

# Synthèse Service Manager Service SUPPORT

ITIL version 2  
[www.ital.fr](http://www.ital.fr)

Version 1.0

Référence : Synthèse Service Manager ITIL version 2  
Référence : Service SUPPORT

Date : 24/11/2010

## SOMMAIRE

<b>1.</b>	<b>SERVICE SUPPORT .....</b>	<b>3</b>
1.1.	BUT DE LA GESTION DE SERVICES.....	3
1.2.	SERVICE DESK .....	3
1.2.1.	Objectifs .....	3
1.2.2.	Processus .....	4
1.2.3.	Activités .....	4
1.2.4.	Implémentation .....	5
1.2.5.	Divers .....	5
1.3.	GESTION DES INCIDENTS.....	6
1.3.1.	Objectifs .....	6
1.3.2.	Processus .....	6
1.3.3.	Activités .....	8
1.3.4.	Implémentation .....	10
1.3.5.	Divers .....	10
1.4.	GESTION DES PROBLEMES .....	11
1.4.1.	Objectifs .....	11
1.4.2.	Processus .....	11
1.4.3.	Activités .....	12
1.4.4.	Implémentation .....	13
1.4.5.	Divers .....	14
1.5.	GESTION DES CONFIGURATIONS .....	15
1.5.1.	Objectifs .....	15
1.5.2.	Processus .....	15
1.5.3.	Activités .....	16
1.5.4.	Implémentation .....	18
1.5.5.	Divers .....	19
1.6.	GESTION DES CHANGEMENTS .....	20
1.6.1.	Objectifs .....	20
1.6.2.	Processus .....	20
1.6.3.	Activités .....	21
1.6.4.	Implémentation .....	25
1.6.5.	Divers .....	25
1.7.	GESTION DES MISES EN PRODUCTION (VERSION).....	26
1.7.1.	Objectifs .....	26
1.7.2.	Processus .....	26
1.7.3.	Activités .....	28
1.7.4.	Implémentation .....	29
1.7.5.	Divers .....	31
<b>2.</b>	<b>LEXIQUE.....</b>	<b>32</b>

# 1. Service Support

## 1.1. But de la gestion de services

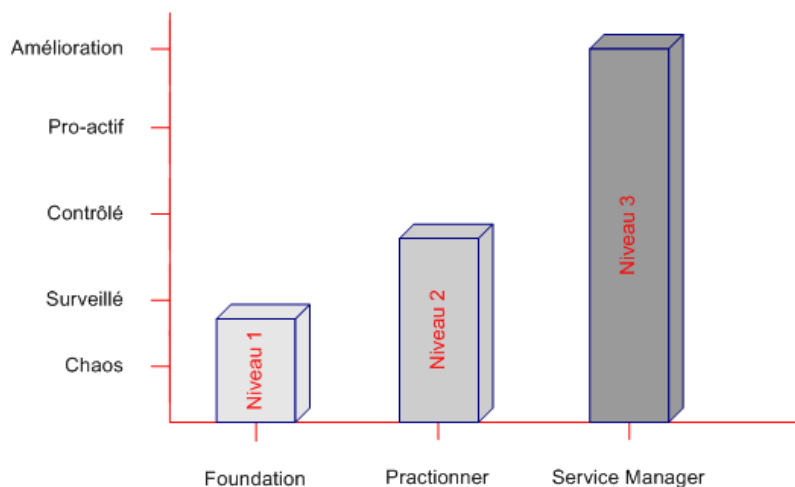
---

Pourquoi :

- Professionnaliser l'activité
- Se concentrer sur les bénéfices pour les clients
- Mesurer pour décider
- Définir des points de contacts clairs
- Mettre en œuvre l'amélioration continue
- Réduire les coûts (efficacité, puis efficience)
- Ne pas réinventer la roue
- Définir les rôles et responsabilités

Challenge :

- Démontrer la contribution de l'IT à l'apport de valeur de manière mesurable
- Fournir des services et pas des produits
- Créer une relation efficace
- Délivrer un service stable et constant
- Compétition économique de l'entreprise
- Développement de nouveaux marchés



## 1.2. Service Desk

---

En tant que SPOC, la mission du SD est d'enregistrer et gérer le cycle de vie de l'incident (suivi, communication, rapports, clôture). Pour les incidents ne pouvant être traités le SD doit escalader, pour les incidents dépassant les SLA la gestion des problèmes doit être sollicitée. Le SD doit faciliter le retour à un service opérationnel normal.

### 1.2.1. Objectifs

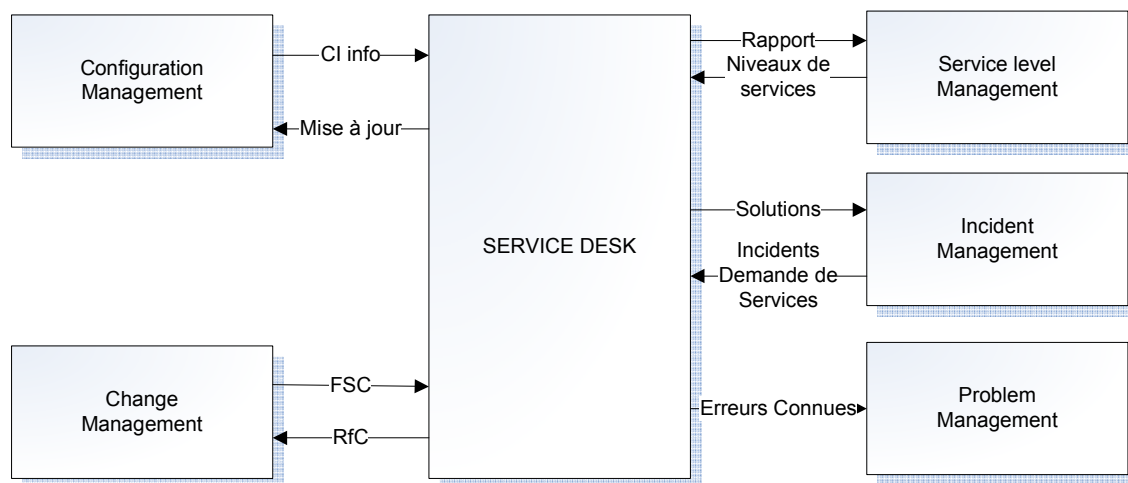
- Fournir un point de contact à tous (clients, fournisseurs, utilisateurs) pour toutes les demandes (incidents, questions, demandes de services, réclamations, RfC)
- Faciliter la restauration du service
- Générer des rapports
- Faciliter l'identification des coûts associés à la gestion de l'infrastructure IT (mesurer les coûts de traitement)
- Supporter la gestion des changements
- Supporter la gestion des services (support) et l'optimisation des investissements
- Contribuer à la satisfaction durable

### 1.2.2. Processus

#### 1.2.2.1. Entrées /Sorties

Entrées	Sorties
Email Appels Internet/extranet Fax Matériels/applications	Solutions Escalades Information RfC rapports

#### 1.2.2.2. Interfaces avec les autres processus



### 1.2.3. Activités

- Support de niveau 1 et coordination niveaux >
- Réception, enregistrement des appels et surveillances statuts (premier point de contact)
- Prioriser puis gérer le cycle de vie des incidents (enregistrement, clôture, suivi)
- Communiquer les changements de SLA
- Identifier les problèmes et les besoins en formation
- Communication et suivi des demandes (incidents, questions, demandes de services, réclamations, RfC)
- Escalade en fonction des SLA
- Générer des rapports
- Audits

#### 1.2.4. Implémentation

- Comprendre les besoins du client
- Engagement de la Direction
- Alignement du service desk sur la stratégie du support
- Identifier, réussir puis communiquer les quick-wins
- Objectifs et livrables précis
- Approche par phase (petits-pas)
- Impliquer/consulter clients et utilisateurs
- Vendre les bénéfices du SD aux clients/utilisateurs
- Former à être des équipes de services
- Sensibilisation interne/externe
- Promouvoir le SD

#### 1.2.5. Divers

##### 1.2.5.1. *Types de SPOC (Structures locales, centrales ou virtuelles)*

- Centre d'appel
- Helpdesk : gère, coordonne et résout les incidents.
- Service Desk : Traite toutes les demandes et fournit une interface avec les autres processus.

