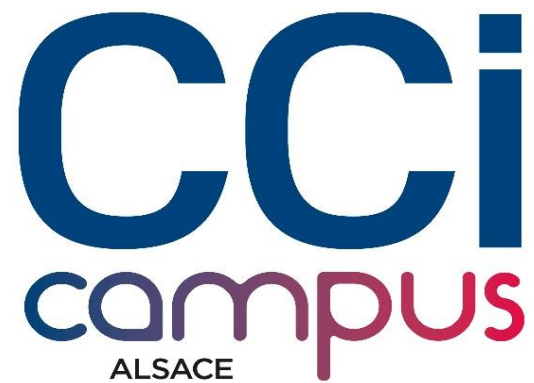


HENRY Alexis,
Rakotozafy Winness,
KOTTO Victor,
Bolidum Théo,
04/04/2022



Gestion des
Incidents.
Gestion d'un
problème.

SOMMAIRE

<u>I.</u>	Gestion des incidents	1
a.	Définition	2
b.	Objectifs	3
c.	Bénéfices	3
d.	Politique	4
e.	Cycle de vie	4
f.	Logigramme	5
g.	Qualification	6
h.	Escalade	7

<u>II.</u>	Gestion d'un problème	8
a.	Définition	8
b.	Objectifs	8
c.	Bénéfices	9
d.	Politique	9
e.	Cycle de vie	10
f.	Logigramme	11
g.	Qualification	12
h.	Escalade	13

I. Gestion des incidents.

La gestion des demandes de service consiste à traiter une demande d'un utilisateur concernant un service à fournir, comme l'accès aux apps, les améliorations logicielles et les informations.

Il peut parfois être difficile de différencier une demande de service d'un incident. En fait, les deux n'étaient pas distingués et étaient regroupés dans la catégorie « incidents » jusqu'à la publication de la version 3 d'ITIL en 2007. ITIL définit maintenant un incident comme « toute interruption non planifiée d'un service informatique ou réduction de la qualité d'un service informatique ».

Une demande de service est définie comme « une demande formelle d'un utilisateur pour la fourniture d'un élément. Par exemple, une demande d'information ou de conseil, la réinitialisation d'un mot de passe ou l'installation d'un poste de travail pour un nouvel utilisateur ».

a. Définition.

« Un incident se définit par 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. »

source : <https://www.appvizer.fr/magazine/services-informatiques/securite-informatique/gestion-incidents>

La gestion des incidents se définit aussi par deux normes, la norme ITIL et l'ISO 20000.

Norme ITIL

ITIL ou Information Technology Infrastructure est un projet développé dans les années 1980 par l'Office public britannique du commerce. ITIL est en quelque sorte un ensemble de documents visant à mettre en place les bonnes pratiques à faire lors de la gestion des services informatiques. L'idée est d'avoir une amélioration continue du projet.

Norme ISO 20000

L'ISO 20000 est une norme de certification des services informatiques. Elle permet de respecter les bonnes pratiques dans une entreprise (informatiquement) et permet d'assurer la qualité des services de celle-ci

b. Objectifs.

Selon ITIL, l'objectif de la gestion des incidents est de pouvoir restaurer aussi vite que possible les services proposés par l'entreprise et ainsi réduire les gênes qu'un dysfonctionnement informatique peut causer.

De plus, il faut pouvoir augmenter la visibilité et la communication des incidents déclaré par les utilisateurs. Enfin, le dernier objectif retenu dans la gestion des incidents est la priorité de gestion des incidents avec ceux de l'entreprise, en effet si un problème mineur à une priorité maximal et qu'à l'inverse un problème majeur à une priorité minimal, l'entreprise ne pourra pas gérer correctement les problèmes.

A chaque fois qu'un incident ne trouve pas de solution il est envoyé à un niveau de traitement supérieur pour un diagnostic plus poussé jusqu'à sa résolution.

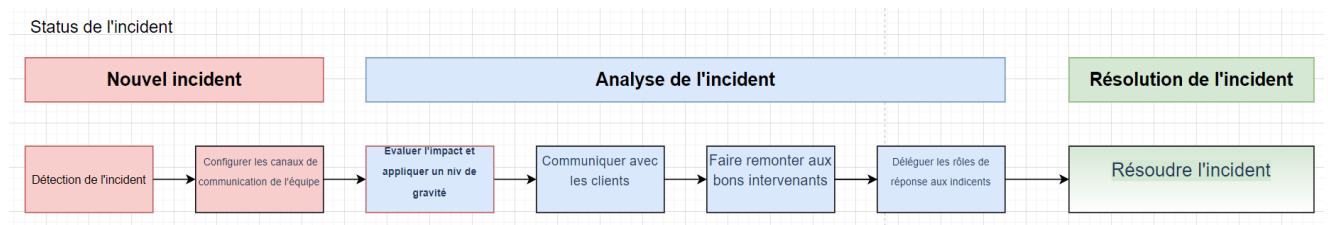
c. Bénéfices.

