

# AMÉLIORATION CONTINUE NORMES ET RÉFÉRENTIELS

*Qualité, amélioration continue,  
normes, référentiels*

**UFR IM<sup>2</sup>AG**

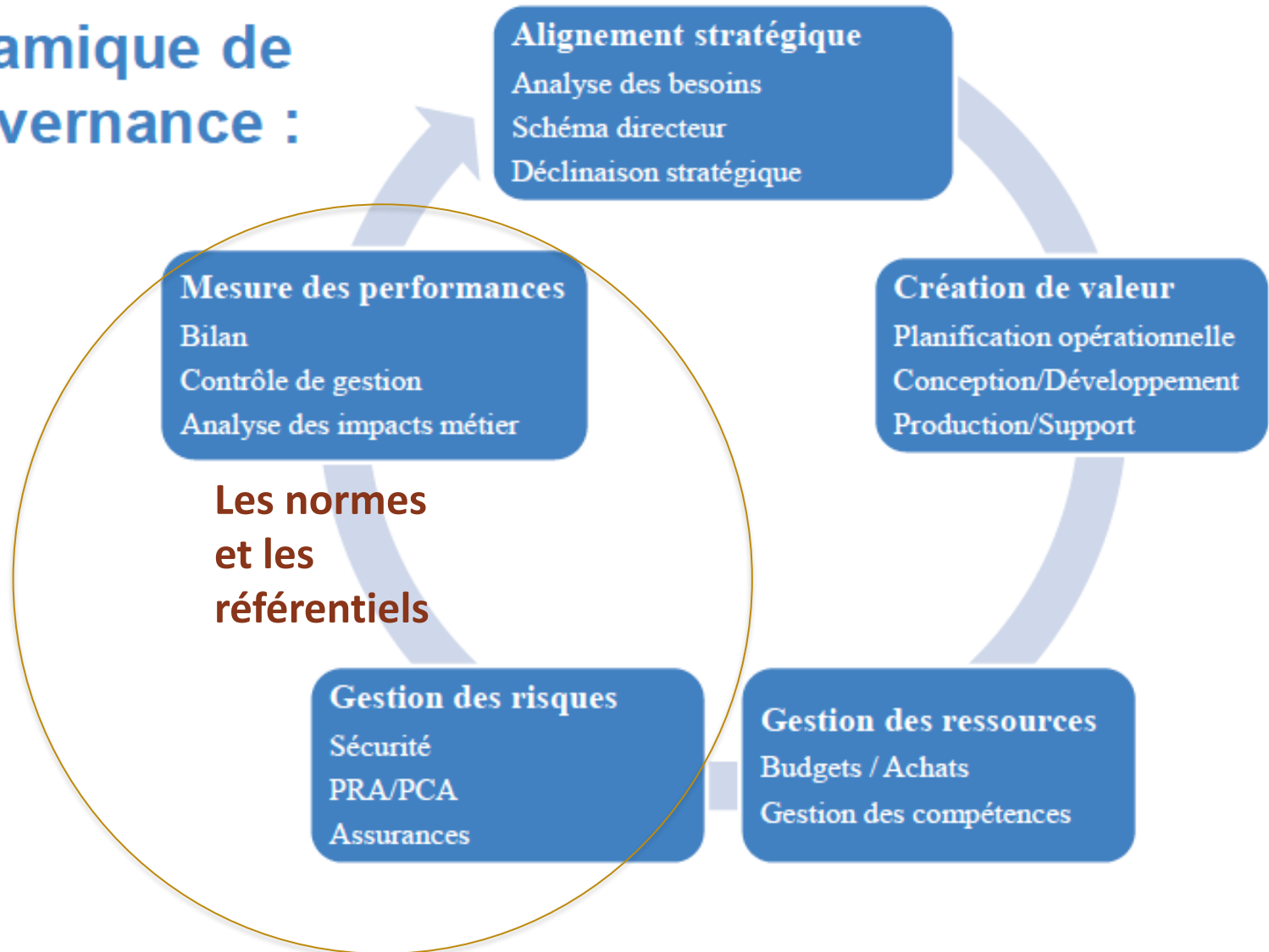
**UNIVERSITÉ  
Grenoble  
Alpes**

Luc Laurens  
Pr Christine Verdier

**MIAGE** RÉSEAU  
DES MIAGE  
DE FRANCE  
Grenoble

A venir....

## Dynamique de Gouvernance :



---

Élément clé de la performance

**QUALITÉ DU SI & AMÉLIORATION CONTINUE**

# Objectif des outils de qualité

---

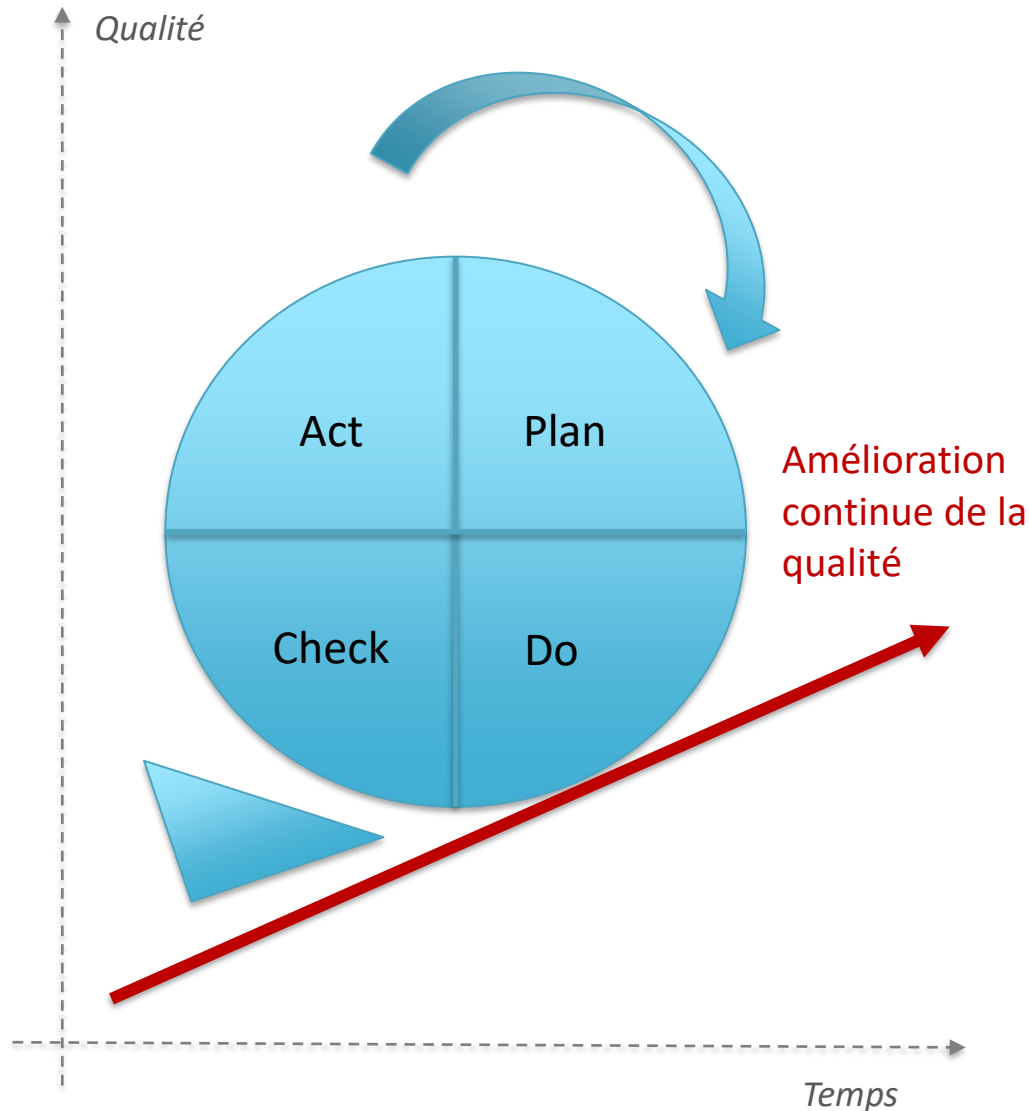
- ☑ Les normes, référentiels et les outils de mesure de la qualité du SI sont focalisés sur l'accroissement de la maîtrise des produits et services délivrés par la DSI dans la perspective de voir progresser régulièrement la satisfaction de toutes les parties prenantes du SI.
- ☑ Ces instruments ont en commun :
  - de contribuer à la construction du système de management de la DSI
  - De privilégier l'orientation client
  - De s'appuyer sur une vision prospective claire des objectifs poursuivis
  - De veiller à l'implication et la qualification du personnel
  - .... Dans une logique d'amélioration continue (performance des processus)

# Amélioration continue du SI

---

- ☑ L'amélioration continue vise à injecter régulièrement dans le système d'information les outils, méthodes, actions, matériels, processus, procédures, etc... utiles pour permettre d'augmenter dans le temps la valeur produite par le SI.
- ☑ L'amélioration continue est donc directement liée aux notions de qualité et performance.
- ☑ Elle se concrétise par des normes et des référentiels.