##### 1.2.5.2. *Principales attentes Clients*

- Fournir un SPOC
- Quel est le niveau de service du SD ?
- Quelle est la priorité de la demande ?
- Estimation de l'avancement de la demande ?
- Etre assuré que les demandes seront bien traitées (ni perdues, ni ignorées)

##### 1.2.5.3. *Technologies*

- Outil de recherche et KB
- Logiciels intégrés de gestion des services
- CTI/SVI
- Email
- Fax
- Pagers
- Outil d'automatisation des opérations, surveillance, monitoring

##### 1.2.5.4. *Compétences*

- Orientation client
- Communication et relations interpersonnelles
- Méthodique
- Multilingue
- Comprendre les objectifs du client
- Comprendre comment les incidents affectent le business client
- Comprendre que le client est l'expert Business
- Vouloir fournir un service de 1<sup>er</sup> ordre

#### 1.2.5.5. Rapports

- Rapports **quotidien** Incidents/problèmes :
  - o en fonction des escalades
  - o Manquement aux SLA
  - o Incidents en cours
- Rapports **hebdomadaires** :
  - o Disponibilité des services
  - o Principaux domaines des incidents (fréquence, temps passé, longueur de traitement)
  - o Incidents nécessitant la création d'un problème
  - o Erreurs connues et RfC liés aux problèmes
  - o Manquement aux SLA
  - o Rapport satisfaction
  - o Tendance affectant le service/business
  - o Charge des équipes
- Rapports **mensuels** :
  - o Disponibilité des services
  - o Performances globales et tendances
  - o Réussites des objectifs de chacun des services
  - o Satisfaction client
  - o Besoin de formation
  - o Performance des supports et fournisseurs
  - o Performance des applications et infrastructures
  - o Coût de la fourniture et de l'indisponibilité des services

### 1.3. Gestion des incidents

---

#### 1.3.1. Objectifs

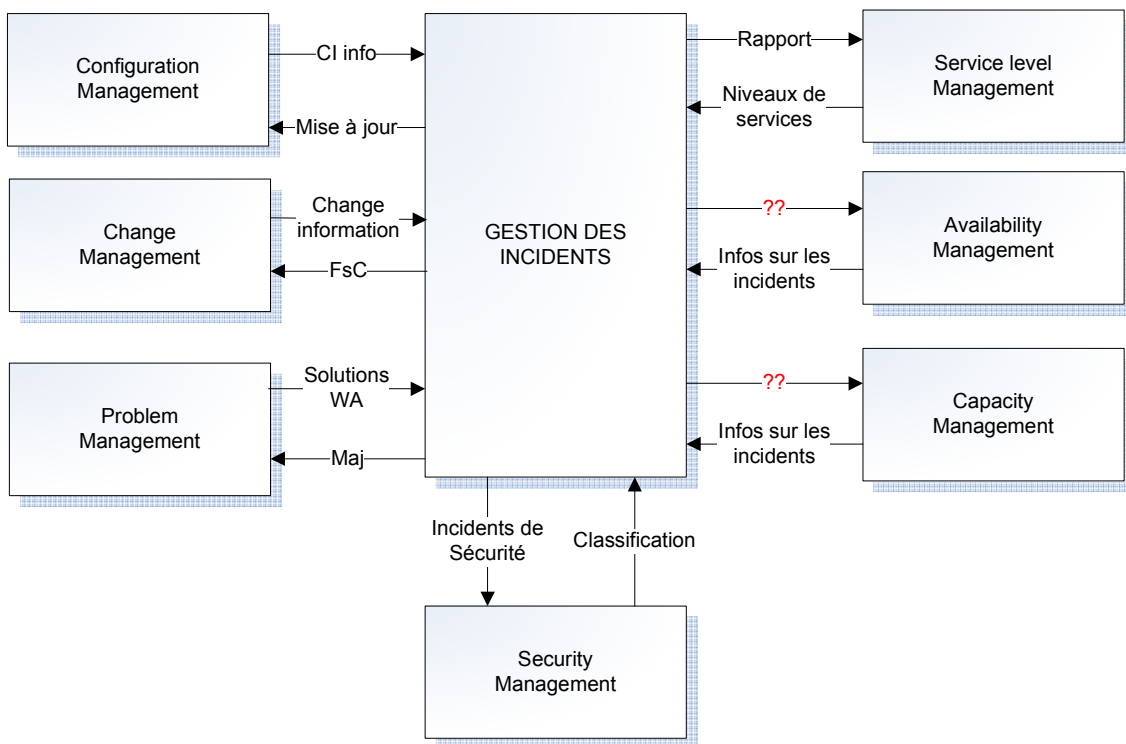
- Restaurer le service normal dès que possible
- Minimiser l'impact sur le business
- S'assurer que les SLA sont tenus

#### 1.3.2. Processus

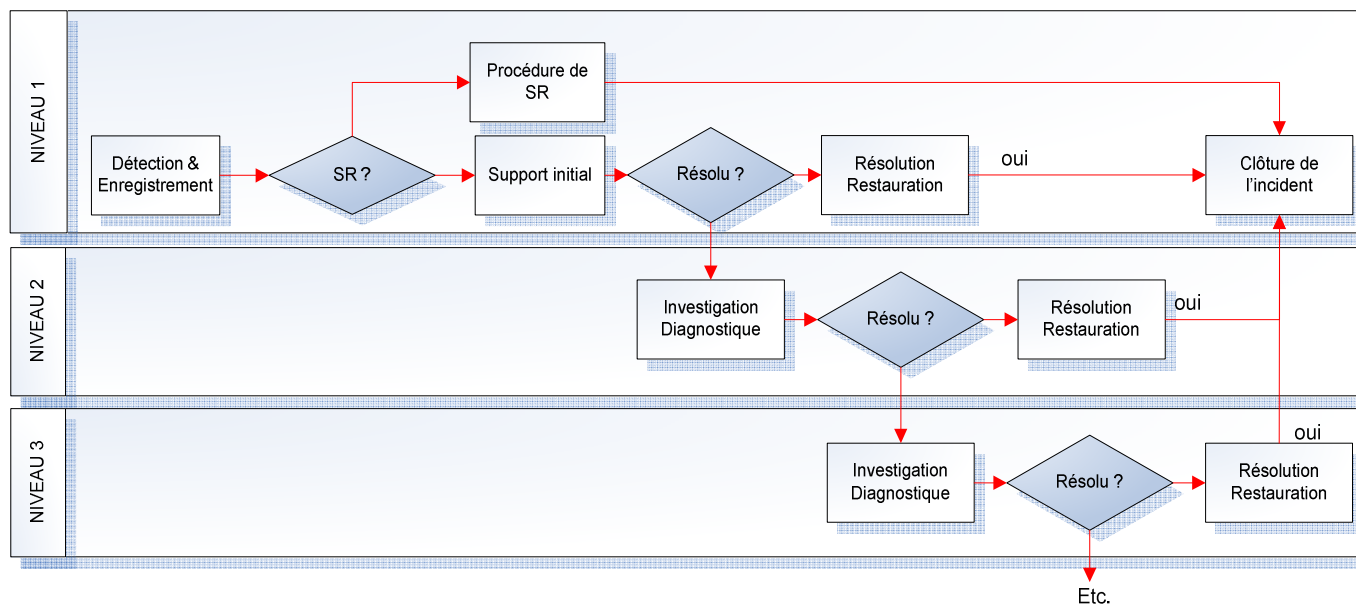
##### 1.3.2.1. Entrées/sorties

Entrées	Sorties
Incidents (SD) Information de configuration (Gestion des configurations) Détail des résolutions Détails des RfC pour la résolution d'incidents Réponses de l'incident management sur la correspondance entre incidents, problèmes et erreurs connues (KB)	RfC pour la résolution d'incidents Mise à jour des incidents Incidents résolus et fermés Communication avec clients/utilisateurs (si inclus au SD) Rapports

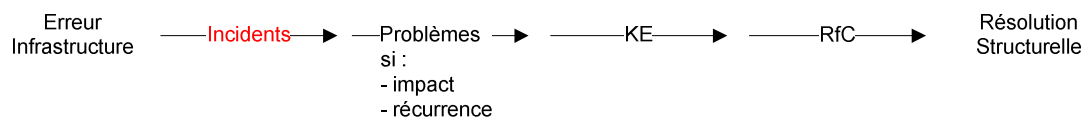
### 1.3.2.2. Interfaces avec les autres processus



### 1.3.2.3. Routage des incidents



### 1.3.2.4. Relations incidents



### 1.3.3. Activités

L'enchainement des étapes de la gestion des incidents est décrit dans le schéma "[routage des incidents](#)".

