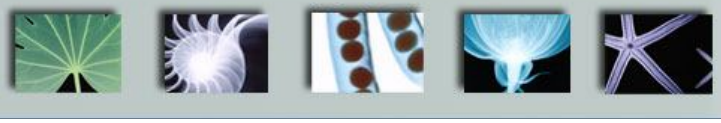
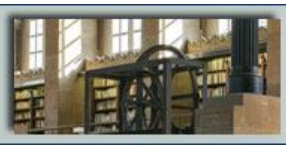


ITIL V2

La gestion des incidents

Création : novembre 2004
Mise à jour : août 2009

Pascal Delbrayelle Consultant
+33 (0)6 61 95 41 40
http://www.itilfrance.com



A propos

A propos du document

Ce document de référence sur le référentiel ITIL a été réalisé en 2004 et la traduction des 2 livres ITIL *Service Support* et *Service Delivery* a nécessité 4 mois de traduction et d écriture.

Il est mis à la disposition de la communauté francophone ITIL pour diffuser les connaissances de base sur ce référentiel.

Ce document peut être utilisé de manière libre à condition de citer le nom du site (www.itilfrance.com) ou le nom de l auteur (Pascal Delbrayelle).

A propos de l'auteur

Pascal Delbrayelle intervient avec plus de 25 ans d'expérience comme consultant sur les projets d'une direction informatique ayant comme facteur de succès la mise en oeuvre des bonnes pratiques ITIL comme, par exemple, la mise en place d'un site de secours, la mise en place d'un outil de gestion des configurations ou la définition des normes et standards techniques des environnements de production.

Ces projets requièrent :

- la connaissance des différents métiers du développement et de la production informatique
- la pratique de la conduite de projets techniques de la direction informatique
- la maîtrise de la définition et de la mise en place de processus pour rationaliser et adapter les méthodes de travail au sein de la direction informatique

A propos de mission et de formation

Si vous pensez que l expérience de l auteur sur le référentiel ITIL ou la formalisation de documents sur le sujet peut vous aider dans vos projets de production ou de mise en oeuvre des processus ITIL, n hésitez pas à le contacter pour toute question ou demande :

- par mail : pascal.delbrayelle@itilfrance.com
- par téléphone : +33 (0)6 61 95 41 40

Quelques exemples de mission :

- Modélisation simple des processus de gestion des changements, des projets et des mises en production en vue de la sélection, l'achat et l'implantation d'un outil de gestion de projets avec planification, gestion des ressources, des budgets, des livrables et des connaissances
- Accompagnement avec la réorganisation d'un DSI passant d'une organisation en silos techniques vers une organisation inspirée du référentiel ITIL et la mise en oeuvre d'outils pour institutionnaliser les processus ITIL
- Accompagnement d'une DSI dans la formulation de l'appel d'offres au futur centre de services en se basant sur les processus et la fonction centre de services du référentiel ITIL

Sommaire

1 Objectif

La définition ITIL de l'objectif de la Gestion des Incidents est la suivante :

Restaurer aussi vite que possible le fonctionnement normal des services et minimiser l'impact négatif sur les activités métiers et s'assurer ainsi que les meilleurs niveaux de qualité de service et de disponibilité sont maintenus.

Le « fonctionnement normal des services » s'entend ici comme le fonctionnement des services dans les limites des Contrats de Niveaux de Service (SLAs)

2 Périmètre

2.1 Définition d'un Incident et extensions

La définition ITIL d'un Incident est la suivante :

« Tout événement qui ne fait pas partie du fonctionnement standard d'un service et qui cause, ou peut causer, une interruption ou une diminution de la qualité de ce service. »

Quelques exemples :

