

L'Audit du Système d'Information

- **Définition**
- **Introduction**
- **Les différents types d'audit informatique**

5 – Définition

Introduction :

Il est bon de clarifier le vocabulaire utilisé par les différents acteurs lors de la mise en œuvre d'un audit.

Nous n'allons pas décrire le déroulement d'une mission d'audit, mais préférer la description des "Fondations" : c'est-à-dire décrire dans les différentes activités de l'organisation auditée les comportements de ses membres, présente des risques de non-conformité avec les règles de l'art, met en danger certains actifs ou pire enfreint la réglementation ou la loi ?

Les termes qui expriment ce qui doit être fait, avec une signification "normative" plus ou moins forte sont les suivants :

norme ou normalisation, standard ou standardisation, référentiel, règles et usages de la profession, certification, conformité, label, code, exigences, principes, déontologie, règles de l'art, règlement ou réglementation ou régulation, loi ou législation.

Nous allons présenter la terminologie employée dans les diverses missions d'audit.

5 – Définition

Norme : (source : AFNOR)

C'est un référentiel élaboré en consensus par l'ensemble des acteurs d'un domaine, d'un marché : producteurs, utilisateurs, laboratoires, pouvoirs publics, consommateurs etc., et reflétant l'état de la technique et des contraintes économiques à un moment donné.

La norme est un document d'application volontaire et contractuelle.

La Directive 98/34/CE indique que la norme est :

" Une spécification technique approuvée par un organisme reconnu à activité normative pour application répétée ou continue, dont l'observation n'est pas obligatoire... . «

Normalisation : (Source : AFNOR)

Le processus de normalisation a pour objet la publication de normes et documents normatifs, aussi bien à l'échelle nationale, européenne ou internationale.

En France, le décret n° 84-74 modifié du ministère de l'industrie et de la recherche, fixant le statut de la normalisation, précise que :

" La normalisation a pour objet de fournir des documents de références comportant des solutions à des problèmes techniques et commerciaux concernant les produits, biens et services qui se posent de façon répétée dans des relations entre partenaires économiques, scientifiques, techniques et sociaux " .

Ce texte définit le système de normalisation français et en confie la gestion à l'AFNOR (Association française de normalisation).

AFNOR est le membre français des structures de normalisation internationale (ISO - Organisation Internationale de Normalisation) et européenne (CEN - Comité Européen de Normalisation).

5 – Définition

Standard ou Standardisation :

Ces termes sont souvent utilisés comme synonymes de norme et normalisation du fait de l'origine anglo-saxonne de ces termes.

En revanche, le "standard" n'a pas la reconnaissance officielle de la "norme".

Il doit être envisagé comme une "norme" de fait, qui a vocation à être validée par l'organisme en charge de la normalisation.

Pour les anglophones, seul le terme "standard" existe et recouvre les deux sens.

Référentiel :

Un référentiel contient des informations de référence.

C'est-à-dire que toute information identifiée comme information de référence doit obligatoirement faire l'objet d'une définition explicite permettant :

- D'apporter une vision claire et précise du contour de cette information de référence (aucune ambiguïté ne doit exister sur les limites et le contenu de cette information de référence) .
- Une adhésion de tous sur la définition et le contour qu'elle porte (on dit : partage de la définition).

Certification:

La certification est une reconnaissance écrite, par un organisme indépendant du fabricant ou du prestataire de service, de la conformité d'un produit, service, organisation ou personnel à des exigences fixées dans un référentiel.

La certification doit être effectuée dans le cadre européen par un organisme accrédité. En France c'est le Comité français d'accréditation (**COFRAC**) qui délivre les accréditations.

Consulter le site : <http://www.cofrac.fr/>

5 – Définition

Les usages de la profession : état de l'art, règles de l'art...

Tous ces termes font référence à des pratiques professionnelles qui sont reconnues comme correctes et qui doivent assurer dans les métiers de services un niveau de prestation conforme aux attentes du client.

Il est à noter que les tribunaux peuvent avoir à apprécier la conformité de cette "obligation de moyens" dans le cas d'un conflit client-fournisseur.

Le rôle des instances professionnelles est donc important pour fixer ces usages.

Le législateur confie d'ailleurs à certaines d'entre elles le soin de les rédiger (par exemple pour la profession réglementée d'avocat, les architectes, ...).

Exemple : " Dans le respect des dispositions législatives et réglementaires en vigueur, le Conseil national des barreaux unifie par voie de dispositions générales les règles et usages de la profession d'avocat. " (art. 22)

Code de déontologie :

Document écrit qui regroupe l'ensemble des règles et devoirs qui régissent une profession, la conduite de ceux qui l'exercent, les rapports entre ceux-ci et leurs clients ou le public. Désormais, de nombreuses professions se sont dotées, avec ou sans l'aval des pouvoirs publics, d'un tel code.

Par exemple, les commissaires aux comptes : décret n° 2005-1412 du 16 novembre 2005 portant approbation du code de déontologie de la profession de commissaire aux comptes.

Consulter le site :

<http://www.admi.net/>

5 – Introduction

Pour faire simple !

L'audit est une démarche, un outil permettant d'observer une activité, un domaine avec un regard extérieur afin de s'assurer que toutes les règles de fonctionnement sont respectées et suivies (c'est l'aspect conformité) et que les activités, les processus sont efficaces c'est-à-dire : capable d'atteindre les objectifs assignés.

De plus :

Il convient de noter qu'en matière d'audit il existe deux sens qui sont :

- C'est un contrôle approfondi qui vérifie la conformité d'une entité à un référentiel donné.
C'est ce que l'on appelle : "**L'audit de conformité**", défini par les normes ISO 19000.
- Soit une enquête participative destinée à examiner avec les intervenants diverses solutions afin d'améliorer l'organisation d'une activité donnée.
C'est ce que l'on appelle : "**L'audit de fonctionnel**".

L'audit de conformité permet de faire respecter les méthodes édictées et les critères d'un label.
Exemple la certification pour être ISO 9000.

Par contre l'audit fonctionnel est différent car son but est, par exemple, d'approfondir un problème de fonctionnement précis en écoutant les différentes parties en présence et en recherchant les solutions possibles.

Cette démarche a des avantages ; intervention d'un œil neuf, écoute du personnel de terrain (meilleures solutions), confiance entre auditeurs et audités, fait progresser l'esprit d'entreprise avec pédagogie ...

5 – Les différents types d'audit informatique

Après s'être cantonné au domaine financier l'audit est maintenant diffusé dans tous les secteurs de l'activité services, industriel, commercial, etc.

L'audit est un travail exercé par un auditeur qui réalise un travail méthodique, indépendant et documenté afin de recueillir des informations objectives.

Cela permet de les comparer à des référentiels du domaine étudié.

Un audit peut être réalisé suivant des contextes différents :

- Dans un cadre légal d'audit des comptes (commissaire aux comptes),
- Dans un cadre d'expertise judiciaire sur requête d'un tribunal,
- Dans un cadre administratif sur demande d'une autorité administrative supérieure,
- A la demande de dirigeants de l'organisation,
- Au sein d'une mission d'audit concernant l'ensemble d'une filiale par exemple,
- A la demande de propriétaires afin de contrôler leurs mandataires.