#### 1.3.3.1. Détection et enregistrement

Actions	
Enregistrer l'incident Alerter les supports si nécessaires Démarrer la procédure de traitement des SR	
Entrées	Sorties
Incidents en provenance du SD Remontée automatiques d'alertes	Mises à jour des incidents Identification des erreurs dans la CMDB Notification des statuts des incidents (client)

#### 1.3.3.2. Classification et support initial

Actions	
Classifier les incidents Lier incidents, problèmes et KE Prévenir la gestion des problèmes de nouveaux problèmes (incidents multiples) Définir impact, urgence = priorité Liaison incident et CI impactés Support initial Ferme ou escalade l'incident	
Entrées	Sorties
Description incident Détails des configurations de la CMDB Base de connaissance et base des problèmes et erreurs connues	RfC concernant la résolution Mise à jour de l'incident WA ou transfert vers les niveaux >

#### 1.3.3.3. Investigation

Actions



Analyse du détail de l'incident Fourniture d'une résolution (y compris WA) ou escalade	
Entrées	Sorties
Mise à jour de l'incident Détail des configurations de la CMDB	Nouvelle mise à jour de l'incident Identification du WA

#### 1.3.3.4. Résolution et restauration du service

Actions	
Résout l'incident en utilisant une solution, un WA ou émettant une RfC Mets en place des actions de restauration	
Entrées	Sorties
Mise à jour de l'incident Réponse de la gestion des changements au sujet d'une RfC (solution incident) Solution ou WA	RfC pour résoudre l'incident Incident résolu Mise à jour de l'incident

#### 1.3.3.5. Clôture

Actions	
Confirme la résolution avec le client ou demandeur Assigne une catégorie "fermé" à l'incident	
Entrées	Sorties
Mise à jour de l'incident Incident résolu	Mise à jour de l'incident Clôture du ticket

#### 1.3.3.6. Surveillance, suivi et communication

Actions	
Surveille les incidents Escalade les incidents Informe les clients	
Entrées	Sorties
Ticket d'incident	Reporting sur la gestion des incidents Détails des incidents escaladés

#### 1.3.4. Implémentation

- Engagement de la direction et budget suffisant
- CMDB à jour
- Annuaire du service support à jour
- Une KB (problème et KE) est nécessaire
- Outil de gestion des incidents
- Lié ce processus à la gestion des niveaux de service
- S'assurer que les besoins business sont bien identifiés

#### 1.3.5. Divers

##### 1.3.5.1. *Bénéfices*

- Meilleure productivité
- Réduction des temps de réponse
- Réduction du nombre d'incident et des difficultés clients
- Identification efficace des problèmes
- Amélioration de la satisfaction client

##### 1.3.5.2. *Rôles*

- Incident Manager
  - o S'assure et surveille de l'efficacité du process
  - o Reporte
  - o Encadre la gestion des incidents et le support
  - o Emet des recommandations d'amélioration
  - o Développe et gère les systèmes de gestion des incidents
- Support 1° niveau :
  - o Enregistre
  - o Route les incidents vers les équipes en charge
  - o Support initial
  - o Suivi, communication et surveillance des incidents
  - o Résout
  - o Ferme
- Support 2° niveau
  - o Gère les SR
  - o Surveille la description des incidents et CI liés
  - o Investigue et diagnostique
  - o Détecte les problèmes
  - o Résolution & restauration

##### 1.3.5.3. *Indicateurs*

- Nombre total d'incidents
- Temps moyen de résolution en fonction de l'impact
- Pourcentage d'incidents traités dans les SLA
- Pourcentage d'incidents traités sans escalade

- Coût moyen par incident

## 1.4. Gestion des problèmes

Lorsque la cause d'un incident ne nécessite pas d'analyse, il n'est pas nécessaire d'ouvrir un problème, ces derniers le sont sur des critères d'impact et de récurrence.

### 1.4.1. Objectifs

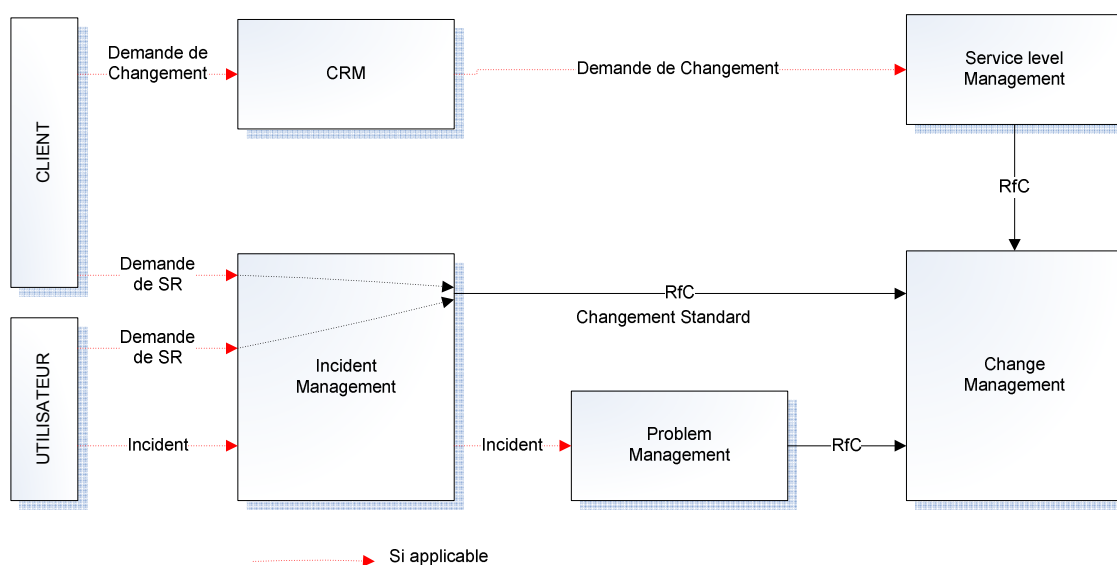
- Minimiser l'impact sur le business des incidents et problèmes causés par des erreurs d'infra
- Prévenir la récurrence des incidents liés aux erreurs

### 1.4.2. Processus

#### 1.4.2.1. Entrées / sorties

Actions	
Contrôle des problèmes et erreurs Prévention des problèmes (pro actif) Fournir de l'information	
Entrées	Sorties
Détail de l'incident Détail des CI Solution de contournement (WA)	Erreurs connues RfC Mise à jour des problèmes avec des WA ou des solutions permanentes Support de la gestion des incidents en mettant en correspondance incidents et problèmes Reporting

#### 1.4.2.2. Interfaces avec les autres processus



### 1.4.3. Activités

#### 1.4.3.1. Contrôle des problèmes

- Identification et enregistrement :
  - o La gestion des incidents fournit les informations liées aux incidents
  - o La catégorisation et l'enregistrement des incidents est essentielle/vitale
  - o La façon d'enregistrer les incidents doit être connue de la gestion des problèmes
- Classification :
  - o Classification : Impact du problème sur les SLA
  - o Catégorie : A quel groupe le problème est lié
  - o Impact : Effet sur le business ? (*degrés de déviation par rapport au service normal*)
  - o Urgence : Quel délai est toléré ? (*disponibilité, impact futur, WA ou non*)
  - o Priorité : fonction de l'impact et de l'urgence
- Investigation et diagnostique :
  - o Méthodes d'analyse (Bon sens, déduction, Kepner et Tregoe, Ishikawa)

#### 1.4.3.2. Contrôle des erreurs

- Identification et enregistrement :
  - o Une erreur est identifiée quand le CI défectueux est détecté
  - o Une erreur connue est identifiée quand le CI défectueux est détecté et que le WA existe
  - o 2 sources d'erreurs existent :
    - Erreurs en production
    - Erreurs liées à un changement
- Analyse/Evaluation :
  - o Etude initiale pour résoudre l'erreur
  - o Emission d'une RfC si nécessaire, puis priorisation de la RfC
  - o 2 environnements d'erreurs supplémentaires
    - Erreurs dans les produits tiers
    - Erreurs dans l'environnement logiciel
- Enregistrement et résolution des erreurs
  - o Stocker les informations dans la KDB (Knowledge data base)
    - CI impliqués
    - Symptômes
    - Résolutions et actions de contournement
  - o Aide à la mise en correspondance des incidents
  - o Aide pour des investigations futures
- Clôture
  - o Clôture de l'erreur connue
  - o Clôturer les problèmes et incidents associés

- Utiliser les PIR (Post Implementation Review) pour s'assurer que les solutions sont correctes.
- Suivi des progrès de résolution des problèmes et erreurs :
  - Le contrôle des erreurs est responsable de suivre la résolution des erreurs connues
  - La gestion des problèmes est responsable de suivre l'impact des problèmes et erreurs sur les services
  - Le progrès de la résolution des problèmes doit être corrélé avec les SLA
- Conseil sur le contrôle des erreurs :
  - Toutes les erreurs n'ont pas besoin d'être résolues
  - Le contrôle de l'erreur doit rédiger des RfC
  - Privilégier la création d'enregistrements standards par Ci ou catégorie de CI
  - Le partage d'information est crucial

#### **1.4.3.3. Prévention proactive des problèmes**

- Identification des tendances (trend analysis)
  - Analyse des tendances
  - Revue des problèmes majeurs
  - Actions de prévention
- Cibler des actions préventives
- Revue des problèmes majeurs
  - Qu'est ce qui a été bien et mal fait ?
  - Qu'est-ce qui pourrait être mieux fait la prochaine fois ?
  - Comment éviter que le problème ne se reproduise ?

