

CHRISTIAN DUMONT

Préface de Patrick Abad



CENTRE DE SERVICES • GESTION DES INCIDENTS • GESTION DES PROBLÈMES • GESTION DES CONFIGURATIONS •

GESTION DES CHANGEMENTS • GESTION DES MISES EN PRODUCTION • GESTION DES NIVEAUX DE SERVICE • GESTION DE LA CAPACITÉ •

GESTION DE LA DISPONIBILITÉ • GESTION DE LA CONTINUITÉ DE SERVICE • GESTION FINANCIÈRE DES SERVICES

CENTRE DE SERVICES • GESTION DES INCIDENTS • GESTION DES PROBLÈMES • GESTION DES CONFIGURATIONS •

GESTION DES CHANGEMENTS • GESTION DES MISES EN PRODUCTION • GESTION DES NIVEAUX DE SERVICE • GESTION DE LA CAPACITÉ •

GESTION DE LA DISPONIBILITÉ • GESTION DE LA CONTINUITÉ DE SERVICE • GESTION FINANCIÈRE DES SERVICES

CENTRE DE SERVICES • GESTION DES INCIDENTS • GESTION DES PROBLÈMES • GESTION DES CONFIGURATIONS •

GESTION DES CHANGEMENTS • GESTION DES MISES EN PRODUCTION • GESTION DES NIVEAUX DE SERVICE • GESTION DE LA CAPACITÉ •

GESTION DE LA DISPONIBILITÉ • GESTION DE LA CONTINUITÉ DE SERVICE • GESTION FINANCIÈRE DES SERVICES

pour un service informatique

optimal

2^e édition

MIS À JOUR
AVEC ITIL V3
ET LA NORME
ISO 20000 !



EYROLLES

iTIL

pour un service informatique

optimal
2^e édition

CHEZ LE MÊME ÉDITEUR —

F. VALLÉE. – **UML pour les décideurs.**

N°11621, 2005, 282 pages.

P. ROQUES, F. VALLÉE. – **UML 2 en action.**

De l'analyse des besoins à la conception J2EE.

N°11462, 2004, 386 pages.

P. MANGOLD. – **Gestion de projet informatique.**

N°11752, 2006, 120 pages.

E. O'NEILL. – **Conduite de projets informatiques offshore.**

N°11560, 2005, 336 pages.

S. BORDAGE. – **Conduite de projet Web.**

N°11911, 2006, 394 pages.

M. RIZCALLAH. – **Annuaires LDAP.**

N°11504, 2^e édition 2004, 576 pages.

R. LEFÉBURE, G. VENTURI. – **Gestion de la relation client.**

N°11331, 2004, 466 pages.

J.-L. MONTAGNIER. – **Réseaux d'entreprise par la pratique.**

N°11258, 2004, 556 pages.

L. VERLAINE, F. HARDANGE, F. BIARD, D. ELIAS. – **Tests de performances des applications Web.**

N°11395, 2003, 246 pages.

P. DEVOITINE. – **Mettre en place et exploiter un centre d'appels.**

N°11122, 2003, 402 pages.

F. RIVARD, T. PLANTAIN. – **L'EAI par la pratique.**

N°11199, 2002, 416 pages.

F. ALIN, X. AMOROS, M. SALIOU. – **L'entreprise intranet.**

Guide de conduite de projet.

N°11118, 2002, 228 pages.

C H R I S T I A N D U M O N T

Préface de **Patrick Abad**

itil
pour un service informatique
optimal
2^e édition

EYROLLES

ÉDITIONS EYROLLES
61, bd Saint-Germain
75240 Paris Cedex 05
www.editions-eyrolles.com

Les dessins figurant pages 8, 68, 86, 98, 112, 128, 142, 156, 172, 186, 208, 224 et en couverture de l'ouvrage ont été réalisés par Cubi (<http://cubiprods.free.fr>).

ITIL est une marque déposée de l'OGC (*Office of Government Commerce*).



Le code de la propriété intellectuelle du 1^{er} juillet 1992 interdit en effet expressément la photocopie à usage collectif sans autorisation des ayants droit. Or, cette pratique s'est généralisée notamment dans les établissements d'enseignement, provoquant une baisse brutale des achats de livres, au point que la possibilité même pour les auteurs de créer des œuvres nouvelles et de les faire éditer correctement est aujourd'hui menacée.

En application de la loi du 11 mars 1957, il est interdit de reproduire intégralement ou partiellement le présent ouvrage, sur quelque support que ce soit, sans autorisation de l'éditeur ou du Centre Français d'Exploitation du Droit de Copie, 20, rue des Grands-Augustins, 75006 Paris.

© Groupe Eyrolles, 2006, 2007, ISBN : 978-2-212-12102-5

Mise en page : TyPAO
Dépôt légal : juin 2007
N° d'éditeur : 7653
Imprimé en France

Préface

Très longtemps, les méthodes furent l'apanage quasi exclusif des départements Études, avec force renforts de méthodologies, d'ateliers de génie logiciel et autres frameworks qui, outre un coût souvent proportionnel à leur niveau d'abstraction, ont eu tendance à rendre encore plus opaques les technologies de l'information. Dans les salles machines de l'exploitation informatique et les centres de support, lorsqu'il n'était plus question de technologie, mais de service, la situation était moins éclatante et le savoir-faire bien plus artisanal.

Issu du terrain et développé en mode collaboratif, le référentiel ITIL consacre les meilleures pratiques dans le domaine de la production informatique. Fondé sur les principes universels des démarches qualité (focus client, orientation processus, amélioration continue), ITIL est l'approche la plus complète et la plus structurée disponible en matière de service informatique.

La bibliothèque ITIL est aujourd'hui le standard incontournable en ce domaine et son succès est avéré ; l'évolution des certifications, du nombre d'adhérents à son forum, l'ItSMF, le ralliement des principaux acteurs de l'industrie... en témoignent.

Ultime consécration, ITIL est aujourd'hui reconnu par l'ISO qui a élaboré la norme ISO/IEC 20000 « Gestion de service » sur ses bonnes pratiques.

Laboutissement de la norme ISO 20000 est la certification de l'entreprise, donc la garantie, pour ses clients internes ou externes, de la mise en place effective des bonnes pratiques dans les services qu'elle propose.

Dans ce contexte, l'approche cosmétique ne suffit pas. Il faut réellement faire évoluer l'organisation, tout en adaptant ses processus en regard des objectifs métiers.

Or, bien plus que dans d'autres domaines, le secteur de l'informatique et des télécommunications se caractérise par la rapidité de l'obsolescence des technologies.

Si l'amélioration des performances et les gains de productivité passent par l'innovation permanente, les retours sur investissement imposent une banalisation des usages auprès des utilisateurs finaux. Cette particularité impose une démarche en grand écart qui associe la standardisation d'une part et l'anticipation des enjeux d'avenir de l'entreprise d'autre part.

Au-delà de l'alignement des services informatiques au métier de l'entreprise par le rapprochement entre les départements informatiques et les directions métiers et leurs processus, comment utiliser ITIL pour créer de la valeur ?

En soulignant l'importance du cycle de vie des services IT et en facilitant la mise en relation avec les thèmes de l'IT Gouvernance, la nouvelle version ITIL V3 fournit des éléments de réponse.

Cette version actualisée du référentiel s'intéresse non seulement au « quoi faire ? » mais aussi au « comment faire ? », et de fait, elle fournit beaucoup d'informations et de recommandations pour faciliter sa mise en œuvre ; une nouvelle approche, plus globale et dynamique, apporte une plus grande souplesse d'implémentation et davantage de flexibilité.

Nul doute que les démarches ITIL seront plus faciles à initier si l'on garde à l'esprit que le danger ne vient pas des méthodes mais de la façon dont on les applique. C'est l'esprit « dogmatique » qui entrave le bon fonctionnement des processus. Rappelons-nous simplement qu'ITIL est un recueil de bonnes pratiques et en aucun cas la vérité absolue !

Si l'on cherche à tout prix à coller aux bonnes pratiques décrites dans les livres de référence, sans comprendre comment celles-ci peuvent s'adapter et contribuer aux objectifs de l'entreprise, on risque de tomber dans le travers qu'ITIL entend combattre : la focalisation sur la technique plutôt que sur les besoins du client... C'est en ce sens que l'ouvrage de Christian Dumont, autre une restitution fidèle du référentiel ITIL, est aussi un guide très pratique d'implémentation et constitue par conséquent une bonne introduction à une démarche ITIL pragmatique et pérenne.

Patrick ABAD
Administrateur ItSMF France

Un grand merci à Nathalie, Jonathan, Noémie, Julien...
pour leur infinie patience.

Salut GLacial à Laurent et sa bande de Nordistes !

Bonne chance à Bob qui va bientôt devenir célèbre...

Merci aux membres du Carros TEAM pour leur amitié.

Enfin, merci à Geooorges et aux « comiques » qui se reconnaîtront.

Table des matières

Introduction	1
Mesurer l'efficacité des services informatiques	1
<i>La réduction des coûts</i>	1
<i>Le contrôle des coûts</i>	2
<i>La préoccupation client</i>	3
<i>Communiquez...</i>	3
<i>La recherche de qualité</i>	3
<i>Répondre aux besoins</i>	3
La réponse d'ITIL	4
Structure de l'ouvrage	4
À qui s'adresse ce livre ?	5

Partie I Présentation d'ITIL

Chapitre 1 – ITIL : les fondamentaux	9
Qu'est-ce que ITIL ?	9
<i>Bibliothèque de référence</i>	9
<i>Un modèle vivant</i>	10
ITIL V2	11
ITIL V3	11
Organismes et certifications	13
<i>Les organismes</i>	13
<i>La certification ITIL</i>	14

Table des matières

La gestion des services informatiques	14
<i>Les attentes de l'entreprise</i>	14
<i>Qu'est-ce qu'un service ?</i>	15
<i>Les concepts fondateurs</i>	15
<i>Les différents acteurs</i>	22
Pourquoi implanter la gestion des services ?	23
La structure ITIL V2	23
<i>La perspective métier</i>	25
<i>Planification de la mise en œuvre de la gestion des services</i>	27
<i>Soutien des services</i>	28
<i>Fourniture des services</i>	30
<i>Gestion des infrastructures TIC</i>	33
<i>Gestion des applications</i>	34
<i>Gestion des actifs logiciels</i>	35
<i>Gestion de la sécurité</i>	37
<i>Implantation dans les petites structures</i>	38
La structure ITIL V3	39
<i>Pourquoi cette nouvelle version ?</i>	39
<i>Ce qui ne change pas !</i>	40
<i>Alors... qu'est-ce qui change ?</i>	41
<i>Le cycle de vie</i>	42
<i>Autour du cœur</i>	49
Chapitre 2 – Les relations entre les processus	51
Les différents processus	51
<i>Gestion de configuration</i>	51
<i>Centre de services</i>	52
<i>Gestion des incidents</i>	52
<i>Gestion des problèmes</i>	52
<i>Gestion des changements</i>	53
<i>Gestion des mises en production</i>	53
<i>Gestion des niveaux de service</i>	53

Gestion de la capacité	54
Gestion financière des services informatiques	54
Gestion de la disponibilité	54
Gestion de la continuité de service	54
Autres processus	55
Gestion de la sécurité	55
Gestion de l'infrastructure TIC	55
Enchaînements des actions	56
 Chapitre 3 – Les conséquences de l’implantation d’ITIL	59
Les apports bénéfiques	59
Les conséquences néfastes	60
Les surcoûts liés	61
Le retour sur investissement	62
<i>Quelques exemples</i>	62
Tendances et réalités	63
Cas d’école	64

Partie II

Soutien des services informatiques

 Chapitre 4 – Le centre de services	69
Vue d’ensemble	69
<i>Pourquoi un centre de services ?</i>	70
Responsabilités	71
Description du centre de services	74
<i>Mise en place d’un centre de services</i>	74
<i>Technologies du centre de services</i>	75
<i>Surveillance de la charge de travail</i>	78
<i>Classement des incidents</i>	78
<i>Escalade</i>	78
<i>Analyse de la satisfaction client</i>	78
<i>Facturation du service support</i>	79
<i>Interaction avec les utilisateurs</i>	79
<i>Compétence et formation du personnel du centre de services</i>	79

Table des matières

<i>Procédures du centre de services</i>	81
<i>Rapport de gestion</i>	83
<i>Avantages</i>	83
<i>Problèmes possibles</i>	84
Conclusion	84
Chapitre 5 – La gestion des incidents	87
<i>Vue d'ensemble</i>	87
<i>Pourquoi une gestion des incidents ?</i>	87
<i>Concepts</i>	88
<i>Périmètre</i>	90
<i>Terminologie</i>	90
<i>Description du processus</i>	91
<i>Flux du processus</i>	91
<i>Planification et mise en œuvre</i>	94
<i>Améliorations</i>	94
<i>Mesures et contrôles</i>	95
<i>Documents et rapports de gestion</i>	95
<i>Conséquences</i>	95
<i>Outils</i>	96
<i>Rôles et responsabilités</i>	97
Chapitre 6 – La gestion des problèmes	99
<i>Vue d'ensemble</i>	99
<i>But et mission</i>	99
<i>Concepts</i>	100
<i>Périmètre</i>	101
<i>Terminologie</i>	102
<i>Description du processus</i>	103
<i>Flux du processus</i>	103
<i>Planification et mise en œuvre</i>	106
<i>Améliorations</i>	107
<i>Mesures et contrôles</i>	108
<i>Documents et rapports</i>	108
<i>Conséquences</i>	109
<i>Rôles et responsabilités</i>	109

Chapitre 7 - La gestion des configurations	113
Vue d'ensemble	113
Pourquoi ?	113
Concepts	114
Description du processus	117
Flux du processus	117
Planification et mise en œuvre	122
Mesures et contrôles	124
Coûts	124
Documents et rapports	124
Conséquences	125
Outils	126
Rôle et responsabilités	126
Chapitre 8 - La gestion des changements	129
Vue d'ensemble	129
Pourquoi ?	130
Concepts	130
Périmètre	130
Terminologie	132
Description du processus	132
Flux du processus	132
Planification et mise en œuvre	134
Mesures et contrôles	138
Coûts	139
Documents et rapports	139
Conséquences	139
Outils	140
Rôles et responsabilités	140
Responsable	141
Comité	141
Chapitre 9 - La gestion des mises en production	143
Vue d'ensemble	143
Pourquoi ?	143
Concepts	144

Table des matières

Périmètre	146
Terminologie	146
Description du processus	147
<i>Flux du processus</i>	147
<i>Planification et mise en œuvre</i>	148
<i>Mesures et contrôles</i>	150
<i>Coûts</i>	151
<i>Documents et rapports</i>	151
<i>Conséquences</i>	152
<i>Outils</i>	152
Rôles et responsabilités	153

Partie III

Fourniture des services informatiques

Chapitre 10 – La gestion des niveaux de service	157
Vue d'ensemble	157
<i>Pourquoi</i>	157
<i>Concepts</i>	158
<i>Périmètre</i>	158
<i>Terminologie</i>	159
Description du processus	160
<i>Flux du processus</i>	160
<i>Planification et mise en œuvre</i>	162
<i>Mesures et contrôles</i>	168
<i>Coûts</i>	169
<i>Documents et rapports</i>	169
<i>Conséquences</i>	169
Rôles et responsabilités	170
Chapitre 11 – La gestion de la capacité	173
Vue d'ensemble	173
<i>Pourquoi</i>	174
<i>Concepts</i>	175
<i>Périmètre</i>	175
<i>Terminologie</i>	175

Description du processus	176
<i>Flux du processus</i>	176
<i>Planification et mise en œuvre</i>	177
<i>Mesures et contrôles</i>	180
<i>Coûts</i>	181
<i>Documents et rapports</i>	181
<i>Conséquences</i>	181
<i>Outils</i>	183
<i>Méthodes</i>	183
Rôles et responsabilités	184
 Chapitre 12 – La gestion de la disponibilité	187
Vue d'ensemble	187
<i>Périmètre</i>	188
<i>Terminologie</i>	189
Description du processus	191
<i>Flux du processus</i>	191
<i>Documents</i>	194
<i>Améliorer la disponibilité</i>	194
<i>Mesures de la disponibilité</i>	196
<i>Coûts</i>	201
<i>Conséquences du processus de gestion de la disponibilité</i>	204
<i>Rôles et compétences du responsable du processus</i>	205
 Chapitre 13 – La gestion de la continuité de service	209
Vue d'ensemble	209
<i>Pourquoi ?</i>	210
<i>Concepts</i>	210
<i>Périmètre</i>	211
<i>Terminologie</i>	211
Description du processus	212
<i>Flux du processus</i>	212
<i>Planification et mise en œuvre</i>	213
<i>Mesures et contrôles</i>	220
<i>Coûts</i>	220

Table des matières

<i>Documents et rapports</i>	220
<i>Conséquences</i>	220
<i>Méthodes</i>	221
Rôles et responsabilités	222
<i>Comité</i>	222
Chapitre 14 – La gestion financière des services	225
<i>Vue d'ensemble</i>	225
<i>Pourquoi</i> ?	226
<i>Concepts</i>	226
<i>Périmètre</i>	227
<i>Description du processus</i>	228
<i>Flux du processus</i>	228
<i>Planification et mise en œuvre</i>	228
<i>Mesures et contrôles</i>	238
<i>Coûts</i>	238
<i>Documents et rapports</i>	238
<i>Conséquences</i>	239
<i>Outils</i>	240
Rôles et responsabilités	240

Partie IV

Mise en place d'un projet ITIL

Chapitre 15 – Projet d'implantation d'ITIL/ITSM	245
<i>ITIL : un projet permanent !</i>	245
<i>Les étapes du projet</i>	246
<i>Par où commencer ?</i>	246
<i>Le choix des processus</i>	248
<i>Le cycle d'implantation ITIL</i>	249
<i>Comment débuter un projet ITIL ?</i>	252
<i>Quelle structure de projet mettre en place ?</i>	252
<i>Sur quels éléments se fonder pour lancer le projet ?</i>	253

<i>Une fois la structure mise en place, comment démarrer ?</i>	253
<i>Quels processus lancer au début ?</i>	254
<i>Comment faire accepter le projet ?</i>	255
<i>Quelle durée consacrer à la formation ou à la sensibilisation ?</i>	256
<i>Comment justifier les investissements budgétaires ?</i>	256
Les ressources du projet	257
<i>Personnel</i>	257
<i>Temps</i>	259
<i>Logiciel</i>	259
<i>Matériel</i>	259
<i>Formation</i>	260
Les facteurs de succès	260
<i>Avoir une vision claire</i>	260
<i>Préparer l'entreprise</i>	260
<i>Prévoir une démarche progressive</i>	262
Conclusion	263
Chapitre 16 – Étude de cas	265
Présentation	265
<i>L'entreprise</i>	266
<i>Le projet</i>	270
Réalisation	273
<i>Changement d'organisation au sein de l'équipe informatique</i>	273
<i>Gestion de l'infrastructure</i>	275
<i>Gestion du support des services</i>	276
<i>Gestion de la fourniture des services</i>	281
Bilan	286
Chapitre 17 – Justifier un projet ITIL	289
Quelle adoption pour ITIL ?	289
<i>Les gains perçus</i>	290
<i>Les obstacles rencontrés</i>	290
<i>Les constats</i>	291
Gérer le changement	291
<i>Changements organisationnels</i>	292
<i>Changements culturels</i>	293

Table des matières

Vendre son projet	296
Identifier les cibles	297
Identifier les sponsors	298
Vendre à la direction	298
Vendre aux équipes	304
Conclusion	307
Du bon sens.....	307

Partie V

Annexes

Annexe A – Certification ITIL	311
Organismes	311
OGC	311
itSMF	311
EXIN et ISEB	312
Certifications	312
Niveau de base, les fondations : « Foundation Certificate in IT Service Management »	312
Niveau de praticien expert : « Practitioner Certificate in IT Service Management »	313
Niveau responsable/gestionnaire : « Service Delivery certificate » et le « Service Support Certificate »	313
Exemple de certification de base	314
Annexe B – Glossaire	325
Termes français	325
Annexe C – Équivalence des termes anglais/français	343
Annexe D – Norme et certification ISO 20000	351
Le contexte de l'ISO 20000	351
Les avantages de ISO 20000	352
Le contenu de l'ISO 20000	352
Description de l'ISO 20000	353
Comment obtenir la certification ISO 20000 ?	365

Annexe E – Bibliographie	369
Livres	369
<i>Ouvrages français</i>	369
<i>Ouvrages anglais</i>	370
Liens Internet	371
<i>Sites en français</i>	371
<i>Sites en anglais</i>	371
Index	373

Introduction

Mesurer l'efficacité des services informatiques

Pendant plusieurs années, les grands travaux occasionnés par le passage à l'an 2000 et l'adoption de l'euro ont provoqué une envolée des dépenses informatiques. Cette situation aurait pu perdurer longtemps avec la trépidante aventure d'Internet, de la « nouvelle économie », et autres start-ups. Malheureusement, la folie des investisseurs de cette époque a été rapidement confrontée aux dures réalités de l'économie. Les sommes colossales mises en œuvre puis englouties dans la « bulle Internet » sont encore dans les esprits et désormais, le mot d'ordre est la réduction des coûts !

La réduction des coûts

Les entreprises en veulent pour leur argent. Cette situation n'est pas nouvelle, mais dans le cas de l'informatique, le choc a été rude. Alors que, durant plusieurs années, les budgets étaient peu discutés dans l'hypothèse d'une croissance importante et de gains exceptionnels, il faut désormais justifier chaque nouvelle dépense mais également chaque poste budgétaire en place. Réduire le coût engendré par le fonctionnement d'un système est une démarche salutaire lorsqu'il s'agit d'éviter le gaspillage de ressources. Cependant, il ne s'agit là que d'une des techniques envisageables d'optimisation de ce système. Alors bien sûr, l'arsenal des méthodes de contrôle de gestion, toujours plus efficaces les unes que les autres, permet de contrôler ces coûts. Avec les ROI, les TCO, les ABB/ABC/ABM, et autres *Balanced Scoreboard*, nous devrions maintenant être totalement équipés pour affronter les futurs projets informatiques, afin que les clients en aient pour leur argent. Certains éditeurs de logiciels ou cabinet de conseil d'audit proposent désormais d'évaluer l'efficacité des services informatiques à l'aide d'outils financiers très efficaces, mais dont l'usage exclusif ne peut garantir la pertinence des conclusions. En effet, n'évaluer les services rendus par l'informatique que sur le critère financier du coût de ces services est tout de même assez réducteur.

Malheureusement, il arrive encore trop souvent que ces méthodes, modèles et tableaux de bord soient utilisés comme unique moyen de mesure de

l'efficacité des services informatiques. Ils sont généralement mis en œuvre par des gestionnaires financiers qui envisagent le problème à l'aide de critères essentiellement basés sur les coûts et à qui l'on demande de faire des économies. De l'autre côté, les gestionnaires en informatique doivent répondre à des demandes de plus en plus nombreuses et exigeantes, et proposer toujours plus de performance et de disponibilité.

La solution pour sortir de ce dialogue de sourds est certainement la mise en place d'un langage unifié qui permette de faire communiquer ces deux mondes en fixant des objectifs communs. En revanche, persister à ne vouloir gérer l'informatique que d'un seul point de vue, qu'il soit basé sur la réduction des coûts ou bien sur la fuite en avant technologique, mène inéluctablement à l'impasse. Utiliser ce genre de démarche est réellement une mauvaise approche. Dans le premier cas, la réduction des coûts sera au rendez-vous, mais le revers de la médaille est de courir le risque de ne plus répondre aux besoins exprimés par les utilisateurs et donc de ne plus apporter le service demandé par l'entreprise. Dans le second cas, les dépenses s'envolent, sans certitude que la solution apportée à l'entreprise réponde à la question posée...

Le contrôle des coûts

Le gestionnaire d'un système doit toujours garder à l'esprit qu'il est responsable d'une entité qui fonctionne, évolue et s'altère dans le temps. En conséquence, il doit accepter les points suivants :

- Si vous ne le mesurez pas, vous ne pouvez pas le gérer.
- Si vous ne le mesurez pas, vous ne pouvez pas l'améliorer.
- Si vous ne le mesurez pas, ce n'est peut-être pas votre problème.
- Si vous ne pouvez pas l'influencer, ne le mesurez pas !

Mesurer les coûts associés aux services rendus est indispensable et les outils de gestion modernes le font très bien. Cependant, il semble plus pertinent d'adopter une vision de l'efficacité informatique plus proche des notions de qualité du service rendu au client au lieu de la considérer uniquement du point de vue des dépenses d'équipements et de ressources. En effet, le fait de maîtriser les coûts ne signifie pas pour autant être efficace. Cela peut même amener à offrir un service de qualité inférieure ou à ne plus satisfaire les besoins de l'entreprise, laquelle doit être en mesure d'obtenir ce dont elle a besoin au bon moment.

Tout cela ne signifie pas non plus qu'il soit préférable d'ouvrir les vannes et de laisser carte blanche aux dépenses, mais plutôt qu'un investissement en équipement puisse certes être plus coûteux, mais avoir un meilleur rapport coût/valeur et faire gagner de l'argent à l'entreprise. Il s'agit donc là d'évaluer le rendement de cet investissement.

Par exemple, pourquoi ne pas supprimer les commissions attribuées aux commerciaux. Cela serait certainement très efficace dans une optique de réduction des coûts... Néanmoins, cette solution serait-elle pour autant pertinente pour l'activité de l'entreprise ? Nous sommes bien là devant le dilemme du rapport coût/valeur !

Des outils de gestion comme le calcul du retour sur investissement, ou ROI (*Return On Investment*), permettent certes de calculer l'impact financier d'un projet, mais là encore, il s'agit d'une analyse qui n'aborde pas certaines questions telles que la satisfaction client ou la réponse effective aux besoins de l'entreprise.

La préoccupation client

Un bon indicateur doit donc prendre en compte cette dimension de satisfaction client. Il peut être obtenu assez simplement en soumettant les utilisateurs à des sondages et des questionnaires. En tout état de cause, si vous ne posez pas de questions, vous n'aurez aucune réponse !

L'un des points de départ de l'efficacité informatique est une meilleure communication entre le service informatique et l'entreprise, afin d'identifier les besoins réels et non supposés.

Communiquez...

Cela peut contribuer à promouvoir la communication interne et le bon fonctionnement de l'organisation dans son ensemble, qui est certainement le critère de l'efficacité du service informatique. Il est évident que pour établir une route il faut savoir où l'on désire se rendre mais également d'où l'on part.

Suivre ces principes est important puisqu'ils insistent sur la communication entre les technologies de l'information et l'entreprise, et qu'ils sont centrés sur la fourniture de services plutôt que sur la technologie. Ils permettent également d'anticiper les évolutions dans l'entreprise, lesquelles se traduisent souvent par des investissements en matériel qu'il convient de maîtriser et non de refuser.

Mettre en place les « bonnes pratiques » rend plus efficace et est un bon moyen de réduire les coûts. L'informatique est là pour offrir un service. Si elle ne remplit pas cet objectif, elle n'est tout simplement pas efficace et rien ne saurait la justifier, quels que soient les coûts mis en œuvre.

La recherche de qualité

Les services informatiques sont mis en place afin de permettre aux utilisateurs de s'appuyer sur les ressources dont ils ont besoin pour faire leur travail. L'utilisation optimale de ces ressources est fortement associée à une démarche qualité, ce qui correspond globalement à la mise en place d'une démarche d'amélioration continue dans le but d'atteindre un système conforme aux objectifs fixés.

Répondre aux besoins

On le comprend, l'efficacité informatique ne se résume pas à réduire les coûts d'année en année. Il est clair qu'il vaut mieux annoncer une hausse

maîtrisée du budget informatique si celle-ci permet à l'entreprise d'accroître ses parts de marché plutôt qu'une baisse de ce budget, obérant le potentiel de croissance de l'entreprise.