Le caractère spécifique de l'audit sont :

- La nature du cadre juridique (cadre légal, réglementaire ou contractuel),
- La nature du lien entre auditeur et audité : même appartenance ou non à l'organisation,
- Le destinataire du rapport,
- Le financeur,
- Le niveau de technicité (famille ou type) de la mission.

Tout ce ci nous amène à définir deux grandes familles d'audit :

- L'audit externe,
- L'audit interne.

5 – Les différents types d'audit informatique

L'audit interne :

L'audit interne est une activité d'assurance et de conseil réalisée par certains employés de l'organisation qui certifie la régularité de la gestion de l'entreprise relativement au suivi de ses procédures.

L'audit interne est exercé dans différents environnements juridiques et culturels ainsi que dans des organisations dont l'objet, la taille, la complexité et la structure sont divers. Il peut être en outre exercé par des professionnels de l'audit, internes ou externes à l'organisation.

L'audit interne est une activité indépendante et objective qui permet de donner à une organisation une assurance sur le degré de maîtrise de ses opérations, lui apporte ses conseils pour les améliorer, et contribue à créer de la valeur ajoutée. Il aide cette organisation à atteindre ses objectifs en évaluant, par une approche systématique et méthodique, ses processus de management des risques, de contrôle, et de gouvernance d'entreprise, et en faisant des propositions pour renforcer leur efficacité.

L'audit interne permet aussi aux grandes organisations de vérifier que les entités sont bien en adéquation avec la stratégie du groupe.

Le contrôle interne peut s'effectuer de façon continue.

L'audit externe :

L'audit externe est effectué par une personne indépendante et extérieure de l'entité auditée. L'audit externe, peut être réalisé par un commissaire aux comptes (si audit légal) ou autre personne spécialisée dans le domaine que l'on souhaite audité.

Exemple: - Contrôle de la tenue des comptes,

- Examen des documents de synthèse (bilan, compte de résultat, annexe).

Contrôle réalisé par des experts comptables considérés comme commissaires aux comptes.

Le but est de s'assurer que les principes comptables fondamentaux sont respectés.

5 – Les différents types d'audit informatique

Tout d'abord il est nécessaire de différencier "deux termes" qui sont l'audit informatique et l'audit du système d'information.

Cette erreur est très courante et demande précisions :

L'audit informatique a pour mission principale :

- De s'assurer que les outils mis à disposition pour l'organisation correspondent bien aux besoins.
- Que ces outils fournissent et réalisent ce pour quoi ils sont prévus.

L'audit du système d'information doit permettre :

- La description des matériels, logiciels et documentations utilisés par l'organisation.
- De vérifier que les besoins et les règles de gestion sont définis correctement.
- D'examiner les méthodes d'organisation, de contrôle et de la planification des services informatiques et de l'aptitude des personnels (formation, niveau, ...).
- Évaluer la sécurité informatique, de son efficacité et de la bonne utilisation des matériels utilisés y compris la gestion de la sauvegarde.
- L'analyse de la bonne gestion informatique des informations manipulées y compris la mise en évidence des utilisations imparfaites.
- L'audit des contrats d'assistance, de maintenance, des logiciels, d'hébergement (sites Web et sauvegarde) et la politique de suivi de tous ces contrats (date, coûts, organisation, ...).

Des méthodes formelles et normalisées sont proposées pour l'organisation en matière d'audit informatique et d'audit du système d'information.

5 – Les différents types d'audit informatique

Dans toute branche de l'activité d'une organisation, l'audit doit exister en informatique, en fonction des vulnérabilités et des coûts qu'elle induit.

Un audit informatique n'a de sens que si sa finalité est définie : contrôle fiscal, juridique, expertise judiciaire, vérification de l'application des intentions de la Direction, examen de l'efficacité ou de la sécurité d'un système, de la fiabilité d'une application, etc.

Quel que soit le type de l'audit (interne ou externe, contractuel ou légal, etc.), la finalité est toujours de porter un jugement sur le management du système d'information et l'exécution de ses objectifs.

C'est donc la comparaison entre ce qui est observé (un acte de management ou d'exécution) et ce que cela devrait être, toujours selon un système de références.

Différents types d'audit informatique existent :

Ces différents types peuvent se grouper dans un seul outil par exemple, mais elles peuvent se réaliser unitairement suivant le besoin et la demande d'une direction générale.

La démarche d'audit informatique est générale et s'applique à différents domaines comme la fonction informatique, les études informatiques, les projets informatiques, l'exploitation, la planification de l'informatique, les réseaux et les télécommunications, la sécurité informatique, les achats informatiques, l'informatique locale ou l'informatique décentralisée, la qualité de service, l'externalisation, la gestion de parc, les applications opérationnelles etc.

5 – Les différents types d'audit informatique

Le but de l'audit de la fonction informatique est de répondre aux préoccupations de la Direction Générale ou de la direction informatique concernant l'organisation de la fonction informatique, son pilotage, son positionnement dans la structure, ses relations avec les utilisateurs, ses méthodes de travail.

Pour ce faire, on se base sur les bonnes pratiques connues en matière d'organisation de la fonction informatique et elles sont nombreuses, on peut citer :

- La clarté des structures et des responsabilités de l'équipe informatique.
- La définition des relations entre la Direction Générale, les Directions Fonctionnelles et Opérationnelles et la fonction informatique.
- L'existence de dispositifs de mesures de l'activité et notamment d'un tableau de bord de la fonction informatique.
- Le niveau des compétences et des qualifications du personnel de la fonction.
- Le rôle des Directions Fonctionnelles et opérationnelles dans le pilotage informatique et notamment l'existence d'un comité de pilotage de l'informatique.
- La mise en œuvre de politiques, de normes, de procédures spécifiques à la fonction,
- La définition des responsabilités respectives de la fonction informatique.
- L'existence de mécanismes permettant de connaître et de suivre les coûts informatiques, comptabilité analytique, ...

*Ces différents objectifs de contrôle correspondent au processus PO 4 de CobiT :
"Définir les processus, l'organisation et les relations de travail"*

5 – Les différents types d'audit informatique

Audit des études informatiques :

Cet audit est un sous-ensemble de l'audit de la fonction informatique. S'assurer que son organisation et sa structure sont efficaces, que son pilotage est adapté, que ses différentes activités sont maîtrisées, que ses relations avec les utilisateurs se déroulent normalement,...

On se base sur la connaissance des bonnes pratiques recensées dans ce domaine.

Elles sont nombreuses et connues par les professionnels

- L'organisation de la fonction études, le choix des personnes, la formation, leurs responsabilités.
- La mise en place d'outils et de méthodes adaptés notamment une claire identification des tâches, des plannings, des budgets, des dispositifs de suivi des études, un tableaux de bord,...
- Le contrôle des différentes activités comme les petits projets, les projets urgents,...
- La mise sous contrôle de la maintenance des applications opérationnelles.
- Le suivi des activités d'études grâce aux jalons et à divers documents de suivis.

D'autres pratiques existent pour auditer les études comme par exemple :

- L'évaluation de l'organisation de la fonction d'études informatiques et notamment la manière dont sont planifié les différentes activités d'études.
- Le respect des normes en matière de documentation des applications et notamment la définition des documents à fournir avec les différents livrables prévues.
- Le contrôle de la sous-traitance notamment la qualité des contrats, le respect des coûts et des délais, la qualité des livrables, ...
- L'évaluation de la qualité des livrables fournis par les différentes activités d'études qui doivent être testables et vérifiables.

