Introduction à ITIL

ITIL : Information Technology Infrastructure Library = bonnes pratiques pour la gestion d'un système d'information

Table des matières

1. La notion de service

La notion de service est un moyen de fournir de la valeur aux clients en facilitant les résultats qu'ils souhaitent obtenir sans porter toute la responsabilité des coûts ou des risques.
En d'autres termes, un service est une application qui fonctionne sur une infrastructure, avec la documentation associée, la formation adaptée, un support mis en place, de l'assistance aux utilisateurs et surtout un engagement sur un résultat. Un service, c'est un engagement de résultat de l'informatique face à ses clients, face aux métiers de l'entreprise, en assumant les risques. Un service permet de rendre plus performantes les activités qui permettent la production de livrables aux métiers, tout en réduisant les contraintes et les risques. Un service est là pour donner de la VALEUR à l'entreprise.
La valeur prend en compte deux notions : l'utilité et la garantie.

L'utilité
L'utilité décrit les fonctionnalités du service et donc les fonctionnalités de l'application qui supporte ce service, c'est-à-dire ce que l'application doit faire pour rendre le service. L'utilité décrit les spécifications fonctionnelles.

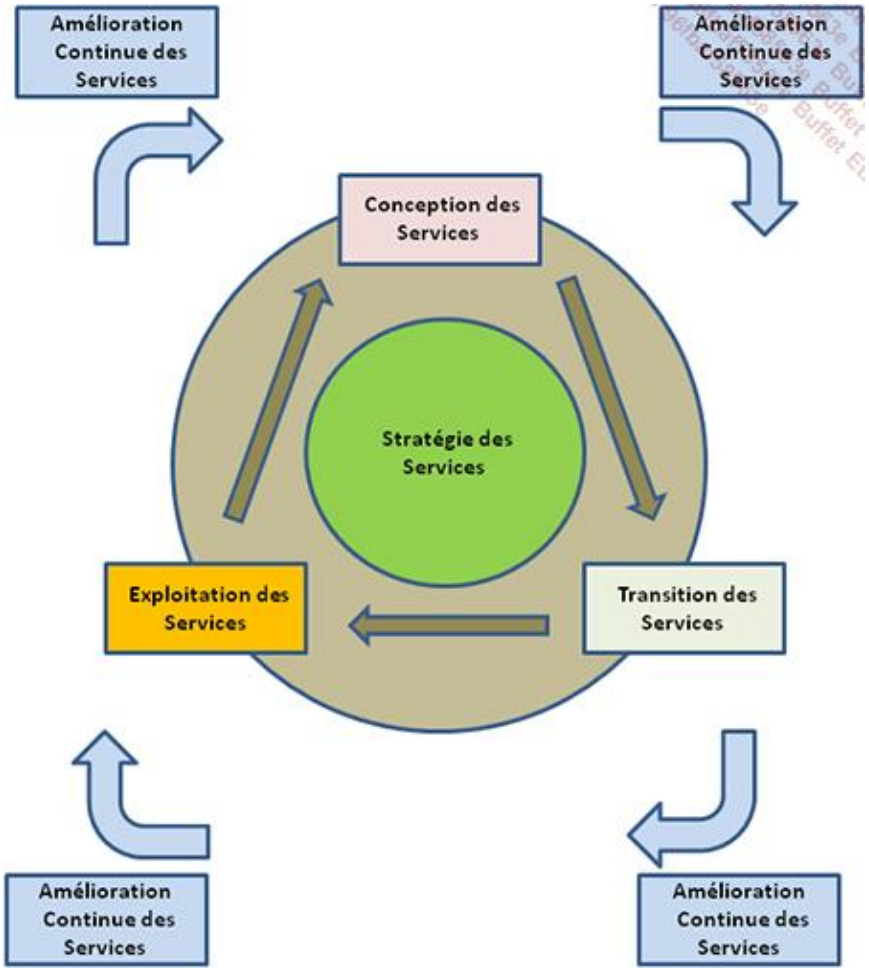
La garantie
La garantie décrit l'usage du service, c'est-à-dire comment les utilisateurs vont utiliser le service. Par exemple, les heures d'ouverture du service (horaire de bureau ou vingt-quatre heures sur vingt-quatre), ou la disponibilité et la continuité du service. La garantie décrit les spécifications non fonctionnelles.