# Fondement de l'amélioration continue : la Roue de Deming



- ☑ **Plan** : Écrire ce que l'on va faire, c'est-à-dire organiser son plan de travail pour atteindre les objectifs
- ☑ **Do** : Mettre en œuvre le plan de travail et déployer les instruments du management
- ☑ **Check** : Mesurer et diagnostiquer les résultats et les écarts entre la prévision et la réalisation
- ☑ **Act** : entreprendre les actions correctives induites par les résultats observés précédemment.

- ☑ Un référentiel est une collection de bonnes pratiques sur un sujet donné. Lorsqu'un référentiel fait l'objet d'une large diffusion et qu'il est reconnu par le marché, on parle alors de standard. Les référentiels doivent être perçus comme une boîte à outils de laquelle l'entreprise extrait la bonne pratique dont elle a besoin pour résoudre un problème donné ou pour répondre à un besoin.

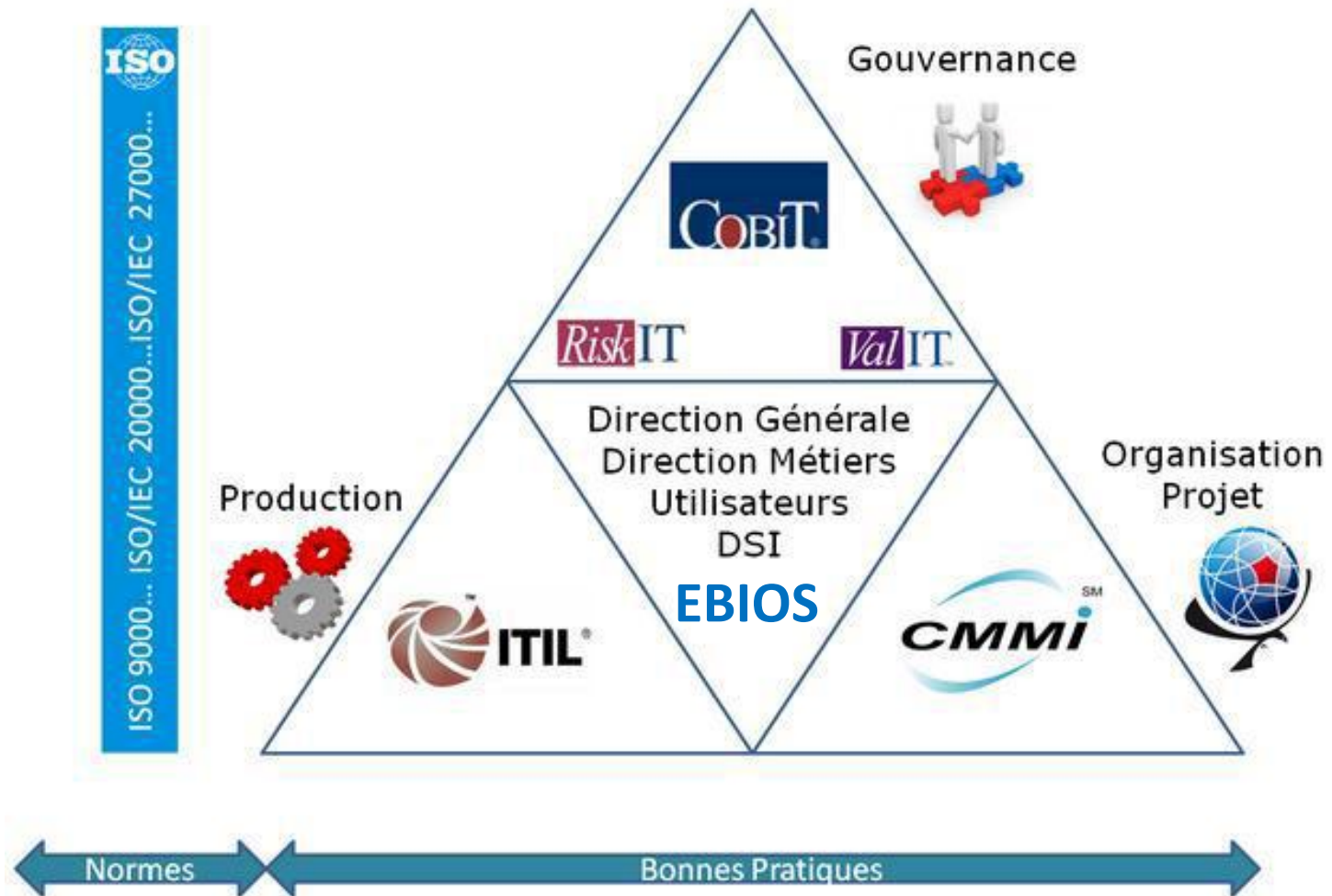
# Les référentiels et les normes

---

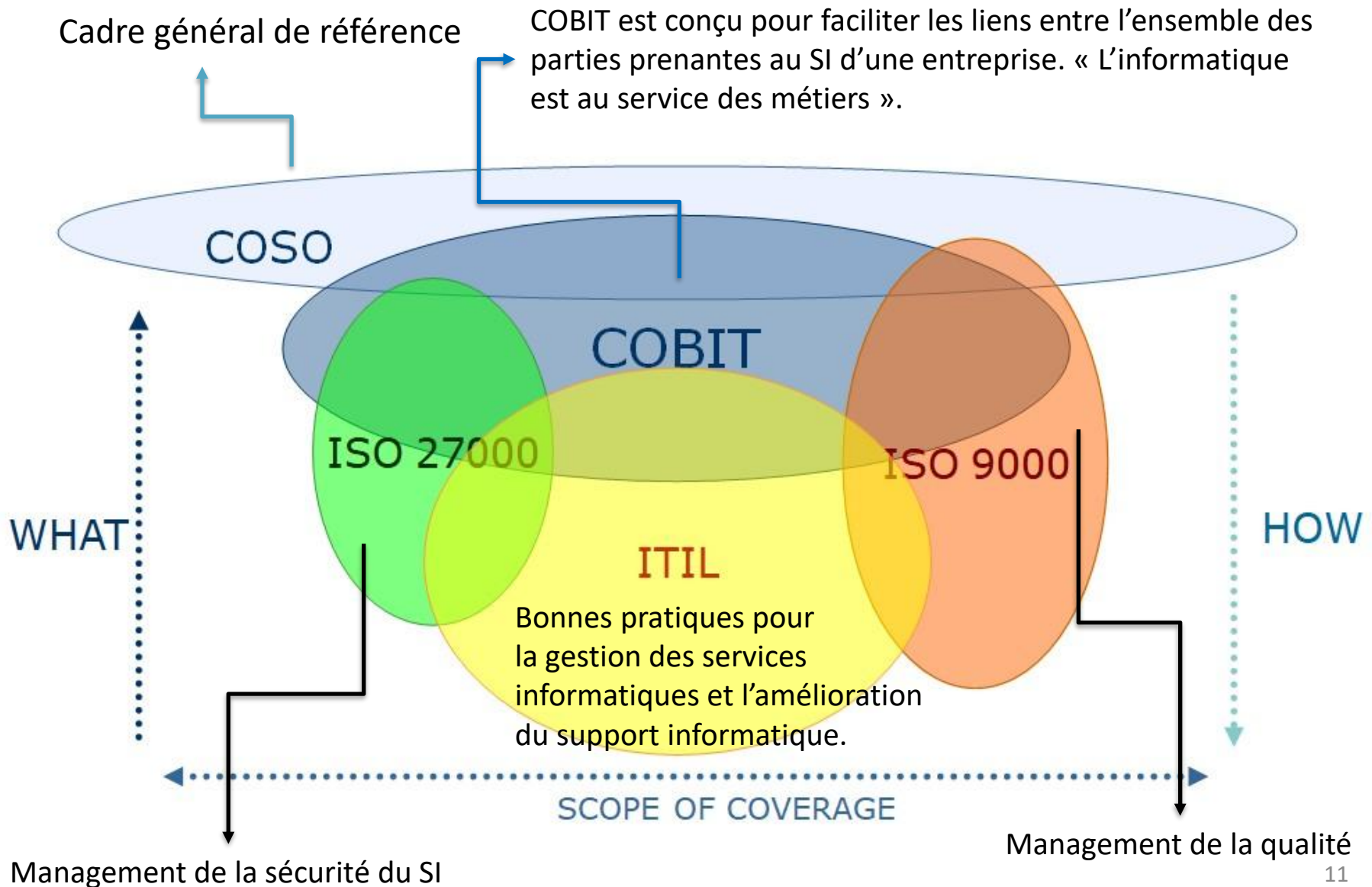
- ☑ La norme se différencie des référentiels dans la mesure où il s'agit d'un document édité par une instance de normalisation indépendante, par exemple l'ISO, faisant l'état de l'art d'un sujet donné (ex : ISO 27001 pour la sécurité de l'information). La norme peut aussi avoir un niveau de contrainte supplémentaire par rapport au référentiel.
- ☑ Les référentiels sont au cœur des processus de la DSI, car ils permettent aux DSI d'améliorer le degré de maîtrise de leur SI.