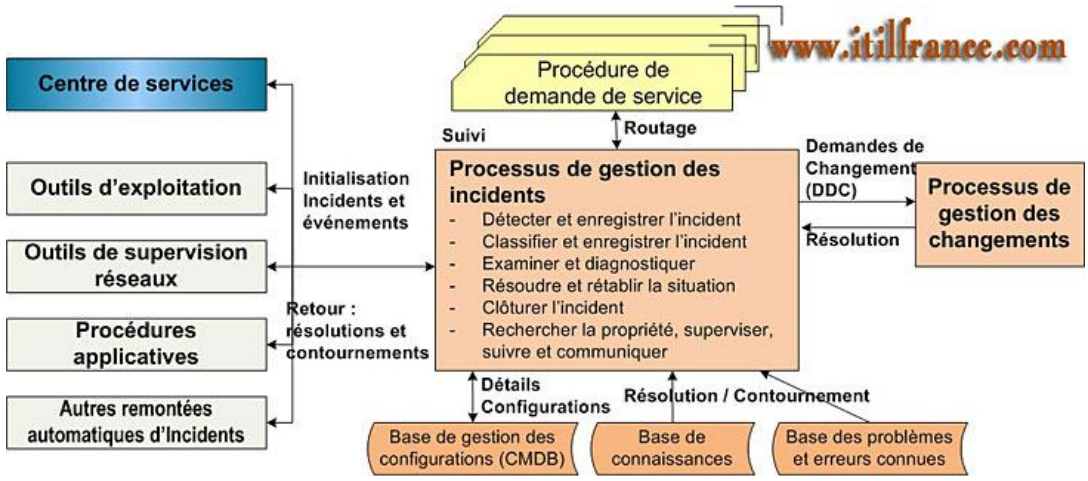
- application : application non disponible, erreur programme empêchant l'Utilisateur de travailler, nombre d'E/S disques excessifs
- matériel : système HS, remontée d'alerte automatique, sortie imprimante bloquée
- demandes de services : demande d'information, de conseil ou de documentation, oubli d'un mot de passe

2.2 Extensions de la définition

Le terme Incident est généralement compris comme un dysfonctionnement signalé par un Utilisateur. Cependant, deux extensions à cette définition sont généralement utilisées car elles vont suivre le même processus de traitement que les dysfonctionnements proprement dits et sont donc assimilés à des Incidents :

- Les **demandes pour un nouveau service (ou l'extension d'un service existant)** sont considérées comme des Demandes de Changement (RFCs) mais assimilées à des Incidents en pratique (traitement identique) et traitées dans le cadre de la Gestion des Incidents
- Les **Remontées d'alertes automatiques** (espace-disque saturé par exemple) : elles sont souvent considérées comme faisant partie de l'exploitation courante ; ces événements sont traités dans le cadre de la Gestion des Incidents même si le service délivré aux Utilisateurs n'est pas affecté

2.3 Processus de Gestion des Incidents



En entrée du processus, nous retrouvons :

- Détails des Incidents (du Centre de Services et des différentes sources automatiques)
- Détails des Configurations (de la CMDB)
- Recherche correspondances (*matching*) entre Incidents et Problèmes & Erreurs connues (de la base de données Problèmes/Erreurs Connues)
- Détails de la résolution de l'Incident de nature similaire (de la même base)
- Retour des Demandes de Changement en correction d'un Incident (du processus Gestion des Changements)

En sortie du processus, nous avons :

- Routage des demandes de services
- Demandes de Changement pour résoudre certains Incidents
- Mise à jour de la base des Problèmes/Erreurs Connues
- Communication aux Utilisateurs (pendant l'avancement et à la fermeture)
- Rapports à la hiérarchie