Suivant les préoccupations du demandeur d'autres contrôles seront nécessaires.

5 – Les différents types d'audit informatique

Audit de l'exploitation :

Cet audit a pour but de s'assurer que le ou les différents centres de production informatiques fonctionnent de manière efficace et qu'ils sont correctement gérés.

Il est pour cela nécessaire de mettre en œuvre des outils de suivi de la production.

Ces outils sont de véritables systèmes d'information dédiés à l'exploitation.

Les bonnes pratiques concernant ce domaine sont :

- La clarté de l'organisation : le découpage en équipes, la définition des responsabilités,...
- L'existence d'un système d'information dédié à l'exploitation notamment pour suivre la gestion des incidents, la gestion des ressources, la planification des travaux, les procédures d'exploitation, ,...
- La mesure de l'efficacité et de la qualité des services fournies par l'exploitation informatique.
- La qualité de la planification de la production.
- La gestion des ressources grâce à des outils de mesure de la charge, des simulations, le suivi des performances,...
- L'existence de procédures permettant de faire fonctionner l'exploitation en mode dégradé de façon à faire face à une indisponibilité totale ou partielle du site central ou du réseau.
- La gestion des incidents pour les repérer afin de les empêcher qu'ils se renouvellent.
- Les procédures de sécurité et de continuité de service d'où un plan de secours.
- La maîtrise des coûts de production grâce à une comptabilité analytique afin de calculer les coûts complets ou des services fournis.

Ces différents objectifs de contrôle correspondent au processus DS 1, DS 3, DS 6, DS 12 et DS 13 de CobiT.

5 – Les différents types d'audit informatique

Audit des projets informatiques :

Le but de cet audit est de s'assurer qu'il se déroule normalement et que l'enchaînement des opérations se fait de manière logique et efficace de façon afin d'arriver à la fin de la phase de développement avec un niveau de performance et opérationnelle.

Un audit projet informatique ne se confond pas avec un audit des études informatiques.

Les nombreuses bonnes pratiques de ce domaine sont :

- L'existence d'une méthodologie de conduite des projets.
- La conduite des projets par étapes : cascade, V, W ou en spirale (processus itératif).
- Le respect des étapes et des phases du projet.
- Le pilotage du développement et les rôles respectifs du chef de projet et du comité de pilotage.
- La conformité du projet aux objectifs généraux de l'entreprise.
- La mise en place d'une note de cadrage, d'un plan de management projet ou d'un plan d'assurance qualité (PAQ).
- La qualité et la complétude des études amont : étude de faisabilité et analyse fonctionnelle.
- L'importance et le niveau accordée aux tests, notamment aux tests faits par les utilisateurs.

D'autres pratiques existent pour auditer les études comme par exemple :

- La clarté et l'efficacité du processus de développement.
- L'existence de procédures, de méthodes et de standards donnant des instructions claires aux développeurs et aux utilisateurs.
- La vérification de l'application effective de la méthodologie.
- La validation du périmètre fonctionnel faite suffisamment tôt dans le processus développement.
- la gestion des risques du projet.

Ces différents objectifs de contrôle correspondent aux processus PO 10, AI 1 et AI 2 de CobiT : PO 10 "Gérer le projet"

5 – Les différents types d'audit informatique

Audit des applications opérationnelles :

Les audits présentés précédemment sont des audits informatiques.

L'audit d'applications opérationnelles couvre un domaine plus large et s'intéresse au système d'information de l'entreprise.

Ce sont des audits du système d'information comme l'audit de l'application comptable, de la paie, de la facturation,.... On s'intéresse à l'audit d'un processus global de l'entreprise comme les ventes, la production, les achats, la logistique,...

Il va en particulier vérifier que :

- Les contrôles en place sont opérationnels et sont suffisants.
- Les données saisies, stockées ou produites par les traitements sont de bonnes qualités.
- Les traitements sont efficaces et donnent les résultats attendus.
- L'application est correctement documentée.
- Les procédures mises en œuvre dans le cadre de l'application sont à jour et adaptées.
- L'exploitation informatique de l'application se fait dans de bonnes conditions.
- La fonction ou le processus couvert par l'application sont efficaces et productifs.

Le but de l'audit d'une application opérationnelle est de donner au management une assurance raisonnable sur son fonctionnement. Ces contrôles sont, par exemple, réalisés par le Commissaire aux Comptes dans le cadre de sa mission légale d'évaluation des comptes d'une entreprise : Est-ce que le logiciel utilisé est sûr, efficace et adapté ?

- Contrôle de la conformité de l'application opérationnelle par rapport à la documentation
- La vérification des dispositifs de contrôle en place. Contrôles sur les données entrées, les données stockées, les sorties, les traitements,... et donnent les résultats attendus,
- L'évaluation de la fiabilité des traitements grâce à l'analyse des erreurs ou des anomalies.
- La mesure des performances de l'application, temps de réponse satisfaisants.

5 – Les différents types d'audit informatique

Audit de la sécurité informatique :

Cet audit a pour but de donner au management une assurance raisonnable du niveau de risque de l'entreprise lié à des défauts de sécurité informatique. Car l'informatique représente souvent un niveau élevé pour risque élevé de l'entreprise.

On constate actuellement une augmentation de ces risques liée au développement d'Internet.

Ils sont liés à la conjonction de quatre notions fondamentales :

1. Il existe des menaces significative concernant la sécurité informatique de l'entreprise et notamment ses biens immatériels.
2. Le facteur de risque est une cause de vulnérabilité due à une faiblesse de l'organisation, des méthodes, des techniques ou du système de contrôle.
3. La manifestation du risque. Il peut être physique (incendie, inondation) mais souvent il est invisible et se traduit notamment par la destruction des données, détournement de trafic,...
4. La maîtrise du risque. Mettre en place des mesures permettant de diminuer le niveau des risques notamment en renforçant les contrôle d'accès, authentification utilisateurs,...

Les contrôle les plus courants sont :

- Repérer les actifs informationnels de l'entreprise. Ce sont des matériels informatiques, des logiciels et des bases de données. Mise en place de procédures de gestion efficaces et adaptées.
- Identifier les risques. Il doit exister des dispositifs de gestion adaptés permettant de surveiller les domaines à risque. Cette surveillance doit être assurée par un RSSI, un responsable de la sécurité informatique.
- Evaluer les menaces. Le RSSI a la responsabilité de repérer et de recenser les principales menaces puis de mesures les impacts. Etablir une cartographie des risques associés au système d'information et construire des scénarios d'agression et d'évaluer les points de vulnérabilité.
- Définir les parades. Diminuer le niveau des risques : contrôles d'accès, cryptage des données, le plan de secours, ...

5 – CobiT et gouvernance

Introduction :

La gouvernance des Technologies de l'Information (IT) regroupe l'ensemble du système de management c'est-à-dire : procédures, processus, traitement, organisation etc.

L'enjeu crucial, face à cette dépendance, est de savoir si les Technologies de l'Information sont en cohérence avec les objectifs pris au sens le plus large, et la stratégie de l'entreprise.

Le CobiT (Common Objectives for Business Information Technology) est un outil puissant qui œuvre dans ce sens.