# Référentiels et bonnes pratiques



# Couverture des référentiels



# Référentiels et bonnes pratiques

---

- ☑ Une étude du CIGREF montre que les référentiels les plus utilisés par les grandes entreprises sont :
  1. ITIL : pour la gestion des services et du support
  2. ISO 27001 : pour la sécurité du SI
  3. Référentiel RH interne au CIGREF (pour la gestion des compétences)
  4. COBIT pour la gouvernance informatique.

---

Les normes

## **LES NORMES ISO**

- ☑ Organisation Internationale de Normalisation (International Organization for Standardization). Créée en 1947. 164 pays membres.
- ☑ But : unifier des standards sur des critères variés comme : la sécurité, la production, le transport, le management, l'environnement ou la qualité.
- ☑ Simplifie les échanges mondiaux et apporte une certaine qualité de service.
- ☑ Les normes sont comparables à une formule qui décrirait la meilleure façon de faire. Elles reposent sur les connaissances des experts dans leur domaine de prédilection.
- ☑ Normes sur le management de la qualité, sur le management de l'énergie, sur la sécurité de l'information, etc.



## **ISO 9000 — MANAGEMENT DE LA QUALITÉ**

Avec cette famille de normes, assurez-vous que les produits et les services que vous proposez répondent aux besoins des clients.



## **ISO/IEC 27001 — MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION**

La famille de normes ISO/IEC 27000 pour la sécurité de tous types d'informations numériques est conçue pour les organismes de toutes tailles.



## **NORMES DE SYSTÈMES DE MANAGEMENT**

Ces normes donnent un modèle à suivre pour mettre en place et utiliser un système de management. Apprenez-en plus sur leur fonctionnement et leur application.

## **ISO 31000 MANAGEMENT DU RISQUE**

Gérez les risques susceptibles de compromettre les performances de votre entreprise avec cette norme ISO.

- ☑ Système de **management de la qualité**
- ☑ La qualité s'analyse comme la conformité d'un produit aux exigences du client
- ☑ A pour objectif :
  - De spécifier les exigences à suivre pour définir, mettre en place, exploiter et améliorer un système de management de la qualité (SMQ) documenté.
- ☑ Norme généraliste : pas spécifiquement adaptée à l'IT.

## ☑ Les huit principes :

1. Orientation client : mécanismes d'écoute du client, mesure du niveau de satisfaction, réponse aux attentes
2. Leadership : définir une vision prospective claire pour impliquer pleinement le personnel dans la réalisation des objectifs
3. Implication du personnel : chacun a un rôle et une place
4. Approche processus : dans laquelle on identifie les buts à atteindre (<> de la vision procédure : description du chemin à suivre)
5. Management systémique : « le tout est plus grand que la somme des parties »
6. Amélioration continue : roue de Deming (voir ci-après)
7. Approche factuelle pour la prise de décision : les décisions efficaces sont basées sur l'analyse de données objectives et d'informations tangibles
8. Relation mutuellement bénéfique avec les fournisseurs : les organisations et leurs fournisseurs sont interdépendants, dès lors une relation mutuellement bénéfique améliore la capacité des fournisseurs à créer de la valeur.



- ☑ Technologie de l'information – Gestion des services
  - Famille ISO 20000-1: 2018 : Exigences du système de management des services (SMS).
  - Famille ISO 20000-2: 2012 : Guide pour l'application du SMS
- ☑ Objectifs : Garantir la fiabilité des services afin d'en permettre sa continuité.

# ISO 20000-1: 2018

---

- ☑ Elle spécifie les exigences destinées aux fournisseurs de services pour planifier, établir, implémenter, exécuter, surveiller, passer en revue, maintenir et améliorer un système de management des services (SMS).
- ☑ Les exigences incluent la conception, la transition, la fourniture et l'amélioration des services afin de satisfaire aux nécessités de service.
- ☑ Exemples d'utilisation :
  - Exigence du client lors d'un appel d'offre (facilite les comparaisons entre prestataires)
  - Organisme qui souhaite une cohérence de vue pour tous ses fournisseurs de service
  - Service interne qui veut offrir la visibilité et la transparence sur son offre.
  - Approche globale de l'entreprise (certification processus métier qui implique également les services informatiques requis).

- ☑ **SMSI : Système de Management de la Sécurité de l'Information**
  - 27001 : Définition des exigences pour un SMSI, et pour les organismes certifiant les systèmes.
  - 27003 : Soutien direct pour l'implémentation, recommandations détaillées et/ou interprétation des processus, modèle PDCA
  - 27004 : Définition des indicateurs
  - 27003 : Implémentation de la norme
  - 27005 : Gestion des risques
  - 27006 : Evaluation et conformité d'un SMSI
- ☑ La norme peut s'appliquer à tous les types et à toutes les tailles d'organisations : Entreprises commerciales (PME/ETI/Grands groupes/multinationales), organisations publiques, associations et organisations à but non lucratif.....

# Norme ISO 27001

---

- ☑ ISO/IEC 27001 est la norme la plus connue au monde en matière de **systèmes de management de la sécurité de l'information (SMSI)**. Elle définit les exigences auxquelles un SMSI doit répondre.
- ☑ Elle fournit aux entreprises de toutes tailles, quel que soit leur secteur d'activité, des lignes directrices pour l'établissement, la mise en œuvre, la tenue à jour et l'amélioration continue d'un système de management de la sécurité de l'information.
- ☑ La conformité à ISO/IEC 27001 signifie qu'une organisation ou une entreprise a mis en place un système pour gérer les risques liés à la sécurité de ses données ou des données qu'elle est amenée à traiter, et que ce système est conforme aux bonnes pratiques et principes énoncés dans cette Norme internationale.
- ☑ Un système de management de la sécurité de l'information conforme aux exigences d'ISO/IEC 27001 garantit la confidentialité, l'intégrité et la disponibilité de l'information au travers d'un processus de management du risque et donne aux parties intéressées l'assurance que les risques sont gérés de manière adéquate.

# Norme ISO 27001 : critères essentiels

---

## 1. Confidentialité

→ *Signification* : Seules les bonnes personnes ont accès aux informations détenues par l'organisation.

⚠ *Exemple de risque* : Des criminels s'emparent des identifiants de connexion de vos clients et les revendent sur le Darknet.

## 2. Intégrité de l'information

→ *Signification* : Les données utilisées par l'organisation dans le cadre de ses activités ou celles dont elle assure la sécurité pour d'autres sont stockées de manière fiable et ne sont ni effacées, ni endommagées.