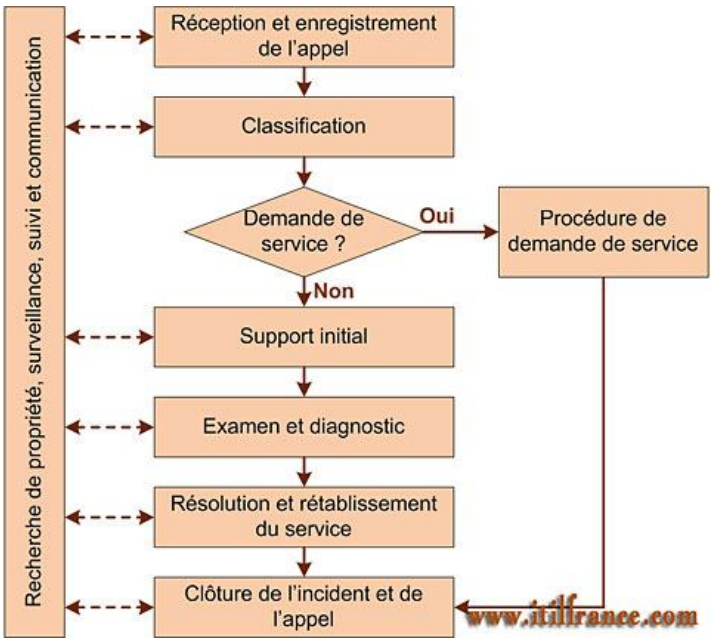
Dans le processus, les activités de la Gestion des Incidents sont les suivantes :

- Détection et enregistrement des Incidents
- Support initial et classification
- Investigation et diagnostic
- Suivi global des Incidents
- Résolution et rétablissement
- Fermeture des Incidents

3 Concepts de base

3.1 Cycle de vie d'un Incident

Le cycle de vie d'un Incident est le suivant :



Quelques remarques :

- Le Centre de Services est responsable de l'aboutissement de tous les Incidents enregistrés (propriétaire des Incidents).
- Le processus de traitement est essentiellement réactif .
- Les Incidents ne pouvant pas être résolus immédiatement doivent être assignés aux groupes de spécialistes.
- La résolution ou une solution de contournement doit intervenir le plus vite possible pour rétablir le service impacté

3.2 Cycle de vie d'un Incident : Préconisations

Tout au long du cycle de vie de l'Incident, l'enregistrement doit être à jour pour permettre à n'importe quelle personne de l'équipe du Centre de Services de communiquer sur l'Incident simplement en consultant l'enregistrement.

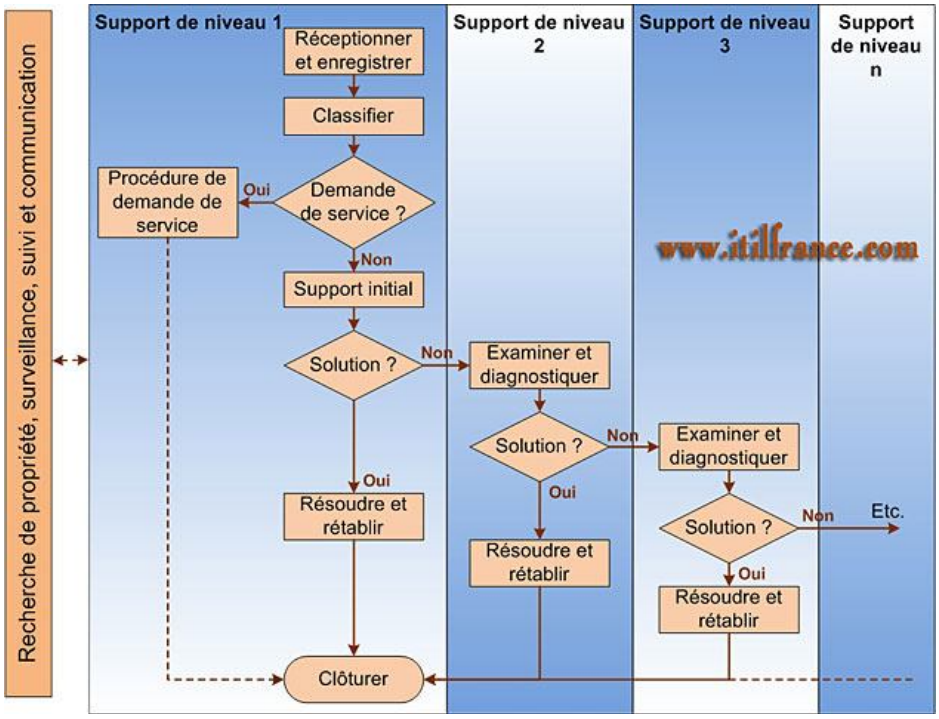
Il est nécessaire de conserver la description originelle de l'Incident même si la description en cours évolue. Par exemple, un Utilisateur signale un Incident avec son imprimante (son édition ne s'imprime pas). Après investigation, il s'agit en réalité d'un problème réseau mais, lorsque l'Incident est clos, il est préférable que le Centre de Services prévienne l'Utilisateur simplement en lui précisant que son problème imprimante est réglé plutôt que de lui expliquer le problème réseau et sa résolution.