Lorsqu'un incident est détecté il est notifié et passe par plusieurs étapes de traitement afin de rétablir au plus vite le fonctionnement normal des services informatiques.

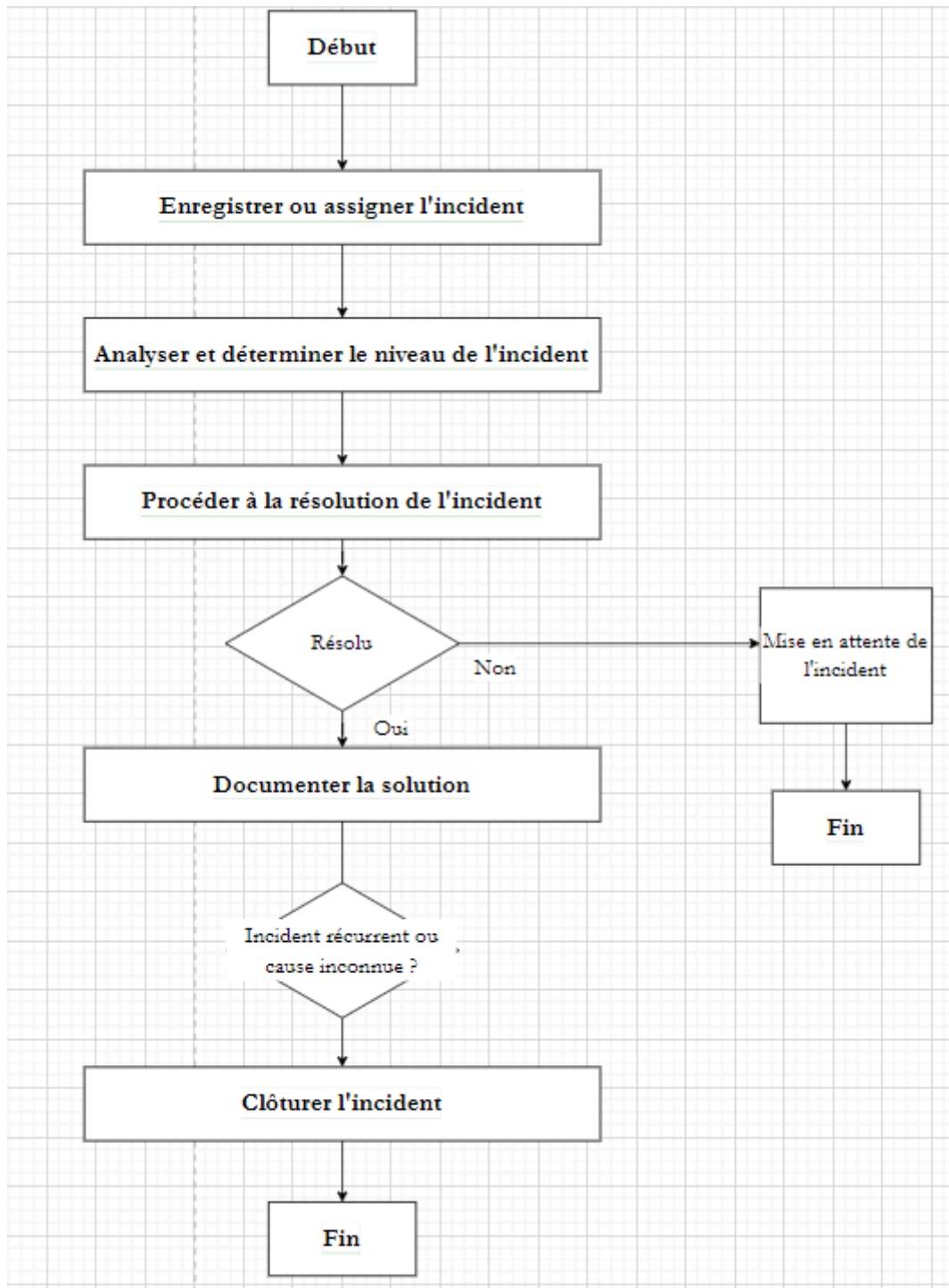
d. Politique .

