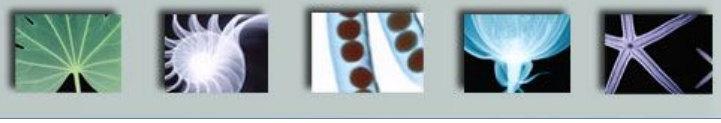
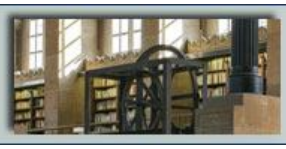


ITIL V2

La gestion de la continuité des services des TI

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 Introduction 5
1.1 Pourquoi ? 5
1.1.1 Pour l'entreprise 5
1.1.2 Pour la DSI 5
1.2 Focalisation sur les processus Métiers critiques pour l'entreprise : quels sont-ils ? 5
1.3 Concepts de base 5
1.4 Bénéfices : la gestion des risques 5
1.5 L'implication de la Direction 6
1.6 Relations avec les autres processus 6
2 Périmètre et risques couverts 6
2.1 Risques couverts 6
2.2 Risques non couverts 6
2.3 Rôles et responsabilités 6
3 Cycle de vie de la continuité des activités métiers 7
3.1 Le processus fait partie d'un projet plus grand. 7
3.2 La Continuité des Activités Métiers 7
4 Etape 1 : Initialisation 7
4.1 Les documents de départ 7
4.2 Les activités 7
4.2.1 Définir d'une politique 7
4.2.2 Spécifier les termes de référence et le cadre 7
4.2.3 Allouer des ressources 8
4.2.4 Définir l'organisation du projet et la structure de contrôle 8
4.2.5 S'accorder sur les plan projet et plan qualité 8
5 Etape 2 : Besoins et stratégie 8
5.1 Analyse d'Impact Métiers (*Business Impact Analysis*) 8
5.2 Evaluation des risques (*Risk Assessment*) 9
5.3 Stratégie de Continuité Métiers (*Business Continuity Strategy*) 9
5.4 Les scénarios de reprise des SIs 10
5.4.1 Solutions manuelles de contournement 10
5.4.2 Reprise graduelle appelée parfois reprise à froid ou *cold stand by* 10
5.4.3 Reprise intermédiaire appelée parfois reprise à chaud (sur site de secours) ou *warm stand by* (*warm* = tiède) 11
5.4.4 Reprise immédiate appelée parfois reprise à chaud (sur site de secours) ou *hot stand by* 11
6 Etape 3 : Implantation 11
6.1 Mettre en place de l'équipe projet 11
6.2 Définir les différents plans de reprise 12
6.3 Mettre en oeuvre les mesures de réduction des risques 12
6.4 Implémenter les accords avec les sociétés tierces 12

6.5 Développer les Plans de Continuité de la DSI 12
6.6 Ecrire les procédures de reprise 13
6.7 Effectuer les tests initiaux 13
7 Etape 4 : Gestion opérationnelle 13
7.1 Pédagogie et sensibilisation 13
7.2 Formation 13
7.3 Revues et audits 13
7.4 Tests 13
7.5 Gestion des Changements 13
7.6 Assurance (qualité) 14
8 Déclenchement 14
8.1 La décision 14
8.2 Déclenchement : pendant et après 14
9 Projet de mise en oeuvre de la continuité 14
9.1 Dépend de la taille de l'entreprise 14
9.2 Opérations normales 15
9.3 Responsabilités en cas de déclenchement 15

1 Introduction

1.1 Pourquoi ?

Lors d'une interruption importante des activités (métiers et/ou informatiques), la DSI doit être capable de continuer à fournir un niveau pré-déterminé et accepté de Services pour soutenir les activités métiers critiques.

L'objectif et de ne pas faire perdre d'argent aux activités métiers ou, en cas d'interruption très importante, pour permettre à l'entreprise de survivre.

Cela concerne l'entreprise entière et dépasse le cadre de la DSI seule.

1.1.1 Pour l'entreprise

Plan d'urgence (*Contingency Planning*) ou Gestion de la Continuité Métiers (*BCM* ou *Business Continuity Management*)

Prévoit tous les scénarios de reprise pour toutes les activités :

- métiers : Plan de Continuité Métiers (*Business Continuity Planning*)
- informatiques : Plan de Gestion de la Continuité des Services (*IT Service Continuity Management Planning*)

1.1.2 Pour la DSI

Sous-ensemble des Plans et Gestions Métiers.

1.2 Focalisation sur les processus Métiers critiques pour l'entreprise : quels sont-ils ?

Cela dépend de la structure organisationnelle, de la culture et de la direction stratégique (métiers et technologiques) de l'entreprise.