Il faut aussi conserver un historique des modifications sur l'enregistrement de l'Incident. Tous les changements d'état doivent être tracés (date/heure, personne qui a provoqué le changement, etc.)

Si l'une des équipes n'a pas accès à l'outil de Gestion des Incidents, il est impératif de bien mettre en place une procédure de mise à jour de ces enregistrements à faire lors des interventions de ces équipes(par exemple: maintenance tierce ou support de nuit n'ayant pas accès à l'outil durant la nuit)

3.3 Premier, deuxième et troisième niveaux de support

Voici un schéma (classique) d'escalade d'un Incident sur les différents niveaux de support, à commencer par le Centre de Services :



Il est à noter que certains niveaux de support peuvent être des sociétés extérieures (externalisation du support ou appel aux constructeur/éditeurs dans le cadre de contrats de support passés entre l'entreprise et ces sociétés extérieures).

3.4 Escalade fonctionnelle et escalade hiérarchique

3.4.1 Escalade fonctionnelle

C'est l'escalade traditionnelle et prévue dans le processus pour transférer un Incident d'un niveau au niveau supérieur .

Cette escalade peut intervenir dans deux cas :

- par manque de connaissance ou d'expertise du niveau en cours.
- par dépassement d'un délai (à définir avec précaution et ne pas dépasser les délais des Contrats de Niveaux de Service)

3.4.2 Escalade hiérarchique

Ce type d'escalade n'est pas réellement prévue dans le processus. Cependant, en pratique, on constate que cette escalade existe et est nécessaire au bon fonctionnement du service dans certains cas.

L'escalade hiérarchique peut intervenir à n'importe quel moment dans le cycle de Gestion de l'Incident lorsqu'il est évident que la résolution interviendra hors-délai ou sera insatisfaisante. Ceci demande un certain recul vis-à-vis du processus qui, s'il est suivi à la lettre, peut aboutir dans certains cas à des situations critiques.

Dans l'idéal , l'escalade hiérarchique devrait intervenir avant la fin du délai pour que la hiérarchie ait le temps de réagir. En pratique, on constate que l'escalade hiérarchique est utilisée lorsque les temps de résolution de l'Incident sont hors délai.

3.5 Enregistrement d'un Incident

Le Centre de Services est propriétaire de l'Incident et en est responsable jusqu'à la résolution et sa fermeture.

L'élément important de l'enregistrement d'un Incident (que l'on peut aussi appeler fiche Incident) est sa priorité de traitement par rapport aux autres Incidents en cours.

3.5.1 Fixer la priorité

La priorité d'un Incident est déterminée par :

- **L'impact sur l'activité de l'entreprise** . L'impact représente la criticité sur l'activité métier (Incident ou Problème). Certaines définitions de la criticité (ou niveau de risque) précisent qu'il y a 3 facteurs : fréquence, gravité, probabilité de non-détection. L'impact est souvent mesuré au nombre de personnes ou de systémes affectés.
- **L'urgence à mettre en place une solution** définitive ou de contournement (urgence: effort attendu et vitesse nécessaire pour résoudre l'Incident)

Pour fixer correctement le niveau de priorité sans perdre trop de temps, il est nécessaire d'avoir un cadre de travail. Ce cadre est fixé par les différents Contrats de Niveaux de Service. En pratique , on retrouvera une codification déjà définie (impact/urgence) dans ces Contrats de Niveaux de Service.