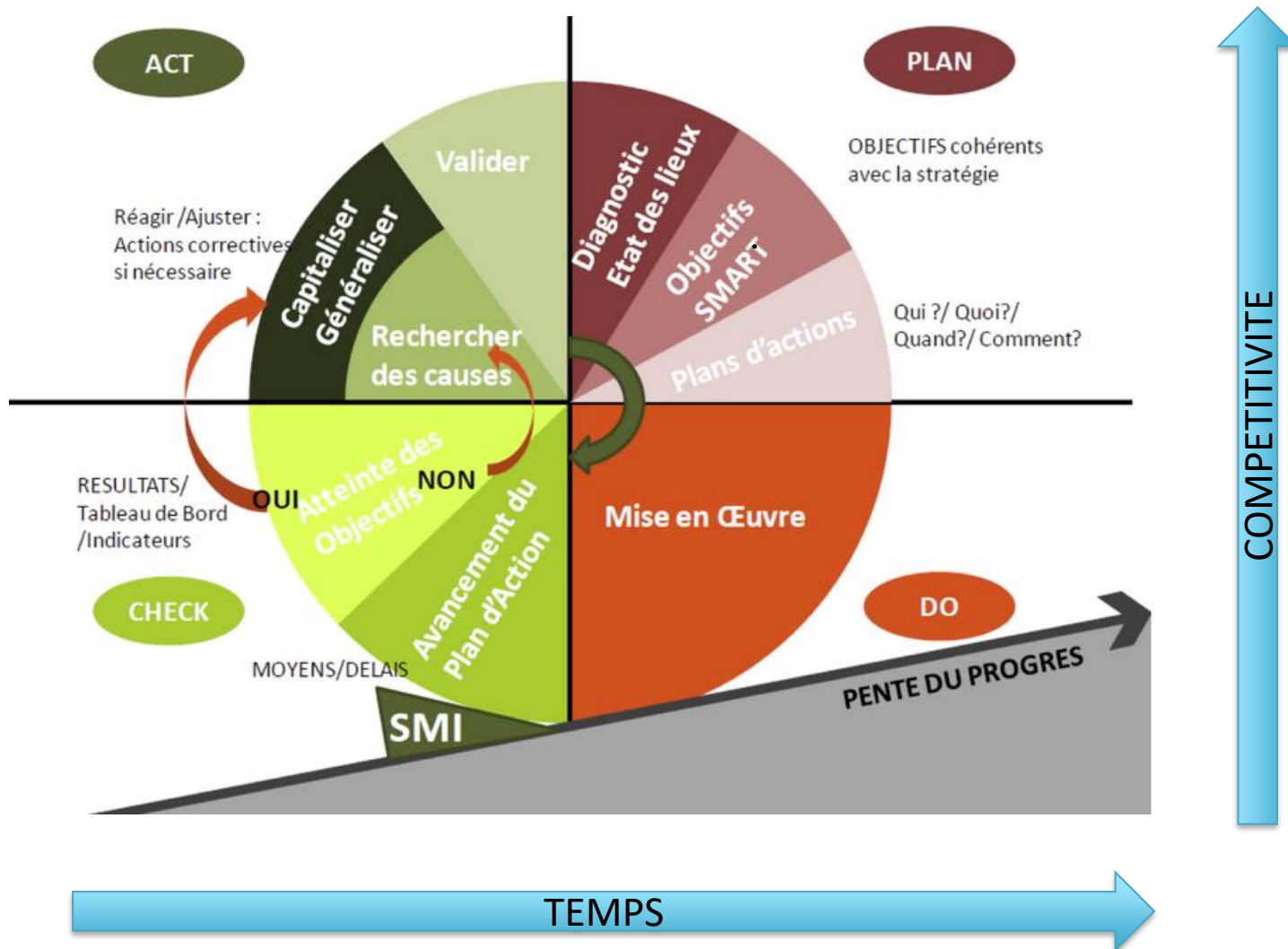
⚠ *Exemple de risque* : Un employé supprime accidentellement une ligne lors du traitement d'un fichier.

## 3. Disponibilité des données

→ *Signification* : L'organisation et ses clients ont accès aux informations à tout moment afin de répondre aux objectifs opérationnels et aux attentes des clients.

⚠ *Exemple de risque* : La base de données de votre entreprise est indisponible en ligne en raison de problèmes liés aux serveurs et de lacunes en termes de sauvegarde.

# Amélioration continue



# Références

---

- ✓ BNP Paribas : ISO 9001, 20000, 27000, 14001 (environnement), 26000 (RSE).
- ✓ Française des jeux : ISO 27000 (janvier 2009)
- ✓ Crédit Agricole (private banking) : ISO 9001, 27001
- ✓ Orange Business Services (périmètre Cloud) : ISO 27000 (datacentre : Val de Reuil, Rueil, Chevilly, sites : Cesson, Lyon, Boulogne, etc...)
- ✓ Solucom : ISO 27000 (prestation d'audit).
- ✓ Cisco (produits et solutions) : ISO 27000 (valable de mars 2019 à Février 2020).
- ✓ Avaya (Private Cloud Services) 2015 : ISO 27000.
- ✓ Juniper (ISO 9001).

## Remarques :

Vigilance sur les périmètres de certification et les dates.

Certification nécessaire sur la chaîne complète (sous-traitance incluse).

---

## Information Technology Infrastructure Library

**ITIL®**



- ☑ ITIL : Information Technology Infrastructure Library
- ☑ Référentiel international dédié à la gestion des services informatiques
- ☑ Ensemble cohérent et complet des meilleures pratiques
- ☑ Expérience collective d'acteurs publics ou privés
- ☑ Démarche de management par processus
- ☑ ..... de facto un standard reconnu !

- ✓ ITIL est un ensemble de bonnes pratiques permettant de gérer les services IT (une application, un site web ou tout « produit » numérique fourni par l'entreprise).
- ✓ Principe de base : considérer l'IT comme un service et appliquer des pratiques cohérentes tout au long du cycle de vie de ce service.
- ✓ 5 grandes lignes directrices :
  - ITIL service strategy : définit les objectifs métier et les besoins des clients
  - ITIL services design : montre comment transformer les stratégies en plans concrets au sein de l'entreprise
  - ITIL service transition : indique comment introduire les services et les changements dans l'environnement de production
  - ITIL service operation : délivrer les services au bon niveau de qualité et de coût
  - ITIL continual service improvment : amélioration continue des services