L'impact de la perte d'un processus Métier (pertes financières, dommages sur la réputation, dérégulations de marchés, etc.) est étudié dans une Analyse de Risques Métiers (*Business Impact Analysis*).

1.3 Concepts de base

Les activités métiers sont de plus en plus dépendantes des Services fournis par la DSI.

La Disponibilité des Services (Gestion de la Disponibilité) met en place et gère des technologies permettant de diminuer les risques (redondance du matériel, politique de sauvegarde/restauration, etc.).

La Gestion de la Continuité des Services s'appuie sur la Gestion de la Disponibilité des Services (et d'autres processus) et nécessite l'implication de la Direction de l'entreprise (et tous les niveaux hiérarchiques).

Des tests réguliers doivent aussi être effectués pour vérifier la coordination de l'ensemble des techniques prévues sur une interruption importante.

1.4 Bénéfices : la gestion des risques

La Gestion de la Continuité est à considérer comme une assurance couvrant des risques pré-déterminés à l'avance.

Cela permet à une entreprise d'identifier, d'analyser et de prendre ses responsabilités face à une éventuelle concrétisation de l'un de ces risques.

La DSI peut gérer de manière pro-active son Infrastructure pour réduire l'impact de dysfonctionnements de ses éléments (d'un composant à un site).

La DSI peut aussi, au travers de la Gestion de la Continuité, contribuer à la création de valeurs :

- Diminution potentielle des primes d'assurance : la DSI peut aider à démontrer que l'entreprise pro-activement gère ses risques métiers pouvant entraîner une baisse du montant des assurances contractées pour se protéger de tels risques
- Obligations de régulation : certaines activités nécessitent de montrer à une organisation de régulation que l'entreprise gère un niveau de risques obligatoire du fait de l'activité de l'entreprise (exemple : les banques avec la norme IAS)
- Relations poussées avec les organisations métiers : la gestion des risques entraîne une compréhension accrue par la DSI des besoins métiers
- Marketing positif sur les capacités de reprise en cas de sinistre majeur : un avantage concurrentiel ; ceci peut être utilisé comme atout pour convaincre des clients et ainsi contribuer au chiffre d'affaires de l'entreprise.

1.5 L'implication de la Direction

La mise en place des mécanismes de la Gestion de la Continuité doit être basée sur les exigences métiers dans sa recherche à diminuer l'impact en cas de sinistre voire à assurer la survie de l'entreprise.

Ceci est une problématique de la Direction de l'entreprise.

L'implication de la Direction doit continuer après la mise en place de ces mécanismes en veillant à ce qu'ils soient toujours à jour.

Les pressions métiers font évoluer l'infrastructure et les Plans d'Urgence sont mis au second plan.

Une directive stratégique de la part des hauts dirigeants doit rappeler en permanence que la pression du marché ne doit pas être utilisée comme excuse pour ne pas mettre en place les moyens de reprise.

Les Plans d'Urgence deviennent très rapidement caduques.

1.6 Relations avec les autres processus

- Gestion des Niveaux de Service : comprendre les obligations dans la fourniture des Services
- Gestion de la Disponibilité : délivrer une réduction des risques pour maintenir à un niveau normal les activités métiers
- Gestion des Configurations : gérer l'Infrastructure associée
- Gestion des Capacités : s'assurer que les besoins métiers sont pleinement supportés par les ressources informatiques adéquates
- Gestion des Changements : s'assurer que les Plans de Continuité soient à jour au travers de processus établis et des revues régulières
- Centre de Services/Gestion des Incidents : utiliser les statistiques

2 Périmètre et risques couverts

La Gestion de la Continuité n'est peut-être pas suffisante pour rétablir un fonctionnement minimum après un sinistre :

- avoir des locaux de remplacement pour accueillir les utilisateurs
- avoir la copie des dossiers papiers critiques
- avoir des services courrier et téléphoniques pour pouvois communiquer avec les Clients et les sociétés extérieures

La Gestion de la Continuité des Services est une partie de la Gestion de la Continuité Métiers (*BCM* ou *Business Continuity Management*)

2.1 Risques couverts

Sinistre : sinistre d'un département jusqu'aux sinistres majeurs affectant une partie de l'entreprise.

Les risques à prendre en considération dépendent de l'activité de l'entreprise et évoluent avec elle.