Si aucune solution n'est trouvée le problème est envoyé à chaque fois à un niveau de traitement plus élevé jusqu'à ce qu'une solution soit trouvée

e. Cycle de vie.



f. Logigramme.



g. Qualification.

Pour pouvoir qualifier la gestion des incidents, nous devons comprendre les différentes catégories d'incident dans un système d'information :

- **Les incidents types logiciels ou applicatifs** : bug/erreur programme sur un application métier freinant les activités de l'utilisateur
- **Les incidents types matériels** : par exemple malfonctionnement d'une imprimante, câbles Ethernet usés, etc...
- **Les demandes de services** : non accès à une application pour cause d'oubli de mot de passe, non accès à des fichiers/dossiers (problème de droits d'accès), etc...

Ensuite, en plus des types d'incidents, il existe également plusieurs degrés de priorité, en fonction de la gravité de l'incident et de l'urgence à le traiter.

Ces urgences et le degré de priorité sont définis par le **DSI** (Direction Système d'Information), ce sont l'impact sur l'activité de l'entreprise, et l'urgence à mettre en place une solution qui déterminent la classification des priorités. Ces paramètres sont généralement définis par :

- La perte financière pour l'entreprise générée par l'incident,
- L'impact de l'incident sur des utilisateurs VIP,
- Le non-respect des réglementations et des lois auquel l'incident peut conduire, etc.

		IMPACT		
		Élevé (Organisation en entier)	Moyen (Département, service ou > 5 utilisateurs)	Bas (1-5 utilisateurs)
URGENCE	Urgent	P1 - Majeure	P2 - Élevée	P3 - Normale
	Normal	P2 - Élevée	P3 - Normale	P4 - Basse

Source : octopus-itsm.com

Tableau 1 : Matrice sur l'évaluation des incidents

h. Escalade.

Comme mentionné dans la définition : « *A chaque fois qu'un incident ne trouve pas de solution il est envoyé à un niveau de traitement supérieur pour un diagnostic plus poussé jusqu'à sa résolution.* » c'est la notion d'escalade de traitement d'incident.

Il y existe différents acteurs dans l'escalade de traitement des tickets, généralement définit comme support de niveau n allant de 1 à 3.

Les niveaux de support sont généralement définis par le niveau de compétences techniques, et les diplômes.

Pour chaque incident, de base il passe par le support de niveau de 1, qui sera traité par ce dernier, jusqu'à ce que le problème ne soit plus géré par l'équipe de support et faire remonter le traitement du ticket par le support de niveau n+1.

- Support de niveau 1

Le support de niveau 1 correspond aux demandes présentées au centre support, et est généralement assurés par des techniciens juniors non spécialisés, généralement appelé « technicien helpdesk »

- Support de niveau 2

Le support de niveau 2 est plus complexe à traiter, il s'agit d'incident de type applicatif, messagerie, CRM, ERP, réseau, système, etc. Les techniciens de niveau 2 ont généralement une expérience de plusieurs années et/ou une spécialisation.

- Support de niveau 3

Le support de niveau 3 est celui qui regroupe tous les incidents lourds, problématique serveur, réseau, cybersécurité, etc. Généralement contacté en situation de crise, le personnel intervenant en niveau 3 est de niveau technicien spécialisé, administrateur ou ingénieur.

Lorsque qu'une demande ne peut pas être traitée par le niveau inférieur elle est escaladée vers le niveau supérieur, c'est ce principe qui permet une meilleure prise en compte des demandes et de leur résolution, l'essentiel étant de faire traiter une demande par le groupe ayant le niveau adéquat et éviter ainsi une perte de temps et donc de garantir le meilleur niveau de service, afin de respecter un indicateur important dans les traitements des tickets que ce soit pour les problèmes ou les incidents (GTR = Garantie de Temps de Rétablissement).

II. Gestion d'un problème.

a. Définition.

Selon l'ITIL la gestion d'un problème est un processus responsable de la gestion du cycle de vie de tous les problèmes.

Les missions d'une équipe de gestion de problème sont notamment de prévenir les futurs incidents et de minimiser l'impact de ceux-ci s'ils ne peuvent être évités. La définition de la gestion d'un problème est sensiblement similaire à celle de la gestion des incidents.

b. Objectifs.

La principale mission de la gestion des problèmes est de trouver les incidents fréquents ainsi que de trouver une solution aux problèmes pouvant être résolus.

Quant à ceux qui ne peuvent pas être résolus, il s'agit de trouver une solution qui réduit le problème au maximum.

c. Bénéfices.