2. Le cycle de vie des services

Le cycle de vie des services informatiques est structuré comme suit :

- Réflexion sur un service répondant à un besoin des métiers : stratégie des services
- Étude des spécifications du service : conception des services
- Construction et réalisation du service : transition des services
- Production du service : exploitation des services
- Évolution et amélioration : amélioration continue des services

Le cycle de vie est symbolisé par le schéma suivant :



Voici les cinq phases du cycle de vie :

- La stratégie des services définit les politiques et les objectifs.
- La conception des services va décliner la stratégie des services en spécifiant ces derniers.
- La transition des services va réaliser ce que l'on a défini dans la phase de conception des services.
- L'exploitation des services va produire ce que la conception des services a défini et ce que la transition des services a implémenté.
- L'amélioration continue des services met en œuvre et priorise les programmes d'amélioration basés sur les objectifs stratégiques.

Le référentiel du BTS SIO se concentre sur l'exploitation des services, et de manière annexe, sur la transition des services et l'amélioration continue des services.

3 pratiques d'ITIL sont de ce fait essentielles à connaitre et maitriser. La gestion des incidents, la gestion des problèmes et la gestion des changements.

3. Gestion des incidents

Objectifs de la pratique

- Rétablir le service dans un état normal le plus rapidement possible, conformément à l'accord de niveau de service associé.
- Minimiser l'impact de l'incident sur les utilisateurs.

a. Rétablir le service
Rétablir le service ne veut pas dire trouver une solution, mais bien remettre en marche le service pour qu'il fonctionne à nouveau dans un état dit normal (ou standard).
Rétablir le service, c'est souvent relancer le serveur ou l'application sans comprendre la cause. Si le service marche à nouveau dans l'état normal (ou standard), l'incident est résolu. C'est l'essentiel pour le client et les utilisateurs du service. Ce n'est en revanche peut-être pas satisfaisant pour les équipes informatiques. La section suivante, Gestion des problèmes, abordera la manière de répondre à cette situation.
Pour résumer, rétablir le service, c'est trouver une solution, voire un palliatif, qui va relancer le service dans son état normal.

b. Minimiser l'impact
Le deuxième objectif de la gestion des incidents est de minimiser les conséquences pour les utilisateurs.
Rétablir le service dans les délais contractuels, c'est un engagement de résultat auprès du client. Minimiser l'impact de l'incident, c'est s'engager sur des moyens et de ce fait, le département informatique fera au mieux suivant ses ressources disponibles (*best effort*, comme disent les Anglo-Saxons).

c. Ce que ne fait pas la gestion des incidents
La pratique Gestion des incidents n'a pas comme objectif de trouver les causes des incidents. Elle est focalisée sur la restauration du service. L'analyse des causes est de la responsabilité de la pratique Gestion des problèmes, qui effectuera cette analyse en back office en dehors de la pression de la gestion de l'incident. Bien sûr, si la gestion des incidents comprend les origines du dysfonctionnement, le processus en tiendra compte pour restaurer le service et les communiquera à la gestion des problèmes.
L'objectif est de dégager du temps pour les équipes de gestion des incidents et de les rendre plus disponibles pour traiter les nouveaux incidents.