Quelques exemples de risques :

- Problèmes majeurs sur l'infrastructure : site Internet inaccessible suite à une attaque par déni de service
- Catastrophes naturelles : tremblement de terre (Los Angeles, USA, Janvier 1994), inondations (Paris et la Seine, 1910)
- Attentats terroristes : Bombe (World Trade Centre, New York, USA, Février 1993)

2.2 Risques non couverts

- Risques à long terme sur les activités métiers (changement de stratégie, diversification, restructuration, etc.) : généralement inclus dans la stratégie de la DSI puis concrètement dans la Gestion des Changements
- Dysfonctionnements techniques mineurs (erreur disque non critique) sauf s'il y a un risque fort sur l'activité : en principe gérés par le Centre de Services et la Gestion des Incidents et éliminés sous l'action conjuguée de la Gestion de la Disponibilité et de la Gestion des Problèmes

2.3 Rôles et responsabilités

Projet piloté par un haut niveau dans la hiérarchie.

En étroite collaboration avec la Gestion de la Sécurité (*Security Management*) et l'Analyse Métiers (*Business Analysis*) dans la DSI en raison des nombreux objectifs communs.

Habituellement constaté : la responsabilité du processus est confiée à la fonction de Sécurité de l'Information (*Information Security*).

3 Cycle de vie de la continuité des activités métiers

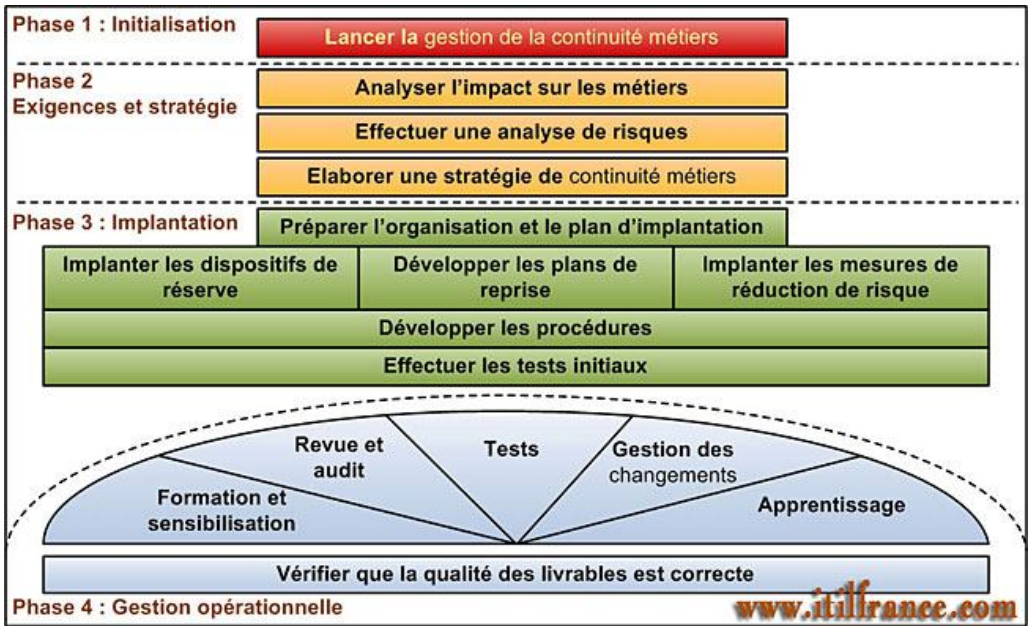
3.1 Le processus fait partie d'un projet plus grand.

Il est impossible de développer de manière isolée la Gestion de la Continuité des Services.

Il doit soutenir pleinement les besoins des activités métiers.

3.2 La Continuité des Activités Métiers

Voici les quatre étapes qui sont en relation avec les aspects informatiques :



Le processus de la Continuité des Activités Métiers est décrit complètement dans d'autres documents ITIL de l'OGC.

4 Etape 1 : Initialisation

4.1 Les documents de départ

Il faut partir de probables documents existants :

- Organisation métiers : Plans de Continuité sur une activité basé sur des solutions de contournement
- DSI : Plans de bascule/reprise sur des systèmes ou configurations perçus comme critiques

Mais le seul moyen efficace d'élaborer une Gestion de la Continuité des Services (*ITSCM*) passe par l'identification des processus métiers critiques et l'analyse (et la coordination) de l'Infrastructure utilisés et les Services fournis

4.2 Les activités

4.2.1 Définir d'une politique

Ceci devrait être établi et communiqué le plus tôt possible pour que tous les acteurs concernés soient sensibilisés à la Continuité des Activités Métiers.

4.2.2 Spécifier les termes de référence et le cadre

Il faut préciser le périmètre et les responsabilités des responsables et des équipes.