3.5.2 Rôles du Centre de Services dans la Gestion des Incidents

Les points importants à prendre en considération sont les suivants :

- tous les Incidents sont remontés vers le Centre de Services et doivent être enregistrés par celui-ci (y compris les remontées automatiques dans l'idéal)
- la majorité des Incidents (jusqu'à 85%) pourront être résolus par le Centre de Services (constaté lorsqu'une Gestion effective des Incidents est en place)
- le Centre de Services est la fonction « indépendante » de suivi de l'ensemble des Incidents jusqu'à leur résolution
- le Centre de Services effectue la coordination des équipes de support intervenant dans la résolution des Incidents.

3.5.3 Actions principales à l'enregistrement

- enregistrement du détail (symptôme, etc.)
- s'il s'agit d'une Demande de Service, utilisation de la procédure associée
- l'Elément de Configuration (CMDB) à l'origine probable de l'Incident est associé à la fiche
- assignation de la priorité adéquate et communication à l'Utilisateur d'un identifiant d'Incident
- l'Incident est évalué et, si possible, la solution est donnée (Incident fréquent ou Erreur Connue)
- l'Incident est assigné au support de niveau deux si besoin ou
- la fiche est complétée et fermée si la solution a été donnée

3.5.4 Actions principales à la fermeture

- confirmer la résolution avec l'Utilisateur ou l'émetteur
- définir la catégorie de la solution apportée

- compléter l'enregistrement de l'Incident
- fermer l'Incident en vérifiant que :
- les détails de la solution sont clairs et lisibles
- les codes de refacturation sont renseignés (*cost-centre*)
- les temps passés sur l'Incident sont renseignés

Ceci est indispensable pour éviter les conflits entre équipes de support et Clients sur la validité de la fermeture

Il est nécessaire d'avoir un accès restreint à l'option de fermeture des Incidents (typiquement le responsable du Centre de Services gère ces accès)

3.6 Incidents, Problèmes, Erreurs Connues et Demandes de Changement

Un Incident est la conséquence d'échecs ou d'erreurs de traitements dans l'infrastructure informatique

La cause d'un Incident peut être évidente et peut être éradiquée directement par le Centre de Services sans investigation complémentaire en :

- réparation immédiate
- solution de contournement
- Demande de Changement

Quand la cause sous-jacente d'un Incident n'est pas connue, il est nécessaire d'initialiser un Problème dans le processus de Gestion des Problèmes.

Un Problème est ainsi le signe d'une erreur inconnue dans l'infrastructure.

Plusieurs Incidents peuvent sembler partager la même origine donnant lieu à la définition d'un Problème unique

Un Problème est indépendant des Incidents associés. L'analyse du Problème peut continuer même si les Incidents ont été résolus et fermés.

Résolution d'un Problème :

1. Identification de l'erreur sous-jacente
2. Mise au point d'une solution de contournement ou émission d'une Demande de Changement

Le Problème devient alors une Erreur Connue.