#### **1.4.3.4. Fournir de l'information à l'entreprise**

Une fois que les problèmes sont identifiés, les actions mises en œuvre induisent

- L'émission de RfC
- Un retour sur les tests, les procédures, les formations et les documentations
- L'initialisation de formation pour les clients/utilisateurs
- La vérification du respect aux procédures de gestion des incidents et problèmes
- L'amélioration des processus et procédures

### **1.4.4. Implémentation**

#### **1.4.4.1. Rôles et tâches**

##### **1. Problem Manager :**

- Contrôle des erreurs et problèmes
- Surveille l'efficacité et l'efficience des activités de contrôle des erreurs et problèmes
- Produit des rapports destinés au management
- Manage les équipes de gestion de problème
- Alloue les ressources pour l'effort de support
- Maintien et développe les systèmes de gestion des problèmes et erreurs

## 2. Equipes de support :

- Responsabilités réactives :
  - Identifie et investigue les problèmes
  - Emet des RfC pour supprimer les erreurs
  - Surveille les progrès liés à la résolution des erreurs connues
  - Conseille la gestion des incidents sur la meilleure solution de contournement disponible
  - Assiste dans la résolution des incidents majeurs
- Responsabilités pro actives :
  - Identifier les tendances et les sources de problèmes potentiels
  - Emettre les RfC pour prévenir la récurrence des problèmes
  - Prévenir la réplication des problèmes

### 1.4.4.2. *Meilleures pratiques*

- Etre à l'écoute des spécialistes, ils peuvent avoir raison
- Vérifier les idées en fonction du Business plan et non d'un point de vue technologique
- Séparer clairement gestion des incidents et gestion des problèmes
- Allouer du temps à la gestion des problèmes
- Mettre l'accent sur la maitrise et la prévention des incidents

### 1.4.4.3. *Bénéfices*

- Amélioration de la qualité des services
- Réduction des interruptions grâce à l'élimination des incidents récurrents
- Prévention de l'apparition des incidents grâce à des analyses proactives
- Solutions définitives mises en œuvre
- Amélioration de la connaissance IT et de l'organisation

### 1.4.4.4. *Blocages potentiels*

- Allocation de ressources insuffisantes
- Manque de rigueur/discipline pour suivre les processus
- Intégration limitée entre la gestion des incidents et des problèmes
- Manque d'expérience sur l'analyse des tendances
- Manque d'engagement de la direction

## 1.4.5. Divers

### 1.4.5.1. *Indicateurs clés*

- Nombre de RfC émises et impact sur la disponibilité du service
- Temps nécessaire pour l'investigation et le diagnostique
- Nombre et impact des incidents avant la fermeture du problème ou que l'erreur connue soit confirmée
- Plan d'allocation des ressources (personnel, etc.)

## 1.5. Gestion des configurations

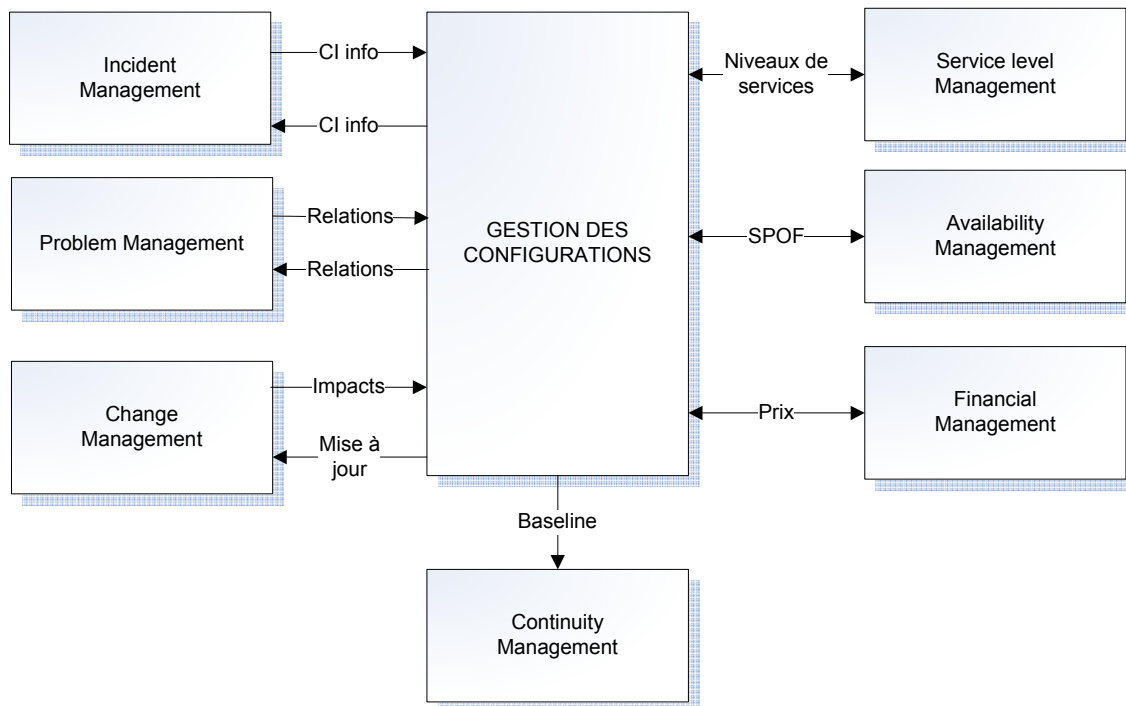
---

### 1.5.1. Objectifs

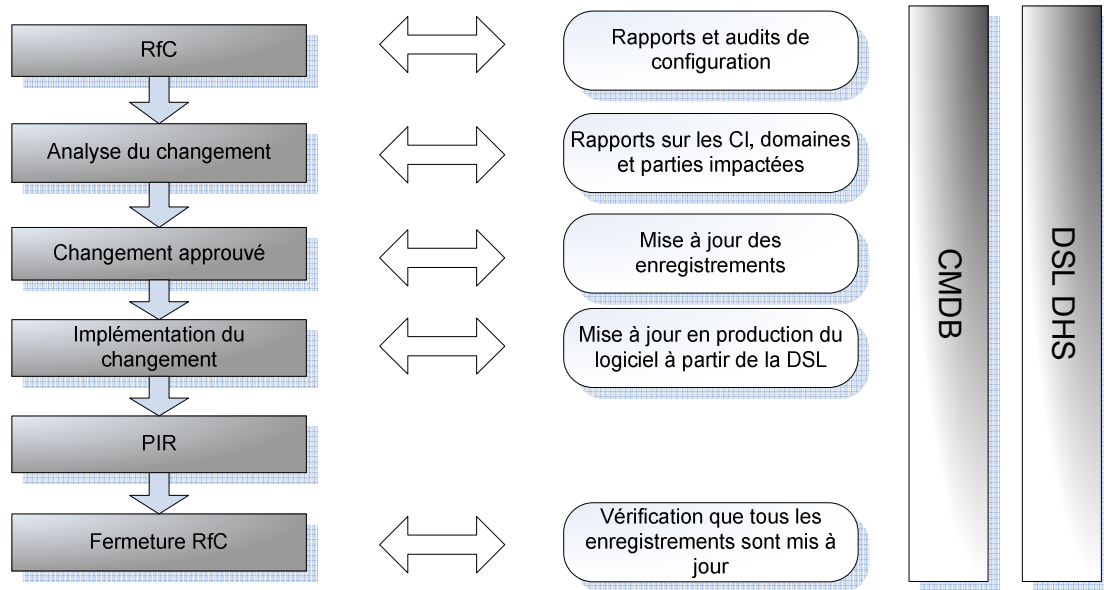
- Fournir des informations fiables sur l'infrastructure et ses composants à tous les processus et à la direction IT :
  - Gestion des incidents
  - Gestion des problèmes
  - Gestion des changements (qui alimente la CMDB et surveille les changements)
  - Gestion des mises en production
- Permettre le contrôle de l'infrastructure en surveillant et en gardant à jour les informations liées aux :
  - Ressources nécessaires pour délivrer des services
  - Statuts et historiques des CI
  - Relations des CI
- Comptabiliser tous les biens de l'entreprise

### 1.5.2. Processus

#### 1.5.2.1. Interfaces processus



#### 1.5.2.2. Interfaces avec la Gestion des changements



### 1.5.3. Activités

#### 1.5.3.1. Planification (amont)

Quel CI est nécessaire par rapport au business ? Quels composants supportent les services IT qui eux-mêmes supportent le Business