Terminologie de la pratique

a. Définition d'un incident

Il est important de bien comprendre la notion d'incident et surtout de ne pas confondre un incident avec un événement ou un problème.
Pour une bonne compréhension, un rappel sur la notion d'événement : un événement est un fait détectable qui arrive sur l'infrastructure du système d'information ; un incident est un événement qui altère ou dégrade un service rendu à un utilisateur. On dit qu'un incident survient lorsque le service est arrêté ou lorsque la qualité du service est diminuée.
Tous les incidents ont comme origine un événement, qu'il soit détecté ou non. En revanche, tous les événements ne vont pas mener à la création d'un incident.
Un incident ne peut survenir que lorsque le service est opérationnel en production, sinon c'est une anomalie.
Un incident est détecté soit par un utilisateur qui va contacter le centre de services, soit par des outils de supervision ou de pilotage via la pratique Gestion des événements.

b. Impact, urgence, priorité

À chaque incident, il est important d'identifier les informations qui vont permettre de codifier cet incident. Codifier un incident, c'est déterminer la priorité que l'on va lui attribuer. Pour cela, on identifiera l'impact et l'urgence de cet incident :

- L'impact est l'effet de l'incident sur l'utilisation du service. Exemples : perte d'exploitation, nombre d'utilisateurs bloqués ne pouvant travailler, non-respect de dispositions légales… L'impact est une notation que l'on positionne souvent sur une échelle de 1 à 3 ou de 1 à 5 (1 = Élevé, 3 ou 5 = Faible).
- L'urgence est le temps dont dispose le département informatique pour rétablir le service avant que les effets de l'incident ne se fassent sentir. Par exemple, si le serveur supportant l'application de gestion de la paie tombe en panne le 3 du mois, l'urgence liée à cet incident est moindre que si ce serveur s'arrête le 25 du mois. L'urgence est une notation que l'on positionne souvent sur une échelle de 1 à 3 ou de 1 à 5 (1 = Élevé, 3 ou 5 = Faible).

La priorité de l'incident est la conjonction de ces deux notions : l'impact et l'urgence. La priorité va donc permettre d'identifier l'importance relative des incidents les uns par rapport aux autres, et permettre d'affecter les ressources en conséquence.
À chaque niveau de priorité (P1, P2, P3), on affectera un délai de rétablissement (par exemple, P1 = 2 h, P2 = 8 h, P3 = 24 h).
Toutes ces notions servant à la codification d'un incident (Impact, Urgence, matrice d'attribution des niveaux de priorité et délais de rétablissement) devront être explicitées dans le document Accord de niveau de service pour chaque service et négociées avec les branches métier, avant la mise en exploitation du service.

c. Incident majeur

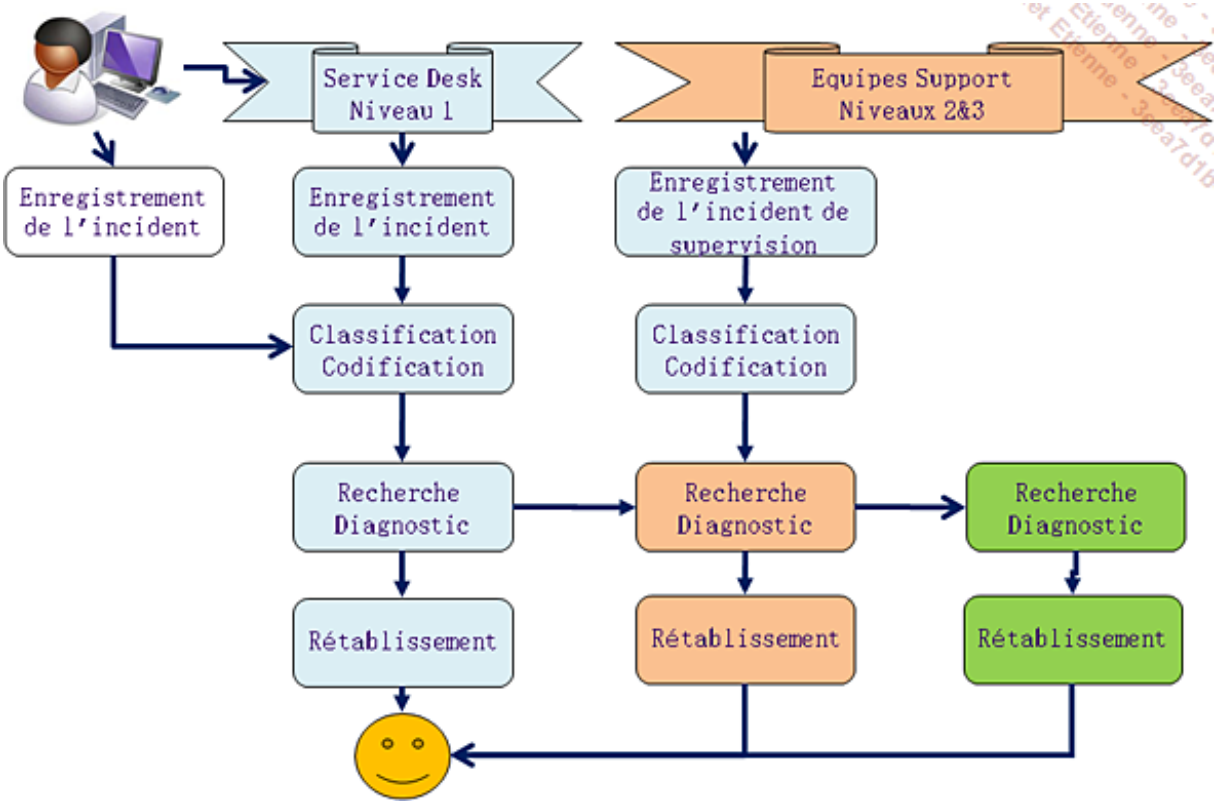
Certains incidents ont un fort impact sur les branches métier ou sur l'entreprise. Ces incidents sont dits majeurs. Ils sont hors grille de codification, et donc d'une priorité plus élevée que P1. Ils sont traités différemment des autres incidents : on va dérouler une procédure dite de "crise", avec la mise en place d'une cellule de crise pour traiter ces