# ITIL : lignes directrices

---

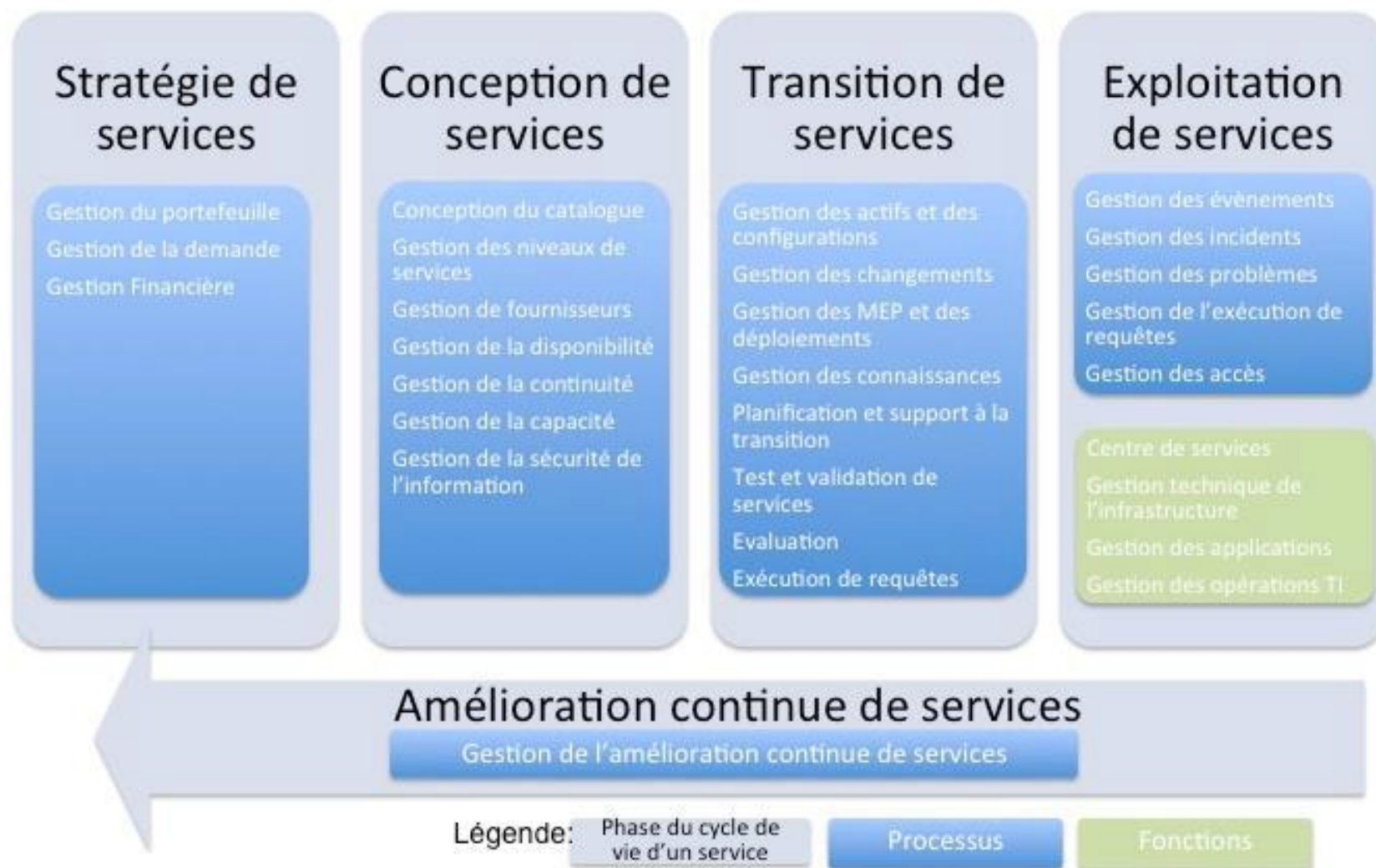
- ☑ ITIL Service Strategy
  - Stratégie des services / 5 processus
  - Définit les objectifs métier et les besoins des clients
- ☑ ITIL Services Design
  - Conception des services / 8 processus
  - Montre comment transformer les stratégies en plans concrets au sein de l'entreprise
- ☑ ITIL Service Transition
  - Transition des services
  - Indique comment introduire les services et les changements dans l'environnement de production
- ☑ ITIL Service Operation
  - Exploitation des services
  - Délivrer les services au bon niveau de qualité et de coût
- ☑ ITIL Continual Service Improvement
  - Amélioration continue des services

- ✓ ITIL a été publié dès 1989 par l'Agence Centrale de l'Informatique et des Télécommunications du gouvernement britannique.
- ✓ L'OGC (Office of Government Commerce) est officiellement en charge d'ITIL et de son développement.
- ✓ ITIL V2 : organisé autour de 8 domaines
- ✓ ITIL V3 - 2007: organisé autour de 5 domaines avec périmètre étendu à la satisfaction de services métiers.
- ✓ ITIL V4 – 2019 : nouvelle version pour mieux coller aux mouvances DevOps et Agile.
- ✓ **Principe** : considérer l'IT comme un service et appliquer des pratiques cohérentes tout au long du cycle de vie de ce service.

# Certification ITIL

---

- ☑ Les certifications ITIL sont des certifications individuelles
- ☑ Il existe 4 niveaux de certification
  - Foundation Certificate= premier niveau / 2 à 3 j de formation + QCM chez un formateur accrédité
  - Intermediate Lifecycle/ Intermédiaire Capacity= niveaux intermédiaires cycle de vie des services / gestion des services – systèmes de «crédits» pour passage au niveau suivant
  - Expert's certificate= formation spécifique Managing Across the Lifecycle+ QCM
  - Master qualification = expert avec 5 ans d'expérience dans le management de services / dossier de candidature + soutenance devant un jury

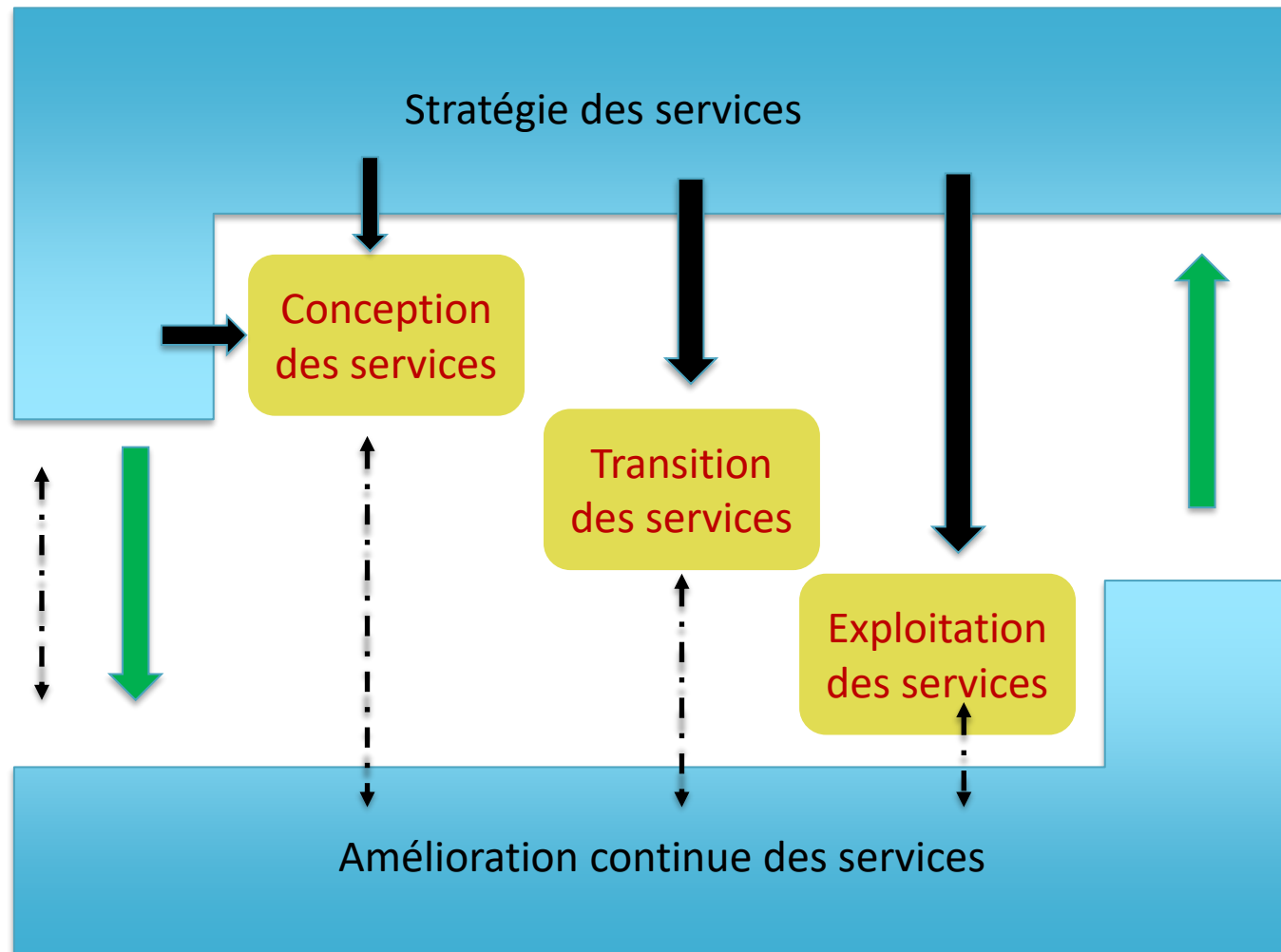


- ☑ Un service est un moyen de générer de la valeur pour un client en facilitant la réalisation de ses objectifs sans y ajouter la prise de risque.
- ☑ Fonctionnalité (niveau de performance, suppression ou allègement de contraintes, etc.) + garantie (disponibilité, capacité, continuité de service, sécurité, etc.) = VALEUR

- ☑ Un service, c'est la résultante des actions d'un fournisseur afin de livrer ce qui a été convenu.
- ☑ La satisfaction face à un service dépend grandement des expériences passées du client, des utilisateurs et de leurs attentes.
- ☑ **Exemples de services** : service de messagerie électronique, application de gestion d'un annuaire, application métier spécifique, service d'impression, etc.