Permet de déposer le problème sur papier pour le rendre visuellement plus claire. Chaque étape est vue au peigne fin (l'environnement dans lequel il est survenu, la cause, le problème et les solutions pour qu'il n'y est plus d'incident à l'avenir).

Le problème est vu dans sa globalité et une fois résolu il y a peu de chance pour qu'il resurviennne.

d. Politique .

La gestion des problèmes ne se résume pas à trouver et à corriger les incidents, c'est également identifier et comprendre les causes sous-jacentes d'un incident, ainsi qu'identifier la meilleure méthode afin d'éliminer cette cause profonde.

De plus, identifier la cause n'a aucune valeur pour une organisation s'il s'agit d'un processus perturbateur effectué par une équipe cloisonnée.

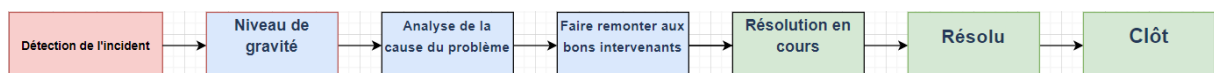
La gestion des problèmes doit donc être constante et largement pratiquée au sein de plusieurs équipes, notamment l'équipe informatique, de sécurité et de développement.

Un incident peut se terminer lorsque le service est à nouveau opérationnel, mais tant que les causes sous-jacentes et les facteurs contributifs ne sont pas traités, le problème demeure.

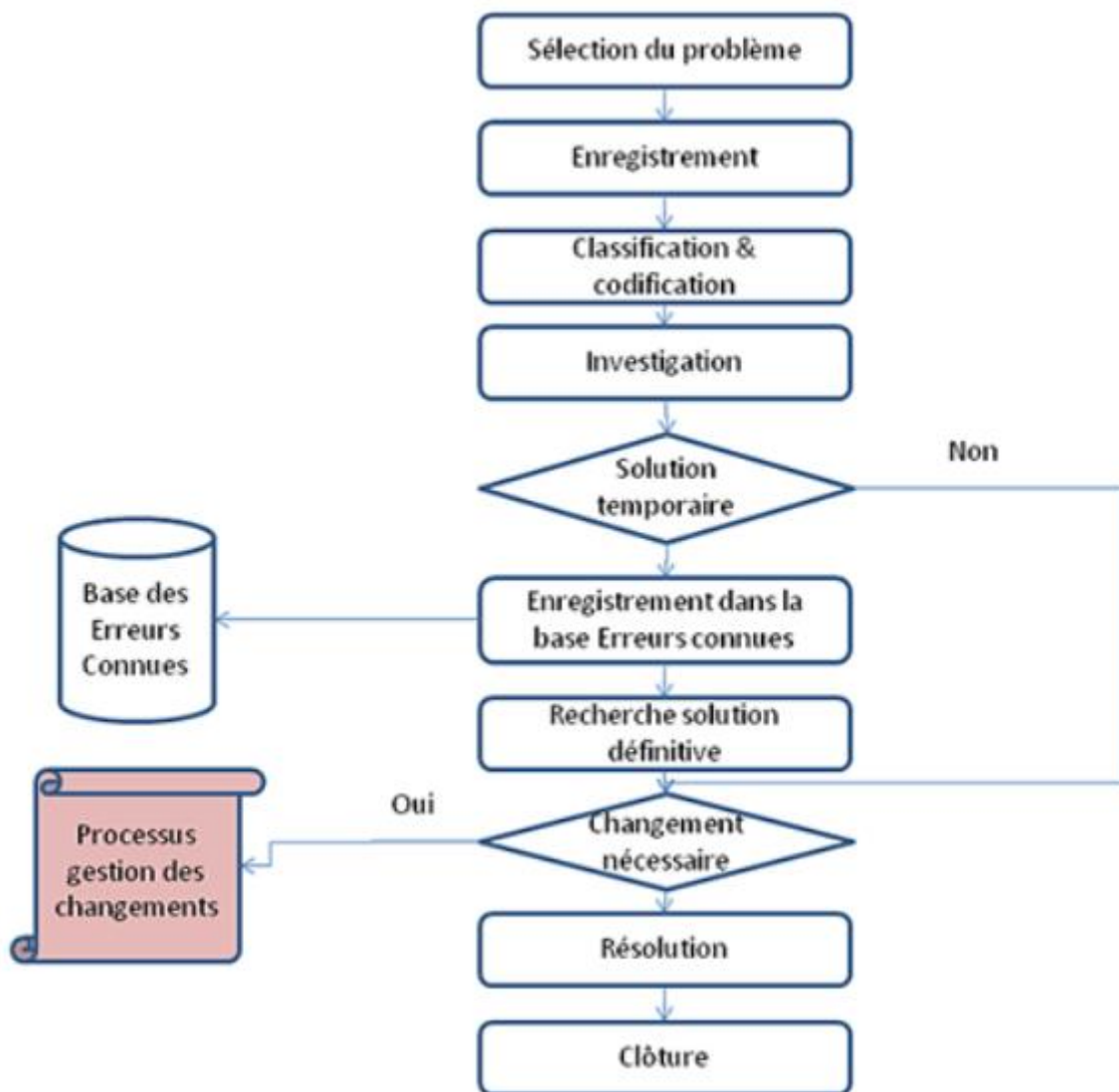
Pour une bonne gestion d'un problème il faut répondre aux questions suivantes :