La réponse d'ITIL

Ce type de problème et ces questions récurrentes ont suscité diverses réactions chez les professionnels de l'informatique, mais également les spécialistes de la qualité ou de l'organisation. Pour résoudre des problèmes liés à l'efficacité et à la réponse aux besoins du client, quelle meilleure réponse que l'utilisation des bonnes pratiques ?

ITIL a été initialement conçu et développé vers la fin des années 1980, sur l'initiative du gouvernement britannique, comme un ensemble de bonnes pratiques destinées à améliorer l'efficacité des services informatiques du secteur public. Cette mission a tout d'abord été confiée au CCTA (*Central Computer & Telecommunication Agency*) puis, a été reprise par l'OGC (*Office of Government Commerce*). Après plusieurs années de travail, et avec l'aide de nombreux professionnels de l'informatique (consultants spécialisés, experts indépendants, formateurs), la première version d'ITIL a pu être publiée. Près d'une quarantaine de livres ont été produits depuis cette époque. La mise à jour de l'année 2000 (V2) a permis de réduire ce nombre aux dix livres que nous connaissons aujourd'hui. Comme nous le verrons dans le premier chapitre, la troisième version (V3), publiée au cours de l'année 2007, propose cinq livres en tout et pour tout dans le cœur du modèle. Cette version n'est pas encore disponible et son adoption devrait prendre un certain temps compte tenu du volume considérable de travail complémentaire à fournir (formation, certification, documents divers...)

Structure de l'ouvrage

Ce livre est découpé en cinq grandes parties qui reprennent peu ou prou les différentes étapes d'un projet d'implantation d'ITIL au sein d'une entreprise : découverte du concept, imprégnation et formation sur les différents modules, planification du projet puis mise en place des processus.

Dans la première partie, vous trouverez une présentation des fondamentaux d'ITIL, des bénéfices que l'on peut tirer de la mise en place de ces meilleures pratiques, ainsi qu'un descriptif des relations qui se tissent entre les différents processus.

Les deux grandes parties suivantes sont consacrées à deux des dix livres du référentiel qui concernent la gestion des services liés aux technologies de l'information et des télécommunications, et couvrent globalement le programme de la certification de base. Ces deux parties reviennent plus en détail sur chacun des processus du soutien et de la fourniture des services. Par ailleurs, il apparaît que le contenu de ces deux livres restera globalement inchangé dans la future version.

La quatrième partie est davantage orientée sur la mise en œuvre des processus lors d'un projet d'implantation au sein d'une entreprise, avec à la clé une étude de cas réel.

La cinquième partie, enfin, est constituée des annexes dans lesquelles vous trouverez un descriptif de la norme ISO 20000, un glossaire des termes français utilisés fréquemment dans ITIL ainsi que leurs équivalents en anglais. Vous y découvrirez également une annexe sur la certification, illustrée par un exemple d'examen type ITIL Foundation.

À qui s'adresse ce livre ?

Différents niveaux de lecture se dégagent de ces cinq parties. La lecture de la première partie est adaptée à toutes les personnes qui désirent en apprendre un peu plus sur ITIL sans pour autant en devenir des spécialistes. Les deux parties suivantes rentrent beaucoup plus dans les détails et sont donc destinées à ceux ou celles qui souhaitent mettre en œuvre ces processus au sein de leurs entreprises. La quatrième partie est quant à elle davantage destinée aux chefs de projets ayant à mettre en place un projet de gestion des services TIC utilisant le référentiel ITIL. La cinquième et dernière partie sera consultée avec profit par l'ensemble des lecteurs et en particulier ceux qui souhaitent faire valider leurs connaissances par une certification.

PARTIE I

Présentation d'ITIL

Dans cette partie, vous trouverez une présentation des principes fondamentaux d'ITIL et, plus particulièrement, des bénéfices que l'on peut tirer de la mise en place de ces meilleures pratiques, ainsi qu'un descriptif des relations qui se tissent entre les différents processus.

- Chapitre 1 – ITIL : Les fondamentaux
- Chapitre 2 – Les relations entre les processus
- Chapitre 3 – Les conséquences de l'implantation d'ITIL

GESTION DES SERVICES



LES BONNES PRATIQUES DE LA GESTION DES SERVICES, C'EST
L'AMÉLIORATION CONTINUE DE LA QUALITÉ EN FONCTION
DES BESOINS DES CLIENTS.

ITIL : les fondamentaux

Qu'est-ce que ITIL ?

Pour comprendre ce qu'est ITIL, le plus simple est encore d'analyser son acronyme. ITIL, ou *Information Technology Infrastructure Library*, signifie plus ou moins bibliothèque d'infrastructure des technologies de l'information. Il s'agit d'un ensemble de livres dans lesquels sont reprises et référencées de nombreuses pratiques, procédures et méthodes permettant de gérer les systèmes d'information.

Bibliothèque de référence

En tant que recueil des « meilleures pratiques », ITIL n'est pas une méthode, mais il en utilise certaines. ITIL n'est pas non plus un langage, mais il en définit un. ITIL n'est enfin pas une norme, malgré ce que laissent entendre certains éditeurs dont les documentations affirment que leurs produits sont totalement « compatibles ITIL ». C'est justement là que se trouve tout l'intérêt de ce référentiel. Les meilleures pratiques offrent aux entreprises une structure éprouvée par des années d'expérience pour formaliser leurs processus et gérer leurs environnements informatiques. Toutefois, elles servent avant tout de lignes directrices aux entreprises afin d'élaborer leurs processus en fonction des besoins spécifiques à leur activité. À la différence de beaucoup de modèles, méthodes et autres solutions d'organisation, ITIL propose un côté non intrusif qui permet de s'adapter à la réalité rencontrée en entreprise. C'est certainement une des raisons de son grand succès au niveau mondial.

Cependant, du fait de l'importante reconnaissance d'ITIL au niveau mondial, le besoin d'une norme basée sur les recommandations d'ITIL a vu le jour.

C'est désormais chose faite depuis janvier 2006 avec la norme ISO 20000 reposant sur la norme britannique BS 15000 (un chapitre spécial est consacré à la nouvelle norme en annexes).

Basé sur des principes forts comme l'orientation client, l'industrialisation des services et l'optimisation des ressources, ITIL permet de guider la transformation des directions informatiques sur les plans organisationnel, culturel et technique, afin qu'elles puissent délivrer des services dont la qualité, la productivité et la maîtrise des coûts soient conformes aux attentes de l'entreprise.

Un modèle vivant

Avec près de 20 ans d'existence, le référentiel ITIL est devenu un élément essentiel de la gestion de services. À la date de publication de cet ouvrage, la version actuelle, sur laquelle sont fondées les certifications, est la version 2. Finalisée en 2000, elle a vu son environnement largement modifié depuis. Ceci a conduit l'OGC à envisager la mise à jour du référentiel en 2004 pour parvenir à la troisième version, qui sera publiée au printemps 2007. Ceci dit, on peut envisager que cette nouvelle version, déjà retardée plusieurs fois, verra son adoption se produire sur une durée de six à douze mois. Cette situation risque de bloquer la mise en œuvre de projets ITIL sur la même période et d'avoir un effet financier sur eux. En effet, cette nouvelle version risque d'encourager les entreprises qui souhaitent adopter ITIL à attendre que la mise à jour soit prête avant de lancer leur projet.

Pourtant, bien qu'elle apporte un certain nombre d'améliorations de taille, cette nouvelle version ajoute des couches à une version d'ITIL déjà très complète. Les principaux processus seront repris à l'identique. Ceci explique que le noyau d'ITIL ne changera pas de manière substantielle avec cette nouvelle version.

ITIL est une bibliothèque ouverte disposant d'un certain nombre de livres. Ses « lecteurs » sont libres de choisir entre la mise en œuvre de la deuxième version (meilleures pratiques et alignement de l'informatique aux métiers) et l'adoption de la troisième version (gestion du cycle de vie des processus). Par ailleurs, une bonne façon de ne pas choisir, est d'adopter une démarche itérative chère à l'esprit de Deming. Dans cette démarche, les nouveaux utilisateurs d'ITIL peuvent débuter avec la version 2 en développant leurs processus ITIL et ajouter par la suite de nouvelles fonctionnalités en utilisant les concepts de la gestion du cycle de vie des processus prônés par la troisième version.

Pour ces raisons, les pages suivantes reprendront l'essentiel de la version 2 et de la version 3 pour les comparer, mais s'attarderont surtout sur la seconde version qui est toujours celle utilisée en entreprise.

ITIL V2

Comme nous le verrons dans la suite de ce chapitre, à la différence de la future version (V3 - 2007) dont le cœur ne sera constitué que de cinq livres, la version actuelle d'ITIL (V2 - 2000) est constituée de dix livres :

- La perspective métier (*Business Perspective*) présente les avantages de la gestion des services pour l'entreprise et permet de mieux en comprendre les enjeux. Ce volume comporte deux tomes.
- La planification de la mise en œuvre de la gestion de services (*Planning to Implement Service Management*) établit un plan d'action.
- La fourniture des services (*Service Delivery*) couvre les processus nécessaires à la conception et à la fourniture des services.
- Le soutien des services (*Service Support*) concerne les processus nécessaires à la maintenance et à l'assistance technique des services.
- La gestion de l'infrastructure TIC (*ICT Infrastructure Management*) expose les processus de conception et de gestion des infrastructures informatiques et télécoms.
- La gestion des applications (*Application Management*) couvre les interactions de la gestion des applications avec la gestion des services.
- La gestion de la sécurité (*Security Management*) reprend l'ensemble des aspects de mise en œuvre et de gestion de la sécurité des systèmes d'information.
- La gestion des actifs logiciels (*Software Asset Management*) illustre la gestion des objets logiciels sur l'ensemble de leur cycle de vie.
- Enfin, le dernier livre intitulé « implantation dans les petites structures » (*Small Scale Implementation*) est orienté sur la mise en place d'ITIL dans une PME.

ITIL V3

Cette nouvelle version d'ITIL se présente comme une évolution majeure par rapport à la V2. En effet, ces livres qui se trouvent dorénavant au cœur du cycle de vie des services (*lifecycle titles*), proposent une nouvelle vision des concepts des versions précédentes, en conservant l'essentiel de leur substance. Ceci dit, cette version entraîne tout de même d'importants changements et en particulier sur la structure globale comme on peut le voir sur la figure 1-1. Le cœur d'ITIL V3 se compose désormais de cinq livres principaux dans le cœur du modèle :

- Stratégies des services ;
- Conception des services ;
- Transitions des services ;
- Opérations des services ;
- Amélioration continue des services.

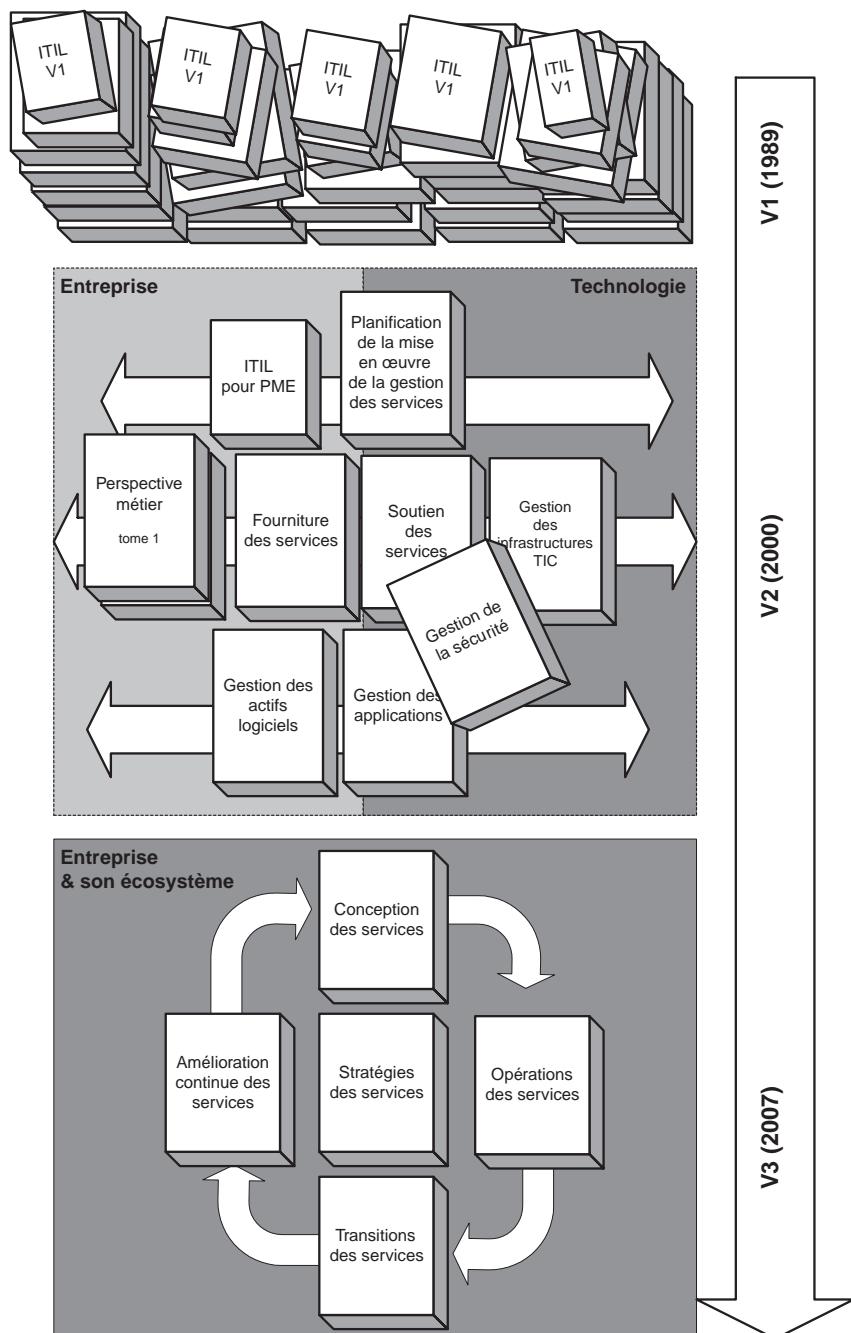


Figure 1-1 : Évolution de la structure ITIL

Ce nouveau référentiel ITIL sera complété par un ensemble de petits guides tels que :

- une introduction à ITIL ;
- un guide des éléments clés (*Pocket Guide*) ;
- un guide du décideur ;
- plusieurs guides complémentaires spécifiques à chaque sujet ;
- des études de cas ;
- des modèles de cycle de vie de service intégré ;
- une aide à la certification ;
- une méthode de gouvernance portant sur le service, l'organisation et les processus ;
- des cartes de processus.

Organismes et certifications

Les organismes

Plusieurs organismes oeuvrent à la promotion et à l'assistance concernant ITIL dans le monde. Parmi ceux-ci, on trouve notamment l'OGC, l'EXIN, l'ISEB, l'itSMF et un ensemble de sociétés plus ou moins impliquées dans l'essor et l'adoption du référentiel.

OGC

L'OGC est l'organisme britannique propriétaire d'ITIL qui en assume la promotion au niveau mondial.

EXIN, ISEB

L'EXIN et l'ISEB sont deux organismes britannique et néerlandais indépendants de l'OGC. Ils assument cependant le rôle de coordinateur des certifications ITIL.

itSMF

Association internationale sans but lucratif dédiée à la promotion d'ITIL dans le monde. Chaque pays dispose de son association locale.

Le chapitre français de l'itSMF est très actif pour la promotion du référentiel. Vous trouverez de nombreux documents sur son site Web (voir en annexe).

Les centres de formation

Les centres de formation qui dispensent les cours ITIL font découvrir ou approfondir les concepts, le vocabulaire et les relations entre les processus d'ITIL. Ces centres sont assez nombreux et une simple recherche sur Internet permet d'en identifier plusieurs rapidement. Cependant, ces centres de formation ne sont pas tous accrédités par les organismes de certification et ne sont donc pas tous habilités à faire passer l'examen. Il est donc indispensable de se renseigner avant de s'engager si l'on souhaite obtenir la certification.

La certification ITIL

Les trois niveaux de certification ITIL valident le niveau de connaissance et de compréhension des principes d'ITIL.

Les bases d'ITIL (ITIL Foundation)

Ce niveau de certification concerne les personnes qui utilisent ou comprennent utiliser ITIL dans leur travail, qui ont besoin d'une vue générale des processus et recherchent les éléments essentiels de la gestion des services informatiques.

Praticien d'ITIL (ITIL Practitioner)

Cette certification plus avancée concerne les personnes qui pratiquent depuis plusieurs années la gestion des services informatiques et qui souhaitent se spécialiser dans un domaine précis d'ITIL et ne font valider qu'un seul processus (exemple : praticien de la gestion de la disponibilité).

Responsable de projet ITIL (ITIL Service Manager)

La dernière certification demande plusieurs années d'expérience et concerne l'ensemble des processus ITIL. Elle est destinée aux consultants, spécialistes, chefs de projet et en général à toutes les personnes qui souhaitent prendre en charge l'implantation des processus ITIL au sein d'une organisation.

La gestion des services informatiques

Les attentes de l'entreprise

En vingt ans, grâce à d'importants progrès technologiques, l'utilisation de l'informatique a favorisé la transition des entreprises de l'ère industrielle à l'ère de l'information.

Ces dernières années ont clairement démontré l'importance stratégique, sinon vitale, pour toute entreprise de gérer cette ressource « informationnelle » au même titre que ses autres actifs.

En conséquence, il faut comprendre à quel point les entreprises dépendent de leurs infrastructures informatiques et de leurs télécommunications lorsqu'elles développent des stratégies commerciales, des produits ou des services destinés à conquérir et à fidéliser des clients. Toutes les fonctions de l'entreprise doivent être coordonnées pour lui permettre d'atteindre ses objectifs de croissance et de rentabilité afin de créer de la valeur. L'informatique est au cœur de cette stratégie car la création de valeur repose également sur la disponibilité et la bonne gestion des applications et des infrastructures.

Plus les services informatiques sont alignés sur la stratégie, plus ils contribuent à l'avantage concurrentiel que l'entreprise s'efforce de développer. L'intérêt d'ITIL est de permettre à la direction informatique de substituer une vision de manager à la trop fréquente vision technique de l'informatique qui se conclut souvent par un dialogue de sourds entre les gestionnaires de l'entreprise et les techniciens du service. Cela permet au service informatique dans son ensemble de mieux se faire comprendre des autres directions de l'entreprise.

Qu'est-ce qu'un service ?

Lorsqu'il est utilisé dans le contexte informatique, on peut donner plusieurs définitions au mot service, mais globalement, il faut retenir trois idées principales de ce terme.

- En premier lieu, le service informatique est entendu comme une unité organisationnelle de l'entreprise au même titre que le service comptabilité par exemple.
- La seconde vision que l'on peut avoir d'un service informatique est davantage liée au système d'information et au service rendu par ce système. Il s'agit dans ce cas d'une ressource dont on peut profiter en devenant client : messagerie, bureautique et autres ERP. Ces services sont comparables aux autres prestations de l'entreprise comme la climatisation, l'eau courante, l'électricité ou même le courrier.
- La troisième et dernière idée que l'on peut exprimer avec le mot service correspond à la prestation, l'aide ou l'assistance que l'utilisateur peut attendre dans le sens « rendre service ».

Les concepts fondateurs

La philosophie d'ITIL repose sur quatre concepts fondamentaux :

- Le premier d'entre eux est la prise en compte de l'attente du client dans la mise en œuvre des services informatiques que les anglophones appellent le *Customer Focus*.

- Le second principe correspond aux cycles de vie des projets informatiques qui doivent intégrer dès leur naissance les différents aspects de la gestion des services informatiques.
- Le troisième concept fondateur préconise la mise en place des processus ITIL interdépendants permettant d'assurer la qualité des services.
- Le quatrième et dernier principe correspond à la mise en place d'une démarche qualité pour les services installés et d'une mesure de cette qualité effectuée du point de vue des utilisateurs.

Il reste deux concepts plus diffus, que nous retrouverons tout au long de cet ouvrage. Le premier correspond à l'importance de la communication entre le service informatique et le reste de l'entreprise. C'est dans ce but qu'ITIL définit un vocabulaire commun aux différents acteurs. Le second concept est lié au fait qu'ITIL est suffisamment souple, et doit le rester, pour s'adapter à toutes les organisations... Le maître mot est donc « adopter ITIL et adapter ITIL ».

La préoccupation client

Les services informatiques sont mis en place afin que les membres du personnel disposent des ressources informatiques nécessaires à leur travail. ITIL insiste sur l'importance de la qualité de service et l'alignement de ces services sur les besoins de l'entreprise. En conséquence, le premier concept important d'ITIL implique un état d'esprit que chaque membre de l'équipe informatique doit adopter. En effet, de trop nombreuses entreprises ont encore à déplorer des systèmes d'information uniquement basés sur la technologie, où l'accent est mis sur la toute nouvelle fonction du *groupware* dont personne ne se sert ou la mise en place d'un puissant serveur de messagerie pour un petit groupe d'employés, quand ce n'est pas une entreprise bridée par des règles de sécurité excessives.

Prendre en compte les besoins du client et de son métier, et les placer au centre de ces préoccupations lors de la mise en place des services, semble être le minimum qu'une direction informatique ait à accomplir. Par la suite, pour parfaire sa compréhension, elle doit se mettre à l'écoute de l'évolution des besoins de ses clients et de l'entreprise pour anticiper l'adaptation indispensable des services.

Pour parvenir à ce niveau de perception, la direction informatique doit mettre en place un ensemble d'actions et de tâches clés qui lui permettront de s'assurer de l'alignement des services avec les besoins.

La première de ces tâches est sans nul doute de s'assurer qu'une organisation d'assistance technique et de conseil efficace, claire et identifiée est mise à la disposition des utilisateurs pour une meilleure utilisation de la ressource informatique. Cette organisation doit évidemment comprendre un programme de mesure de la satisfaction des clients et auditer leurs besoins

afin de les aider à optimiser l'utilisation des services informatiques (exemple : mise en place de groupes d'utilisateurs internes).

Ensuite, il est indispensable de valider l'adoption de cette « préoccupation client » par les membres de l'équipe informatique ou tout au moins de susciter un changement d'attitude de leur part par le biais de formations ou d'autres actions visant à rapprocher ces techniciens des vrais besoins de leurs clients. On peut par exemple fournir un retour d'information régulier au personnel informatique sur la satisfaction client ou sensibiliser les maîtrises d'œuvre aux remarques des clients afin de les insérer dans le cycle d'amélioration des applications informatiques.

Le cycle de vie

Selon des statistiques récentes, de nombreux projets informatiques (plus de la moitié) ne sont jamais mis en exploitation pour cause d'abandon avant la livraison. Les causes des échecs sont généralement multiples et dépassent le thème de cet ouvrage. Il semble néanmoins évident que nombre de ces échecs peuvent être imputés à un déficit de communication entre le client et les fournisseurs du service attendu. ITIL propose la mise en place de processus tenant compte des aspects liés à la mise en production dès le lancement du projet.

Classiquement, les équipes de production sont associées au projet au moment de la phase de mise en exploitation de l'application, ce qui implique inévitablement qu'elles n'ont pas eu leur mot à dire lors de la conception et du développement. Le responsable de la production informatique se voit donc imposer la tâche de s'assurer et d'assumer que ce qui est compris en phase projet puis transmis en production est bien ce que souhaitait le client.

Pour éviter ce genre de situation, ITIL préconise de prendre en considération la gestion des services dès les phases d'études et de définition des besoins des projets informatiques. Ceci procure plusieurs avantages à l'ensemble des équipes, qu'elles soient issues de la production ou du développement, mais permet surtout de proposer un service plus sûr au client.

Cela permet également de valider que l'on dispose bien des ressources et des compétences nécessaires à l'exploitation de cette nouvelle application, ce qui implique de prendre en compte l'impact sur l'infrastructure matérielle dans des domaines tels que la capacité, la performance, la disponibilité, la fiabilité et la maintenance. Enfin, c'est la garantie que l'impact sur les engagements contractuels sera évalué le plus tôt possible, et en tout cas, avant de se retrouver dans une impasse avec un client qui attend son application, au risque d'en déstabiliser d'autres.

La prise en compte du cycle de vie des services aide en outre à gérer les problèmes de calendrier des projets qui divergent selon leurs natures. Les calendriers des projets d'évolution de l'entreprise qui se traduisent par de

nouvelles applications doivent être rapides et sont susceptibles de changer régulièrement. En revanche, les projets liés aux technologies sont souvent destinés à durer dans le temps. En effet, l'implantation d'une infrastructure technique dont la période d'amortissement est assez longue ne peut calquer son cycle de vie sur celui d'une application répondant à un besoin changeant de l'entreprise.

Les processus

Dans le cadre d'ITIL, la qualité de service se fonde sur une structuration des activités en processus interdépendants, mesurables et qui peuvent être répétés. Cette approche de gestion des activités par processus est aujourd'hui reconnue comme la plus efficace par un grand nombre d'entreprises. ITIL a adopté cette solution en découplant la gestion des services informatiques en une dizaine de processus. Ce découpage est une préconisation et peut être adapté aux besoins de chaque entreprise.

Dans ITIL, nous nous intéressons aux liens qui permettent aux différents processus d'interagir. Comme on peut le découvrir sur la figure 1-2, un processus

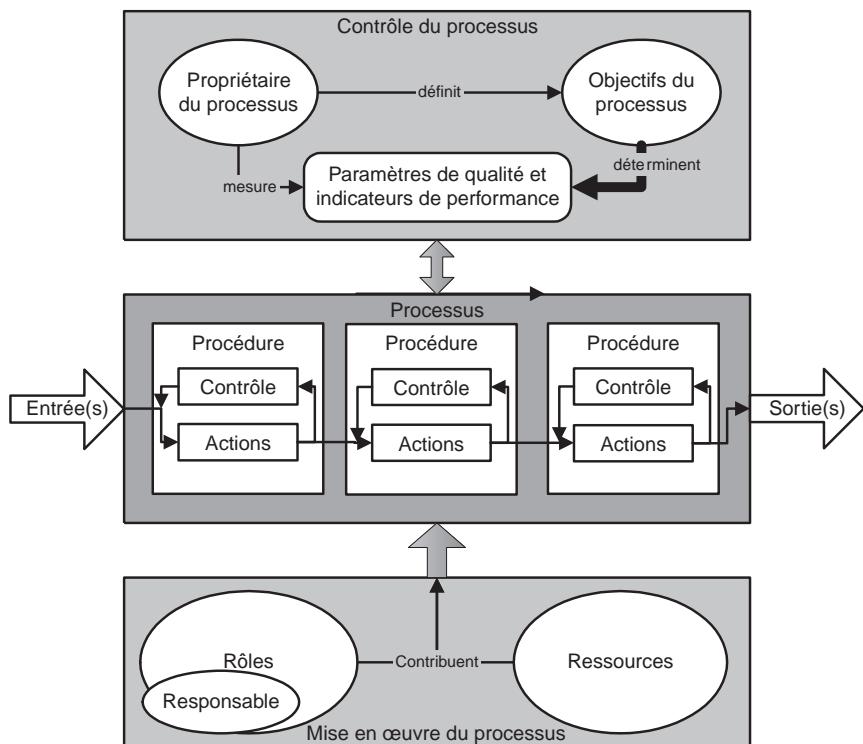


Figure 1-2 : Ordinogramme d'un processus type

est une série d'activités liées logiquement entre elles afin de parvenir à un objectif défini en utilisant des paramètres en entrée et produisant un résultat en sortie. Ces entrées/sorties représentent les interactions entre les processus et sont mesurables. Cela permet, en les comparant aux standards ou aux résultats attendus, de valider le niveau de qualité de chaque processus. Par extension, il est possible d'évaluer l'ensemble de la structure des processus de gestion des services afin de mesurer puis de valider l'efficacité atteinte par la chaîne de valeur en regard des objectifs exprimés par l'entreprise.