Il faut définir une méthode de travail pour, par exemple:

- prendre en charge la gestion d'un risque et l'Analyse d'Impact Métier (*Business Impact Analysis*)
- déterminer la structure de commande et de contrôle utilisée pour supporter une interruption métier
- prendre en compte les audits externes (réguliers et à la demande), prise en compte des besoins Utilisateurs, contenu des contrats d'assurance
- être en conformité avec les standards de sécurité (par exemple, la BS 7799, *British Standard on Information Security Management*)

4.2.3 Allouer des ressources

La mise en place d'une vraie Gestion de la Continuité nécessite des ressources considérables aussi bien en budgets qu'en personnel.

Cela dépend de la maturité de l'organisation, il peut y avoir besoin de familiariser et de former l'équipe mise en place pour accompagner l'étape 2.

L'utilisation de consultants externes peut être une aide non négligeable pour accélérer l'analyse.

Mais il est important qu'une fois le processus mis en place, l'organisation soit autonome et n'en remette plus uniquement à un support externe.

4.2.4 Définir l'organisation du projet et la structure de contrôle

Ces projets peuvent être relativement complexes et il est nécessaire de mettre en place une organisation de projet selon les habitudes de fonctionnement habituels lors de la mise en place de grands projets.

Comme les Systèmes d'Informations sont une composante importante du projet, il est possible que le projet soit mieux piloté par la DSI en reportant au plus haut niveau de la hiérarchie.

4.2.5 S'accorder sur les plan projet et plan qualité

Les plans qualité assureront que les livrables sont fournis et avec un niveau de qualité acceptable.

Ils définissent aussi un mécanisme de communication de tous les documents du projet.

5 Etape 2 : Besoins et stratégie

Cette étape fournit les fondements de la Gestion de la Continuité des Services et détermine comment une entreprise survivra à une interruption métier ou à un sinistre et les coûts que cela induira.

Deux parties :

- Besoins : Impact d'Analyse Métier (*Business Impact Analysis*) et évaluation des risques
- Stratégie : détermination et accord sur les mesures de réduction des risques et les options de reprise pour supporter les besoins

5.1 Analyse d'Impact Métiers (*Business Impact Analysis*)

Une Analyse d'Impact Métier (*Business Impact Analysis*) évalue :

- les processus métiers critiques
- les dommages ou pertes potentiels occasionnés par une interruption de ces processus

Elle identifie aussi :

- les personnes, les compétences et les services nécessaires pour continuer à faire fonctionner les activités métiers critiques et essentielles à un niveau minimum acceptable
- le délai de redémarrage du niveau minimum
- le délai de redémarrage complet des activités métiers critiques

Elle présente divers scénarios de reprise avec leurs coûts et les organisations métiers décident du scénario à mettre en place.

Les impacts métiers à considérer sont les suivants :

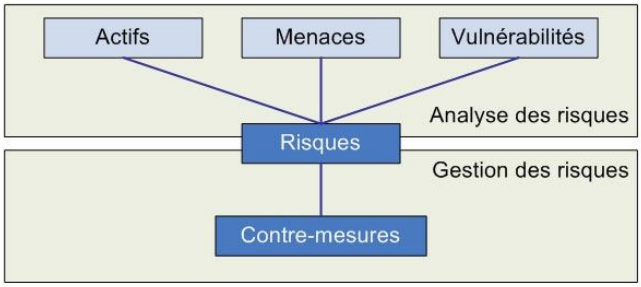
- échec à fournir des niveaux de services internes
- pertes financières
- coûts additionnels
- pertes de marchés immédiates et à long terme
- non respect des lois, de régulation de marchés ou de standards
- risque dans la sécurité des personnes
- embarras du personnel, des dirigeants, de l'entreprise
- perte de clientèle
- perte de crédibilité
- perte d'image et de réputation

Les deux approches complémentaires en matière de Continuité de Service :

- Si impact important immédiatement : approche de réduction des risques (prévention)
- Si impact peu important immédiatement : approche par plan de reprise (restauration puis redémarrage)

5.2 Evaluation des risques (*Risk Assessment*)

La question à analyser est : Quelle est la probabilité qu'un désastre ou une rupture de service sérieuse puisse survenir ?



Le niveau de risque est important si :

- les actifs ont une grande valeur
- les menaces sont importantes
- les vulnérabilités des actifs face à ces menaces sont grandes

Définition d'une Menace : comment une interruption de service peut-elle survenir ?

Définition d'une Vulnérabilité : l'organisation sera-t-elle affectée, et dans quelle mesure, lors de la concrétisation de la menace ?