3.7 Définitions

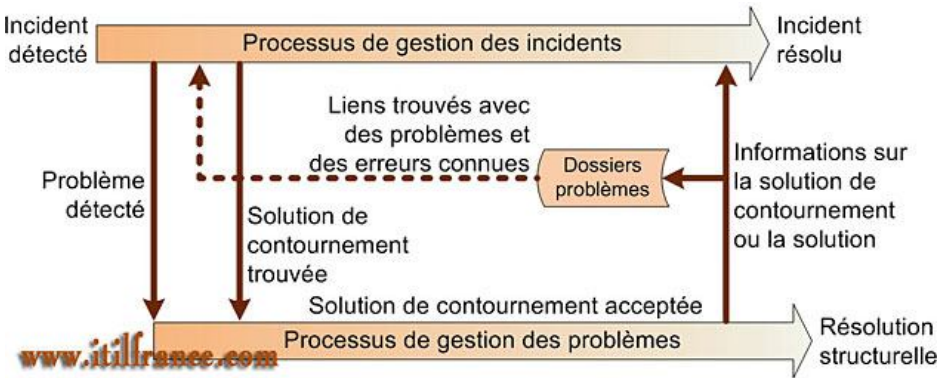
Problème : La cause inconnue d'un ou de plusieurs Incidents

Erreur connue : Problème diagnostiqué correctement et pour lequel il existe une solution de contournement ou une Demande de Changement a été émise

Demande de Changement : Une demande d'ajout, de modification, d'évolution, de suppression de composant(s) de l'infrastructure informatique ou pour tout autre aspect de la Production Informatique

3.8 Incidents, Problèmes, Erreurs Connues et Demandes de Changement

Les interactions entre les processus Gestion des Incidents et Gestion des Problèmes sont complexes mais il est nécessaire de les maîtriser afin de bien séparer ces deux processus dont les finalités sont très différentes.



Dans le processus de résolution d'un Incident, les actions suivantes doivent être entreprises :

- si l'Incident semble avoir une cause inconnue, il faut initialiser un Problème dans le processus de Gestion des Problèmes.
- étudier une correspondance avec les Problèmes référencés et les Erreurs Connues
- étudier une correspondance avec les Incidents référencés (similaires résolus ou en cours)
- si pas de solution, la Gestion des Incidents a la responsabilité d'en trouver une (définitive ou de contournement) avec l'impact minimum sur l'activité de l'entreprise

Les flux entre la Gestion des Incidents et la Gestion des Problèmes sont croisés :

- lors de l'analyse de l'Incident par la Gestion des Incidents pour redémarrer le plus vite possible le service impacté, si une solution de contournement est trouvée, l'information doit être transmise à la Gestion des Problèmes pour analyse
- lors de l'analyse du Problème par la Gestion des Problèmes, une solution définitive ou de contournement à un ou plusieurs Incidents a été trouvée, la Gestion des Problèmes met à jour la base des Problèmes/Erreurs Connues et transmet l'information à la Gestion des Incidents pour action sur les Incidents associés (passage des Incidents en Erreur Connue ou Résolu)

4 Bénéfices

4.1 Pour l'entreprise :

- Réduction de l'impact des Incidents sur les activités métiers augmentant ainsi leur efficacité

4.2 Pour la Production Informatique :

- Surveillance améliorée des Incidents permettant une réelle mesure des performances vis-à-vis des Contrats de Niveaux de Services
- Gestion de la qualité améliorée
- Meilleure utilisation des ressources
- Disparition des Incidents et Demandes de Services perdues ou erronées
- Mise à jour de la CMDB à l'enregistrement d'un Incident
- Augmentation de la satisfaction des Utilisateurs et des Clients

4.3 A contrario, la non-implémentation d'une Gestion des Incidents entraîne :

- Pas de gestion, pas d'escalade des Incidents : ils deviennent plus graves qu'il ne le devraient, ils dégénèrent
- Les équipes de spécialistes sont sujets à de constantes interruptions, les rendant moins efficaces
- Les utilisateurs sont dérangés par des collègues demandant des conseils au lieu d'appeler le Centre de Services
- Résolution fréquente à partir de zéro d'un Incident plutôt que d'utiliser une solution déjà référencée
- Absence d'informations de synthèse pour la hiérarchie
- Incidents perdus ou gérés de manière incorrecte

5 Mise en oeuvre et planification

5.1 Séquencement et calendrier

- Ne pas mettre en place de manière isolée des autres processus et fonctions (Centre de Services, Gestion des Problèmes, des Configurations, des Changements, Gestion des Nouvelles Versions)
- Si cela n'est pas possible, il est nécessaire d'implémenter au moins en même temps Centre de Services & Gestion des Incidents (objectifs rapides à atteindre)