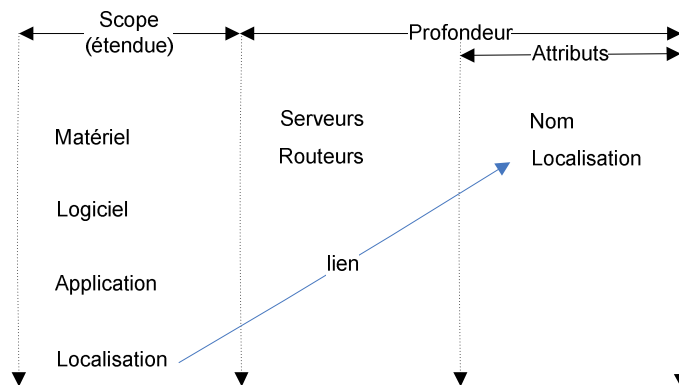
Définir :

- Une stratégie, une politique, un périmètre et des objectifs
- Analyser le statut actuel des biens et des CI
- Définir le but de la CMDB et du processus dans l'entreprise
- Les politiques de relations avec les processus interfacé (changement, incident, etc.)
- Définir les interfaces avec les projets, fournisseurs, application et les équipes de support
- Définir les procédures et processus, les guidelines, les outils de support
- Définir les rôles et responsabilités
- Mise en œuvre des espaces de stockage
  - DSL
  - DHS
  - Documentations

#### 1.5.3.2. Identification des CI

- Sélectionner, identifier (étiquetage) et répertorier les structures de configuration (services, environnement, applications) et les CI,
- Identifier leur propriétaire respectifs, et les relations entre eux.



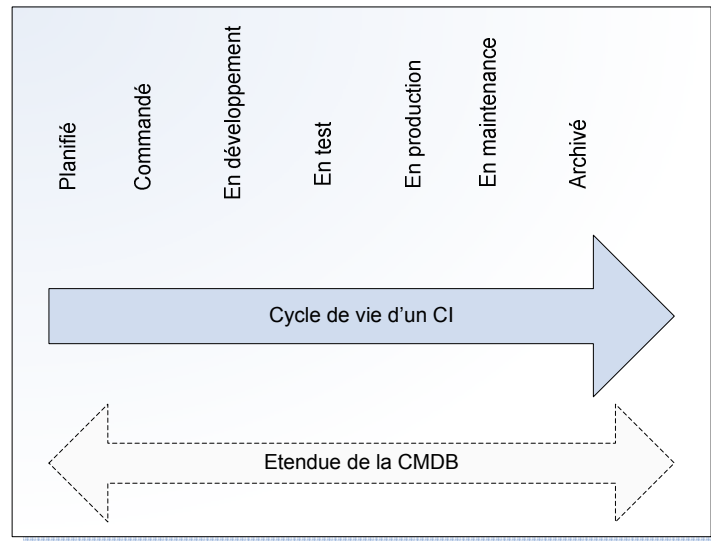


#### 1.5.3.3. *Contrôle*

- S'assure des contrôles par rapport aux changements.
- S'assure que seuls les CI autorisés sont enregistrés (tout le cycle de vie du CI)
- S'assure qu'aucun CI n'est modifié sans une documentation appropriée (ex: RfC approuvée)

#### 1.5.3.4. *Gestion des statuts*

- Suit de toutes les données actuelles et historiques (l'évolution des statuts des CI)
- Suivi des changements des CI et de leurs enregistrements



#### 1.5.3.5. *Vérification et audits*

- Ecart entre la CMDB et la réalité
- Revues et audits
- Vérifie l'existence physique des CI
- Vérifie les enregistrements

#### **1.5.3.6. Configuration de référence (baseline)**

- Configuration d'un produit ou d'un système à un instant "T" (snapshot)
  - Capture à la fois la structure et le niveau de détail
  - Permet une restauration à une version antérieure
  - Comparaison avec l'état réel

#### **1.5.4. Implémentation**

##### **1.5.4.1. Planification du processus**

- S'accorder sur le but, les objectifs, l'étendue, les priorités et l'approche d'implémentation. Tout doit être aligné avec le client
- Nommer un configuration manager et planifier les ressources nécessaires pour le processus de configuration management
- Analyser les systèmes existants
- Développer des plans de gestion de configuration et désigner le système
- Créer une feuille de route détaillée de l'implémentation
- Renseigner la CMDB et la DSL
- Gérer la transition vers le nouveau processus

##### **1.5.4.2. Indicateurs clés**

- Nombre de fois où la configuration n'est pas autorisée
- RfC et changements en échecs à cause d'une mauvaise étude d'impact, de données incorrectes dans la CMDB ou d'une mauvaise gestion des versions
- Licences non utilisées ou perdues
- Exceptions rapportées au cours d'audit de configuration
- Composant IT non autorisés en production
- Nombre de changements apportés à la CMDB par mois pour rectifier les erreurs identifiées dans la CMDB

##### **1.5.4.3. Rôles**

#### **1. Configuration Manager**

- Travail pour la réussite du processus
- Évalue les systèmes de gestion existants
- Propose et valide l'étendue du processus de gestion des configurations
- Gère les campagnes de sensibilisation
- Recrute et forme les équipes
- Évalue les logiciels propriétaires de Gestion des configurations
- Crée et gère les plans de gestion de configuration
- Propose et valide les conventions de nommage des CI
- Propose et/ou valide les interfaces avec les autres processus
- Planifie et s'assure de la saisie des CI dans la CMDB
- Fournit des rapports (ex: Direction)
- Mise à disposition de la CMDB pour les études d'impact
- Crée des "change records", des "configurations baselines" et des "Package Release Records"
- S'assure que la CMDB est mise à jour après un changement
- Mets à disposition la CMDB pour assister à l'identification d'autres CI affectés par une erreur
- Réalise les audits de configuration
- Assiste les auditeurs

## 2. Configuration Librarian

- Contrôle la réception, l'identification, le stockage et le retrait de tous les CI supportés
- Fournit de l'information sur le statut des CI
- Numérote et enregistre les éventuelles anomalies
- Il s'occupe des CI

### 1.5.4.4. Relations de la CMDB

- La CMDB est disponible pour tous les processus (support et delivery)
- Elle est utilisée pour relier les enregistrements des incidents et des problèmes
- La gestion de mise en production (Release Management) peut-être difficile et sujette à des erreurs
- Gestion des niveaux de service
- Gestion financière
- Gestion de la continuité de service et disponibilité
- Gestion des incidents :
  - Vérifier les CI : statuts, incidents/problèmes/erreurs
  - Mise à jour des enregistrements des CI
- Gestion des problèmes
  - Mise en correspondance avec des problèmes connus
  - Mise à jour des enregistrements des CI avec les numéros des problèmes
  - Mise à jour des enregistrements des CI avec les numéros des erreurs et des RfC

### 1.5.4.5. Meilleures pratiques

- Commencer par établir un plan de gestion des configurations
- Sensibiliser sur le sujet du processus de la gestion des configurations
- Importance de la sélection de l'outil
- Rendre obligatoire le processus de gestion des changements pour tous RfC
- Utilisation de logiciels d'inventaires automatiques

### 1.5.4.6. Bénéfices

- Fournir une **information correcte sur les CI et leur documentation**
- Permettre le contrôle des CI
- Faciliter l'adhésion aux obligations légales
- Faciliter l'élaboration des plannings financiers
- Fournir des informations sur les tendances au processus de gestion des problèmes

### 1.5.4.7. Blocages potentiels

- Difficulté à établir l'étendue et la profondeur de la CMDB
- Collecte et enregistrements des données inadéquates et mises à jour insuffisantes
- Rôles et responsabilités par clairement définies
- Difficulté à définir les propriétaires des CI
- Planification et scope trop ambitieux
- Manque d'engagement de la Direction

## 1.5.5. Divers

### 1.5.5.1. Terminologie

	CI	ASSET
--	----	-------

<b>EST</b>	Nécessaire pour délivrer un service Identifiable de manière unique Sujet au changement Gérable	Un composant d'un processus Business Possède une valeur financière N'a pas besoin de relations
<b>A</b>	Une catégorie Des relations Des attributs Un statut	