incidents majeurs. La communication à l'extérieur de l'informatique pour ces incidents majeurs est spécifique à chaque situation et doit être traitée en tant que telle.
Certains incidents majeurs peuvent amener à déclencher le plan de continuité des services informatiques (voir la section consacrée à la pratique Gestion de la continuité des services).

d. Ticket d'incident
Tout incident doit être enregistré dans une base de données des incidents, via un ticket d'incident qui consigne toutes les informations qui lui sont relatives (heure, date, contexte, effet, suivi des escalades, résolution, clôture…).

Gestion des escalades

Les incidents peuvent être diagnostiqués et résolus par différentes organisations suivant la complexité de l'incident. Il va donc être nécessaire de mettre en place un mécanisme d'escalade décrit par une procédure.
Tout d'abord, les utilisateurs eux-mêmes peuvent diagnostiquer et résoudre des incidents.
Le centre de services (*Service Desk* en anglais) est chargé du premier niveau de la gestion des incidents et du suivi de ceux-ci.
Les incidents plus complexes sont escaladés vers les groupes de support de niveau 2 et de niveau 3.
Le logigramme suivant montre comment les groupes de support de niveau 2 et de niveau 3 interviennent en escalade du centre de services (support de niveau 1). Les groupes de support niveau 3 peuvent être des fournisseurs externes.
Lors de leurs interventions, les groupes support peuvent, si nécessaire, être en contact avec les utilisateurs (pour obtenir des informations complémentaires ou pour comprendre un environnement ou un paramétrage, ou encore, pour vérifier une solution).
En tout état de cause, même si les groupes de support résolvent l'incident et restaurent le service, la validation finale avec l'utilisateur reste de la responsabilité du centre de services.



Dans les bonnes pratiques ITIL, on a identifié deux types d'escalade : escalade fonctionnelle et escalade hiérarchique.
Ces deux types d'escalade sont indépendants et doivent être gérés séparément :

- L'escalade fonctionnelle : une escalade fonctionnelle survient lorsqu'une équipe qui a été affectée au traitement de l'incident est dans l'incapacité de réaliser ce traitement (diagnostic ou rétablissement). Cette équipe transfère alors l'incident à une autre équipe de niveau d'expertise plus élevé, ou de même niveau d'expertise mais dans un autre domaine. On appelle cette situation une escalade fonctionnelle. C'est le cas figurant dans le logigramme ci-dessus.
- L'escalade hiérarchique : une escalade hiérarchique permet d'alerter la hiérarchie (le management) sur une situation particulière : incident majeur potentiel, impact fort sur les branches métier, blocage dû à un manque de ressources et de moyens…