Le CobiT est aussi un outil fédérateur qui permet d'instaurer un langage commun pour parler de la gouvernance des systèmes d'information en essayant d'intégrer d'autres référentiels tels que ISO 9000.

Cobit se positionne comme un référentiel d'audit et un référentiel de gouvernance. Au niveau de la gouvernance il se place en alignement avec les métiers et la stratégie de l'entreprise.

Historique :

Développé par l'ISACA (Information System Audit & Control Association) dont l'AFAI (Association Française de l'Audit et du conseil Informatique) assure la diffusion francophone, CobiT est un référentiel de gouvernance des systèmes d'information qui couvre 34 processus se répartissant en quatre domaines différents ayant en tout 215 activités associées avec une partie dite "pratiques de contrôle".

A la suite des scandales au début des années 2000 (Enron, ...) le congrès américain vote en 2002, la loi Sarbanes-Oxley (SOX) afin de redonner confiance aux investisseurs et aux actionnaires en garantissant la transparence des comptes, la prise en compte de processus et le renforcement des contrôles liés aux processus financiers.

CobiT a été retenu et reconnu comme une réponse à ces nouvelles exigences en termes de contrôle et de gouvernance. D'où accélération des versions et de la généralisation .

5 – CobiT et gouvernance

Principe :

CobiT fournit aux gestionnaires, auditeurs et utilisateurs de TIC (Technologies de l'information et de la communication) des indicateurs, des processus et des bonnes pratiques pour les aider à maximiser les avantages issus du recours à des techniques informatiques et à l'élaboration de la gouvernance et du contrôle d'une entreprise.

Il les aide à comprendre leurs systèmes informatiques et à déterminer le niveau de sécurité et de contrôle qui est nécessaire pour protéger leur entreprise, et ceci par le biais du développement d'un modèle de gouvernance des systèmes d'information tel que CobiT.

De ce fait, CobiT fournit des indicateurs clés d'objectif, des indicateurs clés de performance et des facteurs clés de succès pour chacun de ses processus.

Le modèle CobiT se focalise sur ce que l'entreprise a besoin de faire et non sur la façon dont elle doit le faire.

Cobit est compatible avec les autres standards et normes.

En clair, le périmètre de CobiT dépasse celui réservé à la direction des systèmes d'information pour englober toutes les parties prenantes des SI dans l'entreprise c'est-à-dire tous les acteurs (direction, actionnaires, et les métiers).

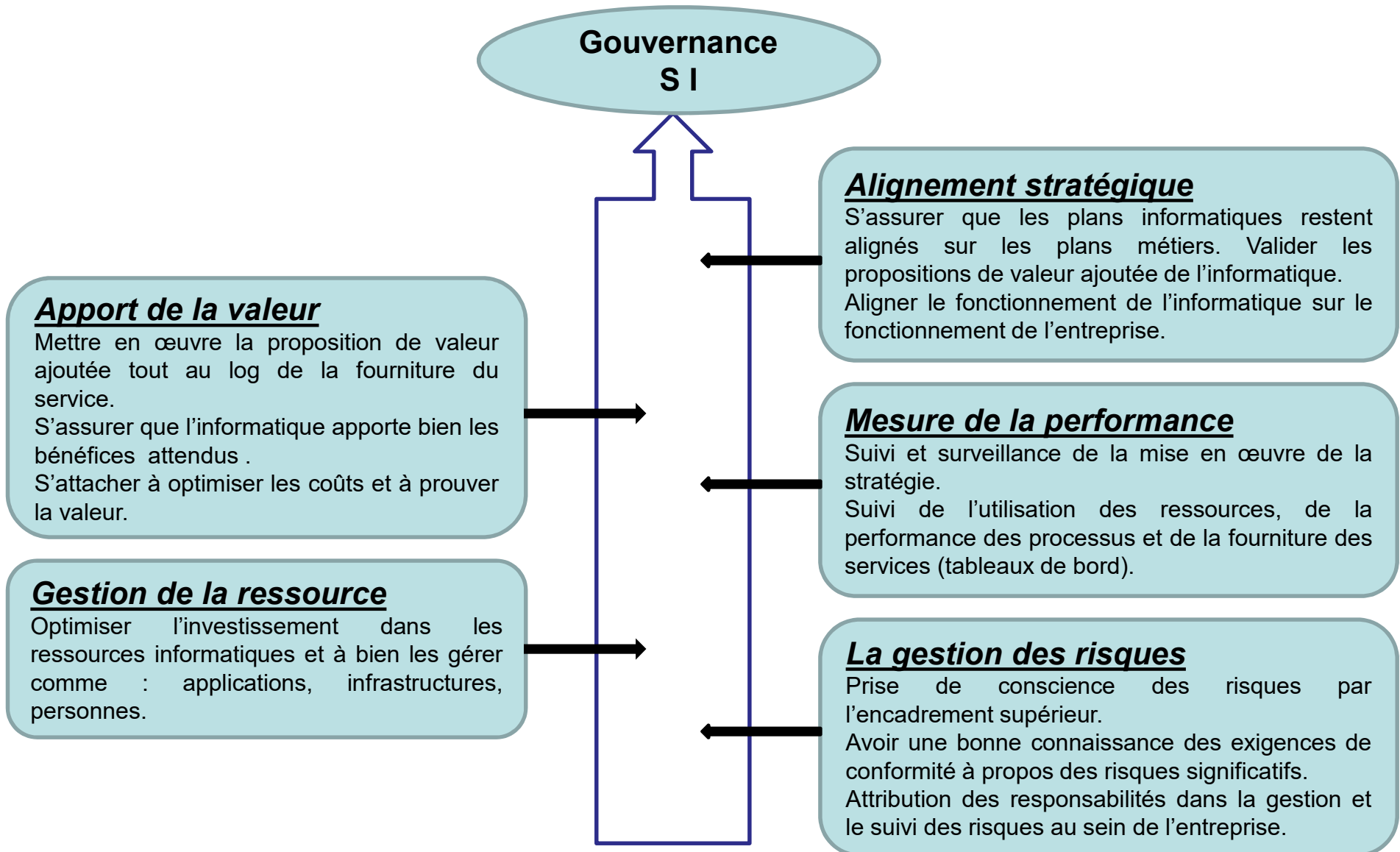
L'intérêt principal de CobiT est d'offrir un cadre général de la gouvernance des SI.

Mettre en place ce cadre, c'est :

- s'assurer de suivre les meilleures pratiques,
- se garantir des risques et de les gérer convenablement,
- être en mesure de se comparer à la fois en interne et en externe avec les meilleures chances de s'aligner sur les besoins métier

5 – CobiT – Les 5 axes stratégiques

Afin de répondre et d'exercer une bonne gouvernance des SI, le CobiT s'intéresse aux 5 axes stratégiques suivants :



5 – CobiT – Les 5 axes stratégiques

L'alignement stratégique :

Les activités informatiques prennent de plus en plus d'importance dans le fonctionnement de l'entreprise.

De ce fait, il est nécessaire et obligatoire que la réponse de l'informatique soit celle que peut attendre les métiers.

Exemple : Une organisation souhaite lancer un nouveau produit. il est bon de s'assurer que le service commercial puisse réaliser le devis du produit concerné dans de bonnes conditions : nomenclatures, prix, quantité, délais, conditions particulières, etc. puis, évidemment de facturer toujours dans des conditions optimales.