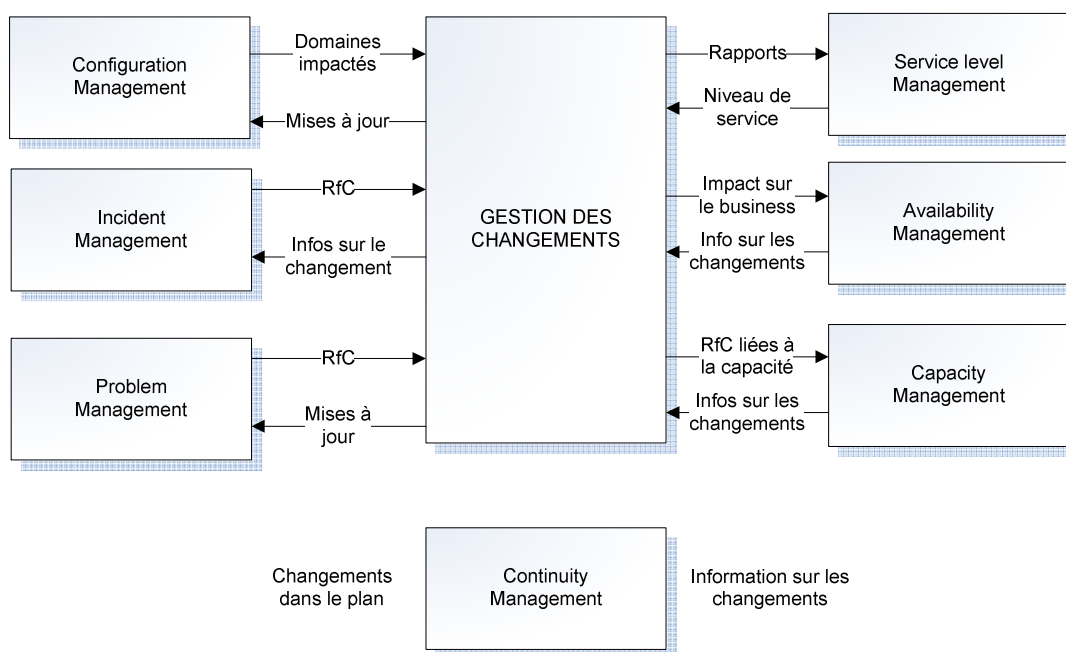
## 1.6. Gestion des changements

### 1.6.1. Objectifs

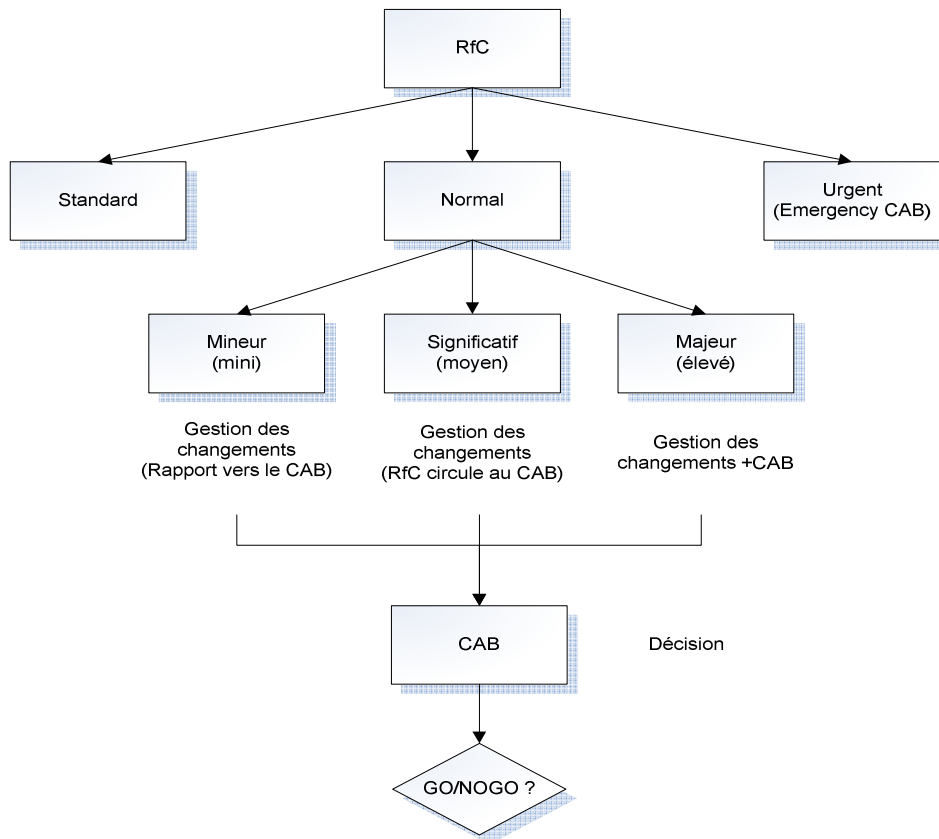
Gérer et coordonner les changements en s'assurant que les impacts négatifs sur les services soient minimisés à un risque acceptable et que les opérations quotidiennes soient améliorées

### 1.6.2. Processus

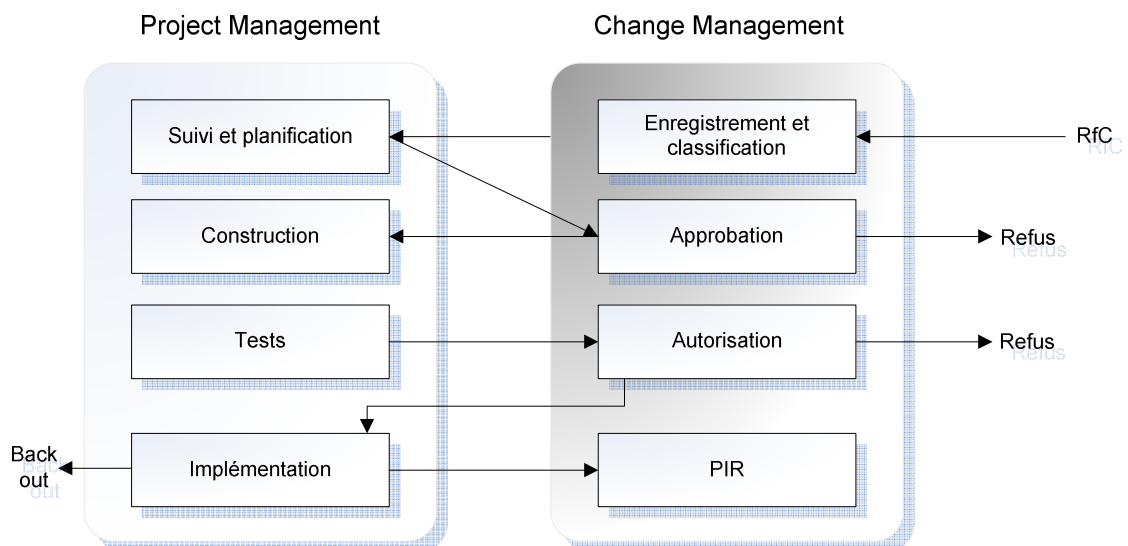
#### 1.6.2.1. Interface processus



### 1.6.2.2. Flux des RfC



### 1.6.2.3. Interfaces gestion des changements et projets



### 1.6.3. Activités

Actions	
Enregistrement et filtrage des changements Gérer les changements et le processus de gestion des changements Présider le CAB, et l'Emergency CAB Revue et fermeture des changements Information de gestion	
Entrées	Sorties
Demandes de changements (RfC) CMDB Forward Schedule of Change (FsC)	Forward Schedule of Change (FsC) mis à jour Demandes de changements (RfC) Comptes rendus et plans d'actions du CAB Rapport concernant le processus de gestion des changements

#### 1.6.3.1. Rôles

##### 1. Change Manager :

- Reçoit, enregistre et priorise les RfC
- Rejette les RfC irréalistes
- Classifie les RfC pour la réunion du CAB, définit l'agenda du CAB et diffuse les RfC avant le CAB
- Décide qui sera présent au CAB
- Organise les réunions CAB/EC
- Préside les CAB et CAB/EC
- Autorise les changements (avec l'avis du CAB)
- Renseigne et publie les FsC
- Communique avec les intervenants pour coordonner la construction, le test et l'implémentation des changements
- Met à jour le journal des changements
- Revoit tous les changements implémentés
- Revoit les RfC en attente
- Analyse les détails des changements pour identifier les tendances et/ou les problèmes potentiels
- Clôture les RfC
- Produit des rapports réguliers destinés à la direction

##### 2. Change Advisory Board :

- Analyse toutes les RfC qui lui sont soumises
- Détermine et fournit les informations sur les impacts éventuels, les ressources et les coûts nécessaires à l'implémentation du changement
- Participe à la planification du changement
- Est disponible en cas de changement urgent
- Conseille le Change Manager sur certains aspects de changement urgents

#### 1.6.3.2. Enregistrement et filtrage

- Tous les RfC doivent être enregistrés
- Prendre en compte uniquement les demandes qui font partie du périmètre

- Standardiser les procédures pour évaluer la validité des requêtes
- Utiliser des outils intégrés