# Phases du cycle de vie



➡ Guide de bonnes pratiques

↔ Amélioration et retour



Cycle de vie des services

## Stratégie de services

Gestion du portefeuille  
Gestion de la demande  
Gestion Financière

## Conception de services

Conception du catalogue  
Gestion des niveaux de services  
Gestion de fournisseurs  
Gestion de la disponibilité  
Gestion de la continuité  
Gestion de la capacité  
Gestion de la sécurité de l'information

## Transition de services

Gestion des actifs et des configurations  
Gestion des changements  
Gestion des MEP et des déploiements  
Gestion des connaissances  
Planification et support à la transition  
Test et validation de services  
Evaluation  
Exécution de requêtes

## Exploitation de services

Gestion des événements  
Gestion des incidents  
Gestion des problèmes  
Gestion de l'exécution de requêtes  
Gestion des accès

Centre de services  
Gestion technique de l'infrastructure  
Gestion des applications  
Gestion des opérations TI

## Amélioration continue de services

Gestion de l'amélioration continue de services

Légende: Phase du cycle de vie d'un service

Processus

Fonctions

# Stratégie de services

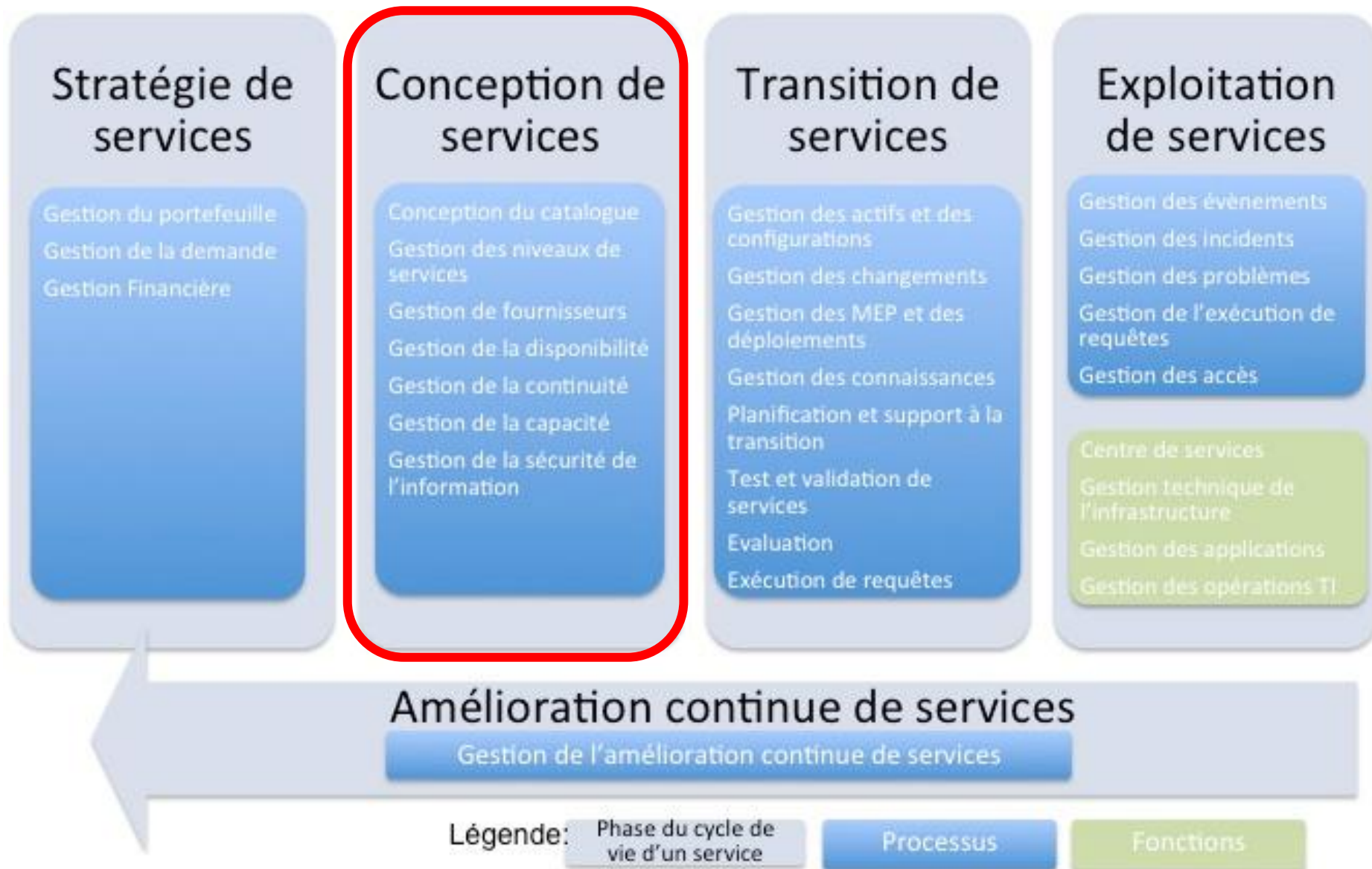
---

- ☑ La stratégie des services ITIL est une phase orientée marché. Elle aide les organisations à déterminer les types de services qu'elles doivent offrir et les marchés à cibler. L'objectif est de prendre des décisions stratégiques lors de la planification et de la fourniture de services ciblés afin de favoriser la croissance et la réussite à long terme.

# Stratégie de services

---

- ☑ Dans la phase de stratégie des services, le fournisseur de service informatique établit une stratégie :
  - En gérant les exigences métier
  - En la traduisant en une stratégie de livraison de services
  - En validant les coûts
  - En introduisant le service dans un portefeuille de services.
- ☑ A ce stade, l'organisation (la DSI) mobilise des ressources. Elle ne fournit pas de valeur à l'entreprise.