Il convient de noter que le terme "alignement stratégique" sous entend la capacité à fournir les services et traitements souhaités en temps et en heure avec le niveau de qualité souhaité.

L'apport de valeurs :

Cela veut dire que l'informatique doit apporter un gain identifiable dans la bonne exécution des divers processus métier.

Cet apport de valeurs se concrétise par la maîtrise des processus mis en œuvre de manière efficace. C'est ici que l'on traitera le pilotage des investissements en coûts et délais en fonction de critères établis : retour d'investissement, amortissement, etc.

Exemple : Dans le cas du service commercial, l'apport de valeurs se matérialisera par la mise en œuvre d'un canal de distribution par internet. Cela permettra à cette entreprise de toucher une nouvelle clientèle.

De ce fait l'informatique doit pouvoir mesurer les ventes, la progression par rapport aux objectifs, progression du CA, des volumes etc.

5 – CobiT – Les 5 axes stratégiques

La gestion des ressources :

Il est nécessaire pour mesurer l'activité informatique d'évaluer toutes les ressources utilisées pour répondre aux exigences métiers.

Les ressources technologiques font partie du périmètre et doivent donner lieu à un plan d'infrastructure.

Il est à noter que le métier doit exprimer ses besoins (exemple commercial : temps de réponses, nombre de clients en lignes etc.).

Exemple : Cas du service commercial, les ressources humaines et technologiques doivent être utilisées aux mieux.

C'est du niveau des ressources : plan de recrutement, disponibilité des personnels dans des créneaux, formation à mettre en place, utilisation de ressources tiers, ...

La mesure de la performance :

Doit répondre aux exigences de transparence au niveaux des coûts, des politiques demandées, des niveaux de services informatiques proposées par rapport aux attentes de la gouvernance des SI.

Le CobiT tente de faire le lien entre les objectifs de la gouvernance et des objectifs des processus ou/et des activités.

La gestion des risques :

Vaste domaine. Le cœur du métier peut être mis en péril en cas d'arrêt ou de dysfonctionnement de son système informatique. La gestion des risques informatiques correspond à un référentiel comprenant : une analyse de risque et un plan de traitement de ces risques.

Exemple : Un arrêt du service vente par internet provoque l'interruption des ventes donc, une perte nette du revenu.

5 – CobiT – Description

Description générale :

Le référentiel CobiT a donné lieu à une série de travaux et publications. Dans la version 3 (et antérieures) la publication principale était le guide d'audit.

A partir de la version 4, le guide de management est devenu l'ouvrage principal de CobiT.

COBIT fût initialement développé par et pour les auditeurs des systèmes d'information à qui l'**ISACA** propose d'ailleurs depuis plus de 10 ans une certification mondiale.

COBIT peut aussi servir d'outil de médiation et de facilitateur du dialogue entre les parties prenantes au sein d'une entreprise, grâce à l'emploi d'un langage commun non technique :

- Directions générales – Optimisation de l'investissement en contrôles en fonction des risques associés.
- Directions métiers – Assurances sur la gestion et le contrôle des services informatiques fournis en interne ou par des tiers,
- Directions informatiques – Fourniture, contrôle et gestion des services informatiques à destination des métiers conformément à la stratégie de l'entreprise.
- Auditeurs et consultants – Conseils au management sur les contrôles internes et la gouvernance des SI.





De plus, le standard **COBIT** peut servir de maître étalon pour l'établissement d'un modèle de gouvernance des systèmes d'information interne permettant d'identifier les pistes de progrès que le management doit prendre en charge :

- Adéquation des compétences aux enjeux,
- Allocation des ressources,
- Définition claire des processus ou réduction des risques en matière de sécurité des systèmes d'information.

5 – CobiT – Description

COBIT répond au besoin des dirigeants de disposer d'objectifs de contrôle et de mesure afin de garantir le succès des objectifs, prévenir et gérer les risques, et identifier les points d'amélioration possibles.

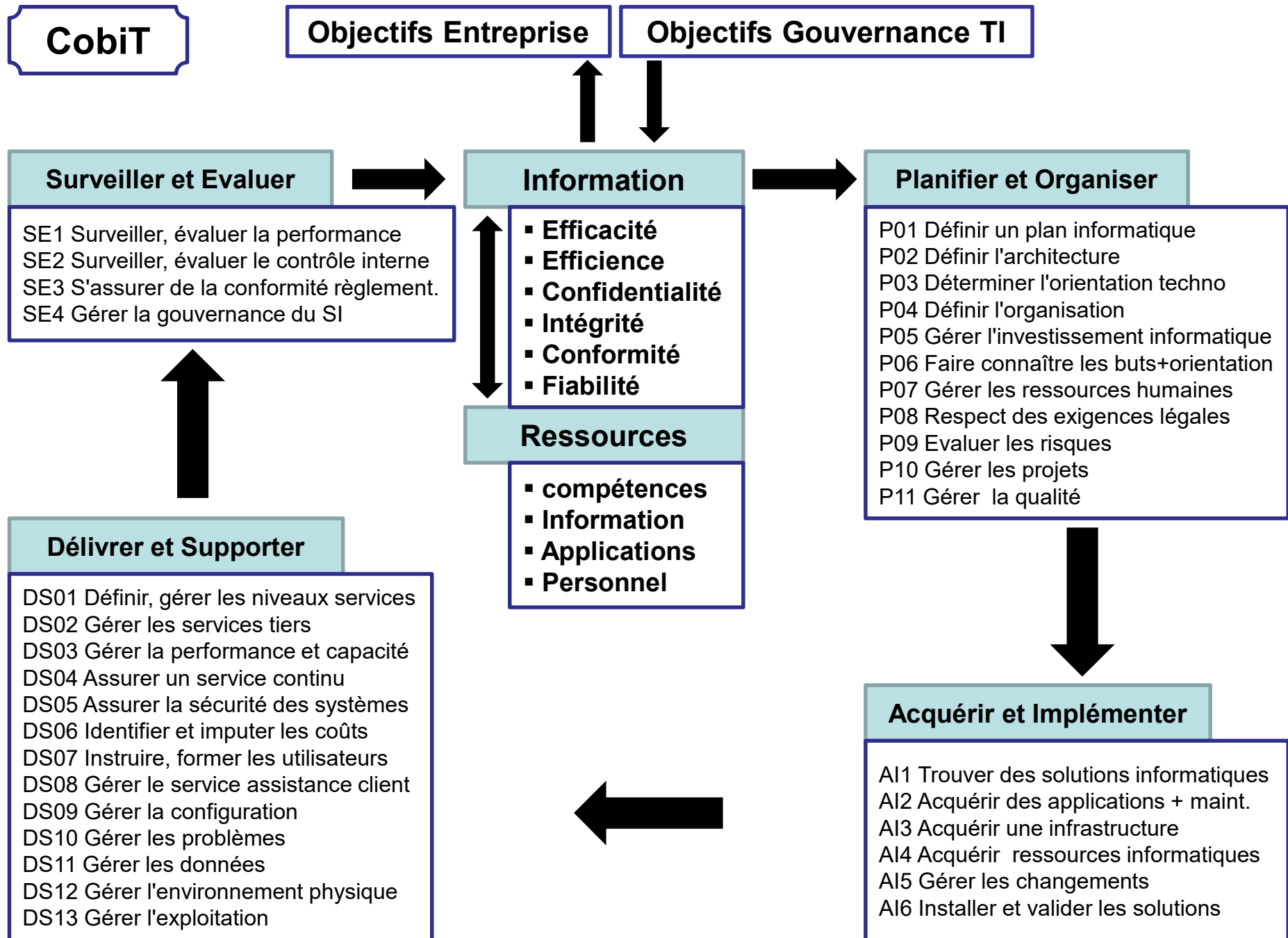
COBIT s'appuie donc sur un framework de 34 processus organisés autour de quatre grands domaines correspondant au cycle de vie des SI donnant ainsi une vision complète de l'activité informatique :