En termes de responsabilité, il convient de définir un vocabulaire de base identifiant les acteurs. Le propriétaire de processus est responsable des résultats et doit ensuite les présenter à l'entreprise. Le gestionnaire du processus est responsable de la réalisation de ce dernier et rend des comptes au propriétaire. Les opérateurs de processus sont responsables des tâches effectuées au sein du processus.

Comme les indicateurs de performance appropriés et les standards sont déjà établis, le contrôle quotidien peut être laissé au gestionnaire du processus. Le propriétaire évaluera les résultats basés sur le rapport de performance afin de valider que le processus remplit les objectifs fixés par l'entreprise.

Les entreprises sont pour la plupart organisées hiérarchiquement. D'autres ont des organisations reposant sur les lignes de métiers ou de produits, l'implantation géographique ou parfois un composé des points précédents. Ces entreprises ont des départements qui sont responsables de groupes d'employés. Une fois de plus, on peut trouver diverses façons de structurer ces départements. Les services informatiques dépendent généralement de plusieurs clients et/ou départements. Toutefois, la structuration des activités des services informatiques en processus ne colle pas nécessairement à cette organisation et la mise en place des processus peut parfois aboutir à ce que des processus transverses recouvrent plusieurs départements de l'entreprise sans correspondre à cette organisation hiérarchique. Par exemple, la mise à disposition de la messagerie électronique fait intervenir plusieurs départements de la direction informatique (réseau, serveur, sécurité, assistance utilisateurs...) et s'adresse à toutes les directions métier indépendamment de la ligne hiérarchique à laquelle elles appartiennent.

La qualité de service

Le client perçoit la qualité globale d'un service par rapport à son besoin métier et n'est pas intéressé par les différentes composantes techniques de ce service. Cette qualité se mesure du point de vue de l'utilisateur et/ou du client et est basée sur l'efficacité de la réponse face à la demande, à la performance obtenue, à la possibilité d'en renouveler l'exécution et surtout aux coûts mis en œuvre pour parvenir à ce résultat. Un dialogue permanent

est essentiel pour affiner les services et assurer que le client et le fournisseur parlent bien de la même chose. Ce dialogue permet également de prendre en compte les évolutions du besoin du client, ce qui peut se traduire dans une modification de la demande et pourquoi pas de la perception de la qualité.

La qualité globale d'un service est le résultat de la qualité des processus qui le composent. Ces derniers forment une chaîne où chacun a un impact sur les autres, ainsi que sur la qualité du service. La coordination efficace impose un niveau de qualité de chaque processus, mais aussi la qualité globale. La gestion de la qualité est l'affaire de toutes les personnes qui contribuent à produire et fournir le service et à en assurer l'assistance technique. Chacun doit être conscient de l'impact qu'il a sur la qualité globale du service perçu par le client. Les personnes qui assument la responsabilité de l'évolution des planifications et des procédures doivent être clairement identifiées et disposer de l'autorité suffisante pour ces évolutions qui sont souvent transversales à l'entreprise.

La qualité d'un service dépend beaucoup de la façon d'organiser les activités qui le composent. ITIL propose une méthode d'amélioration permanente de la qualité du service en utilisant la métaphore de la roue de la qualité issue des travaux du qualiticien américain E. Deming en 1930. Comme on peut le voir sur la figure 1-3, cette technique, appelée également PDCA (Plan, Do, Check, Act) propose de réaliser les quatre étapes qui la composent dans un cycle permanent.

- Planifier : décider des objectifs, du calendrier, des responsabilités et des ressources nécessaires au projet.
- Faire : implanter les activités planifiées dans la phase précédente.
- Contrôler : déterminer si les activités procurent le résultat attendu.
- Agir : ajuster les activités en fonction des informations obtenues lors de la phase de contrôle.

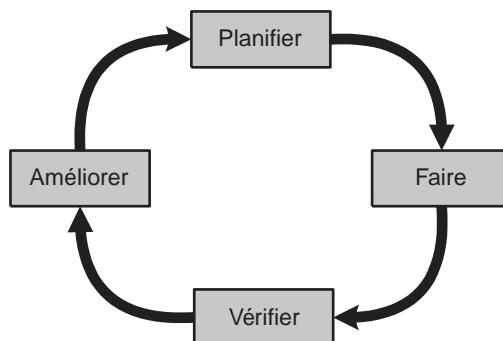


Figure 1-3 : La « roue » de Deming ou le cycle d'amélioration permanente de la qualité

La communication

Un des intérêts d'ITIL est de définir un langage commun aux utilisateurs, aux clients et bien sûr aux membres de la direction informatique. Ce langage définit les termes utilisés dans les rapports de gestion et les contrats de service (SLA) et en règle générale dans tous les documents utilisés conjointement par la direction informatique et les autres directions de l'entreprise. Ce langage lève les ambiguïtés que l'on retrouve souvent dès que l'on commence à parler d'incident ou de problème, de cause et de conséquence ou lorsqu'on est en train d'établir les statistiques de disponibilité du système, mais également lorsqu'il s'agit d'établir les engagements et les responsabilités.

De nombreuses activités impliquent une communication régulière entre les directions métier et le service informatique. Une bonne communication est une composante importante de la qualité du service. Néanmoins, l'environnement économique de l'entreprise n'autorise pas de perte de temps. Les flux tendus, la réduction des délais sont autant de contraintes que l'entreprise doit assumer pour survivre... Pourtant, même si le service informatique n'est pas exclu de cette situation, cette course contre la montre ne doit pas se faire au détriment de la communication lorsque le temps et les ressources sont limités.

L'un des résultats intéressants de la mise en place d'une communication effective de la part de l'informatique est d'obtenir une bonne vision des objectifs de l'entreprise, et des besoins des clients. Cependant, en dehors de ce gain assez classique, il en est un autre qui ne doit jamais être négligé. Il s'agit de mettre en place le « marketing de l'informatique », afin d'éviter que ne ressortent uniquement les points négatifs de la gestion des services et rarement les positifs. Les spécialistes de la qualité savent bien l'effet dévastateur d'un dysfonctionnement sur l'image d'un produit ou d'un service. L'effort à fournir pour communiquer une image de qualité aux clients est sans commune mesure avec celui à fournir pour corriger l'image de non-qualité que véhiculent parfois involontairement les utilisateurs insatisfaits. La direction informatique a donc tout à gagner à mettre en place un plan de communication visant à diffuser des informations vérifiables afin d'éviter le non-dit et les bruits de couloir.

La culture d'entreprise est particulièrement importante pour la mise en place de la gestion des services. Elle joue sur le fonctionnement des relations entre les personnes et les niveaux hiérarchiques, la façon de communiquer et le mode de prise de décision. Elle a également parfois une influence importante sur la fourniture des services informatiques et en particulier dans la perception de l'innovation. Ce point est fondamental lorsque le projet d'implantation d'ITIL est confronté à la résistance au changement. Dans une entreprise stable, où la culture donne peu de valeur à l'innovation,

il sera difficile d'ajuster ces services informatiques conformément aux évolutions de l'organisation du client. Dans le cas contraire, où l'entreprise recherche l'innovation, la mise en place de changements non contrôlés peut poser une menace sérieuse à la qualité de ses services.

Enfin, nous allons être confrontés dans les cinq à dix prochaines années à un volume important de départs à la retraite de personnel issu du « baby-boom ». Ces départs qui touchent toutes les catégories de personnels, qu'ils soient employés, cadres ou dirigeants, toucheront tous les secteurs de métier. Et même si la population informatique est en général assez jeune, il n'en reste pas moins qu'elle peut être en relation avec des personnes qui vont bientôt partir. Il est vital pour l'entreprise qu'une politique de formation et de gestion de la connaissance basée sur les processus de la gestion des services informatiques se mette en place pour pallier les vides de compétences et de connaissances que va provoquer ce départ à la retraite de nos « papy-boomers ».

Les différents acteurs

Concernant le vocabulaire, ITIL propose une distinction intéressante entre les différents acteurs des processus. Quatre termes principaux sont définis : le client, l'utilisateur, le fournisseur interne, et le fournisseur externe.

- Le client est celui qui paye le service et la prestation associée. Il en définit le niveau de service (capacité, disponibilité et coûts).
- L'utilisateur est celui qui utilise effectivement tous les jours le service proposé. Cependant, n'oublions pas qu'un client peut éventuellement être un utilisateur.
- Le fournisseur interne représente l'équipe informatique qui assume la fourniture du service aux utilisateurs, et peut consister en une équipe informatique faisant partie de l'entreprise ou être constitué d'une équipe externalisée.
- Le fournisseur externe est une tierce partie qui assume les fonctions de fourniture ou de soutien d'un ou plusieurs éléments des services (exemple : équipe de maintenance du matériel informatique).

Fréquemment, les intérêts de l'utilisateur et du client divergent. Ceci est particulièrement sensible pour les services d'assistance aux utilisateurs. L'utilisateur demande une disponibilité permanente d'un service alors que le client n'est pas disposé à assumer le coût d'un tel service. Cette divergence doit être résolue dans la définition des applications ou des performances des systèmes et même pour l'assistance aux utilisateurs.

Pourquoi implanter la gestion des services ?

Un des objectifs principaux d'ITIL est d'améliorer l'efficacité des services informatiques et de l'utilisation des ressources en respectant les contraintes de coût imposées.

Les buts spécifiques sont de développer et de maintenir des services informatiques offrant de bons rapports avec les directions métier et répondant aux besoins de l'activité économique. Ces services doivent être simples à développer et à améliorer afin de répondre aux évolutions des besoins en respectant les coûts, les délais et les contraintes de qualité.

Les avantages que l'entreprise peut tirer de la mise en place de telles pratiques sont multiples. Globalement, elles permettent d'obtenir des services plus proches des besoins de l'entreprise et qui répondent à ce qu'elle attend en termes de qualité et de coûts. De plus, on constate également une amélioration continue de ces éléments au cours du temps avec une réduction à long terme des coûts par l'amélioration de processus, une amélioration de la qualité des processus, une meilleure communication entre le service informatique et le reste de l'entreprise.

Cependant, un grand soin doit être apporté au développement de ces processus au sein d'une entreprise. En effet, il est facile de percevoir ITIL comme volumineux et bureaucratique avec en conséquence la mise en place de processus qui entravent les changements plutôt qu'ils ne les facilitent. Il est important qu'ITIL soit mis en œuvre dans une optique d'adoption et d'adaptation.

La mise en place d'un projet de meilleures pratiques impose de rester pragmatique !

L'unique solution pour cela est que le projet d'implantation dispose de métriques issues de l'activité économique, et que le projet réponde réellement aux besoins de l'entreprise dans un souci d'amélioration de la qualité.

La structure ITIL V2

ITIL fournit un recueil complet des meilleures pratiques de la gestion des services informatiques et traite des sujets liés aux personnes, aux processus, aux produits et aux partenaires.

La philosophie ITIL fait adopter une démarche évolutive qui s'appuie sur des processus étroitement liés et intégrés comme le montrent les figures 1-4 et 1-13. ITIL ne décrit pas le meilleur type d'organisation d'un service, mais les relations entre les activités dans les processus. Seules ces relations sont significatives, quel que soit le type d'entreprise.

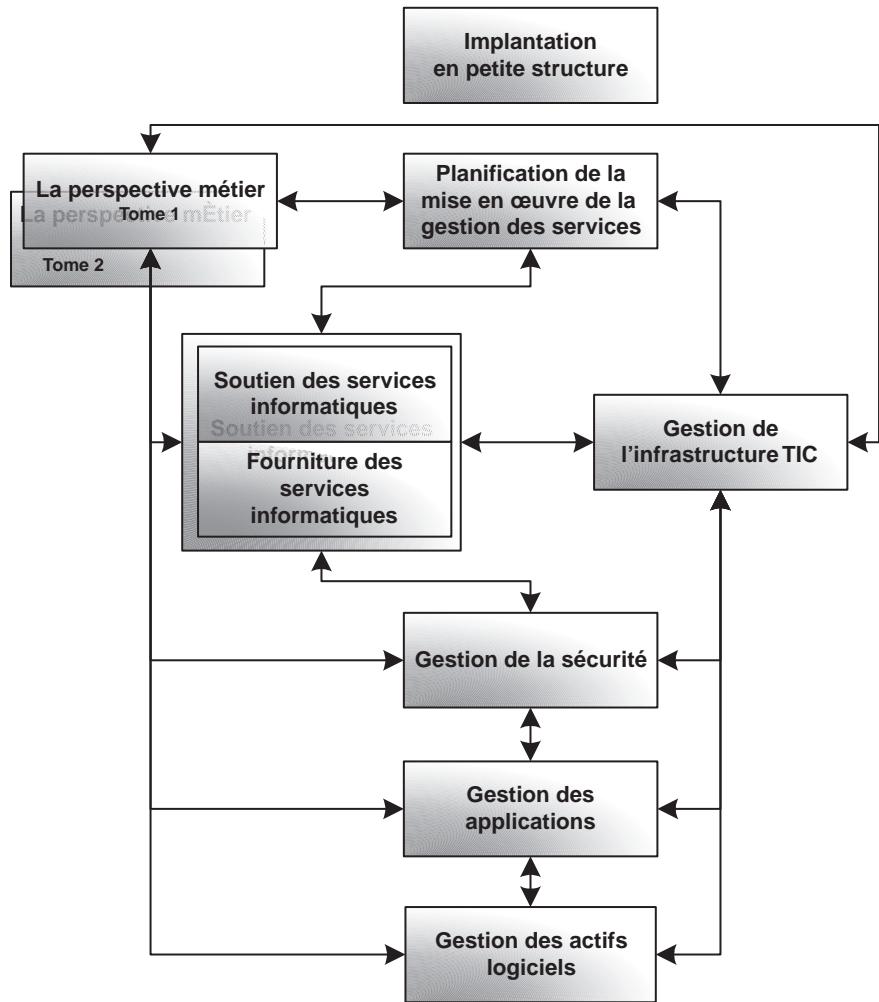


Figure 1-4 : La structure ITIL en dix livres

Comme on peut le voir sur la figure 1-4, ITIL (V2) a été développé dans une structure complète de dix modules : la perspective métier qui revient systématiquement dans les modules, la planification de la mise en œuvre, le soutien des services, la fourniture des services, la gestion des infrastructures TIC, la gestion des applications, la gestion des actifs logiciels, la gestion de la sécurité et enfin l'implantation dans les petites structures.

La perspective métier

L'approche de la fourniture des services informatiques selon une perspective métier se concentre sur les besoins de l'entreprise et de ses opérations. Cette conscience des besoins de l'entreprise permet à la gestion des services d'assurer la fourniture de services au plus près de cette demande et ainsi de maximiser la création de valeur de l'informatique.

L'objectif principal de cette approche est l'alignement de l'informatique sur les besoins de l'entreprise (voir figure 1-5). Il s'agit donc de faire comprendre au personnel informatique comment il contribue aux objectifs de l'entreprise et comment livrer ou améliorer les services informatiques afin de soutenir ces objectifs. Au-delà de ça, et grâce à cette compréhension des besoins métier, il s'agit de demander à l'équipe informatique de maximiser l'utilisation de l'outil informatique par l'entreprise et de proposer des solutions informatiques qui lui donneront un avantage concurrentiel.

Pour être efficace, cette approche suppose un certain nombre de processus destinés à aligner activité économique et informatique. Cet alignement ne s'arrête pas à l'existant, mais doit aussi prendre en compte les évolutions du système d'information et des services informatiques. Il y a donc un besoin d'alignement aux niveaux stratégique, tactique et opérationnel.

Il est particulièrement important de développer des relations saines et durables avec les clients de l'informatique et les directions métier (BRM, *Business Relationship Management*), ainsi qu'avec les fournisseurs (SRM, *Suppliers Relationship Management*).

Il est crucial que les gens travaillant dans le processus de BRM comprennent la valeur de l'informatique et son rôle dans la chaîne de valeur de l'entreprise et vérifie l'alignement entre l'activité de l'entreprise et l'informatique. Ils doivent avoir une synergie et une empathie avec les unités d'affaires et représenter les avis qui en émanent au reste de l'informatique.

Le processus de SRM doit s'assurer que les rapports avec les fournisseurs sont adaptés aux besoins de l'entreprise. Cela inclut la reconnaissance de la nécessité de disposer de différents types de fournisseurs avec un catalogue de fournisseurs, la gestion du cycle de vie des contrats, l'intégration des fournisseurs dans les processus de gestion de service et la gestion de leurs performances.

L'approche de la perspective métier doit également se concentrer sur l'amélioration de la diffusion de l'information, sur la planification, et en règle générale, la communication vers les partenaires internes ou externes et l'utilisation du catalogue de services et des SLA afin de « vendre » ces services aux directions métier.

Dans le cadre de cet ouvrage, nous aborderons plus précisément les livres du soutien et de la fourniture des services. Vous trouverez donc plus de détails sur ces modules au chapitre 2, puis dans les chapitres des parties 2 et 3. La version 3 d'ITIL reprend globalement ces processus dans le cœur du modèle.

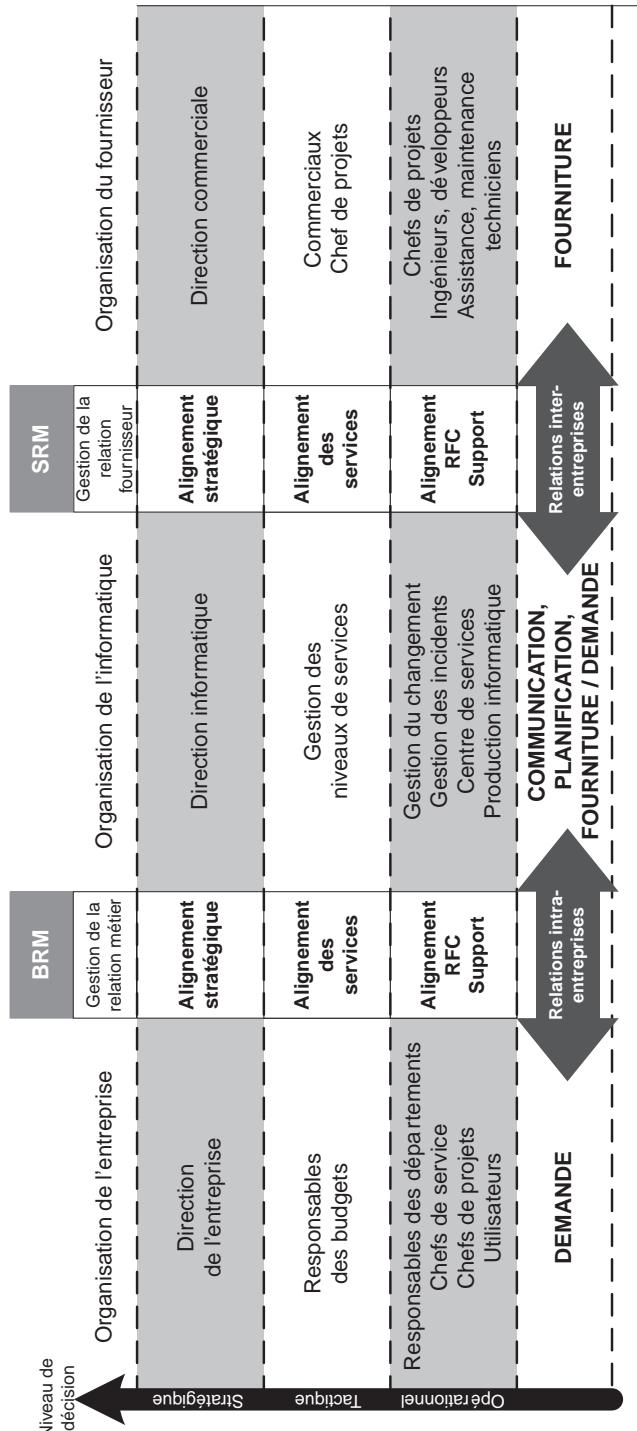


Figure 1-5 : Alignements de l'informatique sur les besoins de l'entreprise

Planification de la mise en œuvre de la gestion des services

Ce module concerne le projet d'implantation ou d'amélioration de processus ITIL dans une entreprise. Il traite un certain nombre d'aspects comme où et quand commencer, la planification du projet, la définition des processus et l'amélioration des performances, mais également les changements organisationnels et culturels que l'on doit envisager (voir figure 1-6).

La première étape est celle de la vision globale du projet de gestion des services informatiques. Elle définit les objectifs les plus stratégiques et doit être le résultat de discussions entre la direction et le service informatique.

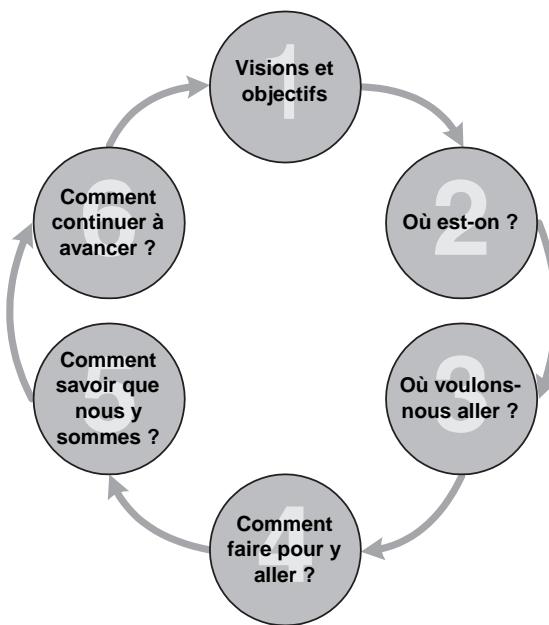


Figure 1-6 : Cycle des activités d'implantation d'ITIL

L'étape suivante consiste à déterminer la situation actuelle de l'organisation informatique en termes de maturité sur des points comme la vision, les processus, la technologie ou la culture et le personnel, et demande l'utilisation de techniques d'entretiens, de *benchmarking* et d'audit.

La troisième étape est celle au cours de laquelle la direction et le service informatique vont déterminer le rôle et les caractéristiques indispensables à la nouvelle organisation informatique.

La quatrième étape définit comment parvenir aux objectifs de la troisième étape en produisant le plan du projet d'amélioration continue des services

(CSIP) dans lequel est expliqué comment les changements vont être réalisés, où commencer et quel élément essentiel doit prendre en compte le CSIP. Les réponses à ces questions déterminent l'approche, le périmètre et le cahier des charges du projet de CSIP.

La cinquième étape consiste en l'identification et la mise en place d'un ensemble de métriques pour évaluer le progrès et la performance du CSIP. Ceux-ci doivent être régulièrement mesurés, contrôlés et passés en revue à chaque étape du projet afin d'en assurer le succès. Il est important d'inclure des mesures qui touchent directement aux avantages procurés à l'entreprise et des améliorations de la qualité de service.

La sixième étape, qui ne doit pas être la dernière, est la plus difficile à mettre en place, puisqu'il s'agit de l'étape de bouclage. En effet, dans la perspective d'amélioration continue (CSIP), il est nécessaire de revenir à la première étape afin de revoir ce qui a été réalisé, les difficultés rencontrées et comment l'améliorer.

Au cours de toutes les activités du CSIP, les messages clés sont de maintenir une vision orientée vers l'activité économique, où la priorité, l'impact et l'alignement sur le métier doivent être soulignés et re-soulignés pour assurer que toutes les améliorations comprennent des vrais avantages pour l'entreprise.

Soutien des services

Le module de soutien des services d'ITIL correspond globalement à l'interface entre les utilisateurs et l'informatique (voir figure 1-7). Il couvre les aspects en rapport avec les processus d'assistance technique quotidienne et de maintenance comme la gestion des incidents, la gestion des problèmes, la gestion des changements, la gestion des configurations et la gestion des mises en production. À cela s'ajoute la fonction de centre de services.

La gestion des configurations fournit la base de la gestion des services informatiques et soutient chaque autre processus. Le concept fondamental est la base de données de gestion des configurations (CMDB), comprenant des bases de données plus intégrées détaillant les composants d'infrastructures informatiques de toute l'organisation et d'autres actifs associés, les éléments de configuration (CI). La CMDB enregistre les détails de tous les incidents, problèmes, erreurs connus ainsi que les changements associés à chaque CI. De plus, la CMDB conserve les liens et interdépendances existant entre ces CI permettant ensuite de réaliser des analyses d'impact lors des demandes de changement ou des recherches de cause de problème.

Le centre de services fournit un point central de contact pour tous les utilisateurs informatiques dans une organisation qui traite tous les incidents, les questions et les demandes.

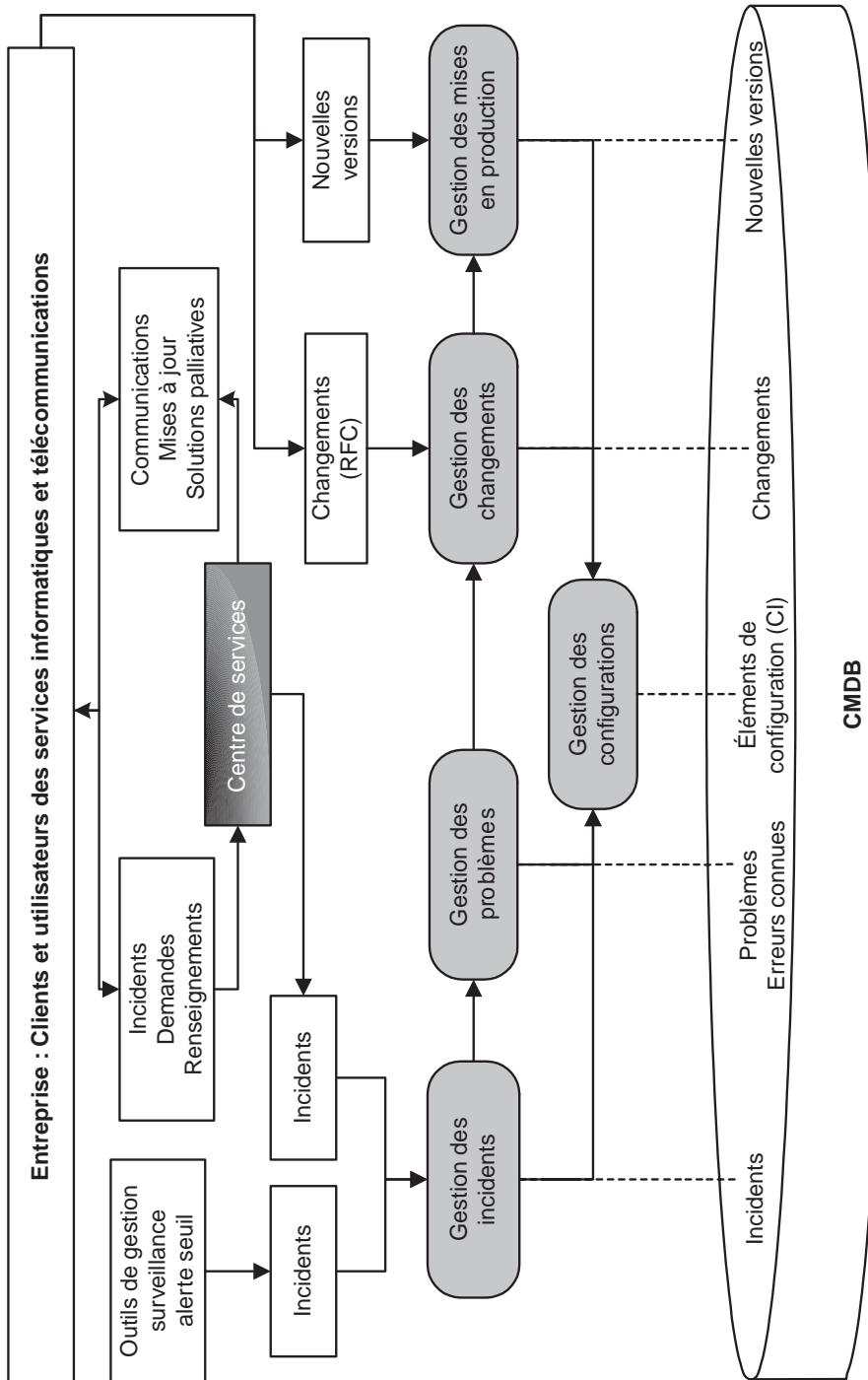


Figure 1-7 : Relations entre les processus du soutien des services

Il fournit une interface pour tous les autres processus de soutien des services et propose également une interface avec les processus de fourniture des services.