- Profiter des démarrages de services importants pour les intégrer tout de suite dans une Gestion des Incidents (même si le nombre d'Utilisateurs ou le nombre d'appels ne justifient pas dans ce cas la mise en place d'un Centre de Services et d'une Gestion des Incidents)
- Planification de la mise en place du processus : 3 à 6 mois
- Mise en place du processus : 3 mois à 1 an
- Choix des outils logiciels : prendre les logiciels conformes à ITIL
- CMDB inexistante ou pas mise en place en même temps : intégrer les informations de configuration dans la base de Gestion des Incidents

5.2 Difficultés à prévoir :

- pas d'engagement de la hiérarchie
- manque de clarté des besoins métiers
- méthodes de travail non révisées
- pas d'informations sur les niveaux de services
- manque de connaissances des Incidents résolus
- manque d'intégration avec les autres processus
- résistance au changement

6 Traitement des Incidents majeurs

Il est à noter que le chapitre sur les Incidents majeurs dans le document ITIL Service Support est léger et que tout le chapitre est mis au conditionnel.

Les Incidents majeurs sont ceux pour lesquels le degré d'impact sur l'ensemble des Utilisateurs est extrême.

Devraient être considérés comme Incidents majeurs les Incidents pour lesquels l'échelle de temps des perturbations devient excessif au regard des temps de résolution (SLAs) (même si cela impacte un petit nombre d'Utilisateurs)

Le Gestionnaire de Problèmes devrait être averti (s'il ne l'est pas déjà) afin d'organiser une réunion (ou une série de réunions) avec toutes les parties concernées :

- équipes de support internes
- équipes de support des matériels/logiciels (et/ou mainteneur)
- équipes de gestion des services de la Production

Le Centre de Services devrait participer à ces réunions et enregistrer dans la base d'Incidents toutes les actions prises et les décisions.

Nous pouvons considérer qu'il s'agit là d'une période de crise qui ne peut pas être décrite de manière exhaustive dans une méthode car l'important est d'agir vite malgré le nombre peut-être important d'intervenants. Cependant, on peut en déduire en pratique deux points à avoir en mémoire :

1. *le traitement des Incidents majeurs est sous la responsabilité du Gestionnaire de Problèmes*
2. *une information à jour et une communication cohérente sont importantes (évolution très rapide des informations et un besoin très fort en informations des équipes de la Production impliqués et des Clients et Utilisateurs impactés). Ce rôle est rempli par le Centre de Services qui doit collecter ces informations et les enregistrer au niveau de ou des Incidents associés au Problème.*

7 Indicateurs clés de performances (*KPI : Key Performance Indicators*)

Juger de la performance du processus : les KPIs (Key Performance Indicators)

7.1 Métriques couramment utilisées :

- nombre total d'Incidents
- temps moyen de résolution par code d'impact

- pourcentage d'Incidents résolus dans les temps contractuels (à définir dans les Contrats par code d'impact par exemple)
- coût moyen de traitement d'un Incident
- pourcentage d'Incidents fermés par le Centre de Services sans support extérieur (la satisfaction Clients est fortement influencée par le fait que le Centre de Services puissent apporter une solution immédiate à l'Incident)
- nombre et pourcentage d'Incidents résolus sans déplacement sur site

7.2 Diffusion des informations

La diffusion se fait par le responsable de l'équipe Gestion des Incidents

Il est nécessaire de définir la périodicité et les listes de diffusion en accord avec le Centre de Services et les différentes équipes de support.

La diffusion doit inclure au minimum l'équipe chargée des Contrats de Niveaux de Services et les équipes de support

Il faut aussi considérer aussi une diffusion vers les Clients et Utilisateurs (par le biais des rapports sur les Contrats de Niveaux de Service par exemple)