- | | |
|---|--|
|  PO | Planifier et Organiser – Représente la dimension stratégique de la gouvernance des TI. |
|  AI | Acquérir et Implémenter – Rassemble tous les processus qui impactent les Ressources de l'acquisition à l'implémentation y compris les projets et mise en production. |
|  DS | Délivrer et Supporter – Services destinés aux services clients de la DSI. |
|  SE | Surveiller et Evaluer – Contrôle, audit et surveillance de l'ensemble. |

Pour chacun des 34 processus, CobiT décrit le périmètre et l'objet afin de les lister et de les développer comme suit :

- Objectifs et périmètre,
- Description du processus par une représentation des flux internes,
- Une planification et mise en œuvre,
- Mesures et contrôles,
- Rôles et responsabilités,
- Les entrées-sorties du processus

Un exemple est donné plus loin.



5 – CobiT – Les composants

Les critères d'information :

CobiT prend en compte une très riche segmentation de l'information selon des critères précis. Ces critères correspondent aussi bien au point de vue de l'auditeur qu'à celui du manager.

Sept catégories distinctes ont été sélectionnées (ce sont des mesures) :

- **Efficacité** : concerne toute information significative et pertinente pour le processus de gestion, distribuée de manière ponctuelle, correcte, cohérente et utilisable.
- **Efficienne** : concerne la mise à disposition de l'information grâce à l'utilisation optimale (la plus productive et la plus économique) des ressources.
- **Confidentialité** : concerne la protection de l'information sensible contre toute divulgation non autorisée.
- **Intégrité** : touche à l'exactitude et à l'intégralité de l'information ainsi qu'à sa validité au regard des valeurs de l'entreprise et de ses perspectives.
- **Disponibilité** : propriété de l'information qui est d'être disponible et de le rester lorsqu'un processus de gestion en a besoin. Concerne aussi la sauvegarde des ressources nécessaires et des moyens associés.
- **Conformité** : consiste à se conformer aux lois, aux réglementations et aux clauses contractuelles auxquelles le processus de gestion est soumis, c'est-à-dire aux critères de gestion imposés par l'environnement extérieur.
- **Fiabilité de l'information** : s'adresse au management et concerne la fourniture d'informations pertinentes pour le fonctionnement de l'entité et l'exercice des responsabilités sur le plan des finances et des rapports de conformité.

5 – CobiT – Les composants

Les ressources informatiques :

Cette partie concerne plus le directeur des systèmes d'informations (DSI) ou responsable des systèmes d'informations (RSI), pour l'informer des ressources qui vont être impactées par le processus.

Les différentes ressources sont au nombre de cinq :

- **Les compétences** : le personnel, efficacité des collaborateurs (internes et externes).
- **Les applications** : ensemble des procédures de traitement, les systèmes automatisés pour traiter l'information.
- **L'infrastructure** : ensemble des installations : Réseaux, matériels, serveurs, Data Center... qui permet le traitement des applications du SI.
- **Les données** : informations au sens global (format, structure...) y compris les entrées et sorties.
- **Les techniques** : équipement, logiciels, bases de données, réseaux...

Objectifs métier et objectifs informatique :

Le CobiT propose 20 objectifs métier répartis selon les quatre axes suivant :

- Perspective financière,
- Perspective client,
- Perspective interne à la DSI
- Perspective future ou anticipation.

Ces 20 objectifs métier renvoient à 28 objectifs informatiques qui sont eux-mêmes liés aux processus Cobit. De ce fait, on obtient une transitivité entre objectifs métier et informatique, processus et activités.

Cette structuration permet d'obtenir une synthèse de la gouvernance du SI de l'entreprise.

5 – CobiT – Description détaillée des processus

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 œuvre 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 œuvre ?
- Les changements pourront-ils avoir lieu sans perturber les opérations en cours ?

5 – CobiT – Description détaillée des processus

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 Evaluer (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 ?

5 – CobiT – Description détaillée des processus

CobiT est largement décrit dans la documentation officielle.

Il ne faut pas croire que le déploiement de CobiT est simple et partirait d'un modèle unique et immuable pour toutes les DG et DSI qui souhaiteraient le mettre en œuvre.

La représentation du processus tente de mettre en perspective ses activités dans une boucle d'amélioration constante qui est : Définir, mettre en œuvre, améliorer, contrôler et enfin communiquer.

CobiT est un outil fédérateur qui permet d'instaurer un langage commun pour parler de la gouvernance des SI. Son avantage est son approche globale.

Tous les utilisateurs potentiels peuvent tirer parti du contenu CobiT et l'utiliser dans le cadre d'une méthode globale de gestion et de gouvernance des SI, conjointement à d'autres normes plus détaillées telles que :

- ITIL pour la prestation de services,
- CMM pour la fourniture de solutions,
- ISO 17799 pour la sécurité de l'information,
- PMBOK ou PRINCE2 pour la gestion de projets.

Nous allons décrire un processus complet afin de montrer comment atteindre les objectifs métiers.