La gestion des incidents est responsable de toutes les étapes depuis la détection et l'enregistrement d'un incident jusqu'à sa résolution et sa fermeture. L'objectif est la restauration du service le plus rapidement possible avec une interruption minimale pour l'entreprise.

Le but de la gestion des problèmes est d'identifier les causes des incidents récurrents afin de réduire au minimum leur impact sur l'entreprise. Pour cela, la gestion des problèmes est un soutien pour la gestion des incidents récurrents, en identifiant les solutions palliatives et les erreurs connues quand c'est nécessaire et en proposant des solutions permanentes lorsque c'est possible. La gestion des problèmes réalise en outre une analyse proactive des tendances afin d'empêcher l'apparition de nouveaux incidents et problèmes.

L'implantation d'un processus de gestion des changements centralisé, pour le traitement efficace des changements, est vital pour toute organisation informatique. Les changements doivent être soigneusement gérés tout au long de leur cycle de vie en prenant en compte les éléments d'impact et d'urgence sur l'activité de l'entreprise.

Le processus de gestion des mises en production dispose d'une vue complète des changements apportés aux services informatiques, considérant tous les aspects d'une mise en production tant technique que non technique. La gestion des mises en production est responsable de toutes les obligations légales et contractuelles pour l'ensemble des matériels et logiciels utilisés dans l'entreprise (exemple : surveillance des licences des logiciels installés). La gestion de mise en production doit mettre en place un environnement sécurisé pour le stockage du matériel dans une zone de réserve dédiée (DHS) ainsi que pour le logiciel dans la bibliothèque logicielle (DSL).

Fourniture des services

Le module de fourniture des services d'ITIL correspond globalement à l'interface entre les clients et l'informatique (voir figure 1-8). Il couvre les aspects prévisionnels à plus long terme de fourniture des services et correspond aux processus de gestion des niveaux de service, de gestion financière des services informatiques, de gestion de la capacité, de gestion de la continuité de service informatique et de gestion de la disponibilité. Ces processus sont principalement concernés par le développement de plans d'amélioration de la qualité des services informatiques livrés.

Le processus de gestion des niveaux de service (SLM) négocie, documente, autorise et passe en revue les besoins métier. Il conduit à un document formel d'expression des besoins de niveau de service (SLR) qui représente un cahier des charges. Ce document donne lieu à un accord lui-même formalisé

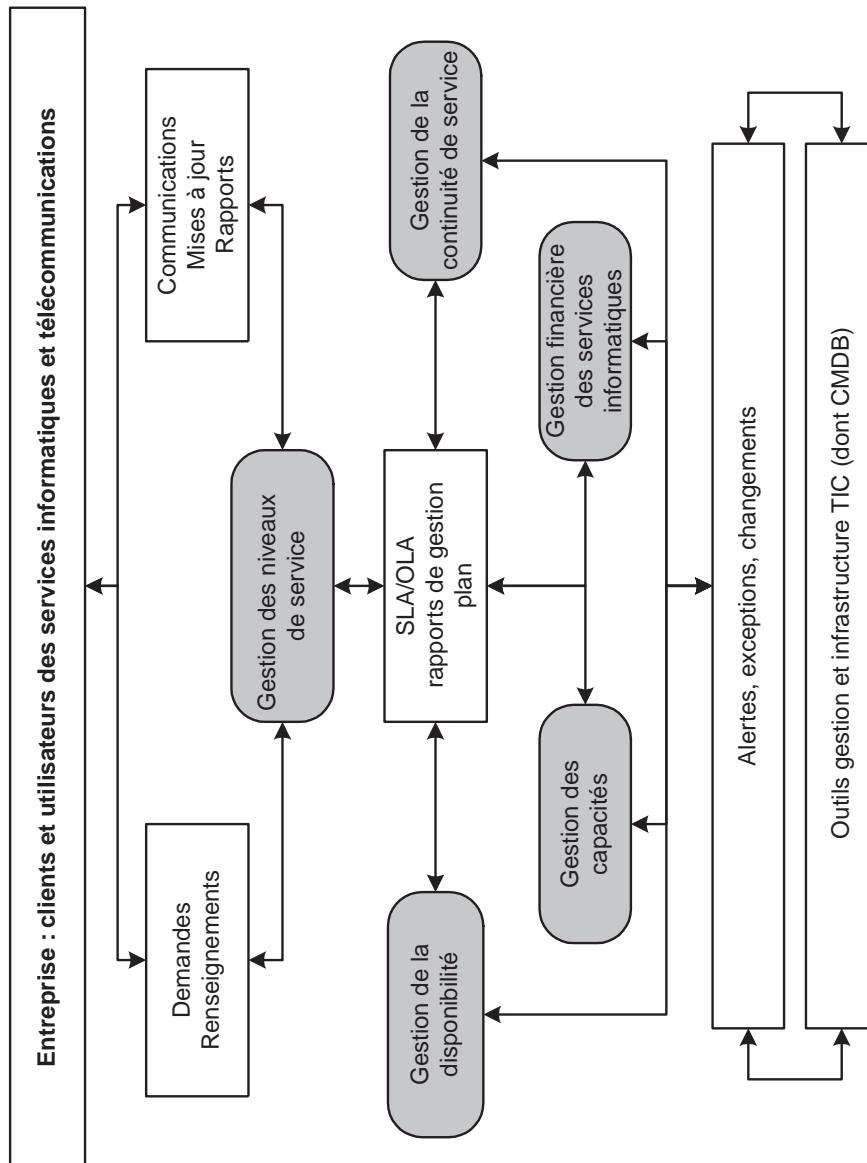


Figure 1-8 . Relations entre les processus de fourniture des services

au sein d'un autre document de niveaux de service (SLA) dans lequel sont stipulés les types de mesure, de rapport et de revue de processus qui seront réalisés afin de valider la qualité de service proposée par le service informatique à l'entreprise. Il existe également un document dans lequel est négociée la dimension technique du SLA. Cet accord de niveau opérationnel (OLA) permet d'aligner les équipes internes dans la réponse aux besoins métier et formalise les accords de service négociés avec les fournisseurs externes.

Les autres rôles principaux du processus de SLM sont la production et la maintenance du catalogue de service qui fournit l'information essentielle sur le portefeuille complet des services informatiques proposés puis le développement, la coordination et la gestion du programme d'amélioration de service (SIP) ou le programme d'amélioration de service continu (CSIP), qui est le plan complet pour l'amélioration continue de la qualité de services informatiques orientés vers l'activité économique.

La gestion financière des services informatiques fournit la base pour gérer l'organisation informatique interne, comme une entreprise dans l'entreprise, et pour développer une organisation consciente des coûts financièrement efficace. Les principales activités sont de comprendre et de comptabiliser les dépenses de mise à disposition de chaque service informatique et la prévision du budget informatique.

La dernière mission est optionnelle mais très utile : elle correspond à la mise en œuvre d'une stratégie de facturation des utilisateurs/clients afin de financer les dépenses engagées.

Le processus de gestion de la capacité assure que la capacité adéquate est disponible à tout moment pour remplir les exigences de l'entreprise en équilibrant la demande de l'activité économique et de la fourniture informatique. Pour réaliser cela, un plan de capacité étroitement lié à la stratégie de l'entreprise est produit et passé en revue régulièrement. Ceci couvre trois zones qui correspondent à la gestion de la capacité du *business* (BCM), du service (SCM) et de la ressource (RCM) qui comprennent les activités nécessaires pour s'assurer que la capacité informatique et le plan de capacité sont conformes aux besoins de l'entreprise. Les activités communes utilisées dans ces secteurs sont la gestion de performance, la gestion de charge, la gestion, la modélisation et le dimensionnement de la demande en capacité.

La gestion de la continuité de service informatique produit des plans de rétablissement conçus pour assurer un niveau de service minimal requis par l'entreprise pour continuer son activité après un incident majeur. L'objectif principal est de réduire l'impact et la durée d'interruption de processus métier essentiels à l'entreprise durant un incident majeur. La continuité de service informatique est un composant du plan de reprise d'activité (PRA) au niveau de l'entreprise ou *Business Continuity Plan* (BCP) qu'il convient de réévaluer régulièrement afin de coller aux évolutions de l'entreprise.

La disponibilité d'un système est un aspect clé de la qualité de service. La gestion de la disponibilité doit s'assurer que la disponibilité de chaque service, matériel ou logiciel correspond aux besoins exprimés par l'entreprise et soit améliorée régulièrement. Pour cela, la gestion de la disponibilité contrôle, mesure, produit des rapports et passe en revue un ensemble de métriques pour chaque service et composant, qui inclut la disponibilité, la fiabilité, l'aptitude à la réparation, le niveau d'assistance et la sécurité.

Gestion des infrastructures TIC

La gestion des infrastructures des technologies de l'information et des communications (TIC) couvre cinq grands processus sur l'ensemble de l'infrastructure technique de l'entreprise que sont la gestion complète et l'administration, la conception et la planification, le soutien technique, le déploiement et la gestion des opérations.

Comme on peut le voir sur la figure 1-9, la gestion de l'infrastructure TIC est responsable de chacune des étapes du cycle de vie de l'infrastructure, depuis l'expression des besoins dans le cahier des charges, jusqu'au moment où l'équipement est retiré du système pour obsolescence, le tout en passant par la conception, l'étude de faisabilité, le développement, l'installation, les tests, le déploiement, le fonctionnement et l'optimisation.

Le responsable de la gestion d'infrastructure joue un rôle important dans la coordination des évolutions du système en participant au processus de gestion des changements, aux revues d'audit qualité ainsi qu'aux cellules de gestion de crises. Il doit également s'assurer que les processus d'assistance technique sont en place pour que tous les autres secteurs informatiques puissent fonctionner efficacement, ce qui exige donc un engagement fort dans les autres processus ITIL.

- Le processus « Gestion et administration » doit s'attacher à créer l'environnement efficace et sécurisé le plus approprié pour héberger les services informatiques actuels et futurs qui permettront à l'entreprise d'atteindre ses objectifs.
- Le processus « Conception et planification » de l'infrastructure doit se faire en concertation avec la direction de l'entreprise et les directions métier afin de disposer d'informations sur la stratégie, l'évolution des activités et les projets à court, moyen et long terme.
- Le processus « Soutien technique » assure que l'assistance, les compétences et la connaissance nécessaire sont disponibles pour soutenir les services fournis par l'infrastructure TIC. Un groupe d'expertise technique est maintenu afin de fournir, d'une part les conseils et les ressources nécessaires à la recherche et au développement de nouvelles solutions techniques, et d'autre part, le troisième niveau de soutien technique pour tous les autres secteurs.

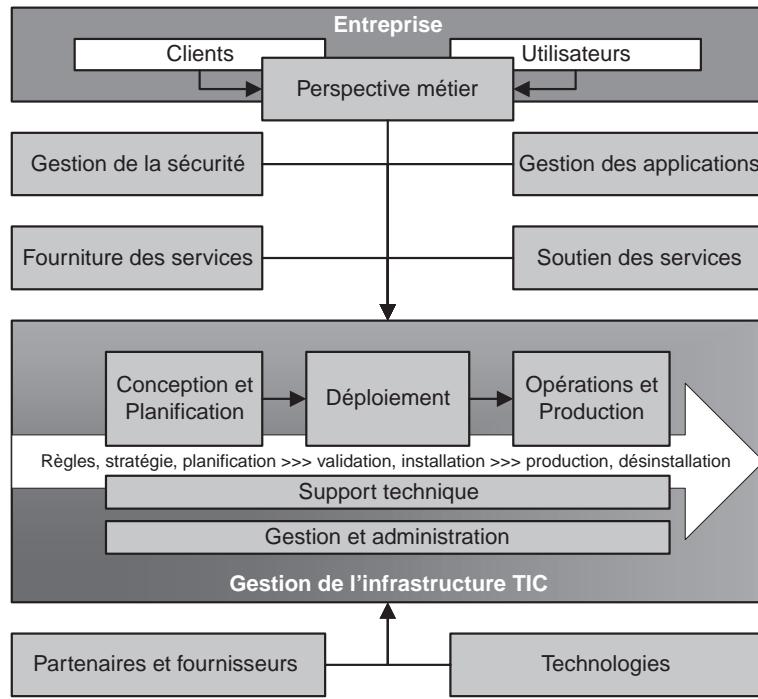


Figure 1-9 : Activités de la gestion de l'infrastructure TIC

- Le processus « Déploiement » est en charge de l'installation des solutions informatiques, qu'elles soient nouvelles ou issues de l'évolution des besoins, tout en respectant les exigences de qualité, de coût et de délai. Le déploiement implique principalement l'utilisation de méthodes de projet pour assurer que ces nouvelles solutions TIC soient livrées avec les moins de désagréments et de ruptures pour l'entreprise.
- Le processus « Gestion des opérations » doit s'assurer que les services et les composants répondent aux attentes opérationnelles des clients, comme convenu dans les engagements de niveaux de services (SLA/OLA). La « Gestion des opérations » est aussi responsable du réglage et de l'optimisation de tous les éléments de l'infrastructure TIC.

Gestion des applications

La gestion des applications est destinée à rapprocher les phases des projets de développement de la gestion des services informatiques afin que le cycle de vie de l'application prenne en compte des éléments tels que la disponibilité, la fiabilité, l'aptitude à la réparation, la performance et la facilité de gestion (voir figure 1-10).

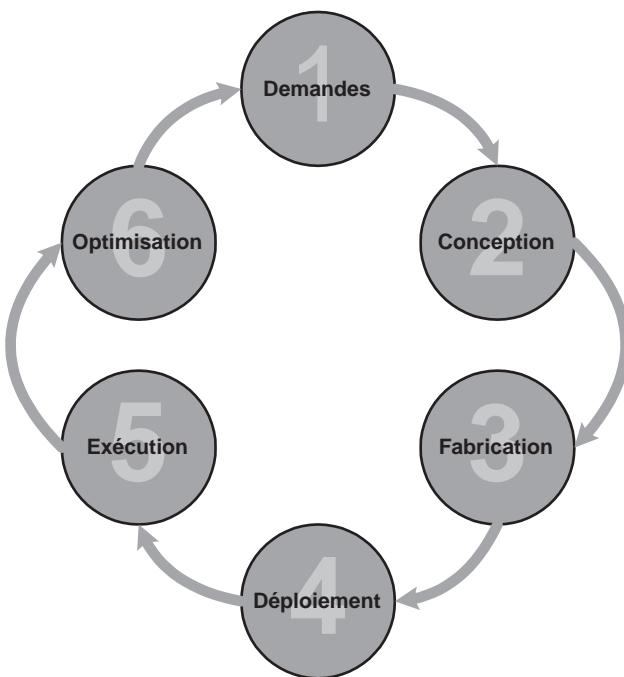


Figure 1-10 : Cycle de vie des applications

Le résultat de ce processus est un meilleur alignement de l'application avec les objectifs de l'entreprise en termes d'exploitation, et une amélioration de sa documentation.

L'accent doit être mis sur l'importance de traiter ces questions le plus tôt possible dans le cycle de vie du projet puisqu'elles peuvent avoir un impact important sur l'efficacité de la fourniture et du soutien du service.

Pour chaque phase du cycle de vie de l'application, une liste de contrôle doit être développée pour s'assurer que tous les aspects de la gestion de service soient pris en compte.

Gestion des actifs logiciels

La gestion des actifs logiciels s'occupe plus particulièrement des questions liées à l'utilisation des logiciels au sein de l'entreprise. Ce module représente l'infrastructure et les processus nécessaires à la gestion efficace, au contrôle et à la protection des actifs logiciels dans l'entreprise durant toutes les étapes de leur cycle de vie (voir figure 1-11).

L'objectif du processus de gestion principal est d'établir la politique de l'entreprise concernant les actifs logiciels, les besoins en formation, ainsi

que la gestion des risques résultant de l'utilisation de ces logiciels. Néanmoins, il sert globalement à préparer l'action des quatre autres processus.

- Le premier d'entre eux est le processus de gestion des actifs qui est chargé d'identifier et de maintenir les informations (comptables et financières, numéro de série, numéro de version, etc.) pendant leur cycle de vie.
- Le second processus est dédié aux actions logistiques et doit contrôler toutes les activités affectant la mise en place du logiciel pendant son cycle de vie (cahier des charges, évaluation, achat ou développement, déploiement, etc.).
- Le troisième processus concerne la vérification de la conformité du logiciel à la politique de l'entreprise. Il s'agit là de détecter et de gérer toutes les exceptions aux règles, aux procédures et aux licences des logiciels (exemple : utilisation d'une copie illicite de logiciel sur un poste de travail).
- Le quatrième et dernier processus s'occupe des relations avec les partenaires internes ou externes et réalise les rapports associés (exemple : contrat de maintenance).

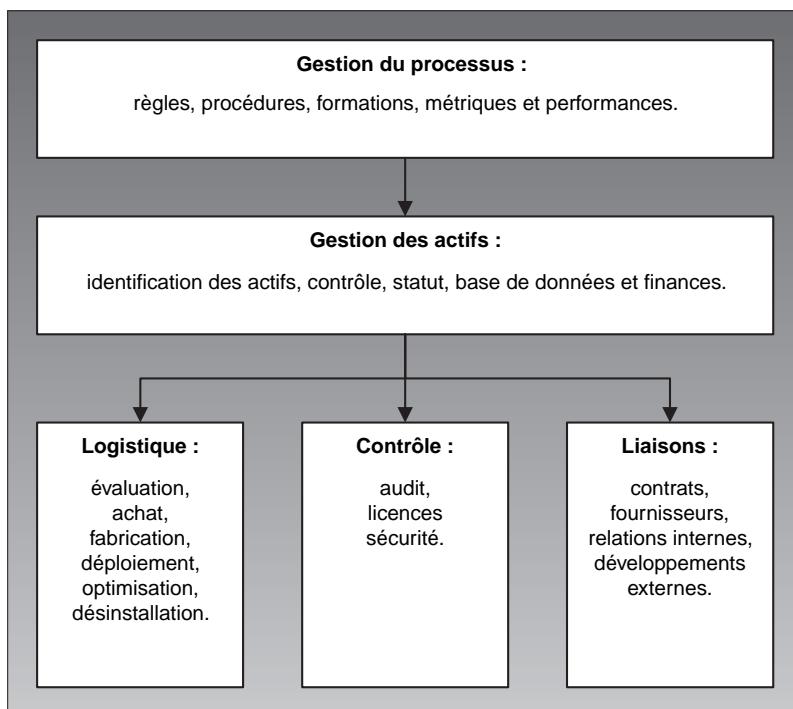


Figure 1-11 : Activités de la gestion des actifs logiciels

Gestion de la sécurité

La gestion de la sécurité informatique est le processus permettant de gérer un niveau défini de sécurité des services informatiques, de l'infrastructure et de l'information qui y transite. Ce processus prend en compte les évolutions des besoins métier inhérentes aux marchés ou à la législation, les modifications du système d'information et des éléments d'architecture informatique, mais également l'évolution des menaces dans une démarche cyclique d'amélioration du processus (voir figure 1-12).

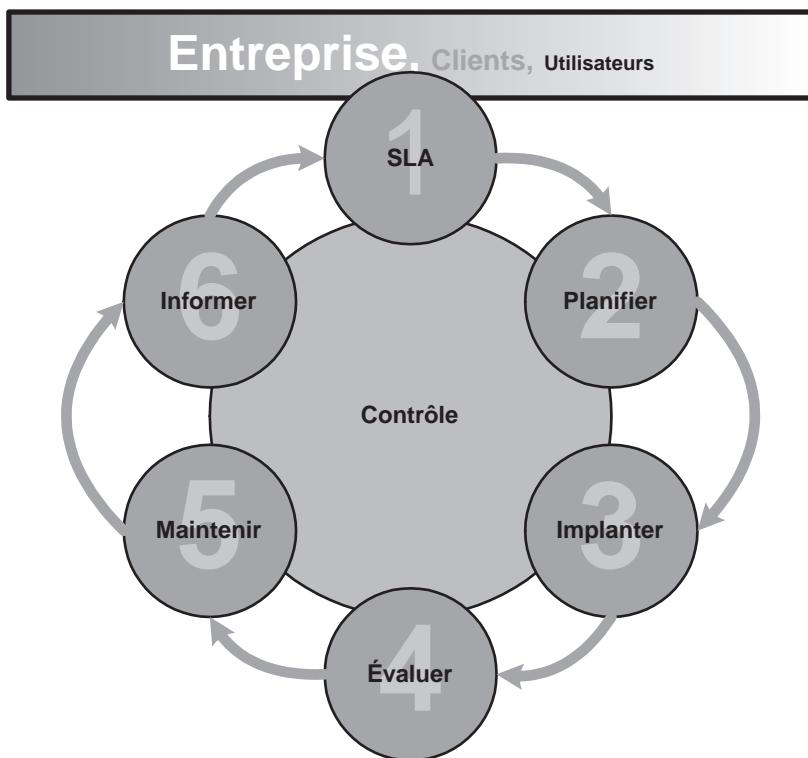


Figure 1-12 : Cycle de gestion et d'amélioration de la politique de sécurité

Des audits doivent démontrer l'adéquation des contrôles de sécurité et des mesures prises pour pallier les éventuels problèmes ou alertes. Par la suite, le processus doit produire les rapports permettant d'illustrer les résultats de ces actions.

La gestion de sécurité informatique est partie prenante dans la plupart des processus de la gestion de service et doit être prise en compte par l'ensemble

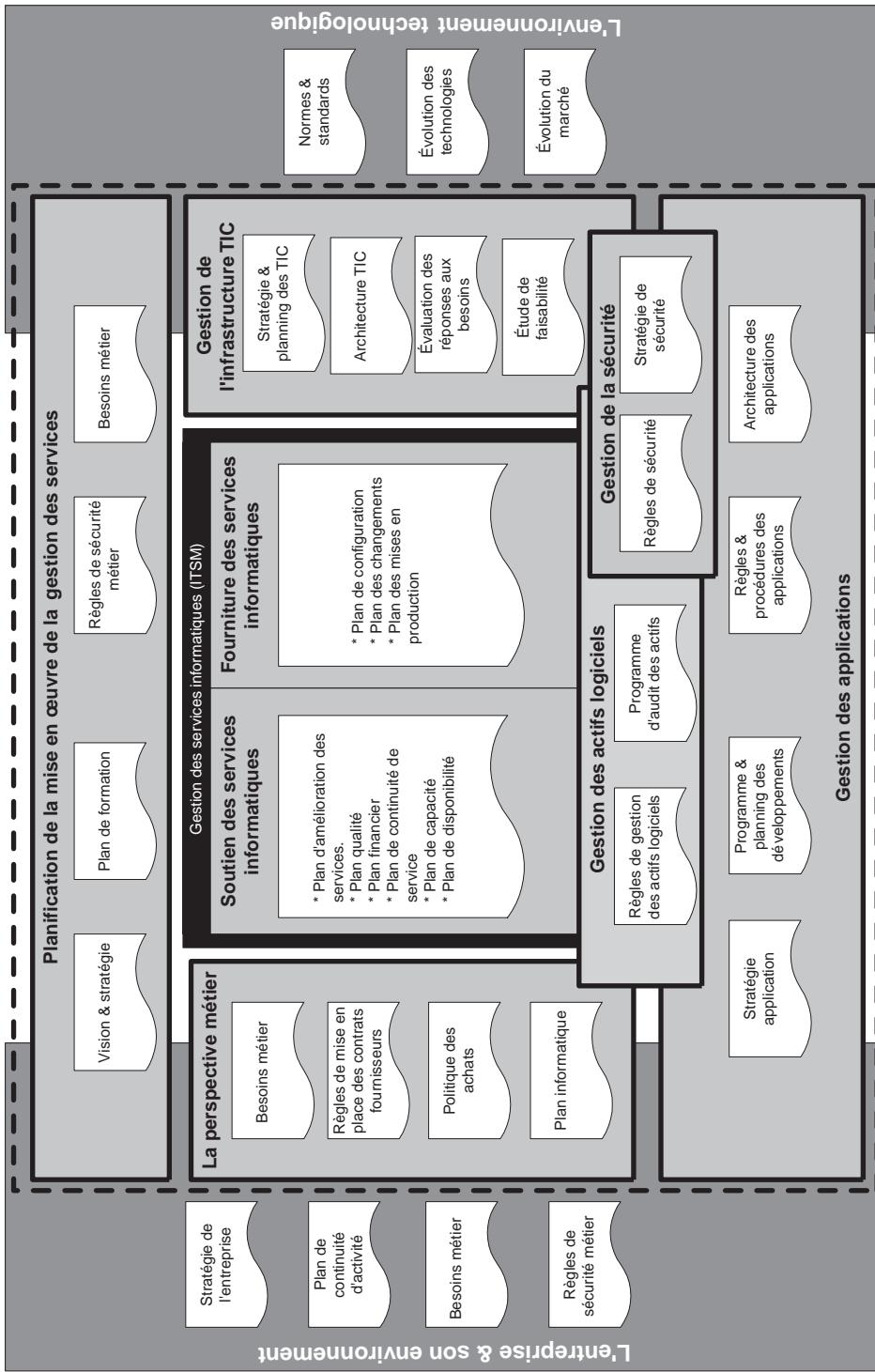


Figure 1-13 : La structure d'ITIL V2, ses principaux documents et rapports

des responsables de processus afin de réduire à un niveau acceptable les éventualités d'un incident de sécurité. C'est le processus d'évaluation de risque.

La direction générale de l'entreprise est responsable devant les clients et les actionnaires de la sécurité et doit définir la politique de sécurité de l'entreprise. Celle-ci s'impose au processus de gestion de la sécurité.

L'existence de cette politique illustre et renforce la décision de l'entreprise d'investir dans la sécurité informatique, envoyant un message rassurant aux investisseurs et aux partenaires. Elle fournit aux responsables les directives à suivre dans les divers aspects de l'organisation et indique par un message fort à l'attention des salariés de l'entreprise ce qui est permis et ce qui ne l'est pas dans l'utilisation de systèmes TIC et des données.

La politique de sécurité de l'entreprise doit ensuite être largement diffusée au sein de l'organisation, en étant éventuellement annexée au contrat de travail de chacun, puis mise en application et soumise à des révisions périodiques.

Les éléments de base de ce processus sont d'une part l'évaluation du risque et des vulnérabilités et d'autre part la gestion et la mise en œuvre des solutions permettant de maintenir la vulnérabilité et les risques en deçà du niveau exprimé par les directions métier et à un coût justifiable.

Ces activités doivent être étroitement coordonnées avec l'aide de tous les autres secteurs de la gestion de service, et en particulier la gestion de la disponibilité et la gestion de la continuité de service.

Ceci est particulièrement important en France, où le dirigeant de l'entreprise est pénalement responsable des carences en sécurité de l'entreprise.

Implantation dans les petites structures

Ce module a été écrit pour les petites et moyennes entreprises qui étudient la gestion de leurs services informatiques et qui souhaitent adopter ITIL pour les aider dans cette démarche. Les recommandations ITIL sont également applicables aux petites organisations, même si les méthodes d'implantation divergent de celle d'une grande multinationale et en particulier en adoptant une approche très pragmatique.

La structure ITIL V3

Pourquoi cette nouvelle version ?

La dernière mise à jour d'ITIL date de l'année 2000 (version 2). L'objectif principal de la troisième version (V3) est que le référentiel de meilleures pratiques suive les évolutions du marché des technologies. Un autre objectif était que les recommandations du référentiel soient plus applicables et utiles en prenant en compte les évolutions des besoins dans les services et leurs complexités grandissantes. Ce besoin est très lié à un mouvement

actuel du marché très orienté vers l'externalisation des services et leur corollaire de relation client/fournisseur. Enfin, un troisième objectif était qu'ITIL soit plus facilement utilisable et utilisé dans les petites structures. Un guide dédié à cette question est disponible dans la version 2, il est reconduit dans les guides complémentaires de la version 3.

