
  - AI6.2 Évaluation de l'impact, choix des priorités et autorisation
  - AI6.3 Modifications d'urgence
  - AI6.4 Suivi et compte-rendu des changements
  - AI6.5 Clôture et documentation des changements

- AI7 Installer et valider les solutions et les modifications:
  - AI7.1 Formation
  - AI7.2 Plan de tests
  - AI7.3 Plan d'implémentation
  - AI7.4 Environnement de tests
  - AI7.5 Conversion des systèmes et des données
  - AI7.6 Test des modifications
  - AI7.7 Tests de recette définitive
  - AI7.8 Mise en production
  - AI7.9 Revue post-implémentation

- CONTENU FRAMEWORK
  - ✓ Planifier et Organiser.
  - ✓ Acquérir et Implémenter.
  - ✓ **Délivrer et Supporter**.
  - ✓ Surveiller et Evaluer.

- DS1 Définir et gérer les niveaux de services:
  - DS1.1 Référentiel pour la gestion des niveaux de services
  - DS1.2 Définition des services
  - DS1.3 Contrats ou conventions de services (CS)
  - DS1.4 Contrats d'exploitation (CE)
  - DS1.5 Surveillance et comptes-rendus des niveaux de services atteints
  - DS1.6 Revue des conventions de services et des contrats

- DS2 Gérer les services tiers:
  - DS2.1 Identification des relations avec tous les fournisseurs
  - DS2.2 Gestion des relations fournisseurs
  - DS2.3 Gestion du risque fournisseurs
  - DS2.4 Surveillance des performances fournisseurs

- DS3 Gérer la performance et la capacité:
  - DS3.1 Planification de la performance et de la capacité
  - DS3.2 Performance et capacité actuelles
  - DS3.3 Performance et capacité futures
  - DS3.4 Disponibilité des ressources informatiques
  - DS3.5 Surveillance et comptes-rendus

- DS4 Assurer un service continu:
  - DS4.1 Référentiel de continuité informatique
  - DS4.2 Plans de continuité informatique
  - DS4.3 Ressources informatiques critiques
  - DS4.4 Maintenance du plan de continuité des SI
  - DS4.5 Tests du plan de continuité des SI
  - DS4.6 Formation au plan de continuité des SI
  - DS4.7 Diffusion du plan de continuité des SI
  - DS4.8 Reprise et redémarrage des services informatiques
  - DS4.9 Stockage de sauvegardes hors site
  - DS4.10 Revue après redémarrage

- DS5 Assurer la sécurité des systèmes:
  - DS5.1 Gestion de la sécurité informatique
  - DS5.2 Plan de sécurité informatique
  - DS5.3 Gestion des identités
  - DS5.4 Gestion des comptes utilisateurs
  - DS5.5 Tests de sécurité, vigilance et surveillance
  - DS5.6 Définition des incidents de sécurité
  - DS5.7 Protection de la technologie de sécurité
  - DS5.8 Gestion des clefs de chiffrement
  - DS5.9 Prévention, détection et neutralisation des logiciels malveillants
  - DS5.10 Sécurité des réseaux
  - DS5.11 Échange de données sensibles

- DS6 Identifier et imputer les coûts:
  - DS6.1 Définition des services
  - DS6.2 Comptabilité de l'informatique
  - DS6.3 Modèle de coûts et facturation
  - DS6.4 Maintenance du modèle de coûts

- DS7 Instruire et former les utilisateurs:
  - DS7.1 Identification des besoins en savoir et en formation
  - DS7.2 Fourniture de formation et d'enseignement
  - DS7.3 Évaluation de la formation reçue

- DS8 Gérer le service d'assistance client et les incidents:
  - DS8.1 Service d'assistance client
  - DS8.2 Enregistrement des demandes des clients
  - DS8.3 Escalade des incidents
  - DS8.4 Clôture des incidents
  - DS8.5 Rapports et analyse des tendances

- DS9 Gérer la configuration:
  - DS9.1 Référentiel de configuration et configuration de base
  - DS9.2 Identification et maintenance des éléments de configuration
  - DS9.3 Revue d'intégrité des configurations

- DS10 Gérer les problèmes:
  - DS10.1 Identification et classification des problèmes
  - DS10.2 Suivi et résolution des problèmes
  - DS10.3 Clôture des problèmes
  - DS10.4 Intégration de la gestion de la configuration, des incidents et des problèmes

- DS11 Gérer les données:
  - DS11.1 Exigences des métiers pour la gestion des données
  - DS11.2 Dispositifs de stockage et de conservation
  - DS11.3 Système de gestion de la médiathèque
  - DS11.4 Mise au rebut
  - DS11.5 Sauvegarde et restauration
  - DS11.6 Exigences de sécurité pour la gestion des données

- DS12 Gérer l'environnement physique:
  - DS12.1 Sélection du site et agencement
  - DS12.2 Mesures de sécurité physique
  - DS12.3 Accès physique
  - DS12.4 Protection contre les risques liés à l'environnement
  - DS12.5 Gestion des installations matérielles

- DS13 Gérer l'exploitation:
  - DS13.1 Procédures et instructions d'exploitation
  - DS13.2 Planification des travaux
  - DS13.3 Surveillance de l'infrastructure informatique
  - DS13.4 Documents sensibles et dispositifs de sortie
  - DS13.5 Maintenance préventive du matériel

- CONTENU FRAMEWORK
  - ✓ Planifier et Organiser.
  - ✓ Acquérir et Implémenter.
  - ✓ Délivrer et Supporter.
  - ✓ **Surveiller et Evaluer.**

- SE1 Surveiller et évaluer la performance des SI:
  - SE1.1 Approche de la surveillance
  - SE1.2 Définition et collationnement des données de surveillance
  - SE1.3 Méthode de surveillance
  - SE1.4 Évaluation de la performance
  - SE1.5 Comptes-rendus destinés au conseil d'administration et à la direction générale
  - SE1.6 Actions correctives

- SE2 Surveiller et évaluer le contrôle interne:
  - SE2.1 Surveillance du référentiel de contrôle interne
  - SE2.2 Revue générale
  - SE2.3 Anomalies détectées par le contrôle
  - SE2.4 Autoévaluation du contrôle
  - SE2.5 Assurance de contrôle interne
  - SE2.6 Contrôle interne des tiers
  - SE2.7 Actions correctives

- SE3 S'assurer de la conformité aux obligations externes:
  - SE3.1 Identification des obligations externes : lois, règlements et contrats
  - SE3.2 Optimisation de la réponse aux obligations externes
  - SE3.3 Évaluation de la conformité aux obligations externes
  - SE3.4 Assurance positive de la conformité
  - SE3.5 Intégration des rapports

- SE4 Mettre en place une gouvernance des SI:
  - SE4.1 Mise en place d'un cadre de gouvernance des SI
  - SE4.2 Alignement stratégique
  - SE4.3 Apport de valeur
  - SE4.4 Gestion des ressources
  - SE4.5 Gestion des risques
  - SE4.6 Mesure de la performance
  - SE4.7 Assurance indépendante