Exemple pris : **Processus DS11 – Gérer les données**

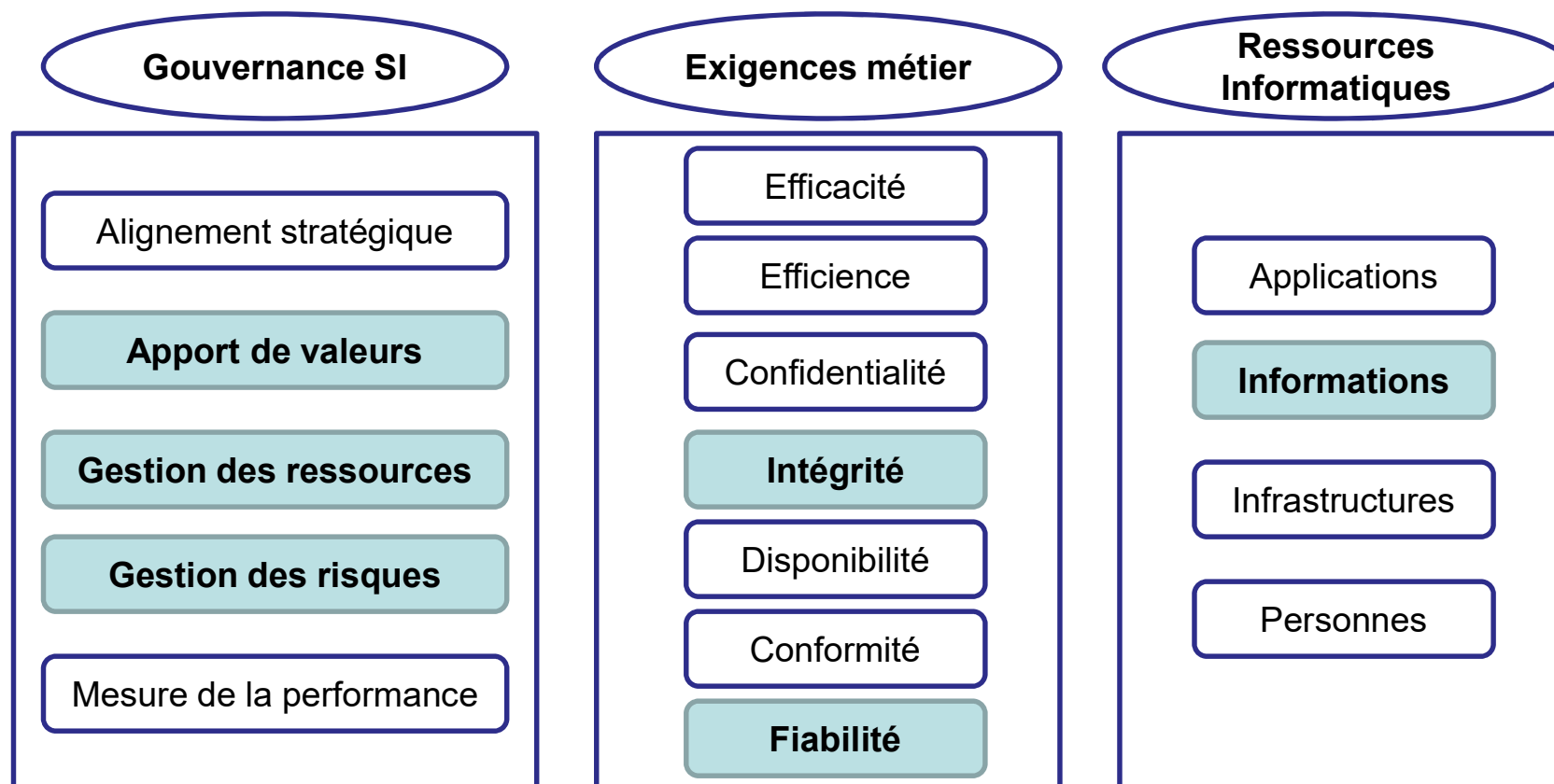
5 – CobiT – Description détaillée : Processus DS11

Les données constituent pour l'entreprise une valeur et un actif considérable qu'il faut impérativement gérer en termes de fiabilité, de protection et de conservation.

Cette gestion des données vise à garantir la qualité et la disponibilité des données métier au moment opportun.

La mise en valeur et la mise à disposition de toutes les informations constitue un apport essentiel pour les utilisateurs.

Il convient d'y associer la bonne gestion des risques de ces données.



5 – CobiT – Description détaillée : Processus DS11

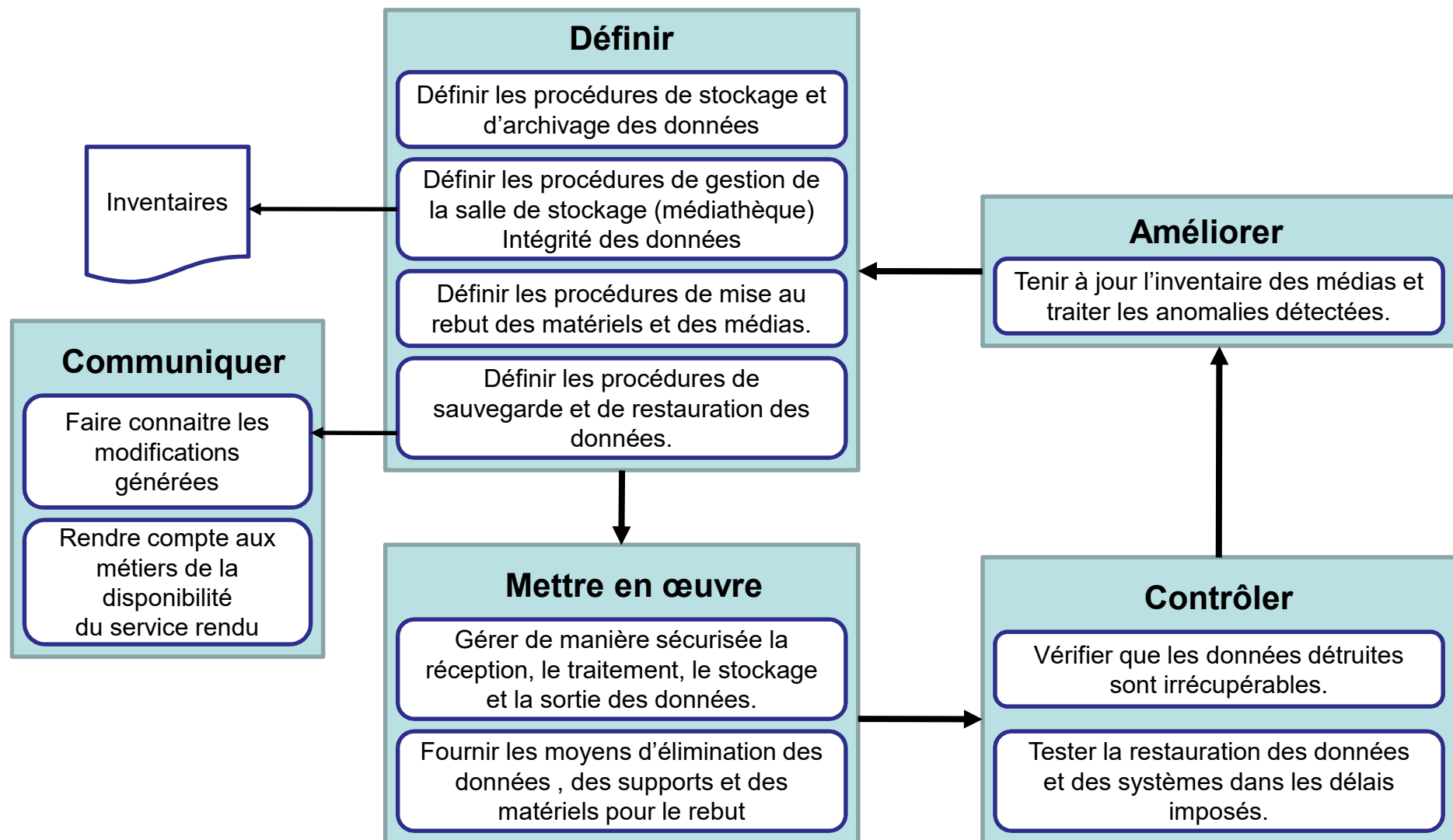
Pour les exigences métier il est bon de privilégier l'intégrité et la fiabilité des données.
Il convient de noter que la confidentialité, la disponibilité et la conformité seront prises en compte dans d'autres processus.

Par rapport aux 28 objectifs globaux ,le processus DS11 doit permettre de maitriser les objectifs suivants :

04	Optimiser l'utilisation de l'information
19	S'assurer que l'information critique et confidentielle n'est pas accessible à ceux qui ne doivent pas y accéder
27	Assurer la conformité de l'informatique aux lois et aux règlements.