Les consultations de l'OGC et de l'itSMF ont obtenu plus de 530 dossiers de réponse écrits et plus de 6 000 commentaires électroniques. Ces réponses représentent 80 % des pays dans lesquels se trouve un chapitre itSMF.

Les principales demandes de changements portaient sur :

1. Fournir une structure cohérente et une navigation au travers de l'ensemble du référentiel.
2. Préserver les recommandations des livres du soutien et de la fourniture des services, et améliorer leurs concepts fondamentaux.
3. Ajouter de meilleures pratiques qui étendent les concepts de gestion des services dans une vue plus orientée métier et prenant en compte les cycles de vie de l'entreprise.
4. Prendre en compte les aspects structurels et culturels des organisations et créer des interfaces avec les autres modèles, normes et standard de gestion des technologies de l'information (ex : COBIT, CMMI, ISO, ...).
5. Proposer une stratégie de gestion des connaissances qui permettent de soutenir les besoins métier de la gestion des services.
6. Démontrer et illustrer la valeur, les bénéfices et le retour sur investissement de l'implantation d'ITIL.
7. Refléter la réalité de l'entreprise d'aujourd'hui et en particulier concernant son environnement technique et opérationnel.

Ce qui ne change pas !

Dans cette nouvelle version, on retrouve avec bonheur ce qui a fait le succès des deux versions précédentes... le bon sens ! En effet, les meilleures pratiques identifiées ou élaborées en vingt ans de travail ne vont pas disparaître sous prétexte qu'une nouvelle version du référentiel doit voir le jour. Ceci permet d'ailleurs de confirmer aux utilisateurs d'ITIL que leur investissement ne sera pas perdu. Tout ce que vous avez appris et utilisé dans la version 2 sera utilisable dans cette nouvelle version...

Tout ceci implique un autre point particulièrement important. Les certifications ITIL obtenues en utilisant la version 2 resteront valables après le passage à la version 3. Étant entendu que ces examens ne portent que sur les deux livres du soutien et de la fourniture des services, comme ceux-ci sont largement reconduits dans le nouveau référentiel, toute personne qui a bien intégré les concepts exposés les comprendra immédiatement dans la nouvelle version.

Alors... qu'est-ce qui change ?

Cette version d'ITIL se présente comme une évolution majeure par rapport à la V2. De nombreuses études ont révélé qu'un des freins à l'adoption d'ITIL par les entreprises était l'absence de pénétration du référentiel auprès des décideurs autres qu'informatiques. L'accent de la V3 a donc été mis sur ce public afin d'améliorer l'adoption d'ITIL par les dirigeants. Ainsi, les avantages d'ITIL sont présentés à l'aide d'un vocabulaire métier, afin de familiariser les dirigeants et les responsables métier à ce référentiel. Dès lors, il est plus facile de voir comment ITIL s'intègre dans le cycle de vie de chaque organisation.

Une des améliorations clés de la V3 est l'introduction d'un système de gestion des connaissances des services. Le SMKS (*Service Management Knowledge System*) incorpore les anciennes bases de connaissances qui nous sont familières comme la base des erreurs connues et la CMDB, mais propose d'être beaucoup plus large dans sa portée.

Orientation métier

Pour illustrer cette démarche, la V3 propose des études de cas concrètes, qui mettent en avant le retour sur investissement (ROI), des métriques et les compétences clés. Le but avoué est clairement que les dirigeants prennent conscience de la valeur et du sens d'ITIL comme outil d'alignement et de changement.

Pour ces promoteurs, ITIL V3 reflète mieux le cycle de vie des services informatiques qui va de leur conception à leur retrait lorsqu'ils deviennent obsolètes. En outre, cette version identifie plus précisément les rôles de ceux qui contribuent à la décision, au développement et à la fourniture des services et reconnaît que ces actions se déroulent dans différentes entités de l'entreprise et sur plusieurs niveaux hiérarchiques et organisationnels.

Une synthèse

Un effort important a également été concédé à la réécriture et à la synthèse des livres de la V2. Certains concepts, méthodes et techniques se trouvaient parfois de façon redondante dans les différents volumes. Bien qu'une grande partie du référentiel précédent soit conservée, et en particulier les deux livres du soutien et de la fourniture des services, l'ensemble des dix livres disparaît au profit d'un nombre inférieur d'ouvrages plus synthétiques. Le cœur du modèle se compose désormais de cinq grandes parties, appelées « titres de cycle de vie » (*lifecycle titles*) :

- stratégies des services ;
- conception des services ;
- transition des services ;
- opérations des services ;
- amélioration continue des services.

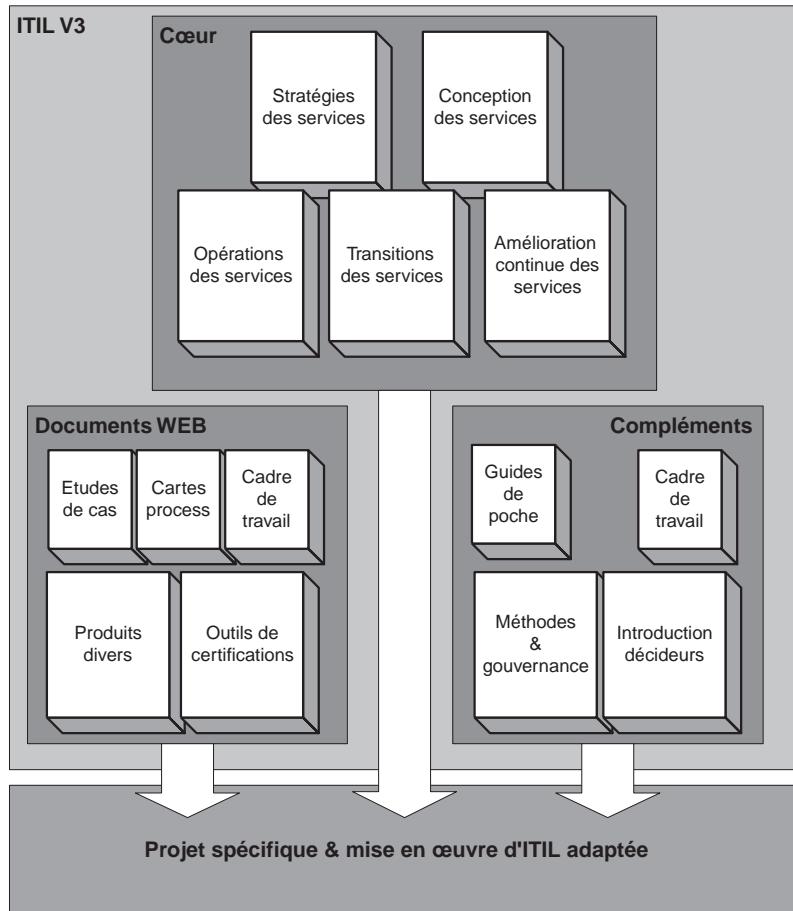


Figure 1-14 : Le modèle documentaire de la version 3 d'ITIL

Comme on peut le voir sur la figure 1-14, la version 3 d'ITIL est scindée en trois grandes parties. La première correspond au cœur avec ses cinq livres. La seconde partie (Compléments) propose un ensemble de documents, étude de cas, méthodes et guides complémentaires spécifiques à chaque sujet. La troisième et dernière partie du référentiel correspond à un ensemble de documents situés sur un serveur web et qui n'est accessible qu'après souscription au contrat « ITIL online » de l'OGC.

Le cycle de vie

Pour répondre à ces constats, l'organisation de la version 3 repose sur le concept de cycle de vie des services.

Subtilité du vocabulaire

Les termes utilisés dans cette nouvelle version sont également révélateurs du changement d'orientation d'ITIL et en particulier vers les métiers.

Si la V2 d'ITIL préconise l'alignement des services informatiques sur le métier de l'entreprise, la V3 préfère la notion d'intégration entre le métier et l'informatique. Au premier abord, ceci tient plus à une subtilité marketing qu'autre chose, mais il n'en est rien. En effet, dans le premier cas, le service informatique s'aligne sur le besoin. L'effort est donc situé du coté technique. En revanche, dans le second cas, l'intégration entre le métier et l'informatique implique une réflexion plus poussée sur ce que l'informatique peut apporter au métier. Ici, les deux parties doivent travailler conjointement.

Un autre point traité par cette nouvelle version aborde la création de valeur dans l'entreprise. Si la V2 utilise l'image de la chaîne de valeur, la version suivante préfère la notion d'innovation du réseau de valeur. Encore une fois, cette finesse dans les termes est volontaire. Alors que la V2 envisage la chaîne de valeur, c'est-à-dire un ensemble de processus linéaires, la V3 reconnaît que la réalité est plus complexe et que la création de valeur prend souvent plus de deux dimensions, les entrées/sorties se faisant au sein d'un réseau complexe d'acteurs liés entre eux par un intérêt commun : le fonctionnement de l'entreprise.

Enfin, la V2 propose un catalogue de services linéaires alors que la V3 avance un portefeuille de services dynamiques. On le retrouve d'ailleurs dans le fait que la V2 repose sur un ensemble de processus intégrés et relativement statiques alors que la V3 insiste sur le concept de gestion globale des services par les cycles de vie.

Le changement dans la continuité

Après la simplification du processus de *refresh* mené pendant deux ans par l'OGC, la nouvelle version d'ITIL se compose désormais des cinq *Lifecycle titles*. Ces volumes partagent une structure commune et cohérente :

- Introduction.
 - Vue d'ensemble
 - Contexte
 - But
 - Utilisation
- Principes des meilleures pratiques.
- Initiation aux processus.
- Méthodes, pratiques et outils.
- Implantation des services et stratégie de gestion de services.
- Mesure et contrôle (maîtrise).
- Les défis, les facteurs de succès et les risques.

ITIL V3					
	Stratégies des services	Conception des services	Transition des services	Opérations des services	Amélioration continue
	70 %	40 %	40 %	30 %	70 %
Perspective métier	40 %	X	X	X	
Planification de la mise en œuvre	60 %	X	X	X	X
Soutien des services	70 %	X	X	X	X
Fourniture des services	70 %	X	X	X	X
Gestion de la sécurité	20 %	X	X	X	X
Gestion des infrastructures	40 %	X	X	X	
Gestion des applications	40 %	X	X	X	
Gestion des actifs logiciels	30 %	X	X	X	
Implantation PME	80 %	X	X	X	

Figure 1-15 : Équivalences entre la version 2 et la version 3 d'ITIL

- Résumé.
- Annexes.

En outre, ces livres se caractérisent par leurs interactions et leurs relations. Ayant conservé une grande part de l'existant ITIL (V1 & V2) le contenu est en continuité avec ces versions précédentes. Comme on peut le voir dans le tableau de la figure 1-15, une grande part des précédentes versions est réutilisable. En revanche, il sera nécessaire de s'approprier les nouvelles dénominations et la nouvelle organisation du référentiel de gestion des services informatiques.

Le cœur du modèle V3

La nouvelle version d'ITIL reflète plus fidèlement la vie des services informatiques et en particulier dans leur complexité. Il n'est pas rare que la production d'un même service à destination des clients et utilisateurs fasse appel à plusieurs profils totalement différents entre les étapes de conception, de planification et de mise en œuvre. Le référentiel fait donc appel à un large spectre de personnes qui occupent des rôles aux différentes étapes. Comme le but avoué est désormais d'initier les directions métier au référentiel ITIL, les promoteurs de cette nouvelle version suggèrent fortement que chacun ait lu le cœur des documentations. La rédaction dans un langage plus proche des métiers va certainement favoriser cette approche. Cela implique que chacun des cinq livres s'adresse à un public varié et parfois différent tel que les représentants du service informatique ou les acteurs métier des autres directions.

Stratégies des services

Le premier volume de la version 3 se nomme « Stratégies des services ». Ce livre est destiné à ceux qui ont besoin de comprendre l'analyse stratégique, la planification, la position et la mise en œuvre en ce qui concerne les modèles de service et les objectifs stratégiques.

Il permet de vérifier que chaque étape du cycle de vie d'un système d'information est parfaitement en adéquation avec les compétences métier dont une entreprise a besoin.

Ce livre fournit des conseils sur la façon de démultiplier les capacités de gestion de service qui peuvent efficacement livrer la valeur aux clients mais également créer la valeur en interne. Les conseils proposés concernent les modèles d'organisation, les portefeuilles de service, le développement de leurs capacités et l'efficacité opérationnelle. Enfin, une large part est donnée à la gestion de la connaissance qui fait enfin son apparition formelle dans le référentiel ITIL.

Les autres livres qui composent le cœur de cette troisième version s'appuient sur lui pour fournir et soutenir les services, conformément aux besoins métier ainsi qu'aux principes de la gestion des services décrits.

La cible principale de ce livre est plutôt orientée vers le responsable de division, en particulier le DSI. Mais il peut ou doit également être lu par les directeurs des autres divisions (direction commerciale, direction financière, direction marketing...). Ces interlocuteurs sont en général les responsables de service (*service manager*) et les responsables opérationnels.

Les concepts et les conseils contenus dans cet ouvrage portent sur :

- l'écosystème de l'entreprise ;
- la planification de la stratégie et de la valeur de la gestion des services ;
- comment lier la stratégie métier et la stratégie informatique ;
- la planification et la mise en œuvre des stratégies de service ;
- les rôles et responsabilités ;
- les défis, les facteurs de succès et les risques.

Conception des services

Ce deuxième livre s'intitule « Conception des services » (*service design*). Il propose des conseils pour la production et la maintenance de la politique, de l'architecture et des documentations informatiques. Ceux-ci seront utilisés lors de la conception de processus et d'infrastructures informatiques innovants, adaptés aux exigences présentes et futures du métier.

Ce livre traduit les plans stratégiques et les objectifs élaborés à l'aide du livre précédent en règle de conception et en spécifications des services et des opérations. Il fait appel à ceux dont le rôle est de faire travailler l'infrastructure, les applications et les systèmes au sein d'un même outil d'entreprise. Il permet également la mise en place des processus avec l'aide des partenaires et des fournisseurs afin d'offrir une offre de service de grande qualité.

La cible principale de ce livre est plutôt orientée vers le responsable de service (*service manager*). Les interlocuteurs sont en général les membres de l'équipe informatique, les « propriétaires » de services et les fournisseurs de services (externes).

Les concepts et les conseils contenus dans cet ouvrage couvrent :

- le cycle de vie des services ;
- les objectifs de la conception de services ;
- les éléments de la conception de services ;
- comment choisir un modèle de conception de service ;
- les services, les acteurs, les processus, les connaissances, les outils ;
- les rôles et responsabilités ;
- la modélisation du coût ;
- les bénéfices et l'analyse des risques ;
- l'implantation de la conception des services ;
- surveillance, mesures et maîtrise ;
- les défis, les facteurs de succès et les risques.

.C'est dans ce livre que l'on retrouve l'essentiel du livre « Fourniture des services » de la version 2.

Transition des services

Le troisième livre s'intitule « Transition des services » (*Service Transition*). Il adopte une vision plus large et à long terme de la gestion des changements et la gestion des mises en production. Ce point de vue met l'accent sur les risques, les bénéfices, les processus de fourniture et de suivi lors de l'évolution des services.

Ce livre s'assure que le service conçu précédemment respecte les décisions stratégiques décidées avant sa mise en œuvre et que le service proposé peut être produit et maintenu efficacement.

Ce livre présente également des conseils et les activités nécessaires à l'évolution des services dans l'environnement de l'entreprise.

La cible principale de ce livre est plutôt orientée vers les responsables de services informatiques, les propriétaires des services et l'équipe de production de ces services. Les interlocuteurs principaux sont les clients, les utilisateurs finaux et l'équipe d'assistance.

Les concepts et les conseils contenus dans cet ouvrage portent sur :

- la gestion des changements organisationnels et culturels ;
- la gestion de la connaissance ;
- les systèmes de gestion des connaissances des services ;
- la gestion et l'analyse des risques ;
- les phases du cycle de vie ;
- les principes de la transition de service ;
- les méthodes, pratiques et outils ;
- surveillance, mesures et maîtrise ;
- les défis, les facteurs de succès et les risques ;
- un guide des meilleures pratiques.

Une partie du livre « Soutien des services » de la version 2 se retrouve dans ce volume, en particulier la gestion du changement et les mises en production, ainsi qu'une partie de la gestion des configurations.

Opérations des services

Le quatrième titre s'appelle « Opérations des services » (*Service Operations*). Il met l'accent sur les activités quotidiennes de fourniture (production informatique) et de contrôle pour proposer et mettre en œuvre un niveau stable et satisfaisant de service.

La cible principale de ce livre est plutôt orientée vers les propriétaires des services, l'équipe de production et les éventuels fournisseurs de service externe et les sous-traitants. Les interlocuteurs principaux sont les clients, les utilisateurs finaux et la direction de la DSI.

Les concepts et les conseils de ce livre portent sur :

- les phases du cycle de vie de mise en œuvre des services ;
- les principes des mises en œuvre des services ;

L'autre partie du livre « Soutien des services » de la version 2 se retrouve dans ce volume, en particulier la gestion des incidents et des problèmes.

- les fondements des processus ;
- les fonctions ;
- la gestion des applications ;
- la gestion de l'infrastructure ;
- la gestion des opérations ;
- les fonctions et les processus de contrôle ;
- les pratiques évolutives ;
- surveillance, mesures et maîtrise ;
- les défis, les facteurs de succès et les risques.

Amélioration continue des services

Fidèle aux principes de Deming depuis ses débuts, ITIL préconise l'utilisation des itérations successives pour obtenir une amélioration continue des services (PDCA). La V3 ne déroge pas à la règle, et le dernier livre, « Amélioration continue des services » (*Continual Service Improvement*) y est entièrement consacré.

Ce livre s'assure qu'un service fournit le maximum de bénéfices à ses clients et mesure ses performances puis propose des améliorations durant son cycle de vie.

La cible principale de ce livre est plutôt orientée vers les concepteurs et les planificateurs des services, les responsables informatiques et responsables métier, l'équipe de production et les éventuels fournisseurs de service externe et les sous-traitants. Les interlocuteurs principaux sont les responsables métier et informatiques, les clients et les utilisateurs finaux et enfin les propriétaires des services et le service qualité.

Les concepts et les conseils de ce volume portent sur :

- les critères métier de l'amélioration des processus ;
- les critères technologiques de l'amélioration des processus ;
- la justification de ces améliorations continues ;
- les bénéfices métier, financiers et organisationnels ;
- les principes de l'amélioration continue ;
- les fondements des processus ;
- les rôles et responsabilités ;
- méthodes, pratiques et outils ;
- l'implantation de l'amélioration des services ;
- surveillance, mesures et maîtrise ;
- les défis, les facteurs de succès et les risques ;
- guide des meilleures pratiques.

Autour du cœur

Dans le but d'alléger le cœur du référentiel, les promoteurs de cette nouvelle version ont choisi de ne livrer que cinq livres officiels. Cependant, le contenu d'ITIL V3 ne se limite pas à ces cinq volumes.

Guides divers

En périphérie du cœur se trouve un ensemble de documents complémentaires :

- une introduction à ITIL ;
- un guide du décideur ;
- un guide des éléments clés (*Pocket Guide*) ;
- plusieurs guides complémentaires spécifiques à chaque sujet ;
- des études de cas ;
- des modèles de cycle de vie de service intégré ;
- une aide à la certification ;
- une méthode de gouvernance portant sur le service, l'organisation et les processus ;
- des notions avancées spécifiques aux secteurs d'activité ;
- des cartes de processus ;
- bien d'autres documents accessibles par le Web dans la version électronique.

Traduction

Dans le but d'accélérer l'adoption de cette nouvelle version, un effort particulier est fait sur la traduction. Disponible à l'origine uniquement en anglais, les cinq livres du cœur sont traduits dans plusieurs langues dont le français.

Accréditation

Le système d'accréditation des centres de formation a également évolué. L'OGC et l'ICMB (*Itil Certification Management Board*) ont désigné un organisme centralisateur, en charge de l'organisation des formations et des certifications. Désormais, c'est l'APM Group qui est en charge de négocier les agréments de formation et de certification pour le compte de l'OGC. Bien évidemment, l'EXIN et l'ISEB resteront fournisseurs d'exams, mais le contenu et le mode de certification de la version 3 peuvent trouver quelques modifications. Aussi, renseignez-vous bien avant de vous inscrire, et en particulier si vous envisagez de réviser sur des exams blancs qui ne concernent actuellement que la version 2 du référentiel.

Concernant les entreprises, il n'existe toujours pas de certification ITIL pour les services, les produits ou les organisations. Pour ce type de certification, il est indispensable de se tourner vers la certification de conformité à la norme CEI/ISO 20 000-1:2005 et CEI/ISO 20 000-2:2005 qui correspondent respectivement aux spécifications et aux bonnes pratiques de la gestion des services.

Les relations entre les processus

Bien que chaque composant du soutien et de la fourniture des services soit discuté séparément dans le livre, le but de ce chapitre est de mettre en évidence les liaisons et les rapports principaux entre les différents processus de la gestion de service et d'autres processus tels que la gestion d'infrastructure.

Les différents processus

Gestion de configuration

La gestion de configuration est une partie intégrante de tous les autres processus de la gestion de service à qui elle procure un ensemble d'informations précises et complètes sur tous les composants de l'infrastructure qu'ils soient matériels, logiciels, procédures ou autres. La gestion des changements est le processus qui profite le plus de la gestion des configurations, ce qui permet d'ailleurs une éventuelle intégration de l'un dans l'autre.

Le système de gestion des configurations identifie les rapports entre un élément de configuration qui doit être changé et les autres composants de l'infrastructure, permettant ainsi aux propriétaires de ces composants d'être impliqué dans le processus d'évaluation de l'impact. Chaque fois qu'un changement est apporté à l'infrastructure, les enregistrements de la configuration associée doivent être mis à jour dans la CMDB.

La CMDB doit être accessible à l'équipe de support pour que les incidents et les problèmes puissent être résolus plus facilement en comprenant la cause possible du composant défaillant.

La CMDB devrait aussi être utilisée pour établir un lien entre l'enregistrement de l'incident ou du problème à d'autres enregistrements appropriés

comme l'élément de configuration (CI) défaillant et les utilisateurs touchés. La gestion de mise en production utilise également très souvent les informations provenant du processus de gestion des configurations.

La gestion de niveau de service doit identifier les composants qui se combinent ensemble pour livrer le service afin d'établir le niveau de SLA.

La gestion financière des services doit connaître les composants utilisés par chaque direction métier particulièrement quand une re-facturation est mise en place.

La gestion de la continuité de service et la gestion de la disponibilité doivent identifier les composants pour exécuter l'analyse de risque et l'analyse d'impact des défaillances.

Centre de services

Le centre de services est le point de contact unique entre des fournisseurs de services internes ou externes et les utilisateurs. C'est également l'endroit où l'on peut déclarer les incidents et faire des demandes de service.

En tant que contact unique, c'est le centre de services qui doit tenir les utilisateurs informés de tous les événements se déroulant sur le système d'information. C'est le cas de tous les changements et mises en production.

Le centre de services est également l'interlocuteur privilégié de la gestion de configuration et de gestion de la capacité. Enfin, il faut noter également que toutes les informations de SLA passent par le centre de services.

Gestion des incidents

La gestion des incidents possède des liens forts avec la gestion de problème pour l'identification des causes, et la gestion des changements pour la mise en place des modifications après identification des causes. Il existe également des liens avec la gestion des configurations.

Mais le lien le plus fort est sans nul doute établi avec le centre de services dont les membres sont souvent les mêmes et qui est l'interface entre tous ces processus.

Gestion des problèmes

Le processus de gestion des problèmes tisse des relations étroites avec le processus de gestion des incidents et de gestion de la disponibilité. En effet, il demande un enregistrement précis et complet des incidents afin d'identifier efficacement les causes et les tendances, ce qui permet par la suite de concevoir les actions correctrices permettant d'éviter les indisponibilités.

Gestion des changements

Le processus de gestion des changements dépend de l'exactitude des données de configuration pour s'assurer que l'on connaît l'impact des changements envisagés lors de la validation d'une demande. Il y a donc un rapport très proche entre la gestion de configuration, la gestion de mise en production et la gestion des changements, tout ceci passant évidemment par l'intermédiaire du centre de services.

Les détails du processus de changement sont documentés dans les SLA pour permettre aux utilisateurs de connaître la procédure de demande de changement ainsi que les temps estimés et l'impact de la mise en œuvre de ces changements.

Le comité consultatif du changement (CAB) constitue un groupe de personnes qui participent en tant qu'experts à l'équipe de direction des changements. Ce conseil est composé des représentants de tous les secteurs de la direction informatique ainsi que de représentants des directions métiers.

Gestion des mises en production

Les changements peuvent souvent entraîner un besoin de nouveaux matériels, de nouvelles versions de logiciel, et/ou de nouvelles documentations, le tout créé en interne ou acheté puis contrôlé et distribué, comme un nouvel ensemble. Les procédures permettant de réaliser un lancement sûr doivent être étroitement intégrées avec celles de la gestion de changement et de la gestion de configuration. Les procédures de mise en production peuvent également être partie intégrante de la gestion des incidents et de la gestion des problèmes pour l'évaluation des régressions éventuelles, mais aussi de la gestion des configurations et en particulier de la CMDB.

Gestion des niveaux de service

Le processus de gestion des niveaux de service (SLM) a pour responsabilité de négocier, puis d'assurer les accords de niveau de service (SLA) avec les clients/utilisateurs et de prendre des accords de niveau opérationnels (OLA) en interne ou avec des fournisseurs externes, ces OLA n'étant que la transcription technique des engagements fonctionnels pris avec les clients. Le processus doit également mesurer l'impact des changements sur la qualité de service et SLA, tant lors de l'évaluation des demandes de changement qu'après leurs mises en œuvre. Le but le plus important dans le SLA se rapportera à la disponibilité de service et exigera ainsi la résolution d'incident dans des périodes consenties.

Le processus de gestion des niveaux de services est la charnière entre le soutien des services et la fourniture des services. Il ne peut pas fonctionner dans l'isolement car il repose sur l'existence et le travail efficace d'autres

processus. Un SLA sans service de support des processus est inutile, car il n'aurait aucune base pour valider son contenu.

Gestion de la capacité

La gestion de la capacité doit assurer que les ressources adéquates sont disponibles pour répondre aux besoins de l'activité économique. Ce processus peut donc être sollicité par les gestions des incidents et des problèmes lorsqu'un défaut de capacité est responsable du dysfonctionnement ou du non-respect de l'engagement pris dans le SLA. Dans cette hypothèse, la gestion de capacité sera également en liaison avec la gestion du changement et la gestion de la mise en production lors de demande d'évolution de l'infrastructure. Ceci implique évidemment, que la gestion de la capacité soit fortement liée à la gestion de configuration et à la gestion de l'infrastructure TIC.

Gestion financière des services informatiques

La gestion financière est responsable de la comptabilisation des dépenses du service informatique ainsi que de l'évaluation du retour sur investissement. En fonction de la politique de l'entreprise, son rôle peut également être de récupérer ces dépenses auprès des clients sous forme de refacturation.

Ceci suppose des liens étroits avec la gestion de la capacité afin d'identifier les besoins en investissement, mais également la gestion de configuration pour l'évaluation des amortissements des matériels et enfin la gestion des niveaux de service pour identifier les vraies dépenses de service. Le responsable du processus financier va probablement travailler étroitement avec la direction pendant les négociations des budgets de département.

Gestion de la disponibilité

La gestion de la disponibilité est concernée par la conception, la mise en œuvre, la mesure et la gestion des services informatiques pour assurer que les besoins de disponibilité exprimés par l'entreprise sont atteints. Elle doit donc disposer d'informations en provenance de la gestion des incidents ainsi que de la gestion des problèmes afin de comprendre les raisons des défaillances de service et le temps nécessaire pour reprendre le service.