4. Gestion des problèmes

Objectif de la pratique

La pratique Gestion des problèmes est basée sur le processus Gestion des problèmes défini dans les versions ITIL V2 et ITIL V3.
La pratique Gestion des problèmes a quatre objectifs majeurs :

- Faire diminuer le nombre d'incidents : c'est l'objectif principal de ce processus.
- Prévenir l'apparition de nouveaux incidents et problèmes : cet objectif est le corollaire de l'objectif précédent, mais il va prendre en charge des actions beaucoup plus orientées vers l'anticipation, la proactivité.
- Minimiser l'impact des incidents.
- Optimiser l'efficacité des équipes support.

Terminologie de la pratique

a. Définition d'un problème

Un problème est une situation où l'on recherche la cause inconnue d'un ou plusieurs incidents.
Tout d'abord, on ne peut pas parler de problème s'il n'y a pas eu au préalable un ou plusieurs incidents. Les incidents sont traités par le processus de gestion des incidents et vont amener une restauration du service. La gestion des problèmes va, elle, regarder les vraies causes, pour y apporter des solutions.
La gestion des incidents traite en temps réel les situations (en *front line* comme disent les Anglo-Saxons) et la gestion des problèmes traite plus tard les causes de ces situations (en back office).
Il n'y a pas de problème s'il n'y a pas eu au préalable au minimum un incident. Par contre, tous les incidents ne génèrent pas une situation de problème. Cette phrase est très importante car elle est la base de la gestion des services. L'important, c'est de rétablir le service. On essayera plus tard, de comprendre les causes des incidents et de leur trouver des solutions. Comprendre les causes et trouver des solutions coûte du temps et de l'argent.
On ouvre un problème dans le cas d'incidents récurrents. La récurrence dépend du contexte de l'entreprise. Noter que la récurrence commence à deux ! Un autre cas d'ouverture d'un problème, est un contexte d'incident majeur. On voit bien que lorsque l'on a rétabli le service sur un incident majeur, à fort impact sur l'entreprise, on n'a pas envie qu'il se reproduise ; on ouvrira donc systématiquement un problème, même si la récurrence est à un.

b. Définition d'une erreur connue

Une erreur connue (en anglais *known error*) est un problème dont on connaît la cause et dont on a identifié une solution temporaire ou définitive, mais que l'on n'a pas encore mise en œuvre.
On investigue sur la cause, on trouve cette cause et/ou on trouve une solution (solution temporaire ou correctif), le problème devient alors une erreur connue.
Pour autant, on ne ferme pas le problème lorsque l'on est passé en erreur connue ; on attendra la mise en place de la solution définitive, celle qui éradique le problème, pour réaliser cette fermeture.

La base des erreurs connues contient l'ensemble des informations concernant les problèmes dont on a trouvé la cause et une solution temporaire ou définitive. Cette base, sous la responsabilité des groupes de support, est aussi mise à disposition du centre de services.

c. Définition d'une solution temporaire ("workaround")

Une solution temporaire (en anglais *workaround*) est une solution qui réduit ou élimine l'impact d'un incident ou d'un problème, lorsqu'une solution définitive n'est pas disponible.

3. Les activités de la pratique

Les principales activités de la pratique Gestion des problèmes sont les suivantes :

- L'analyse des situations d'incidents éligibles en problème.
- La détection de situations déjà enregistrées comme problèmes.
- La transformation des problèmes en erreurs connues.
- La gestion des incidents majeurs transformés en problèmes.
- La gestion de correction de l'erreur via la pratique Gestion des changements.
- L'analyse en proactivité des informations transmises par les fournisseurs internes ou externes sur des situations qui pourraient dégrader le niveau des services.