5 – CobiT – Description détaillée : Processus DS11

La description suivante représente les flux internes du processus DS11.



5 – CobiT – Description détaillée : Processus DS11

Ce processus doit répondre à des exigences de sécurisation des données vis-à-vis des ressources informatiques (taille des B. d D., saturation médias, temps d'accès etc.) et aussi aux exigences métiers comme la durée de conservation, délais et modalités de restauration des données etc.).

Une attention doit être portée sur la destruction physique des données : supports et matériels.

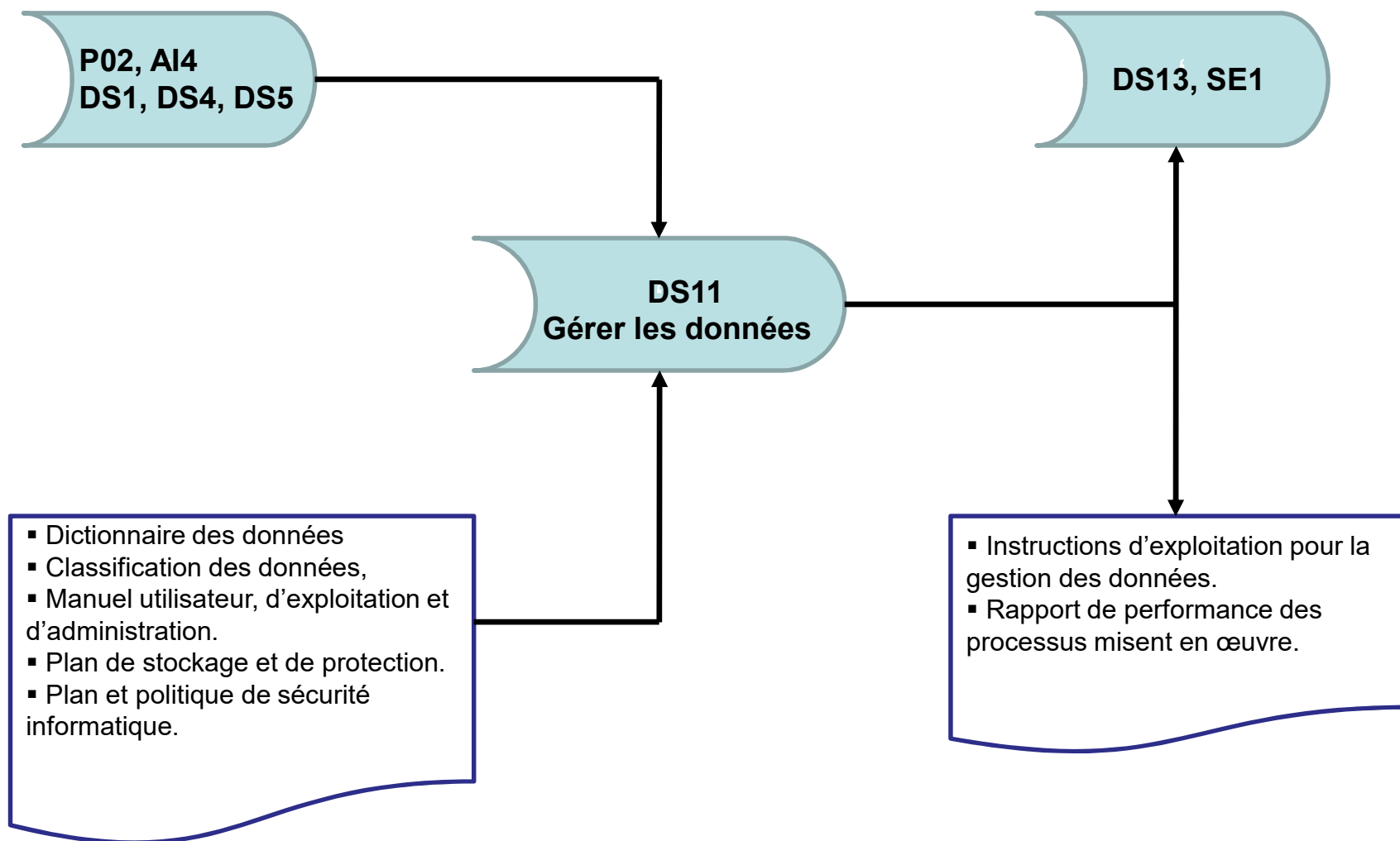
Cette rigueur doit impérativement passer par la mise en œuvre de procédures, de standards, ...

Ce processus doit aussi permettre le contrôle et la mesure de certaines opérations.

- Procédures de sauvegarde et d'archivage avec contrôle de la mise en œuvre et des résultats.
 - Mesure des incidents qui peuvent apparaître lors des traitements.
 - Vérification de la cohérence des données après opérations.
-
- Cette responsabilité des travaux exécutés dans ce processus est généralement supportée par le « Responsable d'exploitation ».

5 – CobiT – Description détaillée : Processus DS11

Les entrées sorties du processus DS11.



5 – Quelques sites sur le domaine de l'audit

www.afai.asso.fr (site de l'Association Française de l'Audit et du Conseil Informatiques)

<http://www.webtrust.fr> (site français de la certification des sites Web par les Expert-comptable: le réseau Web Trust)

<http://www.webtrust.net> (site du cabinet canadien Bennet Gold spécialisé dans la certification Web Trust)

<http://www.webtrust.org> (site international de la certification Web Trust)

<https://www.clusif.asso.fr> (site du Club de la Sécurité des Systèmes d'Information Français)

<http://www.isaca.org> (site américains de l'Information Systems Audit and Control Association & Fondation)

<http://www.cigref.fr> (site du Club Informatique des Grandes Entreprises Françaises)

<http://www.abrema.net> (site Australien sur l'audit basé sur une approche par les risques)

<http://www.cncc.fr> (site de la Compagnie Nationale des Commissaires aux Comptes)

www.crcp-paris.fr (site de la Compagnie Régionale des Commissaires aux Comptes de Paris)

www.cnejta.org (site de la Compagnie Nationale des Experts Judiciaires en Informatique et Techniques Associées)

<http://www.bibliotique.com> (site du centre de documentation des Experts-comptables & Commissaires aux Comptes)

www.oec-paris.fr (site du Conseil Régional Paris Ile de France de l'Ordre des Experts-comptables)

www.experts-comptables.fr (site du Conseil Supérieur de l'Ordre des Experts-comptables)

<http://www.acl.com> (site de la société canadienne éditeur du logiciel d'audit intégré ACL)

<http://www.auditware.net> (site de la société audiware éditeur d'un logiciel d'analyse de données: IDEA)

<http://www.theiia.org/itaudit> (site dédié aux outils informatiques pour l'auditeur)

<http://www.auditnet.org> (site dédié au partage des connaissances des auditeurs)

<http://www.cnil.fr> (site de la Commission Nationale de l'Informatique et des libertés CNIL)

<http://www4.gartner.com> (site de conseil stratégique et informatique)

<http://www.ifac.org> (site de l'International Federation of Accountants)

<http://www/aicpa.org> (site de l'American Institute of Certified Public Accountants)

<http://www.cica.ca> (site de l'Institut Canadien des Experts- Comptables)

<http://www.cima.org.uk> (site anglais du Chartered Institute of Management Accountants CIMA)