Un lien avec la gestion des niveaux de service permet de fournir les mesures et le rapport de disponibilité qui assurent que le niveau de disponibilité livrée est en accord avec le SLA.

Gestion de la continuité de service

La gestion de la continuité de service doit définir, valider et mettre à jour les procédures de sauvegarde, de haute disponibilité et les plans de reprise

d'activité (PRA) afin de garantir la capacité de l'organisation à soutenir les exigences minimales de l'activité économique après une interruption.

La continuité de service exige un équilibre entre les mesures de prévention des risques comme des systèmes à haute disponibilité et les options de rétablissement rapide de service incluant des équipements de sauvegarde.

Les données provenant de la gestion de configuration sont nécessaires pour faciliter cette prévention et cette planification. Les processus de gestion de l'infrastructure et des changements doivent être impliqués pour leur impact potentiel sur les plans de continuité du service.

Autres processus

Les deux processus suivants sont normalement situés hors du cadre de la gestion des services informatiques et ITIL les positionne d'ailleurs dans deux livres séparés. Cependant, les interactions entre ces deux processus et les dix processus de la gestion des services (ITSM) sont très fortes et la mise en place de l'un ne peut que difficilement se faire sans l'autre.

Gestion de la sécurité

La gestion de la sécurité est impliquée dans tous les processus où les questions de sécurité apparaissent. De telles questions touchent à la confidentialité, l'intégrité et la disponibilité des données, aussi bien qu'à la sécurité des matériels et des composants de logiciel, à la documentation et aux procédures. À ce titre, elle est présente dans la gestion de la disponibilité et de la continuité de service pour valider les menaces sur la disponibilité du service. Elle est également présente dans la gestion des changements et la gestion des mises en production pour valider qu'une demande de changement ou qu'une installation n'a pas d'impact sur la sécurité du système d'information.

Gestion de l'infrastructure TIC

Les fonctions de gestion de l'infrastructure des TIC sont impliquées dans la plupart des processus de soutien et de fourniture des services où des questions plus techniques se présentent. On trouve en particulier la gestion des configurations et la gestion de capacité, mais également la gestion de la disponibilité. On recommande également que les modifications de l'environnement (électricité, climatisation, sécurité d'accès, protection incendie, etc.) soient prises en compte par la gestion de l'infrastructure.

Enchaînements des actions

Chaque processus décrit dans ITIL est en relation avec les autres processus. Le scénario suivant, bien que fictif, illustre certaines de ces relations.

Un utilisateur subit une importante baisse de performance, suivie d'une interruption lors de la consultation d'un service de l'intranet de l'entreprise. Il passe alors un appel auprès du centre de services pour signaler l'incident et demander de l'aide.

La gestion des incidents prend en charge la requête de l'utilisateur. Malheureusement, après avoir cherché une réponse dans la base de connaissance, il apparaît que cet incident n'est pas répertorié. Le technicien de l'équipe tente alors d'établir un diagnostic rapide de l'incident.

Cependant, depuis quelques minutes, le centre de services constate une recrudescence des appels signalant le même incident. Le temps passant, le gestionnaire des niveaux de service est prévenu que l'accord pris avec les utilisateurs n'est plus respecté. Le processus de gestion des incidents déclenche alors une procédure d'escalade vers le second niveau qui propose une solution palliative permettant à l'utilisateur de reprendre son travail. Par la suite, l'incident est transféré à l'équipe de gestion des problèmes afin que ses membres puissent identifier la cause du dysfonctionnement.

Puisque les utilisateurs signalent tous une baisse de performance avant l'interruption totale, l'équipe de gestion des problèmes a demandé des informations aux membres de la gestion de la capacité. Après quelques recherches, la cause du problème est identifiée. La solution proposée par l'équipe de gestion des problèmes consiste en une modification de l'architecture informatique qui passe par la mise à jour d'un équipement. Une demande de changement ou « Request for Change » (RfC) est enregistrée.

Le comité de gestion du changement (CAB) est réuni afin d'examiner et de valider cette évolution de l'infrastructure. Cette réunion exige la participation des responsables d'autres équipes gérant d'autres processus.

Le service gérant le processus de gestion financière des services assiste à la réunion de gestion du changement et prend en compte les éléments de coût de cette modification de matériel et valide l'adéquation entre le surcoût et le budget du service.

La gestion de la continuité de service examine la modification envisagée sur l'infrastructure et s'assure qu'une solution de retour à la situation précédente est envisageable en cas de fonctionnement anormal de la future configuration.

Le processus de gestion de la disponibilité s'assure que le nouveau matériel remplit bien les conditions de disponibilité et de fiabilité exigées par les engagements de service.

Une fois cette modification validée, le matériel est installé sous contrôle de l'équipe de gestion de l'infrastructure TIC (hors gestion des services).

La gestion de mise en production contrôle la méthode de remplacement du matériel et enregistre les détails et les versions des nouveaux matériels et logiciels installés puis transfère les informations vers la gestion des configurations.

La gestion des configurations s'assure que les modifications apportées au système d'information sont bien mises à jour dans la base de données des configurations (CMDB).

Le centre de services est averti de la modification afin de tenir les utilisateurs informés de la correction du problème si nécessaire, voire de l'abandon de la solution palliative.

Les conséquences de l'implantation d'ITIL

Le choix d'implanter ITIL au sein d'une entreprise n'est pas sans conséquence. Outre les surcoûts engendrés par la mise en place des processus, il arrive que d'autres désagréments se produisent comme le rejet du changement par le personnel. Néanmoins, les avantages qu'apporte ITIL sont bien réels et faire aboutir le projet ne peut qu'être bénéfique. Les changements constatés tant au niveau du service informatique qu'au niveau de la confiance accordée par les clients et les utilisateurs en sont la preuve. Au lieu d'être considéré comme un centre de coûts, le service informatique devient un vecteur de profits.

Les apports bénéfiques

Les bénéfices de la mise en place des meilleures pratiques d'ITIL sont multiples. On gagne tout d'abord en efficacité et en qualité de service, mais on constate également une confiance accrue de l'entreprise dans ses services informatiques.

L'implantation du centre de services a plusieurs autres conséquences bénéfiques. La première d'entre elles est d'accroître l'accessibilité et d'améliorer la perception des services fournis aux utilisateurs par un point de contact unique. Associé à la gestion des incidents, il améliore la qualité et la rapidité des réponses apportées aux requêtes et aux plaintes des clients, ainsi que le contrôle des performances vis-à-vis des engagements pris envers le client (SLA).

Les gains en qualité sont issus de l'approche cohérente et systématique de tous les processus et de la formalisation précise des rôles et responsabilités de chacun. De cette façon, les éventuels points faibles des opérations précédentes sont mieux identifiés, ce qui encourage les améliorations

permanentes. Cette mise en place des processus donne également des résultats tangibles dans l'assistance aux utilisateurs avec des temps de résolution plus courts, des services informatiques plus fiables et la mise en œuvre de solutions permanentes aux problèmes de fond. Cette approche proactive de la gestion de service induit une réduction du volume d'incidents et une réduction de leurs impacts sur l'entreprise. De plus, cela améliore le taux de résolution en premier niveau, ce qui procure encore plus de crédibilité au centre de services et à ses techniciens et augmente le climat de confiance envers le service informatique. On retrouve ce sentiment de confiance au sein de l'équipe informatique dont les membres, qui se considèrent plus proches des utilisateurs, sont désormais également plus efficaces.

D'un point de vue financier, ITIL donne un meilleur contrôle par l'identification des coûts liés à la gestion des services. Associée à l'expression des besoins des utilisateurs, cette identification aide à justifier le coût des services en les alignant sur les demandes. Elle permet également de maîtriser l'offre en capacité face aux demandes des utilisateurs et donne un meilleur contrôle de l'infrastructure informatique. Cette amélioration de l'efficacité et du rendement des ressources matérielles et humaines entraîne une réduction des coûts (baisse du coût total de possession TCO).

Les conséquences néfastes

Le projet ITIL classique sera certainement confronté à des écueils relatifs à l'implantation des processus dans l'entreprise. Ceux-ci sont en général la cible d'attaque en règle de la part des acteurs concernés, qui considèrent ces nouvelles organisations comme étant lourdes et bureaucratiques. Tout cela tient en général plus du rejet pur et simple du changement que d'une analyse objective, mais il est important d'en tenir compte dès le début du projet.

« On ne change pas une équipe qui gagne ». Cet adage populaire correspond à un sentiment largement partagé, mais il implique que l'équipe gagne. Or, lors d'un rejet de projet de type ITIL, les changements organisationnels sont envisagés afin de remplacer une organisation au mieux défaillante, sinon inefficace.

Il semble indispensable, dans le processus d'acceptation d'ITIL, de préparer le projet bien en amont, expliquant la teneur des changements envisagés, et de le faire suivre d'une formation appropriée pour les membres de l'équipe informatique.

Toutefois, le manque d'adhésion au projet peut se situer au sein de l'équipe informatique comme au niveau des utilisateurs. Cette situation se présente

la plupart du temps si l'on constate un manque d'engagement de la part des responsables et/ou de la direction de l'entreprise.

Il s'agit là du scénario catastrophe à éviter absolument. Si le soutien au projet et/ou la décision d'implanter ITIL ne vient pas du plus haut niveau de l'entreprise, le projet est perdu d'avance. À la vue des changements organisationnels, de l'investissement en temps et des décisions à prendre pour l'ensemble de l'entreprise, le directeur informatique désireux de mettre en place des services soutenus par les meilleures pratiques doit impérativement obtenir l'assentiment de sa direction, mais également son engagement total sur le long terme.

Les surcoûts liés

Un investissement en personnel semble indispensable, pas nécessairement en embauchant de nouvelles recrues, quoique cet engagement puisse souvent être justifié, mais plus dans la formation individuelle. Il ne faut cependant pas négliger le besoin en ressource supplémentaire, par exemple pour le centre de services qui demande parfois des horaires décalés.

Il faut aussi proposer des personnes pour occuper les nouveaux rôles issus de la mise en place des processus. Gardons à l'esprit qu'un processus transverse peut recouvrir plusieurs départements, services, organisations, etc. Toutefois, plusieurs processus ne demandent pas nécessairement plusieurs personnes pour les prendre en charge. Une même personne peut être responsable ou gestionnaire de plusieurs processus et assumer d'autres rôles dans l'entreprise. Ainsi, il y a de grandes chances pour que le responsable du centre d'assistance technique ait également à prendre en charge la gestion des incidents et, pourquoi pas, la gestion des configurations.

L'inactivité du personnel qui attend l'appel au centre d'assistance a également un coût qu'il faut quantifier car la tentation est grande de supprimer un poste de ce centre lorsque tout va bien, sans envisager le risque potentiel. La formation supplémentaire des personnels du centre de services ainsi que le coût du logiciel spécifique de gestion de l'assistance et de la base de connaissance CMDB, représentent eux aussi un surcoût non négligeable qui peut s'élever à plusieurs dizaines de milliers d'euros.

Tout cela a un coût, mais il faut le comparer à ceux qui sont engendrés dans toute l'entreprise par la décision de ne pas l'implanter...

L'autre investissement qui vient immédiatement à l'esprit est celui du matériel supplémentaire de recharge, ou *spare*, qui doit être approvisionné pour pallier la défaillance d'un élément de configuration, afin d'éviter une interruption de service trop longue. En conséquence, il faut également investir sur un lieu de stockage sécurisé pour ce matériel.

Le retour sur investissement

Même si elle représente un critère fondamental, la réduction des coûts n'est que la conséquence des améliorations apportées aux services informatiques, en particulier grâce à l'alignement des services aux métiers. Cet alignement des services informatiques sur les besoins exprimés par les clients et les utilisateurs donne à la direction informatique la même vision que celle de l'entreprise et permet de commencer à améliorer ces processus internes afin de démontrer clairement et sans équivoque la plus-value du département informatique envers l'entreprise.

Il n'est donc pas impossible que l'implantation des processus ITIL ait pour conséquence une hausse des coûts directs de la direction informatique. Cependant, si ceux-ci sont compensés par un soutien plus efficace aux services de l'entreprise et conduisent à une hausse de la valeur créée par l'entreprise, le retour sur investissement (ROI) est avéré. De plus, il est clair que plus les processus ITIL sont maîtrisés, plus la qualité du service et l'efficacité augmentent ce qui a pour conséquence d'inévitables réductions de coûts.

Le calcul du retour sur investissement doit donc prendre en compte les dépenses liées aux personnels, aux matériels et aux services proposés, et les comparer aux réductions de coûts occasionnées par les gains d'efficacité et la maîtrise des dépenses d'une part, mais également aux bénéfices obtenus par les différents services de l'entreprise d'autre part.

Quelques exemples

Après l'implantation d'ITIL il y a quelques années, le chimiste Procter & Gamble a réduit les coûts d'exploitation de son système d'information de près de 8 %, en liaison avec une réduction de près de 10 % du nombre d'appels signalant des incidents au centre de services. On imagine aisément les économies engendrées par des résultats d'une telle importance (source : Pink Elephant).

La chaîne de télévision par satellite MTV a constaté une hausse sensible du taux de résolution des incidents dès le premier niveau (Source : Axios System).

En alignant précisément le nombre d'ordinateurs de bureau à la demande des utilisateurs, la société de travail intérimaire Randstad a économisé 10 % sur son parc de matériel PC (Source : Axios System).

Citons également Ontario Justice Enterprise, chez qui l'implantation d'un centre de services virtuel a entraîné une réduction des coûts des services de soutien de près de 40 % (source : Pink Elephant).

Moins d'un an après l'implantation des processus ITIL, le fabricant de véhicules industriels Caterpillar a constaté une augmentation du taux de réponse pour les incidents liés aux services Web et réalisés dans le temps convenu. Ce taux est passé en un an de 60 à 90 % (source : Pink Elephant).

En revanche, une gestion des mises en production non maîtrisée peut entraîner des dommages importants, si l'on en croit la douloureuse expérience qu'en a récemment faite l'éditeur d'antivirus Trend lors d'une mise à jour de la base de signatures disponible pendant moins de 90 minutes sur son serveur Web au mois d'avril 2005. L'éditeur estime à 8 millions de dollars le coût de cette mise à jour défectiveuse de ses produits qui a bloqué près de 230 000 de ses clients. Ces coûts sont principalement liés à l'ouverture, en urgence, d'un centre d'appel durant un week-end férié au Japon. L'estimation intègre également des coûts marketing pour redorer le blason de l'entreprise. En revanche, cette somme ne prend pas en compte les éventuels dommages et intérêts que peuvent demander les clients particuliers et entreprises qui ont été obligés de faire travailler l'ensemble du personnel informatique pendant le week-end pour revenir à une situation stable (source : ZDNET).

Le centre de services virtuel correspond à une organisation de réponses distribuée sur plusieurs centres de services qui peuvent éventuellement répondre en horaires décalés.

Tendances et réalités

Selon une étude d'IDC et Osiatis, 56 % des entreprises françaises utilisent une méthode interne pour la gestion de leur système d'information, mais 80 % d'entre elles restent sur un mode réactif qui ne permet pas d'anticiper ni d'avoir la visibilité nécessaire sur les processus clés. Seules 25 % d'entre elles se basent sur la certification ISO et 11 % mettent en œuvre ITIL. Cependant, la maturité des entreprises dépend de la taille du parc géré. Il n'y a donc rien d'étonnant à ce que les PME soient peu sensibilisées aux méthodologies d'ITIL qui, pour l'heure, ne sont pas adaptées à leur taille. Sachant que ces entreprises (moins de 200 salariés) représentent plus des trois quarts des entreprises, la marge de progression d'ITIL est considérable. Les indicateurs de l'itSMF rapportent d'ailleurs qu'on observe une explosion de l'intérêt que portent les entreprises à ITIL avec une augmentation du nombre d'inscriptions à la certification ITIL de base, multipliée par huit en quelques années.

Parmi les entreprises interrogées, le secteur bancaire arrive en tête en terme de maturité globale dans la gestion des services informatiques, suivi par celui des services, de l'industrie, du public et enfin du commerce.

Cet engouement n'est certainement pas étranger au fait que les entreprises cotées en bourse doivent désormais se mettre en conformité avec les normes IAS-IFRS, la loi de sécurité financière et autres « Sarbanes Oxley

Act » (SOA). Ces obligations s'appliquent d'ailleurs aussi bien aux sociétés américaines qu'aux européennes.

Aux États-Unis, le SOA prévoit jusqu'à 20 ans de prison pour les gestionnaires coupables de malversations. Or, les sections 302 et 404 de cette loi imposent des contraintes fortes aux systèmes d'information des sociétés qui rentrent dans cette catégorie.

Une étude récente met en évidence un manque de préparation. En 2003, seules 20 % des 100 plus grandes sociétés françaises ont été en mesure de fournir un rapport détaillé répondant aux exigences de ces nouvelles réglementations et de fournir la garantie de conformité de leur système d'information.

La mise en place d'ITIL représente une véritable opportunité pour l'entreprise d'engager une amélioration de ses processus métier et de son contrôle interne, ce qui passe nécessairement par une amélioration de l'efficacité du système d'information.

Cas d'école

Pour illustrer plus concrètement les bénéfices attendus lors de l'implantation des processus ITIL, voici la simulation des conséquences financières sur une entreprise industrielle de taille moyenne dont les données à prendre en compte dans les calculs sont les suivantes :

- personnel de 1 000 salariés dont 600 utilisateurs de l'outil informatique ;
- salaire chargé moyen dans l'entreprise de 22 €/heure (Insee/2005) ;
- environ 8 000 incidents par an ;
- temps moyen de réparation de 10 minutes ;
- 200 jours ouvrables dans l'année.

En premier lieu, on constate qu'après l'implantation de la gestion des configurations, le centre de services dispose d'une meilleure vision de relation entre les utilisateurs, les éléments de configuration (CI) et les incidents. Il résulte de cela un gain de temps dans la résolution des incidents par l'identification plus rapide des éléments touchés. De plus, le nombre de techniciens assignés à la mise en relation des incidents avec les éléments de configuration peut être réduit de trois à deux. Le technicien supplémentaire est alors affecté à un autre poste sans nécessiter d'embauche, ce qui constitue ainsi une économie de salaire de $200 \times 8 \times 22 \text{ €} = 35\,200 \text{ €}$.

Avant la mise en place du centre de services, les utilisateurs perdaient du temps à identifier le bon interlocuteur ou à faire le diagnostic des incidents. Les conséquences éventuelles de ce type de fonctionnement étaient l'erreur de diagnostic, l'appel perdu ou dirigé vers la mauvaise personne.

Avec la mise en place d'un point d'appel central, le résultat est un gain de temps pour chaque utilisateur, mais également pour les membres de l'équipe technique, qui ne sont plus dérangés à mauvais escient. Si le temps gagné sur chaque incident est d'une minute, le gain potentiel est de $8\,000 \times 1 / 60 \times 22 \text{ €}$, soit environ 2 900 €.

Le cas de la gestion des incidents est particulièrement symptomatique des gains immédiats. Son implantation a conduit à une diminution du temps d'attente passé par un usager au téléphone avec un agent du centre de services et durant lequel l'usager ne peut travailler. Si cette durée est réduite d'une minute par usager et par jour, cela représentera un bénéfice pour l'entreprise de $600 \times 200 \times 1 / 60 \times 22 \text{ €} = 44\,000 \text{ €}$.

L'implantation de la gestion des problèmes est également intéressante, puisqu'elle touche à la proactivité du soutien aux services. Si le processus permet de réduire de 30 % le nombre d'incidents récurrents annuels, cela représente un gain pour l'entreprise de $2\,400 \times 10 / 60 \times 22 \text{ €} = 8\,800 \text{ €}$ par an.

Suite à une mésentente entre les services, et en l'absence d'une gestion des changements efficace, deux modifications importantes sont implantées simultanément sur le système d'information et provoquent un arrêt de l'application de suivi des commandes d'une heure. Malheureusement, la clientèle professionnelle ne peut plus commander, et certains clients décident d'acheter leurs produits à la concurrence. Il en résulte une perte de 50 clients sur un niveau moyen de commande estimé à près de 800 €, soit un manque à gagner de 40 000 € pour l'entreprise.

Supposons qu'un module logiciel récemment installé contienne un bogue et nécessite la réinstallation de la version précédente. Malheureusement, une version erronée est installée en raison d'une mauvaise gestion des mises en production et provoque une panne de deux heures qui n'affecte qu'une centaine d'utilisateurs, mais qui provoque également un arrêt de la production dans l'usine et fait stopper le travail à 300 personnes supplémentaires. Le coût pour l'entreprise s'élève donc à $400 \times 2 \times 22 \text{ €} = 17\,600 \text{ €}$.

Un serveur bureautique hébergeant les fichiers d'une centaine d'utilisateurs tombe en panne en raison d'une défaillance de disque dur. Malheureusement, la gestion de la disponibilité n'ayant pas été implantée, ce serveur ne dispose pas de disque en mode miroir, et il faut six heures au prestataire de maintenance pour livrer et installer le nouveau disque, puis faire la restauration des données avant de pouvoir relancer le système. Coût de la panne : $100 \times 6 \times 22 \text{ €} = 13\,200 \text{ €}$.

Suite à un important pic d'activité commerciale, l'entreprise a décidé d'embaucher temporairement 60 personnes. Grâce à la gestion de la capacité, le service informatique a anticipé cette évolution du besoin. Cette charge supplémentaire équivaut à 10 % des possibilités de l'infrastructure mais elle

est couverte par la surcapacité de réserve, ce qui évite un nouvel investissement en matériel. Même si cette réserve de capacité doit tôt ou tard être remise à disposition, si l'infrastructure a coûté 8 millions d'euros, l'économie réalisée correspond à peu près à 800 000 €.

Une machine à café défectueuse a mis le feu au bâtiment, ce qui a déclenché l'aspersion par les *sprinklers* anti-incendie. La salle machine a été peu endommagée, mais n'est plus utilisable, comme un grand nombre de bureaux et les cartouches de sauvegarde sont détruites. Heureusement, la gestion de continuité de service avait prévu ce cas et une sauvegarde complète des données était stockée à l'extérieur du site dans une salle de secours en mode dégradé. Il ne faut que cinq jours pour redevenir complètement opérationnel à l'aide de bâtiments préfabriqués. En moyenne, les membres du personnel ont perdu quarante heures de travail. Le coût total hors location de bâtiments représente $1\ 000 \times 40 \times 22 = 880\ 000$ euros. Néanmoins, l'entreprise existe toujours...

Quant à la gestion financière des services, son impact n'a pas été des moindres sur les économies réalisées. La publication des coûts liés à la mise en œuvre des SLA et l'éventualité d'une refacturation interne a provoqué une prise de conscience des clients et des utilisateurs. Ceux-ci ont alors revu à la baisse leurs demandes, et des besoins plus réalistes ont été envisagés, particulièrement en ce qui concerne les horaires de disponibilité du système et le temps de reprise après incident.

Bien que fictifs, ces chiffres sont totalement réalistes mais doivent être tempérés par l'investissement consenti auparavant pour l'implantation des processus ITIL. Il n'en reste pas moins que les gains espérés sont bien réels. Alors, on peut objecter que plusieurs des bénéfices annoncés ici ne sont que les résultats de l'implantation de l'assistance aux utilisateurs (exemples 1 à 4) et que beaucoup d'entreprises ont obtenu ces résultats avant de connaître ITIL. Ce serait oublier qu'en complément, ITIL apporte un grand nombre de bénéfices dont la quantification financière est moins immédiate ou moins voyante. Pour finir, il faut se souvenir qu'ITIL est un recueil de bonnes pratiques, et qu'à ce titre, il recense ce qui est communément reconnu comme la bonne solution pour prendre en compte un processus de la gestion des services informatiques. En ce sens, beaucoup d'entreprises, à l'image de monsieur Jourdain, font de l'ITIL sans le savoir...

PARTIE



Soutien des services informatiques

Au sein d'ITIL, le livre couvrant le soutien des services informatiques correspond aux activités plus opérationnelles que l'on peut qualifier de « tactiques » et qui sont en prise directe avec les utilisateurs ou leurs postes de travail tel que l'assistance et le support, la mise en place des matériels et des logiciels permettant l'utilisation du système d'information, et surtout le suivi et la gestion du cycle de vie de cet ensemble complexe. Cette partie détaille chacun des processus du soutien des services.

Vous trouverez en particulier :

- Chapitre 4 – Le centre de services
- Chapitre 5 – La gestion des incidents
- Chapitre 6 – La gestion des problèmes
- Chapitre 7 – La gestion des configurations
- Chapitre 8 – La gestion des changements
- Chapitre 9 – La gestion des mises en production

CENTRE DE SERVICES



LE RÔLE DU CENTRE DE SERVICES EST DE PRENDRE EN COMPTE LES APPELS DES UTILISATEURS ET DE LES ASSISTER LORS DES INCIDENTS.

Le centre de services

Le but de la gestion des services informatiques est de délivrer un niveau de service prédéterminé aux utilisateurs. Il est donc indispensable de proposer une organisation dont les principales fonctions sont, d'une part d'assister les utilisateurs lorsqu'ils rencontrent un dysfonctionnement ou un manque dans le système d'information, et d'autre part de surveiller l'environnement informatique afin de valider que celui-ci est bien en adéquation avec le niveau de service requis par les utilisateurs.

Vue d'ensemble

Le centre de services n'est pas un processus mais une fonction au sens organisationnel de l'entreprise. Il remplit le rôle de point de contact unique (SPOC : *Single Point of Contact*) entre l'utilisateur et la gestion des services informatiques.

Le rôle principal du centre de services est de prendre en charge les incidents qui surviennent au sein du système d'information afin d'en assurer le traitement rapide et efficace dans le but de restaurer le service le plus rapidement possible pour l'utilisateur.

Le centre de services a également pour fonction de traiter les demandes et de proposer une interface aux autres activités d'ITIL, telles que la gestion des problèmes, des changements, des configurations, des mises en production, des niveaux de services, et de la continuité des services.

Enfin le centre de services est le fournisseur principal des statistiques permettant d'établir les rapports de gestion destinés à être communiqués vers les directions métier lors des réunions de validation des niveaux de services. Ces rapports sont indispensables à une parfaite maîtrise des services informatiques.

Pourquoi un centre de services ?

Plus que n'importe lequel des processus présents dans ITIL, le centre de services est indispensable à la gestion des services informatiques. Il assume un double rôle. En effet, au-delà d'une fonction classique d'assistance aux utilisateurs, il représente l'interface principale entre ces derniers et le service informatique pour toutes les questions relatives au système d'information.

L'absence de ce service place en contact direct les utilisateurs et les techniciens chargés de l'exploitation et de la gestion du système d'information. La tendance naturelle induit une réactivité des équipes techniques en mode « pompier ». Cette situation, que l'on retrouve dans de nombreuses sociétés, peut produire plusieurs conséquences néfastes. On trouve en particulier une perte de confiance des utilisateurs qui se traduit souvent par la naissance d'un support parallèle issu des utilisateurs eux-mêmes, entraînant une perte de temps pour ces derniers, ainsi qu'un problème de qualité dans la résolution des incidents. Parmi les effets de bord induits par une absence de centre de services, on trouve également le manque d'organisation et de structure dans le support aux utilisateurs. Cela entraîne des délais plus importants dans la résolution des incidents et ce, indépendamment de la compétence de l'équipe technique, puisque celle-ci ne parvient pas à capitaliser sur les expériences antérieures. Par l'apport de sa couche d'abstraction, le centre de services permet aux techniciens de se concentrer sur leur mission première et non de s'occuper de l'organisation ou de la répartition du travail.

Quand un client ou un utilisateur rencontre un problème, expose une demande ou juste une question, il souhaite obtenir une réponse rapidement. Mieux encore : il veut un résultat !