5. Gestion des changements

Introduction

Cette pratique est basée sur le processus Gestion des changements défini dans les versions V2 et V3 d'ITIL.
Cette pratique ne doit pas être confondue avec la pratique décrite dans le chapitre précédent, qui se nomme Gestion des changements organisationnels et qui traite, elle, des changements en termes d'organisation.

Objectif de la pratique

La mission de la pratique Gestion des changements est de maximiser les succès de la mise en œuvre des changements sur les produits et les services. Elle garantit que tous les changements sont enregistrés, évalués, autorisés, priorisés et que leurs réalisation, intégration et déploiement suivent une procédure définie.

Les activités de la pratique

Les activités de la pratique Gestion des changements sont de :

- s'assurer que les procédures et les méthodes utilisées pour traiter les changements sont efficaces, voire efficientes
- s'assurer que les modifications apportées aux éléments de configuration lors d'un changement sont bien enregistrées dans la base de données appropriée,
- répondre aux évolutions exprimées par les besoins des clients en minimisant les risques d'interruption de service et en maximisant la valeur fournie,
- tenir un planning complet de tous les changements en cours ou futurs.

Périmètre de la pratique

La pratique Gestion des changements s'applique sur un périmètre qui doit être défini explicitement (en mentionnant aussi ce qui ne fait pas partie de celui-ci). Il est propre à chaque organisation.
Il couvre :

- toute modification, ajout ou retrait d'un élément de configuration tout au long de son cycle de vie, qu'il soit en interne ou chez un fournisseur externe.

Il ne couvre pas :

- les changements d'activité ou d'organisation métier,
- les changements au niveau opérationnel liés à du consommable (exemple, changement de cartouche d'encre).

Terminologie de la pratique

a. Définition d'un changement
Cette définition d'un changement est importante car elle fait souvent l'objet de beaucoup de discussions dans les entreprises. Au sens ITIL, un changement est une modification d'un ou

plusieurs éléments de configuration (CI's, *Configuration Items*) composant le système d'information, ou d'un ou plusieurs services fournis par ce système d'information. Modification voulant dire ajout, modification d'un ou plusieurs attributs du CI ou retrait d'un ou plusieurs CI's. Un changement a un impact direct ou indirect sur un ou plusieurs services. Voici quelques autres exemples de changements : une nouvelle version d'un logiciel applicatif, l'installation d'un poste de travail, l'introduction d'un nouveau serveur, le remplacement d'une imprimante…
Une modification d'une documentation ou d'un contrat est un changement (voir la section concernant le processus gestion des configurations).
La modification d'une donnée (Data) n'est donc pas un changement. L'attribution d'un droit d'accès n'est pas un changement. Une modification d'une activité d'un processus métier n'est pas un changement.
Un changement a des origines diverses. On peut en donner une liste non exhaustive :

- Les correctifs (événement, incident, problème…)
- La législation
- L'organisation
- Des directives ou des standards
- Des évolutions des services existants
- De nouveaux services
- Un nouveau modèle de sourcing
- Une innovation technologique…

b. La demande de changement

Une demande de changement, RFC (*Request For Change* en anglais) est la formalisation d'une modification d'un ou plusieurs éléments de configuration (CI, *Configuration item*, en anglais). Tout changement doit être formalisé par une RFC. Il existe différents types de RFC, correspondant aux différents types de changement.
Tous les utilisateurs ou les branches métier sont habilités à émettre une demande de changement, mais cela ne veut pas dire qu'elle sera acceptée.

c. Les types de changement

Dans les bonnes pratiques ITIL 4, on identifie trois types de changement :

- Le changement dit normal : il nécessite une évaluation complète et une autorisation avant sa réalisation.
- Le changement standard : cela concerne les changements pré-autorisés et qui vont suivre des procédures prédéfinies.
- Le changement urgent : il demande une réaction plus rapide que prévu pour limiter les impacts sur le métier.

d. Les caractéristiques d'un changement dit normal

C'est un changement qui n'est pas standard ni urgent. On le caractérise par une nécessité d'évaluation et de suivi (ou de contrôle) qui sera plus ou moins importante en fonction des risques, de la complexité, et de l'effort nécessaire à la réalisation du changement.
L'autorité de gestion du changement est une instance qui va évaluer, autoriser, ou refuser le changement, le planifier et le suivre jusqu'à sa clôture. Ce comité des changements doit être adapté à la nature du changement proposé.