Voici quelques exemples de menaces :

- interruptions délibérées ou non de services (piratage interne de systèmes informatiques, rupture d'un service critique de la part d'un fournisseur externe, etc.)
- les processus métiers sont vulnérables s'ils sont basés sur des Services des SIs non redondants (*SPOF* ou *Single Point Of Failure*)

L'évaluation des risques peut ensuite être effectuée à partir de toutes ces informations :

- soit quantitativement (si des données sont disponibles)
- soit qualitativement par exemple : bas, moyen ou haut
- Les contre-mesures et les mécanismes de réduction des risques peuvent ensuite être définis

5.3 Stratégie de Continuité Métiers (*Business Continuity Strategy*)

Les éléments précédents permettent de définir une stratégie appropriée pour l'entreprise :

- impact fort à court terme :
    - prévention des risques (redondance, clustering, load-balancing, systèmes à tolérance de pannes, etc.)
    - généralement traité par la Gestion de la Disponibilité
- impact faible à court terme : mise en place de plan de reprise
    - tout risque ne peut être écarté donc à prévoir dans tous les cas même si les composants des SIs sont redondants

La réduction des risques inclut :

- une stratégie de sauvegarde ET de restauration, incluant un stockage externe des sauvegardes
- l'élimination des points non redondants (*Single Point Of Failure*) tels que alimentation électrique de bâtiment ou de salle
- services externalisés sur plusieurs fournisseurs (lignes télécom par exemple)
- contrôles de sécurité d'accès sur les zones sensibles
- détection des problèmes de salles comme les incendies et mise en place de systèmes de lutte
- amélioration des procédures pour réduire la probabilité d'erreurs (contrôle des Changements)

La réduction des risques ne fait pas disparaître tous les risques.

Exemple : Panne nationale Bouygues Telecom le mercredi 17/11/2004 empêchant les abonnés de recevoir des appels téléphoniques.

Bouygues Telecom a expliqué dans son communiqué que la panne informatique « s'est produite sur deux serveurs jumeaux au même moment, dans deux endroits différents. En fonctionnement normal, ils se secourent en prenant le relai l'un de l'autre. La panne est de nature exceptionnelle. »

Attention aussi à ce qu'une mesure de prévention d'un risque n'augmente pas un autre risque : L'externalisation d'une salle informatique peut permettre de réduire les risques d'un sinistre mais peut augmenter les risques sur la sécurité des données

Une stratégie complète est un équilibre entre :

- le coût des mesures de réduction des risques et
- les scénarios de reprise

pour supporter le redémarrage des processus métiers critiques dans les délais prévus.

Les scénarios de reprise globaux doivent inclure :

- personnes et bureaux
- systèmes et réseaux informatiques
- services critiques comme l'alimentation électrique, les télécommunications, le courrier, etc.
- actifs critiques comme les documents papiers indispensables pour travailler

5.4 Les scénarios de reprise des SIs

5.4.1 Solutions manuelles de contournement

L'informatique permet aux entreprises de traiter les informations plus rapidement (et surtout à moindre coût) qu'avec du personnel.

Dans certains cas, il est possible de revenir à des procédures manuelles pendant une certaine période sans mettre en péril l'entreprise.

5.4.2 Reprise graduelle appelée parfois reprise à froid ou *cold stand by*

A utiliser lorsque l'organisation peut fonctionner jusqu'à 72 heures ou plus sans informatique.

Cela peut inclure des locaux vides proposant tous les services et dans lesquels les SIs sont réinstallés.

La salle fournie par un prestataire externe ou par l'organisation elle-même (par exemple, s'il existe deux sites importants possédant chacun leur salle informatique, ils peuvent être sites de reprise croisés).

Attention aux composants informatiques à réinstaller :

- soit ils sont suffisamment standards pour qu'ils soient achetables à tout moment sur le marché
- soit il faut prévoir les stocks (*spares*) en interne lors de l'achat initial des configurations

5.4.3 Reprise intermédiaire appelée parfois reprise à chaud (sur site de secours) ou *warm stand by* (*warm* = tiède)

A utiliser lorsque le rétablissement des services critiques doit intervenir entre 24 et 72 heures.

Ce scénario est proposé par des entreprises spécialisées dans les sites de reprise : bureaux, télécommunications, systèmes et réseaux informatiques.

Le redémarrage peut être long car le prestataire doit reconfigurer son site pour s'adapter à la configuration de l'entreprise sinistrée.

L'accès au site de reprise est sécurisé et immédiat.

Attention : Le site de reprise n'a pas la capacité à héberger simultanément un nombre important de sites sinistrés.