Il n'y a rien de plus irritant que d'appeler une entreprise, une administration, un service quelconque et de se promener entre les différents interlocuteurs avant de trouver la bonne personne. Le centre de services permet de résoudre en grande partie ces désagréments en proposant une interface unique quel que soit le problème rencontré par la personne qui appelle.

La perception que les utilisateurs vont avoir de leurs premiers contacts est particulièrement importante. C'est ce sentiment qui va déterminer le niveau global de confiance et donc d'adhésion de l'ensemble de l'entreprise à ce centre de services, et par conséquent, le soutien de la direction générale à la direction informatique. Il est indispensable que les utilisateurs aient une bonne première impression de l'équipe du centre de services et en particulier de ses performances et de son attitude.

Cette « attitude service » doit, comme son nom l'indique, être au cœur de la documentation, des procédures et des formations des personnels du centre de services. L'équipe du centre doit garder à l'esprit que son rôle principal n'est pas de résoudre l'incident et encore moins le problème,

mais bien de rendre le service disponible pour l'utilisateur. On peut ainsi éviter la dérive classique de la focalisation sur la technique plutôt que sur le besoin métier de l'utilisateur.

Mais comment est-on arrivé à ce concept de centre de services ? Au-delà d'un simple changement de nom, on constate que l'évolution du métier est bien réelle. En quelques années, on est passé du centre d'appel, au centre d'assistance et enfin au centre de services. Cette modification dans le rôle d'une organisation désormais dédiée au contact avec les utilisateurs et les clients est le révélateur d'un besoin fort. La mission du centre de services n'est plus simplement de régler les dysfonctionnements du système d'information en mode réactif, mais bien de les anticiper, de les corriger avant qu'ils ne se produisent. De plus, le centre de services, en tant qu'interlocuteur privilégié, se voit confier des missions tenant à l'organisation, la médiation et bien sûr la communication. Paradoxalement, l'abandon du tout technologique au profit de l'expression du besoin métier s'accompagne d'une forte demande en termes d'efficacité technique et de compétences multiples. Et on le constate aisément par le nombre croissant d'organisations qui cherchent à augmenter de façon significative le pourcentage d'appels résolus dès le premier contact.

Une entreprise doit inévitablement investir dans un centre de services pour obtenir ces résultats.

Un des apports du centre de services est d'offrir un point de contact unique à l'utilisateur (SPOC) permettant d'éviter les allers-retours entre différents interlocuteurs. Ceci permet de fournir rapidement un support de haute qualité, avec des temps d'intervention et de résolution réduits, afin de répondre à l'attente des utilisateurs et de les maintenir satisfaits.

Le centre de services peut également aider l'entreprise à mieux connaître la réalité de la consommation des services en centralisant toute demande d'intervention suite à incident ainsi que toute demande d'évolution. En consolidant également les informations en provenance des différents processus, comme la gestion de la capacité, le centre de services peut établir une cartographie des coûts. Ce contrôle plus efficace permet souvent d'envisager une réduction du coût de possession (TCO) pour l'ensemble des services liés aux technologies de l'information.

Enfin, la centralisation de l'information peut également permettre, par recouplement, d'identifier de nouvelles opportunités d'activité économique.

Responsabilités

En tant qu'interlocuteur privilégié des utilisateurs et des clients, la plupart des activités mises en œuvre par le centre de services sont issues de l'un des processus de gestion des services. Il est donc nécessaire de déterminer le rôle et les responsabilités du centre de services pour chacun de ces processus, et en particulier dans le cadre de la production des comptes rendus

d'activité. Comme on peut le voir sur la figure 4-1, parmi toutes ses missions, le centre de services doit assumer un haut niveau de disponibilité pour certaines d'entre-elles. On retiendra en particulier la réception et l'enregistrement des appels des utilisateurs concernant un incident sur le système d'information, mais également la prise en charge des demandes et réclamations simples. S'ajoute à cela la résolution de premier niveau de tous les incidents ou tout au moins la tentative de résolution. En cas d'incapacité du premier niveau à résoudre la demande de l'utilisateur, celle-ci doit être transférée au deuxième niveau d'assistance. Lorsque le service est rétabli après l'intervention de la gestion des incidents, il est possible que la cause de cet incident ne soit toujours pas identifiée. Dans ce cas, le centre de services transfère l'information au processus de gestion des problèmes dont le rôle est justement d'identifier la cause puis de proposer une solution. Cette solution peut éventuellement faire l'objet d'une demande de changement. Cette demande de changement peut ensuite donner lieu à une implantation gérée par le processus de mise en production. En définitive, un bilan permet de déterminer si la modification corrige bien le problème identifié, et permet également de valider si l'incident/problème de départ peut être clos auprès de l'utilisateur. Dans tous les cas le suivi de tous les incidents, qu'ils soient transférés ou pas, est de la responsabilité du centre de services qui doit tenir régulièrement informés les utilisateurs sur l'état et le déroulement de leurs demandes.

Enfin, le centre de services a également la responsabilité de produire des tableaux de bord qui seront diffusés au management pour une partie d'entre eux, puis aux utilisateurs pour certains autres.

Si les termes semblent définir les mêmes concepts, la réalité est tout de même sensiblement différente. On peut définir plusieurs types de centres de services.

- En premier lieu, on trouve le classique centre d'appel, *call center*, qui peut recevoir un volume important d'appels en provenance des utilisateurs. Il doit ensuite les enregistrer et les transférer vers l'équipe compétente.
- En second lieu, on retrouve l'assistance technique, *help desk*, qui traite les incidents et les demandes informatiques aussi rapidement que possible en s'assurant qu'aucune demande ne se perd.
- Enfin, le troisième type que l'on peut identifier, est le centre de services. C'est aussi le plus complet . Outre les services d'assistance technique, il offre une gamme plus étendue tel que le point de contact unique, et exerce le pilotage et l'interface des processus ITIL.

Il faut noter que chacun des services ci-dessus est un sur-ensemble du service précédent. Qui peut le plus, peu le moins. Chaque type de service propose alors des compétences plus larges associées à une couverture fonctionnelle plus importante.

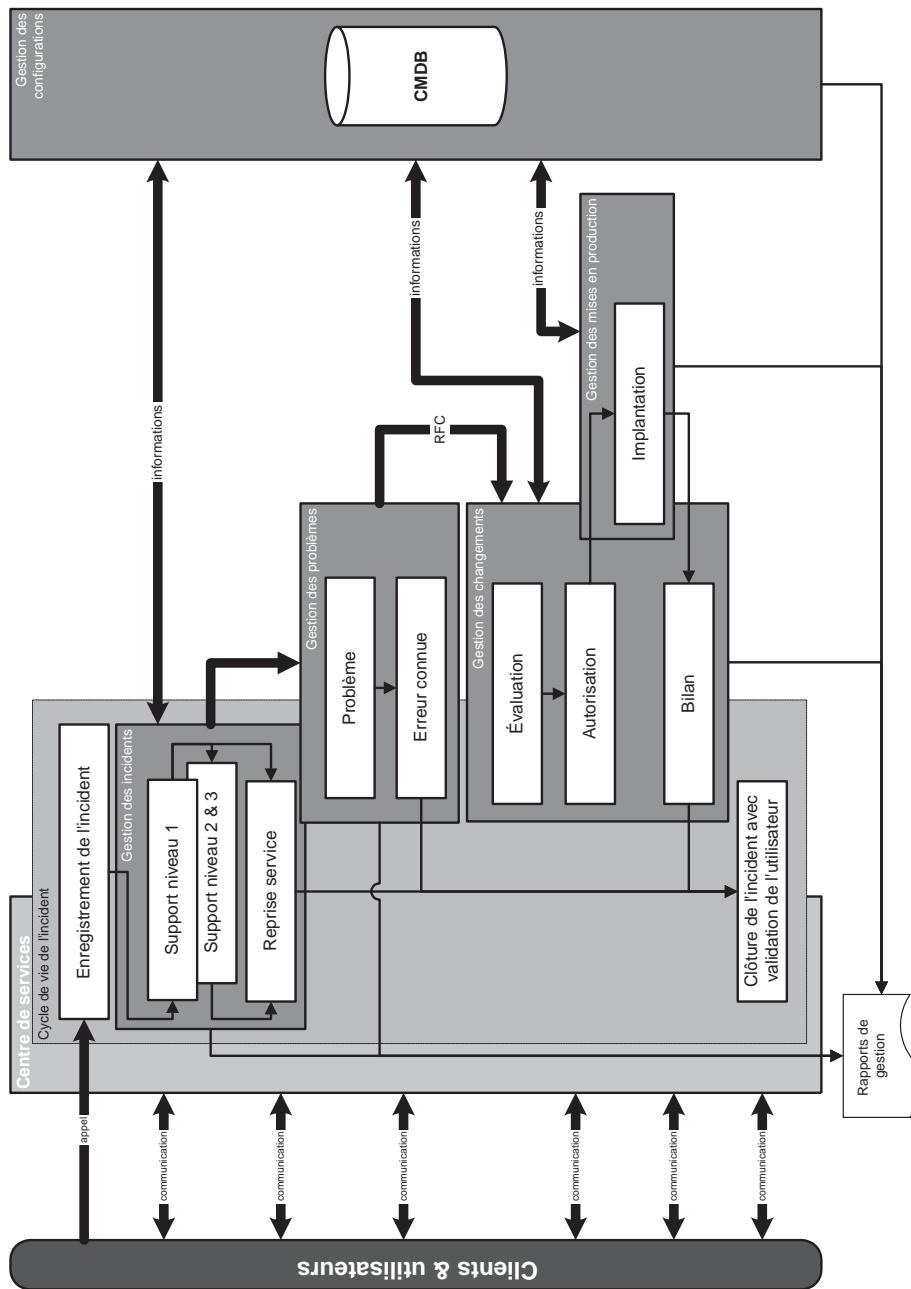


Figure 4-1 : Le rôle du centre de services dans le cycle de vie d'un incident

Description du centre de services

Mise en place d'un centre de services

Lors de la mise en place d'un centre de services, plusieurs questions se posent : les objectifs fixés par l'entreprise, les besoins exprimés par les différentes directions fonctionnelles, les choix liés à la technologie et enfin, les budgets envisageables (voir figure 4-2).

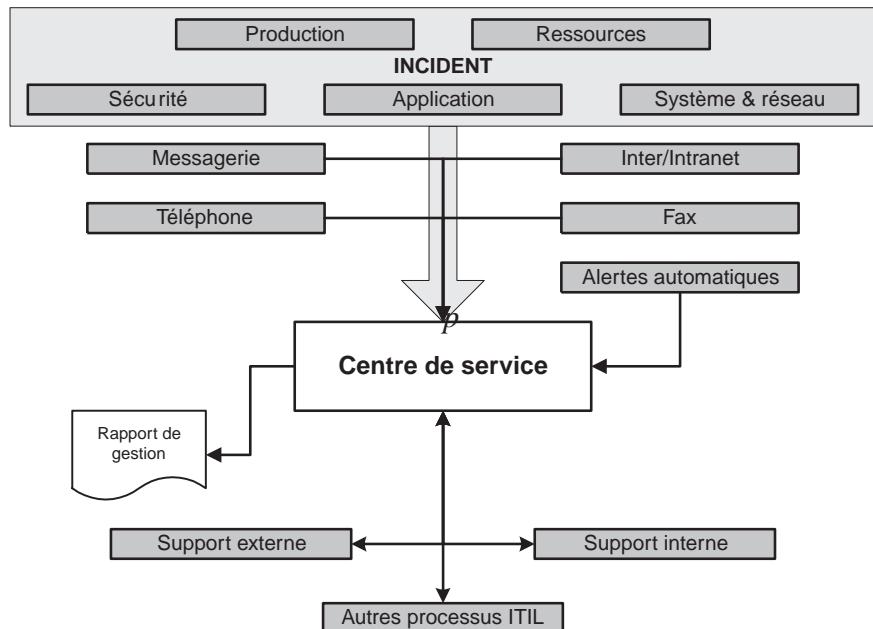


Figure 4-2 : Les types d'appels du centre de services

Les réponses à ces questions ont un fort impact sur le projet de mise en place d'un centre de services et sa future infrastructure. Ces réponses doivent fournir des objectifs métier bien définis et partagés par les différentes directions de l'entreprise. Les responsabilités de chaque intervenant, client et utilisateur doivent être clairement identifiées. Un langage commun permet à ces personnes de déterminer et de valider les termes contractuels, les rapports et les résultats attendus. Le tout doit s'accompagner d'un engagement fort de la direction.

Une stratégie prudente consiste à débuter par un centre de services assez simple (centre d'appel) en ajoutant par la suite les fonctions complémentaires

en plusieurs phases (assistance technique, application de support, base de connaissances, etc.), chacune donnant lieu à évaluation et recette.

La promotion du centre de services doit être engagée dès le lancement du projet dans le but d'éviter un risque de rejet assez classique provoqué par la résistance au changement et la perception d'une nouvelle bureaucratie. Faire participer les utilisateurs et les former à l'utilisation de la solution d'assistance reste le moyen le plus sûr d'obtenir leur adhésion, sans oublier de former le personnel informatique en parallèle, afin d'en faire un personnel de support.

Technologies du centre de services

La technologie peut apporter une aide précieuse à l'équipe du centre de services dans la prise en charge de ses missions. Toutefois, il faut garder à l'esprit que la technologie n'est pas un but, mais bien un moyen, et ne doit être utilisée qu'en ce sens et en complément de procédures et méthodes efficaces.

La mise en place de cette technologie associée à l'automatisation d'un grand nombre de tâches nécessite une discipline plus importante. L'informatique n'est en réalité qu'un amplificateur de l'organisation et des processus associés. Si ceux-ci sont défaillants dès l'origine, la mise en place d'outils informatiques ne fera qu'accélérer et amplifier la défaillance.

Il n'y a pas d'organisation universelle et les modalités d'implantation d'un centre de services doivent être modulées en fonction d'un grand nombre de critères. Cependant, en fonction de l'activité, de la localisation et de l'importance de l'organisation, trois types de structures de centre de services peuvent être envisagés.

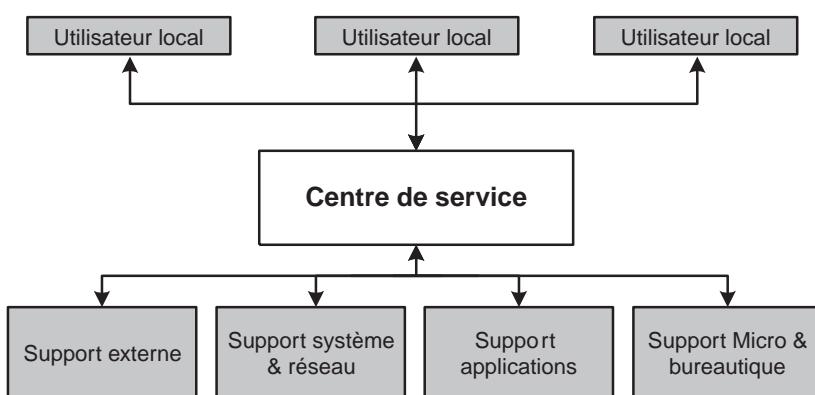


Figure 4-3 : Centre de services local

Le centre de services local illustré sur la figure 4-3, est sans doute le plus traditionnel et est souvent associé à l'implantation historique de l'organisation. Dans ce cas, le centre de services est situé sur le site et est destiné à assumer le support des utilisateurs locaux. Ce modèle peut également s'appliquer à une entreprise disposant de plusieurs localisations géographiques, mais il faudra prendre garde à garantir une compatibilité matérielle entre les sites, à établir des procédures communes, à mettre en place des indicateurs et une activité de compte rendu communs, et si possible, à partager les compétences entre les centres de support afin de ne pas dupliquer les ressources.

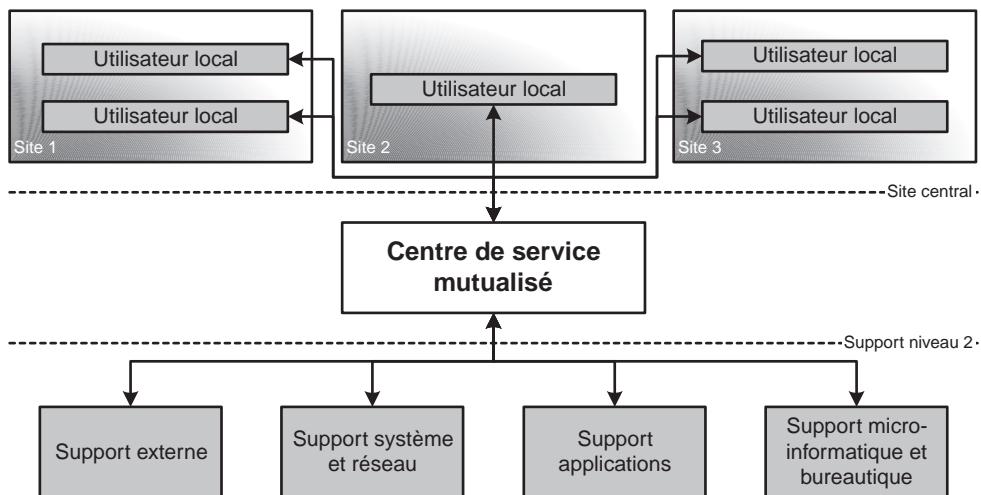


Figure 4-4 : Centre de services mutualisé

Dans le cas du centre de services mutualisé (figure 4-4), l'organisation qui possède plusieurs établissements peut avantageusement remplacer plusieurs centres de services locaux par une organisation centralisée. Dans ce cas, tous les utilisateurs répartis sur les différents sites peuvent contacter un service unique qui procure la même assistance à tous les sites. La relative perte de proximité des utilisateurs est compensée par le gain en coût opérationnel direct (infrastructure téléphonique, salles, matériels, personnel, etc.), par la consolidation des informations de support, et par la mise en place d'une base de données centralisée.

Le centre de services virtuel est une combinaison des deux modes précédents (figure 4-5). Grâce aux progrès des télécoms et des réseaux, on peut envisager qu'un ensemble de centres de services locaux réponde à l'ensemble des sites de l'organisation. Les deux avantages de cette configuration sont la proximité des techniciens en cas d'intervention sur site, et la faculté de répondre à tous les sites quelle que soit l'heure de la journée, dans le cas

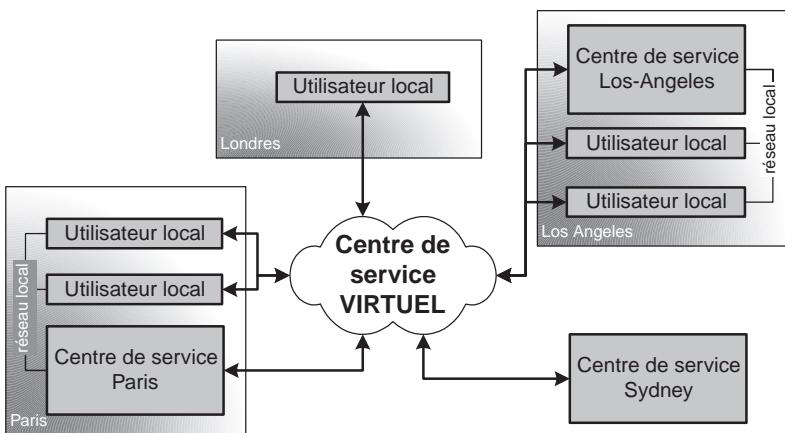


Figure 4-5 : Centre de services virtuel

d'une organisation qui dispose de localisation sur plusieurs continents. Cela permet de proposer un service réparti en fonction du décalage horaire. Attention cependant au problème du langage qui reste encore le principal frein à la mise en place d'un support virtuel.

Concernant les technologies employées dans les centres de services, le choix est vaste. La fonction de base est certainement la réponse téléphonique. Il existe pour cela de nombreuses solutions, des plus simples aux plus évoluées, offrant des systèmes de messagerie vocale, des capacités de routage automatique des appels, et une gestion des files d'attentes (ACD), mais également un couplage téléphonie/informatique (CTI), qui permet lors de la réception d'un appel d'en identifier la provenance, et de présenter à l'opérateur le dossier de la personne qui appelle.

En dehors de l'aspect téléphonique, on peut proposer aux utilisateurs d'exprimer leurs demandes ou de signaler leurs incidents par le biais d'une application dédiée ou d'un serveur intranet, qui permet de prendre en compte les différents environnements informatiques des utilisateurs. Cette interface avec les utilisateurs peut ou doit être connectée à l'application de gestion du support téléphonique qui dispose d'un système de base de données et éventuellement d'une base de connaissances.

D'un point de vue technologique, la mise en place d'une alerte système provenant des différents équipements et applications présents sur le réseau, apporte une importante capacité de proactivité. Cette alerte émise depuis l'infrastructure elle-même apporte des gains largement supérieurs aux coûts de leur implantation. Il n'y a rien de pire pour l'image d'un centre de services que l'opérateur qui apprend un incident ou la défaillance d'un système de la bouche du client.

Surveillance de la charge de travail

Cette surveillance permet de déterminer les ressources, et en particulier les équipes à mettre en place pour répondre à un éventuel pic de charge. Cette analyse a posteriori permet de détecter les évolutions dans l'activité du centre. On peut ainsi découvrir un problème cyclique dont la fréquence d'apparition peut conduire à affecter plus de personnel sur une certaine période (exemple : changement de mot de passe chaque mois entraînant une augmentation des appels au centre de services).

Classement des incidents

Classer les incidents, c'est-à-dire déterminer leurs niveaux d'urgence, et leurs impacts sur le système d'information, permet d'établir un niveau de priorité pour chacun d'eux. Ce niveau détermine ensuite l'ordre de prise en charge des incidents par l'équipe technique. Évidemment, la répartition des incidents en fonction des compétences techniques de chacun peut modifier cet ordre dans les faits. Dans ce cas, il est possible qu'un incident peu urgent soit traité rapidement par un membre de l'équipe dont c'est la spécialité mais qui n'a pas d'action programmée, alors qu'un incident assorti d'une priorité supérieure reste en attente en raison d'une équipe surchargée.

La classification d'un incident ou d'une demande est déterminée par l'opérateur après avoir interrogé l'utilisateur sur les symptômes de cet incident. Mais il peut arriver qu'un incident soit reclassé après analyse par l'équipe technique, s'il s'avère que l'utilisateur a communiqué des informations erronées.

Escalade

En fonction de l'importance de l'incident (impact, durée) une procédure d'escalade pourra être déclenchée. Cette opération consiste à transmettre l'ensemble du dossier à un niveau technique ou hiérarchique supérieur, lorsque le problème posé ne peut trouver de réponse à l'échelon inférieur. Il peut également arriver qu'un incident soit qualifié de prioritaire, auquel cas son statut passe automatiquement au deuxième niveau afin d'attribuer rapidement un technicien compétent pour le régler.

Analyse de la satisfaction client

Le suivi de la satisfaction client est un indicateur prioritaire de l'efficacité du centre de services. Il détermine également le niveau d'adéquation entre la demande du client et le service effectivement proposé.

Pour obtenir les informations permettant d'évaluer cet indice de satisfaction, une enquête doit être menée. Cette enquête peut être systématique ou statistique. Dans le premier cas, un formulaire est envoyé à chaque utilisateur

qui déclare un incident au centre de services. Dans le second cas, le formulaire n'est envoyé qu'aux personnes qui répondent à un critère déterminé à l'avance.

Facturation du service support

Afin de compenser les dépenses liées à la mise en place d'un centre de services, on peut décider de facturer une partie de ces coûts aux services d'où proviennent les utilisateurs. Cette étape de mise en place de la facturation doit se faire lors de la phase projet. C'est à ce moment que sera décidée la méthode de facturation : au forfait, à l'incident, etc. Ce choix est relativement important car il peut induire un comportement particulier chez les utilisateurs qui souhaitent éviter de « coûter » cher à leurs services, ou au contraire abusent puisque cela ne coûte rien !

Parmi les différents modes de calcul permettant de refacturer les services, on trouve notamment le coût par appel, le coût au temps passé, le coût forfaitaire défini dans le contrat de services (niveaux gold, silver ou bronze par exemple) et le coût réparti dans les charges globales facturées par la production informatique.

Notons que la refacturation s'accompagne en général d'une contractualisation fondée sur des engagements de service explicites.

Interaction avec les utilisateurs

Le centre de services est le principal point de contact et de communication entre les utilisateurs et le service informatique. De nombreuses sociétés ont développé des procédures ou des applications permettant à un utilisateur de signaler un incident ou de soumettre une requête. Historiquement, ces procédures utilisent des formulaires papier ou électronique que l'utilisateur doit remplir afin de communiquer les informations de base. Ceci peut former les premiers éléments d'une interaction entre les utilisateurs et le centre de services, mais les moyens modernes de communication sont à privilégier pour un gain de productivité. Un centre moderne ne peut se contenter d'un formulaire à remplir puis à déposer dans une case courrier. La mise en place d'un système téléphonique semble un minimum. Ensuite, on gagnera à étendre les moyens de communication et d'information au-delà du simple contact par téléphone, par exemple en utilisant une application dédiée, les technologies issues du Web tel que l'intranet, le courrier électronique ou le fax.

Compétence et formation du personnel du centre de services

En premier lieu, et en dehors de toute recherche de compétences techniques particulières, il est indispensable de s'attacher à la personnalité des membres de l'équipe du centre de services.

Certaines des compétences et des qualités personnelles évoquées par la suite sont indispensables pour le bon fonctionnement d'un centre de services. Le personnel recruté pour composer l'équipe doit posséder ces capacités ou les développer lors de formations.

Dans cette équipe le maître mot est *service*. Cela implique que ses membres doivent comprendre ce qui en découle. En particulier, il est important d'envisager toute action sous l'angle de la satisfaction du client et de la mise en place de relations durables avec celui-ci.

En premier lieu il convient de bien comprendre que le travail en centre de services est avant tout un travail d'équipe. La communication est au cœur du métier d'un centre de services, ses membres en sont porteurs. Le passage d'information entre les techniciens de l'équipe permet de gagner un temps considérable lors du traitement d'un incident par plusieurs personnes. Ce temps est d'ailleurs largement optimisé lorsque la résolution de l'incident est documentée, afin de profiter aux autres membres de l'équipe. Un même problème peut être traité par plusieurs personnes différentes en fonction de leurs disponibilités ou de leurs compétences, mais l'utilisateur ne doit pas avoir à recommencer la description de son problème à chaque nouvel interlocuteur.

La connaissance du métier de l'entreprise ou tout au moins la connaissance de l'environnement informatique métier (applications métiers, services, organisation, etc.) utilisé dans l'entreprise est aussi importante que les connaissances techniques pures. En fait, beaucoup de centres de services recrutent leurs équipes parmi des personnes issues du métier de l'entreprise ou emploient le personnel d'autres industries à base de service qui est alors, si nécessaire, formé aux métiers et techniques concernés.

Chaque membre du centre de services doit être apte à comprendre les objectifs de l'entreprise et surtout à comprendre et à accepter que les difficultés que l'utilisateur rencontre affectent l'activité de l'entreprise.

La première impression compte. Montrer au client que son problème est pris en compte, parler en termes qu'il comprend en évitant le jargon technique, voir les choses selon sa perspective sont autant de petites choses dont il se souviendra et qui compteront autant que la capacité de l'équipe à lui répondre efficacement.

Enfin, chaque membre de l'équipe doit bien comprendre que bien qu'il soit certainement lui-même très compétent dans son domaine, il n'en reste pas moins que l'utilisateur est lui aussi très compétent dans son métier.

Dans un environnement de support stressant, il n'est pas toujours facile de voir le problème selon le point de vue du client qui lui aussi peut se trouver confronté à un stress important. Comprendre et respecter ce point est particulièrement important pour toute l'équipe. C'est d'ailleurs dans

ces moments que l'utilisateur prendra conscience de la valeur ajoutée du centre de services.