e. Les caractéristiques d'un changement standard

Les actions nécessaires pour mettre en œuvre un changement standard sont connues, documentées, déjà réalisées, et testées (*under control* comme disent les Anglo-saxons). Les risques sont faibles et bien maîtrisés. Les ressources et les coûts sont connus. Une prévalidation technique a déjà été faite. Seule une validation budgétaire est nécessaire.
Les changements standards sont donc des changements pré-approuvés car maîtrisés et associés à des procédures établies. Ils sont souvent associés aux modèles de changements.
Les points clés sont les suivants :

- Le déclenchement est clairement défini.
- Les tâches sont bien maîtrisées et documentées.
- L'autorisation est effectivement donnée.
- L'approbation budgétaire est pré-autorisée ou bien gérée complètement par le demandeur.
- La plupart du temps, ce sont des changements bien connus et à risque faible.

Comme un changement standard a des éléments déclencheurs bien définis, on implémente souvent les demandes de changement standards par des formulaires prédéfinis qui vont donner un mini catalogue de changements pré-autorisés.
La liste suivante donne quelques exemples de changements standards :

- L'installation d'un poste de travail.
- La configuration d'un serveur.
- Le remplacement d'une imprimante, etc.

f. Les caractéristiques d'un changement urgent

Tout d'abord, l'urgence n'est pas la normalité, c'est l'exception. On va utiliser les changements urgents de manière exceptionnelle. L'urgence est demandée par l'émetteur de la demande (RFC), mais elle devra être validée, autorisée par une instance appropriée.
L'urgence va permettre de court-circuiter les procédures de réalisation et de mise en œuvre du changement pour réduire les délais, par exemple en repoussant l'écriture de documentation après la mise en service, voire en minimisant les tests. Par contre, un changement urgent devra toujours appréhender les procédures de retour arrière, et les tester. Un changement urgent peut nécessiter une déplanification d'autres travaux ou une affectation de ressources supplémentaires au détriment d'autres activités.

6. Mises en situation

Objectif : associer une pratique ITIL à chaque situation

Situation 1 :
C'est le soir, il est 22h, je suis d'astreinte et mon téléphone sonne. La personne de la supervision m'informe d'une alerte détectée sur un serveur : « seuil d'utilisation mémoire dépassé ».
Je me connecte en VPN au réseau de l'entreprise, effectue un diagnostic de la situation, puis décide de redémarrer le serveur. Après le redémarrage, l'alerte à disparu.

Situation 2 :
Le lendemain de la situation 1, je me réunis avec mes collègues (une personne de l'équipe infra, une personne de l'équipe de développement, une personne du centre de service) pour évoquer la situation 1 rencontrée la nuit dernière.
Nous décidons d'investiguer ensemble les raisons de cette alerte. La personne de l'équipe infra analyse les logs du système, vérifie les paramètres de configuration du serveur ainsi que le dimensionnement de la machine. Il remarque une fuite mémoire lié au processus de l'application de gestion des frais.
La personne de l'équipe de développement et alors sollicitée pour trouver l'origine de cette fuite mémoire. Elle trouve que celle-ci vient d'un composant assez ancien de l'application qui utilise une framework dont la version n'est plus à jour et qui, dans certaines configurations, génère des fuites mémoires.

Situation 3 :
L'équipe qui s'était réunie dans la situation 2 décide que faire la mise à jour du framework pour corriger le problème de fuite mémoire afin de ne plus rencontrer à l'avenir la même situation. Une série de tests est effectuée avec la nouvelle version du framework sur l'application de gestion des frais de déplacement. Certaines adaptations sont effectuées dans le code pour le rendre compatible avec cette version du framework. Une fois la série de tests bouclée, la mise à jour est effectuée sur l'environnement d'assurance qualité, puis, après validation du fonctionnement, sur l'environnement de production.