- Quelles sont les causes qui ont contribué à la survenue de l'incident ?
- Quelle sont les facteurs qui ont mené à l'incident ?
- Comment est-il possible qu'un fichier de configuration puisse être réécrit ?
- Quelles conditions créent une entrée corrompue dans la base de données ?

e. Cycle de vie.



f. Logigramme.



g. Qualification.

Pour qualifier les problèmes, nous allons exactement reprendre à peu près la même méthodologie pour la qualification des incidents, sur le fait qu'un problème majeure est défini par son impact sur le système d'information, car le traitement d'un problème sera défini selon son impact et son urgence pour les utilisateurs et pour les entreprises

Nous allons appréhender la bonne classification d'un problème, afin de favoriser un meilleur traitement du problème en termes de qualité et de rapidité de correction :

2 grands thèmes permettent de classer un problème :

- la **catégorie** ;
- la **priorité** (déduite de l'urgence et de l'impact du problème).

La catégorie permet de comprendre quel élément du système d'information, quel service SI est concerné par le problème.

Ce sont généralement des familles regroupant des domaines techniques, comme: matériel PC/imprimante, serveur, réseau, téléphonie, messagerie, applications métier, bureautique...

L'utilité de la priorité est d'identifier dans quel **ordre** les problèmes doivent être traités.

Ci-dessous une matrice d'évaluation des problèmes sur un parc informatique. A savoir que certaines solutions de gestion de parc (comme GLPI) permet d'intégrer la matrice

afin de classer automatiquement les problèmes et les incidents.

		Impact		
		Fort	Moyen	Faible
Urgence	Fort	P1 Haute	P1 Haute	P2 Moyen
	Moyen	P1 Haute	P2 Moyen	P3 Basse
	Faible	P2 Moyen	P3 Basse	P3 Basse

h. Escalade.

Comme mentionné dans la définition : « *A chaque fois qu'un incident ne trouve pas de solution il est envoyé à un niveau de traitement supérieur pour un diagnostic plus poussé jusqu'à sa résolution.* » c'est la notion d'escalade de traitement d'incident.

Il y existe différents acteurs dans l'escalade de traitement des tickets, généralement définit comme support de niveau n allant de 1 à 3.

Les niveaux de support sont généralement définis par le niveau de compétences techniques, et les diplômes.

Pour chaque incident, de base il passe par le support de niveau de 1, qui sera traité par ce dernier, jusqu'à ce que le problème ne soit plus géré par l'équipe de support et faire remonter le traitement du ticket par le support de niveau n+1.

- Support de niveau 1

Le support de niveau 1 correspond aux demandes présentées au centre support, et est généralement assurés par des techniciens juniors non spécialisés, généralement appelé « technicien helpdesk »

- Support de niveau 2

Le support de niveau 2 est plus complexe à traiter, il s'agit d'incident de type applicatif, messagerie, CRM, ERP, réseau, système, etc. Les techniciens de niveau 2 ont généralement une expérience de plusieurs années et/ou une spécialisation.

- Support de niveau 3

Le support de niveau 3 est celui qui regroupe tous les incidents lourds, problématique serveur, réseau, cybersécurité, etc. Généralement contacté en situation de crise, le personnel intervenant en niveau 3 est de niveau technicien spécialisé, administrateur ou ingénieur.

Lorsque qu'une demande ne peut pas être traitée par le niveau inférieur elle est escaladée vers le niveau supérieur, c'est ce principe qui permet une meilleure prise en compte des demandes et de leur résolution, l'essentiel étant de faire traiter une demande par le groupe ayant le niveau adéquat et éviter ainsi une perte de temps et donc de garantir le meilleur niveau de service, afin de respecter un indicateur important dans les traitements des tickets que ce soit pour les problèmes ou les incidents (GTR = Garantie de Temps de Rétablissement).