Ce qui nécessite de choisir un bon prestataire fait partie de la gestion des risques mais plus sa capacité est importante, plus le service se paie cher.

Il est important que le contrat signé inclut des fenêtres de tests de reprise sur le site de secours.

5.4.4 Reprise immédiate appelée parfois reprise à chaud (sur site de secours) ou *hot stand by*

A utiliser lorsqu'il est impératif d'avoir un redémarrage immédiat des services critiques métiers pendant les premières 24 heures après le sinistre.

Souvent en complément de la reprise intermédiaire (où on bascule sur un mode à plus long terme et peut-être moins risqué).

Comment :

- en possédant ou louant une salle informatique
- en y installant serveurs et réseaux informatiques
- en mettant en place de la réplication de données sur les serveurs du site de secours (ils doivent être opérationnels)

Ceci nécessite de mettre en place une réplication de données :

- soit par copies régulières (toutes les nuits par exemple)
- soit en temps réel (*SAN/NAS* sur les deux sites avec technologies de réplication temps réel par exemple)

Cette solution la plus efficace mais c'est aussi évidemment la plus chère.

Mais elle est quelquefois obligatoire de par la législation (préservation de données financières par exemple).

La Capacité disponible sur le site de secours est une Capacité dormante. En temps normal, elle peut être utilisée à des activités de développement ou de test mais il faut être clair sur le fait que ces activités seront immédiatement arrêtées en cas de sinistre et les ressources réquisitionnées.

6 Etape 3 : Implantation

Cette étape implique plus fortement la DSI :

- mettre en place l'équipe projet
- définir les différents plans de reprise
- implémenter les mesures de réduction des risques
- implémenter les accords avec les sociétés tierces
- développer les plans de Continuité de la DSI
- écrire les procédures de reprise
- effectuer les tests initiaux

6.1 Mettre en place de l'équipe projet

La DSI est une partie du projet global et la structure de l'organisation est composée de trois parties :

- Direction de la DSI ayant autorité et contrôle à l'intérieur et responsabilité en cas de sinistre
- Coordination : un niveau hiérarchique en-dessous et responsable de la coordination
- Reprise : ensemble d'interlocuteurs dans les différentes équipes de la DSI responsables d'exécuter les plans de reprise et de communiquer avec la Direction, les Clients et les sociétés extérieures

6.2 Définir les différents plans de reprise

Au plus haut niveau :

- Plan de réaction d'urgence
- Plan d'évaluation des dommages
- Plan de sauvetage
- Plan des documents vitaux
- Plan de gestion de crise et de relations publiques

Ensuite, les plans suivants peuvent être considérés :

- Plan sur les bureaux et les services
- Plan sur les serveurs et réseaux informatiques
- Plan sur les télécommunications
- Plan sur la sécurité
- Plan sur les ressources humaines
- Plan sur la finance et l'administration

Enfin, chaque domaine métier critique est responsable de la définition détaillée des actions de reprise.

Les plans de reprise de la DSI contient toutes les informations :

- en situation de désastre à partir du moment où la décision à été prise : pour rétablir les serveurs, les réseaux et les télécommunications
- puis pour gérer le retour à la normale

Il est vital d'examiner les accords clés prévus pour la fourniture des services métiers critiques.

6.3 Mettre en oeuvre les mesures de réduction des risques

Cette activité est souvent traitée par la Gestion de la Disponibilité car cela répond aussi à certains besoins de Disponibilité des Services.

Exemples classiques :

- installation d'alimentations électriques redondantes et de secours
- systèmes à tolérance de pannes, *clusters*
- externalisation de la sauvegarde et de l'archivage
- *SAN/NAS*, systèmes *RAID* et systèmes de réplication de données
- équipements de secours (dormants ou utilisés) ou *spare*

6.4 Implémenter les accords avec les sociétés tierces

Cela comprend :

- négocier avec des sociétés proposant des services de reprise
- préparer et équiper les locaux de repli
- acheter et installer les serveurs de secours
- négocier avec les fournisseurs de services tiers pour être intégré dans leurs propres Plan de Continuité

6.5 Développer les Plans de Continuité de la DSI

Le Plan de Continuité Métiers se base sur ces plans :

- détail de la remise en fonction de l'infrastructure informatique
- compréhension des dépendances entre les SIs
- homologation AVANT sinistre
- validation de l'intégrité et de la consistance des données

Il faut veiller à ce qu'il n'existe en circulation que la dernière version de ces plans.