#### **1.6.3.3. Evaluations (impact et ressources)**

- Evaluation de l'impact sur les processus Business
- Effets sur :
  - L'infrastructure
  - Le service délivré aux clients
  - La capacité, la performance, la fiabilité et la résilience
  - Les plans de continuité
  - Les politiques de sécurité
- Impact sur d'autres services partageant l'infrastructure IT
- Impact sur les éléments de l'organisation ne faisant pas partie de l'infrastructure IT
- Impact de ne pas implémenter le changement
- Ressources nécessaires pour l'implémentation
- FSC et PSA (Projected Service Availability)
- Quantité de ressource récurrente nécessaire

#### **1.6.3.4. Affectation d'une catégorie et approbation**

1. Catégorie 1 : impact mineur sur les services existants. Le change Manager a le pouvoir d'autoriser et de planifier cette RfC
2. Catégorie 2 : impact significatif. La RfC doit être évaluée par le CAB
3. Catégorie 3 : impact majeur. Un nombre important de ressources sont nécessaires à son évaluation et la Direction IT doit approuver cette RfC
4. Catégorie Standard (pré-autorisée): RfC pour laquelle il existe des procédures standard documentées
5. Changements urgents : Ce sont des **changements normaux**, qui induisent un **risque plus important**. Il faut créer des procédures pour les gérer efficacement et ne pas sacrifier les contrôles normaux du processus de gestion des changements

#### **1.6.3.5. Planification**

Pour planifier les changements il faut :

- Des documents, des comités et des outils
- Une stratégie de mise en production définie dans le SLA

Utilisation d'outils pour :

- Suivre les actions
- Obtenir un aperçu de tous les changements planifiés (y compris les changements exceptionnels)

Obtenir un aperçu de la :

- Disponibilité des employés

- Disponibilité des ressources
- Coûts de changement

#### **1.6.3.6. Construire, tester et implémenter**

Transférer les RfC aux groupes appropriés. Les RfC peuvent impliquer

- De construire un nouveau module de production
- Créer une nouvelle version d'un ou plusieurs modules de logiciels
- Acheter des équipements ou des services externes
- Préparer une modification matérielle
- Produire une nouvelle documentation, ou la modifier
- Préparer des formations utilisateurs

#### **1.6.3.7. PIR (Post Implementation Review)**

Son but est de :

- Valider que le changement a atteint son but
- Que les clients soient satisfaits du résultat
- Identifier les imperfections
- Vérifier qu'aucun effet de bord n'est présent
- Que la planification des ressources est correcte
- Que le plan d'implémentation a fonctionné correctement
- Que le changement a été effectué selon le budget et le temps prévu
- D'évaluer l'efficacité du plan de retour arrière le cas échéant
- D'évaluer le nombre d'incidents liés à un changement

#### **1.6.3.8. Change Advisory Board (CAB)**

##### **1. Activités**

- Évalue les risques du changement
- Crée un support pour les changements
- Inclure les personnes impliquées et élabore les recommandations
- Prend les décisions sur
  - L'autorisation
  - La définition de l'impact
  - Définition de la priorité
  - Définition de l'allocation des ressources
- CAB/EC (emergency committee)

##### **2. Agenda du CAB**

- Changement qui ont échoués (avec ou sans procédure de retour)
- RfC qui doit être évalué par le CAB
- RfC qui a été évaluée par le CAB
- Rapport concernant les changements
- Rapport et amélioration possible concernant le processus

##### **3. Membres du CAB**



- Change Manager
- SL Manager
- Application Manager
- Clients
- Problem Manager
- Release Manager
- Finance Manager
- Autres si nécessaire

#### **1.6.4. Implémentation**

##### **1.6.4.1. Implémentation**

- Nommer le Change Manager
- Décider du système qui supportera le processus de change management (papier, logiciel ou mixte)
- Planifier les rapports : les métriques et les audits des processus de change et de configuration management
- Planifier l'implémentation
- Implémenter, en parallèle, avec les processus de configuration et de release

##### **1.6.4.2. Meilleures pratiques**

- Intégrer les processus de configuration et release
- Aller au delà de l'opérationnel et intégrer le développement
- Assigner la responsabilité des processus indépendamment des responsabilités organisationnelles
- "Planifier" les changements urgents plutôt que de réaliser des changements urgents

##### **1.6.4.3. Bénéfices**

- Moins de perturbations des processus métiers
- Amélioration de l'information de gestion
- Amélioration de la productivité des clients et équipes IT
- Meilleure analyse initiale des coûts des changements proposés
- Capacité à absorber un nombre plus élevé de changement sans erreurs

##### **1.6.4.4. Blocages potentiels**

- Contournement du processus
- Les prestataires externes sont difficiles à intégrer dans le processus
- La propriété des changements n'est pas claire
- Procédure de changement trop bureaucratique
- Manque d'engagement de la Direction

#### **1.6.5. Divers**

##### **1.6.5.1. Priorités des changements**

- Urgente : Le changement est nécessaire immédiatement (sinon impact sévère pour le client)
- Haute : Le changement est nécessaire dès que possible (pour éviter des dommages potentiels)

- Moyenne : Le changement va résoudre des erreurs agaçantes ou des fonctionnalités manquantes (qui peuvent être planifiées)
- Basse : Le changement conduit à des améliorations mineures

#### **1.6.5.2. Contenu des rapports**

Gestion des changements :

- Nombre de changements implémentés
- Nombre de changements planifiés
- Nombre de changements rejetés
- Nombre de changements évalués
- Jours homme dépensés

Changements :

- Nombre de retours arrière
- Nombre de CI impliqués
- Nombre de problèmes résolus
- Nombre de plaintes
- Jours homme dépensés

#### **1.6.5.3. Terminologie**

**Changement** : Ajout, modification ou suppression d'un CI approuvé

**Demande de changement (RfC)** : Formulaire utilisé pour enregistrer les détails d'une demande de changement

**Forward Schedule of Change (FsC)**: Planification qui contient des détails de tous les changements approuvés pour l'implémentation et leur date d'implémentation