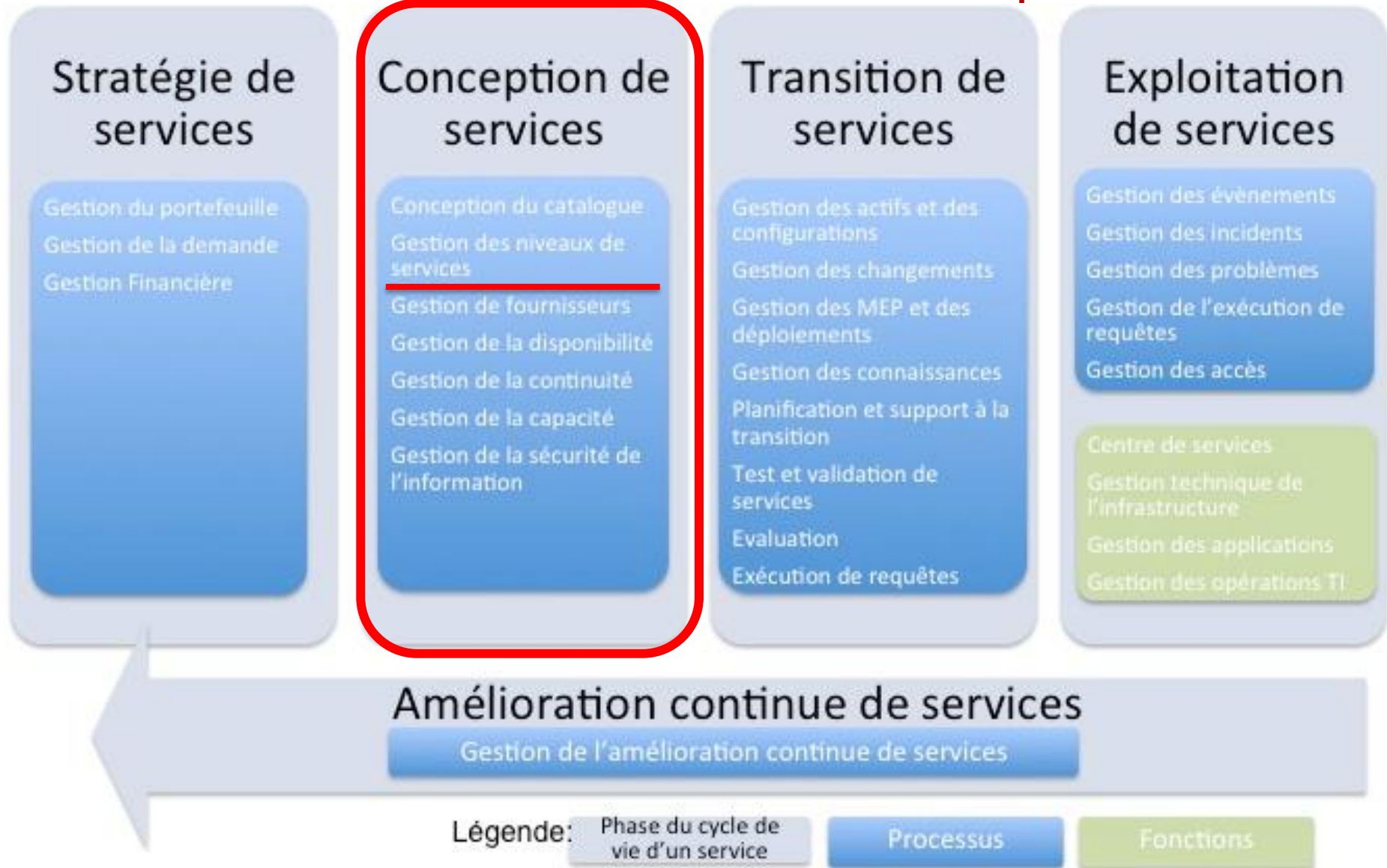
# Conception de services

---

- ☑ Au cours de cette deuxième phase, lorsqu'une stratégie a été définie, l'organisation IT commence à concevoir le service :
  - En établissant les exigences des niveaux de service
    - Les accords de niveaux de services (SLA: Service Level Agreements) définissent des objectifs spécifiques sur lesquels les performances des services sont jugées. La gestion des niveaux de services (SLM: Service Level Management) maintient et améliore la qualité des services IT à travers un cycle permanent d'accords, de suivis, de rapports statistiques sur l'atteinte des objectifs.
  - En étudiant la capacité
    - La gestion des capacités (capacity management) prend en charge l'ajustement de la capacité de l'infrastructure des SI vis-à-vis des demandes des organisations métiers (équilibre coût/capacité et offre/demande).
  - En étudiant la disponibilité
    - La gestion de la disponibilité permet d'optimiser la capacité de l'infrastructure informatique, des services et de l'organisation de support.
  - En gérant la sécurité
    - Il s'agit de protéger les intérêts de l'organisation qui s'appuient sur des données et des infrastructures (flexibilité, continuité opérationnelle, ouverture → augmentation menaces)



# ITIL : Gestion de la disponibilité



# ITIL : gestion des niveaux de services

---

## ☑ Objectif :

- Formaliser de façon contractuelle la relation client/fournisseur entre les bénéficiaires des services et la DSI en définissant bien les périmètres, les engagements réciproques et les niveaux de service attendus.

## ☑ Bénéfices :

- Assurer une meilleure définition et compréhension des besoins en termes de services métiers
- Favoriser l'équilibre optimal entre les exigences en termes de qualité de niveau de service et les coûts d'investissement et d'exploitation
- Etablir des critères de mesure objectifs et sans ambiguïté pour la qualité des services.



# Gestion des niveaux de services : vocabulaire

---

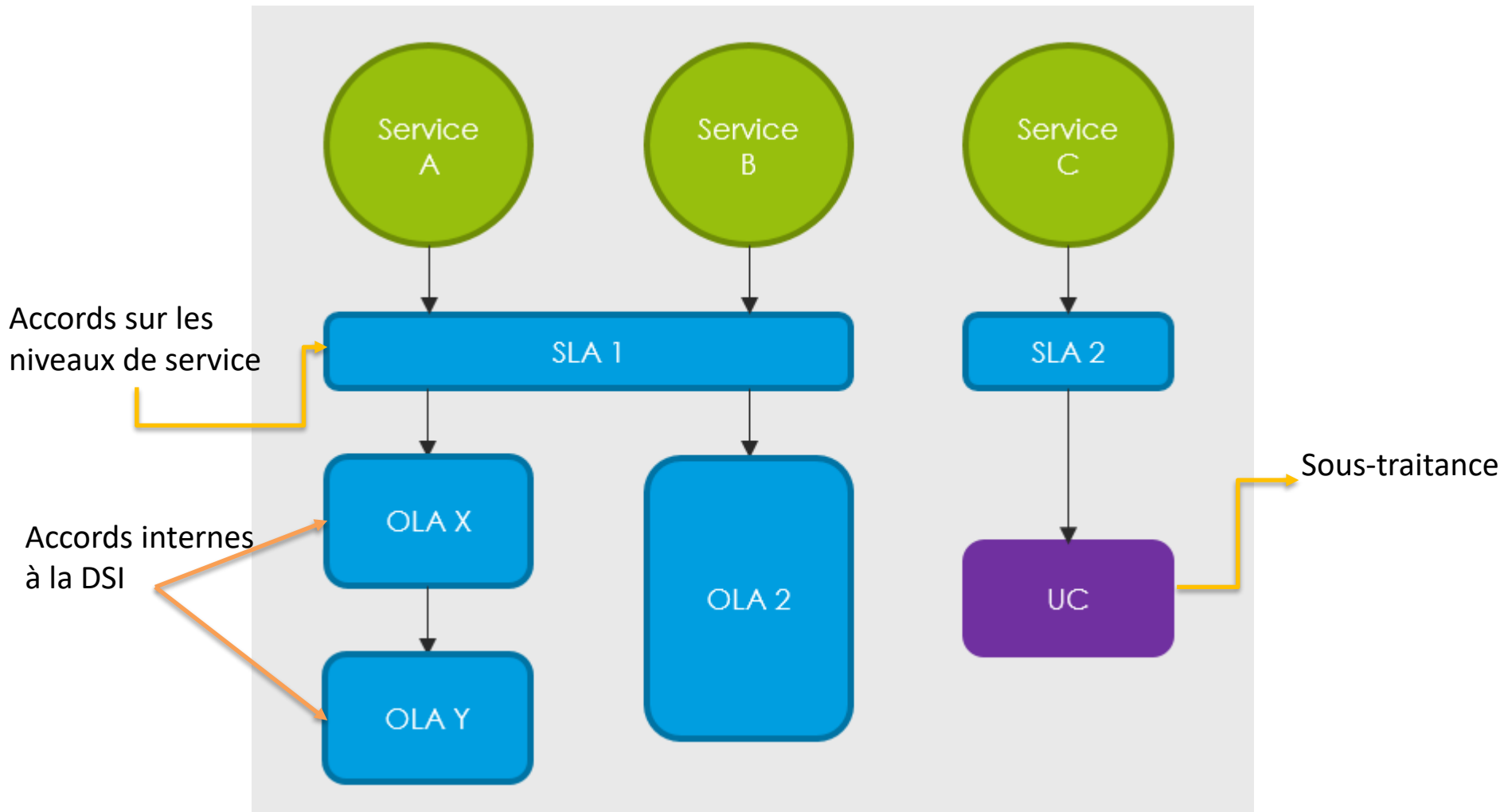
## ☑ Formalisation :

- SLR : Service Level Requirement (exigences clients, servent de base à la rédaction des SLA)
- **SLA : Service Level Agreement (accords entre client et fournisseur sur les niveaux de service)**
- SIP : Service Improvement Program (cible d'amélioration)
- SLM : Service Level Management
- OLA : Operational Level Agreement (accords internes à la DSI)
- UC : Underpinning Contract (contrat de sous-traitance)

## ☑ Indicateurs clés

- MTBF : Temps moyen entre défaillances
- MTTR : Temps moyen de réparation
- MTTF : Temps moyen de fonctionnement avant une panne
- $(MTBF = MTTF + MTTR)$

# ITIL : gestion des niveaux de services



# ITIL : gestion des niveaux de services

---

## ☑ Activités

- Produire et maintenir le catalogue de services
- Négocier et signer les niveaux (contrats) de service : SLR (exigences clients), OLA (accords internes DSI), UC (sous-traitance), SLA (accords clients-fournisseurs)
- Mesurer et comparer le niveau de service réel aux objectifs fixés
- Maintenir les niveaux de service en accord avec les besoins métiers, conformément à leurs évolutions
- Coordonner les autres opérationnels et fournisseurs