Il ne faut pas oublier de prendre en compte aussi :

- une personne technique non familière du document doit pouvoir suivre les procédures et avoir une cartographie simple des SIs
- une check-list à appliquer après chaque étape

6.6 Ecrire les procédures de reprise

Elles doivent inclure :

- installation et tests des matériels et réseaux de remplacement
- restauration des logiciels et applications et des données à partir d'un point de consistance commun à toutes les activités métiers
- gestion des différentes heures locales dans le cas d'une organisation internationale
- les activités métiers stoppées en cas de sinistre

6.7 Effectuer les tests initiaux

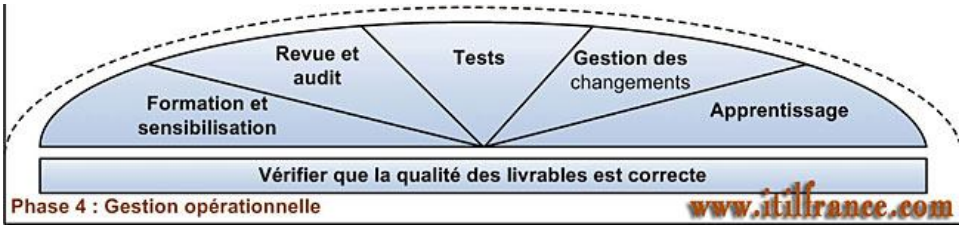
Il est impératif de tester AVANT un sinistre.

Loi classique : toute procédure non testée échouera en situation réelle de sinistre où le l'heure ne sera plus aux mises au point des procédures.

Il faut impliquer les organisations métiers pour des tests poussés car il faut faire intervenir tous les aspects des plans.

Les tests peuvent être annoncés à l'avance ou non (mais la direction de l'entreprise doit toujours donner son accord).

7 Etape 4 : Gestion opérationnelle



7.1 Pédagogie et sensibilisation

S'assurer que toutes les équipes connaissent la problématique et l'intègre dans leurs activités quotidiennes.

7.2 Formation

S'assurer que les équipes de la DSI ont le niveau nécessaire en les formant aux aspects métiers non techniques .

7.3 Revues et audits

S'assurer que tous les livrables et procédures restent pertinentes même en cas de Changement majeur.

7.4 Tests

Effectuer régulièrement un test grandeur nature (au moins une fois par an).

7.5 Gestion des Changements

S'assurer que tout Changement dans les SIs est reporté dans les Plans de reprise et que ces derniers soient à jour.

7.6 Assurance (qualité)

Au final, obtenir de la part de la Direction que les livrables et procédures ont une qualité satisfaisante et que les processus de gestion opérationnelle fonctionnent de manière satisfaisante.

8 Déclenchement

8.1 La décision

Si toutes les étapes ont été respectées, le déclenchement d'un Plan de Continuité Métiers est une opération sans ambiguïté.

L'impact d'un déclenchement est très important et la décision ne peut pas être prise à la légère.

La décision est prise par un comité de crise (*Crisis Management Team*) :

- comprenant des dirigeants métiers et informatiques
- collectant les informations sur les dommages et d'autres sources

Il doit posséder un aide-mémoire avec la localisation de la documentation complète, les points de décision et les actions associées, les coordonnées des membres du comité de crise.

La décision doit être prise rapidement mais elle peut faire partie d'une Gestion de Problème (au bout d'un certain temps de non-résolution, on déclenche le Plan).

8.2 Déclenchement : pendant et après

Une fois la décision prise, il faut communiquer à l'intérieur de l'organisation en informant les personnes essentielles qui redescendront à leur tour l'information.

Il est important que les activités de reprise soient tracées pour analyse ultérieure.