## **1.7. Gestion des mises en production (version)**

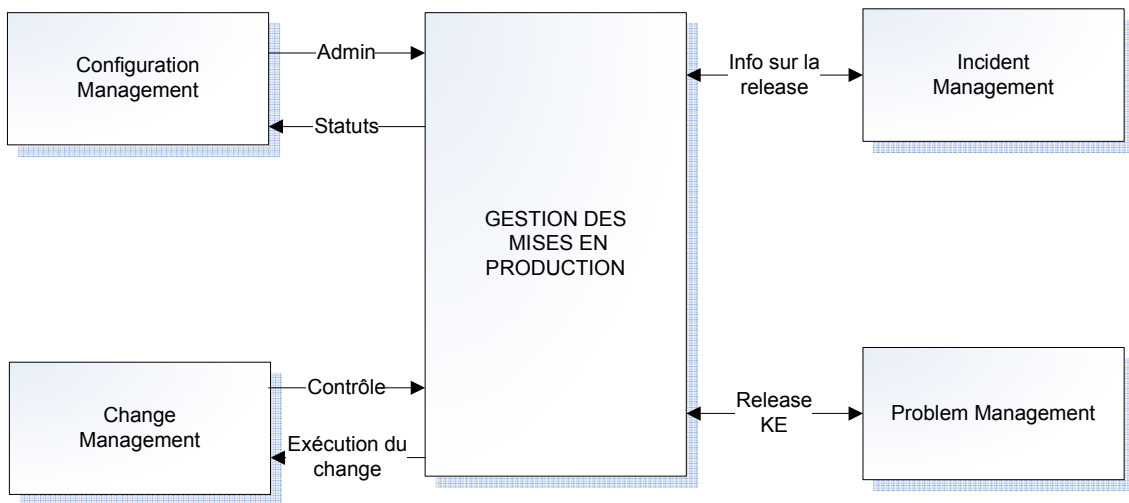
---

### **1.7.1. Objectifs**

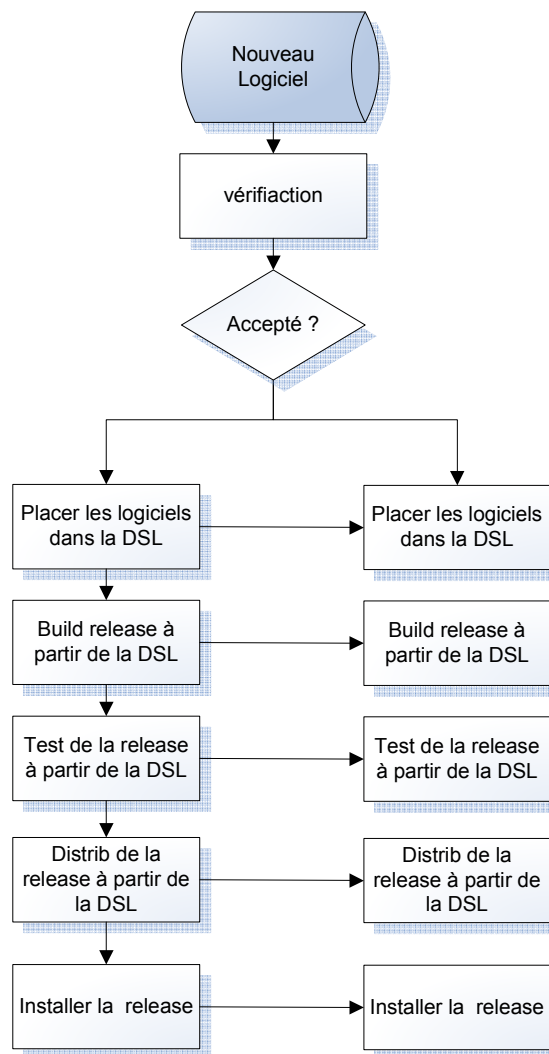
- Planifier et surveiller les déploiements matériels et logiciels
- Mettre en œuvre des procédures efficaces pour la distribution et l'installation des changements
- S'assurer que les changements (matériels/logiciels) sont tracables, sécurisés, corrects, autorisés et testés
- Gérer les attentes client pendant le déploiement
- S'accorder sur le contenu et le plan de déploiement des mises en production avec la gestion des changements
- Implémenter les nouvelles versions dans l'environnement de production en s'appuyant sur la gestion des changements et des configurations
- Sécuriser les sources logicielles et matérielles dans la DHS et DSL
- Mettre à jour la CMDB

### **1.7.2. Processus**

#### 1.7.2.1. Interfaces processus

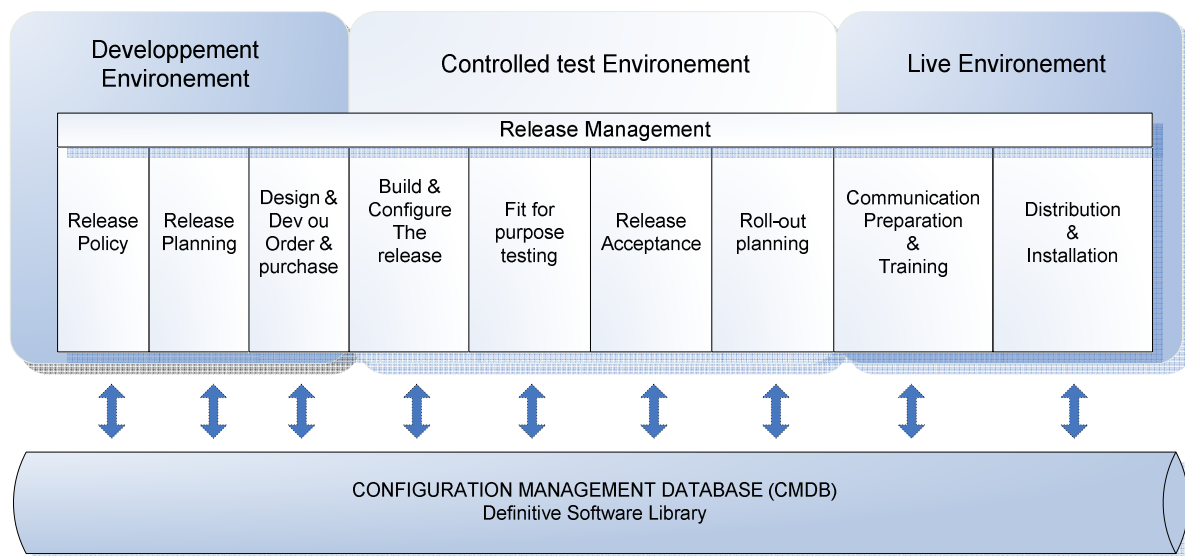


#### 1.7.2.2. Workflow nouveau logiciel



### 1.7.3. Activités

- Planification et politique de mise en production
- Design, build et configuration des mises en production
- Acceptation des mises en production
- Test approfondis en fonction des critères d'acceptation prédéterminés
- Recette des mises en production
- Communication, préparation et formation
- Audits des logiciels et des matériels avant et après l'implémentation du changement
- Installation des matériels
- Stockage des logiciels contrôlés (DSL)
- Mise en production, distribution et installation



#### 1.7.4. Implémentation

##### 1.7.4.1. Politique de mise en production

Elle traite des N° de version, de leur fréquence et des niveaux de l'infrastructure IT qui sera contrôlée par la Gestion des versions.

##### 1.7.4.2. Planification des releases

Entrées	Sorties
Cycle de vie du projet Livrables RfC autorisées Politique de mise en production Vue d'ensemble des besoins de l'entreprise Contraintes et dépendances Avis du CAB Templates	Plan pour une release particulière Plans de tests macroscopiques Critères d'acceptation

##### 1.7.4.3. Design, build (construction) et configuration

Entrées	Sorties
Définition de la version Plans de mise en production	Instructions détaillées de l'assemblage et de la construction des versions Ordre d'achat (licence, maintenance) auprès d'éditeur ou de constructeurs Scripts d'installation automatique et plans de tests associés

	Copie master de l'installation et des instructions stockés dans la DSL Procédure de retour
--	-----------------------------------------------------------------------------------------------

#### **1.7.4.4. Recette de la version**

Entrées	Sorties
Environnement de tests configurés Plans de la version Critères d'acceptation Instruction d'installation Plans de tests pour les scripts d'installation Procédure de retour documentée	Procédure de retour testée Composant de la version testée Erreurs connues Documentation de support Instructions opérationnelles Autorisation d'implémenter la version (change management)

#### **1.7.4.5. Planning de déploiement**

3 types de déploiement :

- Par lots
- Big bang
- Par phases

#### **1.7.4.6. Communication préparation et formation**

Entrées	Sorties
Planning de déploiement détaillé Copie des médias d'installation Manuels d'installation Documentation Formulaires et recettes	Versions finales des documentations de support et utilisateurs et les manuels de formations Release plans mis à jour ainsi que leurs documentations associées

#### **1.7.4.7. Distribution et installation**

Entrées	Sorties
Plan de déploiement détaillé Procédure d'installations testées Composants de la version testée Procédure et plans de retour arrière sont testés	Service informatique mis à jour Enregistrement de la CMDB mis à jour CI retirés de l'environnement de production Enregistrement des nouvelles erreurs connues dans l'environnement de production

#### **1.7.4.8. Meilleures pratiques**

- Stockage physique de tous les logiciels opérationnels dans la DSL
- Distribution des logiciels uniquement à partir de la DSL
- Intégration du processus de Release Management avec les processus de Configuration et de change
- Contrôle de tous les logiciels selon les politiques de versions
- Inclus tous les logiciels et matériels achetés par l'entreprise

#### **1.7.4.9. Bénéfices**

- Construction et implémentation des versions dans les délais impartis
- Elimination des incidents liés à la mise en production des versions
- Gestion sécurisé et à jour de la DSL/DHS
- Facilite la conformité avec les obligations légales
- Distribution précise des versions

#### **1.7.4.10. Blocage potentiels**

- Difficulté d'établir des politiques de versions et de mises en production avec les fournisseurs
- Implémentation de logicielle sans suivi des procédures
- Difficulté pour créer la DSL
- Difficulté d'intégrer la DSL dans un environnement distribué automatisé
- Difficulté pour prévenir les contournements des politiques de numérotation de version

### **1.7.5. Divers**

#### **1.7.5.1. Indicateurs clés**

- Nombre de restauration non autorisées vers des versions antérieures
- Nombre de logiciels non autorisés et utilisés
- Enregistrement des activités de construction, de distribution et d'implémentation dans la CMDB
- Un post mortem est effectué pour toutes les activités de release
- 

#### **1.7.5.2. Terminologie**

Release : collection de changements autorisés par l'IT

Catégories :

- Mises à jour logicielle et matérielles majeures
- Mises à jour logicielle et matérielles mineures
- Mises à jour logicielle et matérielles d'urgence

## 2. Lexique

**Service** : acte de transformer les ressources (humaines, matérielles, logicielles) en service.

**Processus** : série d'activités interconnectées entre elles réalisées par des agents dans le but d'atteindre un objectif.

**Rôle** : Ensemble d'activité d'autorisation et responsabilités

**Incident** : Événement ne faisant pas partie des opérations normales, provoquant ou pouvant provoquer une interruption ou une dégradation de service.

**Service Request** : Incident non lié à une erreur d'infrastructure (ex: mot de passe oublié)

**Problème** : Cause inconnue d'un ou plusieurs incidents

**Erreur** : cause connue d'un ou plusieurs incidents

**Erreur connue (KE)**: problème diagnostiqué et pour lequel une WA a été identifiée

**Work around (WA)** : solution de contournement à un incident