# ITIL : gestion des niveaux de services

SLR: exigences client

SLA : accord C/F sur niveaux de service

SLM : gestion niveau service

OLA : accords internes

UC : sous-traitance

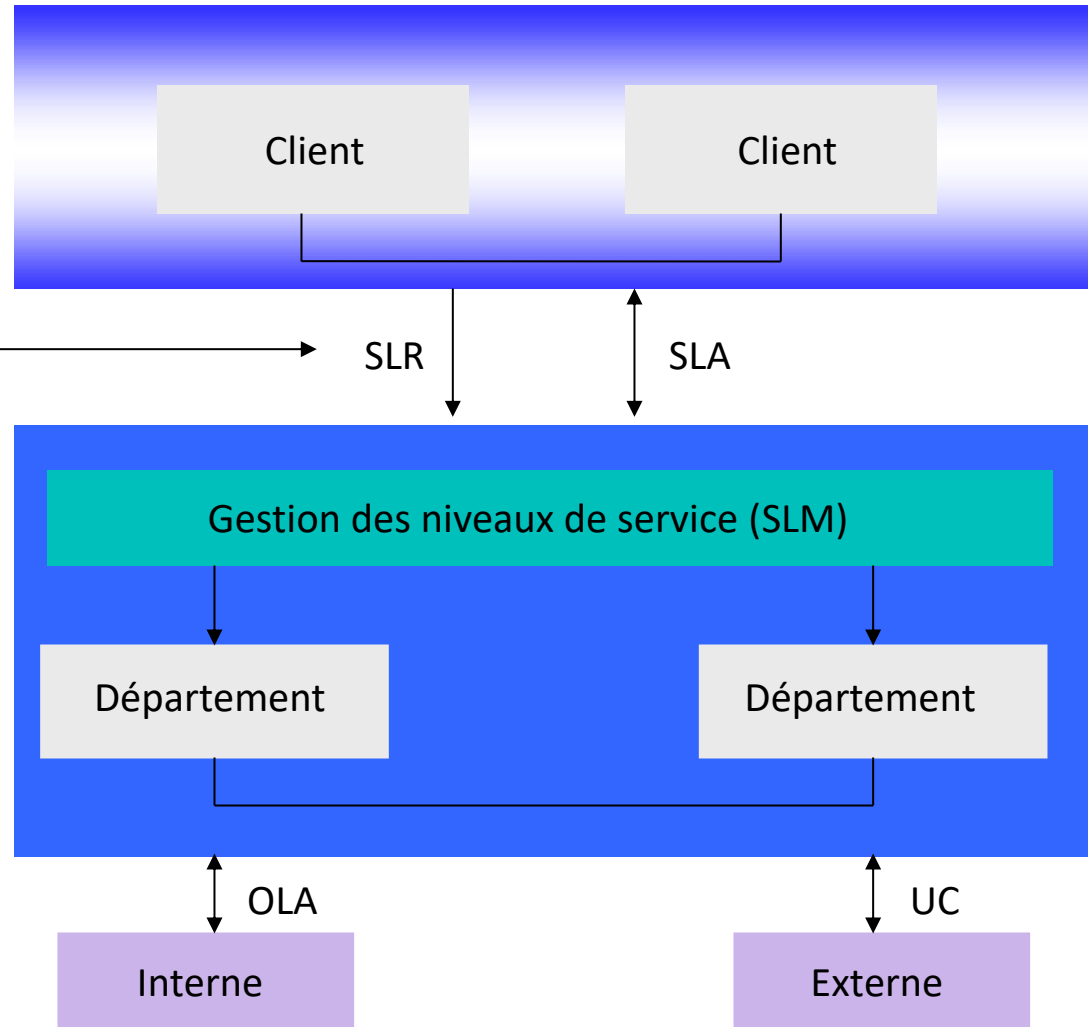
Clients

Catalogue  
de services

DSI

Stop!

Fournisseurs



# Notions clé du SLA (1/2)

- ☑ Description de l'accord
  - Description des services couverts
  - périmètre de l'Accord : couvert/ exclu
  - dates : début, fin, revue
  - responsabilités Fournisseurs / Clients
  - Modalités de modification du document
- ☑ Heure de service
  - Heures normales de service (et jours)
  - Demandes d'extension des heures de couverture (combien de temps à l'avance)
  - Heures et jours spéciaux (jours fériés)
  - calendrier du service
- ☑ Conditions spéciales (closing, fin de mois)
- ☑ Restrictions
  - Nb max d'utilisateurs/ transactions

- ☑ Support
  - Horaire du Service Desk
  - Extension des heures de support
  - Heures et jours spéciaux (jours fériés)
  - Délais de prise en compte, de résolution.
  - Temps maximum de réponse
  - Temps max de résolution des Incidents/ priorité
- ☑ Description des procédures d'évaluations
- ☑ Tableaux de bord et indicateurs
- ☑ Prix et facturation
  - Détail de la périodicité et formules de calcul
  - Pénalités/ Bonus concernant l'Accord
- ☑ Accord des parties

# Notions clé du SLA (2/2)

- ☑ Disponibilité
  - % disponibilité en heures de service
  - Définir les périodes d'indisponibilité maximale acceptables
  - Nb maximum d'interruption
  - Durée maximale d'une interruption
  - Nb de postes disponibles
- ☑ Fiabilité
  - Exprimé comme le nb maximum de ruptures de service ou le temps moyen entre les ruptures (MTBF) ou le temps moyen entre incidents systèmes (MTBSI)

- ☑ Capacité
  - Débit, flux, nb d'accès normaux
  - Performance
    - Temps de réponse
    - Nb de commandes ou transactions
  - Heures début/fin pour traitements batch\*
- ☑ Sécurité et plan de secours
  - Description, déclenchement, acteurs
  - Détail des objectifs de performance des services (fonctionnement en dégradé lors d'un Plan de Continuité)
  - Aspects sécurité, notamment les obligations des utilisateurs (sauvegarde des PCs non gérés par la production, changement régulier des mots de passe).

# Exemple SLA (service paie)

- ☑ Description des services couverts
  - Imprimer les feuilles de paie
  - Archiver pendant 5 ans (légal)
  - Établir bilan social (sécurité sociale)
  - Établir K7 (banque)

- ☑ Disponibilité
  - Du 01 au 21 : 80% des heures ouvrables
  - Du 22 au 27 : 100% des heures ouvrables
  - Du 28 à la fin du mois : 30% des heures ouvrables

- ☑ Continuité
  - Reprise sous 3 jours à 50%
  - Reprise sous 5 jours à 75%
  - Reprise sous 10 jours à 100%

- ☑ Performance
  - Du 22 au 27 : 600 transactions par heure
- ☑ Assistance
  - Service Desk, : 0800 01 13 13 de 8h à 20h hors samedi/ dimanche et jours fériés
- ☑ Capacité
  - Imprimer toutes les feuilles de paie en 2 jours à partir du 22 du mois
  - Établir bilan social en 2 heures le 26
  - Établir K7 en 2 heures avant fin du mois
- ☑ Prix et facturation
  - 0,10 € par feuille de paie
  - 2 € par K7
  - 20 € par bilan social

# Indicateurs SLA

---

## Performance

- Nombre d'appels
- Typologie des appels
- Durée des appels
- Productivité par niveau
- % de résolution
- Délai de résolution
- % escaladés
- Coût total
- Coût par appel
- Coût total du support
- Benchmarking sur l'ensemble

## Qualité de service

- Temps moyen avant décrochage
- % en moins de 20 secondes
- % de dissuadés
- % de résolution en direct
- % de résolution (ou réalisation) dans les délais contractuels

## Défaillances

- Récurrence des appels
- Taux de rappels
- Analyse de criticité
- Typologie des causes
- MTBF (temps moyen de bon fonctionnement)
- MTTR (temps moyen de réparation)
- MTTF (temps moyen de fonctionnement avant une panne)



# ITIL : Gestion des niveaux de service

---

## ☑ Facteurs de réussite :

- Pensez client (ou bénéficiaire)
  - Le contrat est la base d'une culture client !
- Construire les contrats de service sur des critères métier et en évitant le jargon technique (exprimer clairement les besoins métier en termes de services attendus)
- Aligner les contrats internes OLA et externes UC (sous-traitance) sur les niveaux de service (veiller à la bonne appropriation des engagements pour les acteurs internes)
- Distinguer SLM (processus) et SLA (contrat)
- Pas d'engagement SLA sans SLM
- Appropriation des engagements par le client également (droits et devoirs, « un bon client fait un bon fournisseur »)
- Et bien sûr, les moyens techniques et financiers en face sinon on ne gère que des conflits.