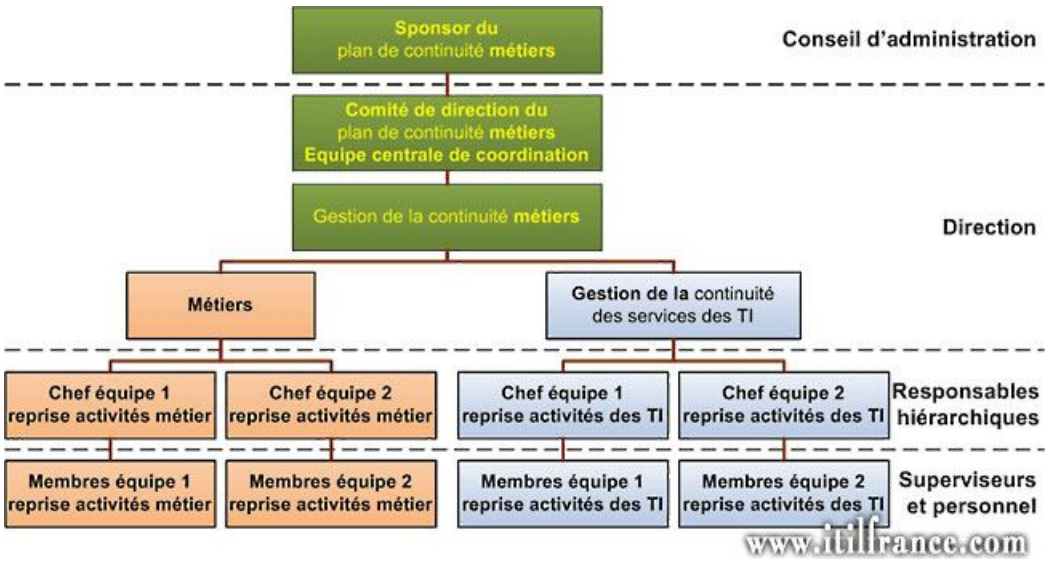
S'assurer que personne ne dépasse ses capacités lors du coup de feu (gérer cette période avec pauses, rotation de personnel, etc.).

Il est vital que les mécanismes et les contrôles de sécurité des informations et de la protection des données soient maintenus et renforcés pendant les opérations.

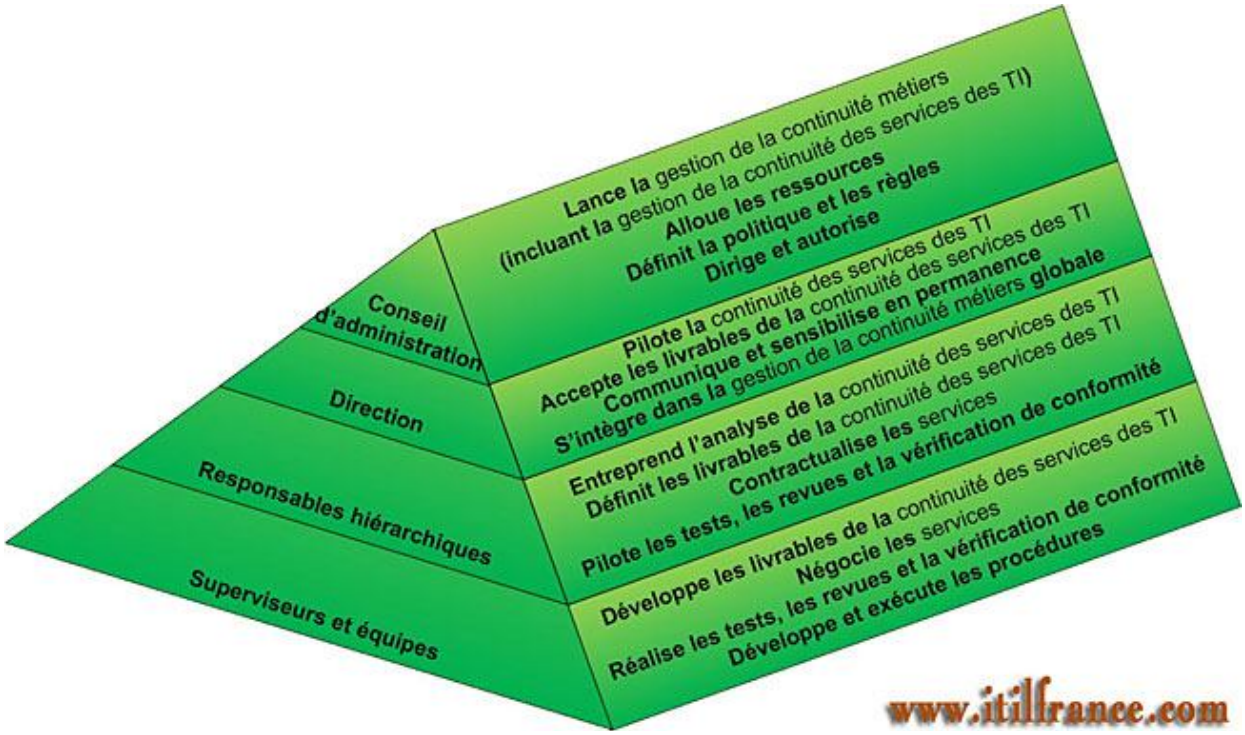
Après le redémarrage de l'activité, apporter la reconnaissance et récompenser aux équipes d'intervention.

9 Projet de mise en oeuvre de la continuité

9.1 Dépend de la taille de l'entreprise



9.2 Opérations normales



9.3 Responsabilités en cas de déclenchement