Concernant le responsable de cette activité, il doit avoir à cœur d'être proche de l'action de son équipe et éventuellement d'y participer afin d'en comprendre la teneur et surtout les difficultés. Le responsable de l'équipe gagnera sans doute à prendre le temps de coiffer le casque du centre d'appel de temps en temps. Cela va lui permettre de mieux comprendre les difficultés que son équipe rencontre face à certains clients et utilisateurs, tout en augmentant la confiance que l'équipe lui accorde.

Savoir encourager son équipe et tenir compte de l'avis de ses membres sont des critères fondamentaux. En impliquant l'équipe dans le processus de décision, les membres vont plus probablement adhérer à la décision finale et on se donne ainsi plus de chance de succès pour ce projet.

En résumé, on peut dire qu'être à l'écoute de son équipe est indispensable, surtout dans le contexte d'un centre d'appel !

Procédures du centre de services

De nombreuses organisations informatiques désirent entreprendre une transition du mode artisanal vers l'ère industrielle. Cette évolution doit s'accompagner de la mise en place de procédures d'exploitation permettant un fonctionnement efficace en toute occasion. Peu importent les absences, les changements de personnel ou chez les utilisateurs. Le centre de services doit offrir une assistance traçable dans le temps. Lors de la mise en place des procédures de fonctionnement d'un centre de services, il faut prendre en compte cet ensemble de critères.

Le premier des points à garantir, est que la procédure de questions/réponses, entre le centre de services et l'utilisateur qui y fait appel, soit formalisée ou tout au moins qu'un scénario basique reposant sur des questions types soit mis en place. Le but de cette formalisation est de garantir qu'aucune information ne manquera lors de la résolution de l'incident soumis au centre de services. Des informations telles que le nom de l'utilisateur, son numéro de téléphone ou un autre moyen pour le joindre, la description de son problème ou de sa demande, sont autant d'informations qu'il faut valider lors de la communication.

L'identification de l'utilisateur peut se faire par son nom ou un numéro de code. L'utilisation d'une base de données doit permettre par la suite de retrouver d'autres informations telles que la localisation, le type de matériel, le numéro de téléphone, l'adresse électronique et l'historique des demandes de cette personne. Ces informations seront utiles dans le processus de résolution d'incident ou de réponse à une demande, si tant est qu'elles soient stockées dans cette base et surtout... à jour ! Pour pallier un éventuel problème de suivi des informations, la procédure doit prendre en compte

la validation par l'opérateur de certaines informations indispensables telles que l'identité exacte de l'utilisateur et le moyen de le joindre facilement, et ce même si les informations semblent complètes sur la base de données.

On voit bien que la maintenance de la base de connaissances du centre de services est extrêmement importante pour son efficacité. Il convient donc d'inclure une procédure de suivi des mises à jour de cette base. On s'appliquera en particulier à valider systématiquement l'identité et les coordonnées de chaque utilisateur faisant appel au centre de services. Mais pour que cette base de connaissances ne reste pas qu'une base de contacts, il faut également s'assurer que le suivi de tous les incidents, actions techniques, ébauches de solution et résolutions finales soit bien intégré dans la base, afin que chaque technicien puisse s'y référer et en profiter.

Enfin, la dernière, et non moins importante, procédure à prendre en compte par le centre de services est celle de la communication vers l'extérieur. Faire connaître le centre de services et ses activités aux utilisateurs est primordial. Il est indispensable de fournir des informations sous forme de rapports de gestion vers la direction afin que celle-ci puisse évaluer la qualité de service et l'adéquation entre les moyens mis en œuvre et le service attendu. Mais il ne faut pas non plus négliger la communication vers les utilisateurs. On peut envisager de communiquer des graphiques et des chiffres illustrant le niveau de service et de satisfaction. En effet, on se souvient mieux des dysfonctionnements que de ce qui fonctionne bien.

La publication des chiffres du centre de services est d'ailleurs souvent l'occasion de remettre les « pendules à l'heure ». En effet, on constate souvent, chez les utilisateurs, une perception assez différente de l'efficacité d'un centre de services lointain dont on ne connaît pas les résultats, même si celui-ci fonctionne parfaitement.

Ainsi, et c'est un état de fait bien connu des spécialistes de la qualité, l'impact de l'insatisfaction causée par un problème est beaucoup plus fort que celui de la satisfaction. Une statistique classique annonce qu'un client satisfait ne cite le produit qu'à sept personnes de son entourage, alors qu'un client insatisfait va communiquer son mécontentement à plus de vingt-huit autres personnes, et ceci indépendamment de l'importance du problème rencontré.

Faire son propre marketing ne peut donc être que bénéfique pour le centre de services. Il doit alors s'attacher à publier des informations sur son efficacité, mais également à se faire connaître par des moyens de communication plus classiques comme des affichettes, des tapis de souris ou tout autre moyen. Le but étant que les utilisateurs associent un service et des personnes à un numéro de téléphone, aussi simple à retenir soit-il.

Rapport de gestion

Les rapports de gestion sont destinés à faciliter l'évaluation du centre de services par son responsable, mais également par la direction et surtout par les utilisateurs. La capacité à produire des rapports de bonne qualité est un critère de maturité de l'organisation de support. Ces rapports permettent d'estimer les charges de travail, les tendances, ainsi que l'évolution des besoins matériels et humains. Grâce à ces rapports, on peut également mieux évaluer la répartition des moyens en fonction de la charge de travail quotidienne ou hebdomadaire. Cette analyse permet en particulier d'identifier les pics réguliers afin d'adapter le planning de présence des membres de l'équipe.

Un rapport de base doit inclure des informations sur le nombre d'incidents total, le nombre d'incidents résolus dès le premier appel, le temps d'attente moyen avant intervention, etc.

Comme le centre de services représente l'interface entre les clients et les utilisateurs d'une part, et le service informatique d'autre part, les rapports proposés par le centre de services doivent inclure des informations provenant de diverses sources.

Pour cette raison, un rapport plus étendu peut inclure des informations sur les performances du système d'information ainsi que sur la disponibilité des différents services et des applications, mais également des informations sur le nombre de demandes de changement. Mais on peut aussi ajouter des tendances sur le taux d'utilisation des ressources, des éléments de planning concernant les prochaines interventions entraînant une indisponibilité, et enfin un indice de satisfaction des utilisateurs...

Tous les rapports du centre de services doivent être proposés et adaptés en fonction du lectorat visé. Les types d'informations communiquées et la fréquence de publication doivent être décidés en amont et validés par un éventuel engagement de service (SLA).

Avantages

Les avantages qu'apporte la mise en place d'un centre de services sont multiples. On peut les classer en trois grandes parties.

La première partie concerne les gains en terme de perception des utilisateurs. En effet, on constate une plus grande facilité d'accès pour l'utilisateur du fait du point de contact unique (SPOC). Cette situation est à opposer à la situation antérieure où l'utilisateur doit appeler plusieurs personnes pour un même problème en faisant parfois lui-même le premier diagnostic. La mise en place du support améliore souvent le temps de réponse aux utilisateurs et réduit considérablement le nombre d'incidents oubliés. En dehors de l'amélioration de la qualité de service, le SPOC s'accompagne souvent

d'une plus grande satisfaction pour l'utilisateur. Mais l'avantage pour l'utilisateur ne se limite pas à une identification précise d'un interlocuteur et la facilité d'accès. La prise en charge de la demande par le centre de services lui permet d'en devenir le propriétaire et d'en assumer la responsabilité jusqu'à l'obtention d'une réponse de la part de l'utilisateur.

La seconde partie représente les avantages retirés par le personnel du centre de services. La mise en place de celui-ci permet d'optimiser le travail d'équipe et la communication entre ses membres qui peuvent alors profiter de l'expérience des collègues afin de gagner du temps sur la résolution d'incident.

Enfin, le troisième type d'avantage regroupe les gains obtenus par le management informatique avec un niveau d'information supérieur qui apporte une réelle aide à la décision. On constate surtout une utilisation plus efficace des ressources du support d'où une réduction des coûts associés, du fait de leur mutualisation.

Problèmes possibles

Malheureusement, la mise en place d'un centre de services central et d'un point de passage obligatoire n'est pas toujours bien acceptée. Elle est parfois perçue comme un élément bureaucratique supplémentaire dont la charge n'est pas compensée par les gains. Cela entraîne régulièrement une résistance au changement. Cette résistance s'observe dans les pratiques de travail qui changent chez les techniciens mais également chez les utilisateurs qui perdent le lien direct qu'ils entretenaient avec ces techniciens.

L'autre écueil que l'on rencontre le plus souvent révèle l'inadéquation entre le niveau de compétence de l'équipe et le besoin sur le terrain. Cela peut également s'appliquer aux ressources humaines ou matérielles qui ne sont pas adaptées à la situation. Ce problème a souvent pour origine une allocation insuffisante de budget et un manque d'engagement de la direction de l'entreprise.

Conclusion

L'implantation réussie d'un centre de services procure des bénéfices immédiats à l'organisation qui en était dépourvue. Parmi ceux-ci on trouve notamment une meilleure organisation du support, une réduction du temps de résolution des incidents avec en corollaire une réduction des coûts de support, et un accroissement de la satisfaction des clients.

GESTION DES INCIDENTS



LE BUT DE LA GESTION DES INCIDENTS EST DE RENDRE LE SERVICE DISPONIBLE, EN UTILISANT ÉVENTUELLEMENT UNE SOLUTION DE CONTOURNEMENT.

La gestion des incidents

Quelles que soient la qualité du système d'information mis en place dans l'entreprise ou les compétences des techniciens qui l'exploitent, des incidents se produiront. Ces incidents ont toujours un effet important sur la confiance que les utilisateurs accordent à l'équipe qui gère ce système d'information. La manière de gérer ces « crises » et la rapidité de leur résolution est un révélateur de la maturité de l'équipe informatique. C'est pourquoi l'implantation du processus de gestion des incidents, véritable fer de lance du centre de services, est particulièrement importante.

Vue d'ensemble

Selon ITIL, un incident peut être défini comme tout événement ne faisant pas partie du fonctionnement normal d'un service (ou d'un équipement) et qui cause ou peut causer une interruption du service ou une altération de sa qualité.

En conséquence, le but principal de la gestion des incidents est de rétablir le fonctionnement normal du service aussi vite que possible et d'en minimiser l'impact pour l'entreprise, tout en assurant le meilleur niveau de disponibilité et de service possible, tel qu'il est défini dans le contrat de services (SLA).

Il s'agit donc de traiter les conséquences et non les causes...

Pourquoi une gestion des incidents ?

Dans un système de support non géré, la fréquence des interruptions est un facteur particulièrement déstabilisant pour les membres de l'équipe technique, ce qui entraîne une baisse d'efficacité. Cette conséquence est aussi largement constatée chez les utilisateurs qui, lorsqu'ils ne trouvent

pas de techniciens pour les aider, ont recours à leurs collègues et les interrompent régulièrement avec les mêmes effets sur la productivité.

De plus, si personne ne gère les incidents, personne n'est en mesure de mettre en place un système d'escalade afin d'éviter qu'un incident mineur au départ ne devienne plus critique et n'affecte la qualité de service.

Lorsque la solution à un incident est connue d'un technicien, si un autre membre de l'équipe est sollicité pour le résoudre, il est possible qu'il lui soit nécessaire de reprendre tout le processus de recherche avant d'arriver à la résolution au lieu de profiter de l'expérience de son collègue.

Tous ces éléments permettent de conclure que la gestion des incidents au sens ITIL a plusieurs avantages. En évitant la dispersion des techniciens sans contrôle et en leur évitant de gérer les utilisateurs en frontal, ce processus permet d'optimiser l'utilisation des ressources matérielles et humaines impliquées dans le processus de support. Cela permet également de garantir qu'un suivi efficace des incidents est réalisé, et qu'un historique des incidents et de leurs solutions permet de capitaliser et de partager l'expérience des différents techniciens. Enfin, la mise en place d'une gestion formelle des incidents permet de développer et d'appliquer une approche systématique du traitement des incidents, et d'éviter la perte d'incidents...

Comme exemples d'incident, on peut signaler la panne de matériel, l'indisponibilité d'une application, un ralentissement du réseau, ou un manque d'espace disque. Mais tous ces incidents renvoient à des dysfonctionnements ou des non-respects du niveau de service négocié avec l'utilisateur.

Dans la pratique, on considère également que toutes les demandes concernant la mise en place d'un nouveau service, d'une application, d'un matériel ou même les demandes concernant l'évolution de ce service, ainsi que toutes les demandes d'assistance simple, de formation ou autres, sont en fait des incidents et doivent être traités comme tel.

Concepts

La plupart des membres de l'équipe informatique participent à la prise en charge des incidents ou au contrôle des étapes de leur résolution. Mais dans les faits, c'est bien le centre de services qui assume la responsabilité de tous les incidents.

Comme signalé plus haut, le but de la gestion des incidents est de rendre disponible le service le plus rapidement possible. Ainsi, lorsque l'incident est déclaré au centre de services, l'équipe en charge de la résolution doit identifier si possible les causes de l'incident en faisant usage de la base de connaissances afin de trouver une solution.

Si l'incident ne peut être résolu rapidement par l'utilisation d'une solution définitive ou par un moyen de contournement, l'incident doit être transféré au niveau de support supérieur.

Une fois l'incident résolu et après restauration du service dans les termes du niveau de service négocié avec les utilisateurs (SLA), l'incident est considéré comme terminé, et son statut est donc mis à jour dans la base (CMDB).

Le statut d'un incident indique sa position dans le flux des traitements. Cette indication est communiquée à toutes les personnes concernées par cet incident. Aussi, est-il indispensable que chacun utilise le même vocabulaire avec des termes comme « nouveau, planifié, assigné, résolu ou fermé » et comprenne l'implication de la situation d'un incident en fonction de son statut.

Lors de la gestion de l'incident, il est important que le dossier de l'incident soit conservé afin que n'importe quel membre de l'équipe de service puisse fournir à un client un compte rendu à jour avec les détails des actions et de leurs résultats, du temps passé, des éventuelles procédures d'escalades, etc.

Lors de l'audit d'un incident, et surtout dans le cas d'une rupture du SLA, il est indispensable de pouvoir auditer les événements qui se sont produits sur la base du support. Afin de réaliser cet audit dans les meilleures conditions, plusieurs informations doivent être consignées dans la fiche de l'incident. Il est indispensable de pouvoir identifier les éventuelles modifications apportées à cette fiche lors des différentes interventions des techniciens. En particulier, on s'attend à trouver le nom de la personne ainsi que la date et l'heure de la modification. Mais on souhaite également savoir ce que la personne a modifié, le temps qu'elle y a consacré et la raison de cette modification.

Les différents niveaux d'escalade

Le premier niveau de résolution des incidents est le centre de services. Si celui-ci ne parvient pas à résoudre rapidement un incident, une procédure d'escalade est engagée. Cette procédure correspond au transfert de l'incident à un niveau de support supérieur (second, troisième niveau, etc.) composé de spécialistes qui disposent de plus de compétences et de temps pour trouver une solution au dysfonctionnement.

Ce type d'escalade « fonctionnelle » permet de disposer de plus de ressource dans la résolution de l'incident. Mais il existe également une escalade « hiérarchique » qui est activée lorsqu'une décision doit être prise concernant la résolution d'un incident, et en particulier lorsqu'il est nécessaire de faire intervenir une ressource externe.

Établissement des priorités

La gestion d'incident demande la mise en place d'un système d'ordonnancement basé sur un critère de priorité. Celui-ci est calculé en fonction de deux éléments qui sont l'urgence et l'impact.

L'urgence est une évaluation de la criticité de l'incident par rapport à l'activité de l'utilisateur et reflète la rapidité nécessaire à la résolution d'un incident.

L'impact concerne davantage le volume et l'ampleur de l'incident sur l'entreprise. On le mesure en général en exprimant le nombre d'utilisateurs ou le nombre de systèmes touchés par un dysfonctionnement. L'utilisation de la base CMDB permet de calculer plus efficacement l'impact d'un incident sur le système d'information, puisqu'elle recense le nombre d'utilisateurs d'une application, d'un matériel ou d'un service.

Lorsqu'un incident présente un impact majeur pour un grand nombre d'utilisateurs, on considère qu'il s'agit d'un incident majeur. Dans ce cas, une réunion spéciale est mise en place par l'équipe de la gestion des incidents avec la participation de toutes les personnes, en interne et en particulier des autres processus comme la gestion des problèmes ou provenant des fournisseurs extérieurs, susceptibles d'aider à rétablir la situation.

Périmètre

Le centre de services a le rôle central dans le processus de gestion des incidents.

Son rôle va de la détection et l'enregistrement des incidents à la surveillance de leur évolution. Le centre a également la responsabilité du classement de tous les incidents et distribue les tâches aux différents techniciens. Les membres du centre de services peuvent parfois s'occuper également du support initial de premier niveau, en s'appuyant sur la base de connaissances et les solutions identifiées (CMDB).

Pour les problèmes non résolus, les techniciens ont alors la mission de réaliser la recherche et le diagnostic de l'incident en vue de lancer la résolution de celui-ci et la reprise du service.

Après clôture de l'incident, le centre de services doit s'assurer de la mise à jour de la base de données CMDB et doit prévenir l'utilisateur du résultat des actions menées par les techniciens.

Terminologie

Très souvent, la cause d'un incident est apparente et peut être traitée immédiatement (exemple : plus de papier dans l'imprimante), mais il arrive parfois que cette cause ne soit pas identifiable simplement. Dans ce cas, une solution de contournement peut être proposée à l'utilisateur (exemple : relancer l'ordinateur en cas d'erreur). Celle-ci permet de rendre le service disponible, mais ne résout pas le problème qui a de grandes chances de se représenter.

On définit alors le vocabulaire suivant :

Un *problème* est la cause inconnue d'un ou plusieurs incidents.

Une *erreur connue* est un problème dont les symptômes sont identifiés mais pour lequel aucune solution définitive ne s'applique, autre qu'une solution palliative permettant de rendre le service de nouveau disponible, ou lorsqu'une solution définitive est identifiée mais que la mise en place de la demande de changement n'est pas encore réalisée.

Une *demande de changement* ou RFC (Request For Change), correspond à la demande de mise en place de la solution à un problème sur un composant ou un service du système d'information. Celle-ci est examinée par le processus de gestion du changement avant mise en œuvre.



Figure 5-1 : Relation entre les incidents, les problèmes et les erreurs connues

Comme l'illustre la figure 5-1, si aucune solution immédiate n'est possible, la gestion des incidents fait appel à la gestion des problèmes. Cette action qu'il ne faut pas confondre avec le système de l'*escalade* décrit plus avant, permet de modifier le flux du traitement de la défaillance en l'identification du problème, la recherche d'une solution palliative qui transforme le problème en erreur connue, puis la mise en place d'une demande de changement. Une fois la demande de changement appliquée sur le système d'information, la solution doit être enregistrée dans la base de connaissances (CMDB) et l'incident peut être corrigé définitivement.

Lorsqu'un nouvel incident est signalé, il doit être comparé aux incidents, problèmes et erreurs connues répertoriés dans la base. Les solutions de contournement disponibles sont appliquées afin d'apporter la résolution la plus rapide de l'incident.

Cette base de connaissances doit être maintenue à jour régulièrement afin de ne conserver que les enregistrements qui apportent une valeur ajoutée au centre de services.

Description du processus

Flux du processus

Comme l'illustrent les figures 5-2 et 5-3, après détection ou déclaration de l'incident, le centre de services débute son action par l'enregistrement du contexte de l'événement (symptômes, premier diagnostic, information sur l'utilisateur et la configuration). Ces premiers éléments permettent entre autres de déterminer si cet incident s'est déjà produit et s'il s'agit d'une

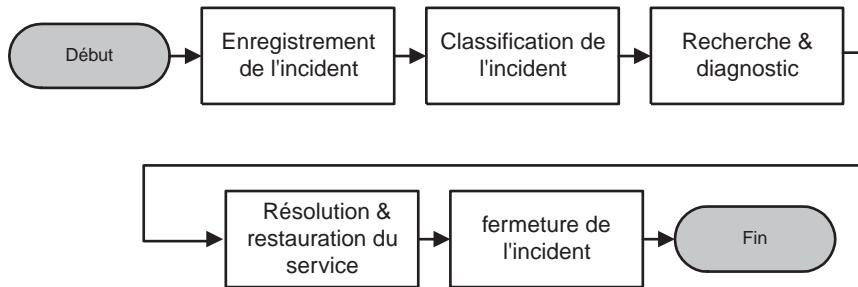


Figure 5-2 : Flux simplifié du processus de gestion des incidents

erreur connue avec une solution palliative, ou éventuellement une solution au sein de la CMDB. Dans ce cas, l'utilisation de cette solution permet de gagner un temps considérable.

L'étape suivante consiste à évaluer la priorité qui va être associée à l'incident en fonction de l'urgence de la situation et de l'impact sur le système d'information. Celle-ci va déterminer les ressources qui seront attribuées à la résolution.

La résolution de l'incident peut très bien se faire dès les premiers instants par le premier niveau en utilisant la base de connaissances et de configuration (CMDB) dans laquelle se trouvent des informations sur les incidents du même type, les erreurs connues et leurs solutions palliatives ou encore des solutions définitives. En l'absence de solution, une priorité de traitement est déterminée et on détermine les compétences nécessaires pour résoudre le dysfonctionnement. Ensuite, si nécessaire, un technicien se voit attribuer le traitement de l'incident sur le site incriminé.

Lorsqu'un problème sans solution est identifié par le technicien, le centre de services communique l'information à l'équipe de gestion des problèmes.

Même si la responsabilité de la résolution a été transférée à un autre groupe de spécialistes, le centre de services garde la responsabilité de l'incident et doit le gérer jusqu'à sa clôture et la satisfaction du client.

Après avoir identifié une solution à l'incident, celle-ci est appliquée en vue de résoudre le dysfonctionnement, puis une éventuelle restauration des données est démarrée afin de rendre le service de nouveau disponible.

Lorsque l'incident est résolu, avec l'accord de l'utilisateur, le centre de services doit clôturer l'intervention et s'assurer que le rapport d'incident est correctement rempli avec le détail des actions et de la solution mise en œuvre, le temps passé et les coûts associés.

Cet événement est sensible puisqu'il détermine l'instant où l'utilisateur est censé être satisfait. Dans les faits, il arrive que celui-ci ne perçoive pas la situation de la même façon. S'ensuit alors une négociation entre

La classification est certainement la phase la plus importante de la gestion des incidents. Elle permet de déterminer quel est le service, l'application ou le matériel impliqué, les personnes touchées et ainsi d'appréhender l'ampleur, donc l'impact de l'incident. En disposant des informations du contrat de services, la classification permet de préciser les délais de restitution garantis et les fonctions prioritaires. La classification permet également de préciser les ressources nécessaires lors de l'investigation en vue de résoudre cet incident, et en particulier les spécialistes qu'il convient de mobiliser.

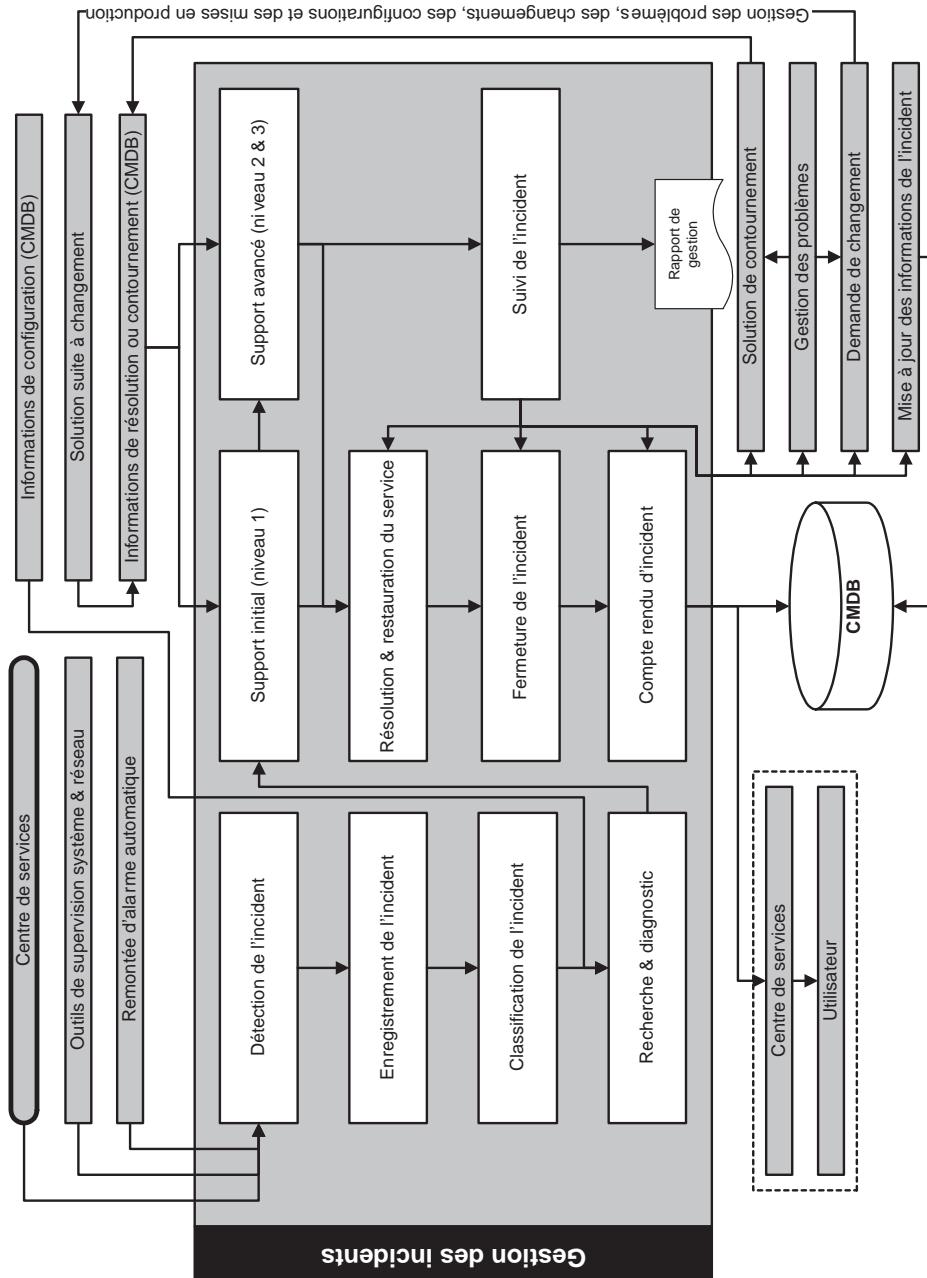


Figure 5-3 : Activités de la gestion des incidents

l'utilisateur et le centre de services avec une éventuelle réouverture de l'incident.

Le centre de services assume la responsabilité de la gestion des incidents et doit en conséquence contrôler le déroulement de leurs résolutions tout en informant l'utilisateur. Ce contrôle doit s'effectuer en surveillant le statut et la progression de chaque incident ouvert, et en particulier ceux qui transittent entre plusieurs groupes de spécialistes afin d'éviter l'effet « ping-pong ».

Comme on a pu le voir précédemment, deux modes de gestion peuvent coexister dans le traitement des incidents. Le premier correspond au principe d'escalade. Si un incident ne parvient pas à être réglé rapidement, et lorsque l'on craint de dépasser le délai négocié du SLA, il est indispensable de changer le statut de cet incident afin de lancer la procédure d'escalade (fonctionnelle ou hiérarchique). Ce type de traitement ne doit pas être confondu avec la gestion des problèmes qui prend en compte le coté récurrent d'un incident. Dans ce cas, lorsque la résolution d'un dysfonctionnement impose un changement dans la configuration, il peut être nécessaire d'imaginer une solution de contournement. Cette solution de contournement doit alors être examinée par le processus de gestion des problèmes, puis approuvée avant sa mise en œuvre, sans oublier de mettre à jour la base CMDB afin que tous les techniciens aient connaissance de cette nouvelle solution, même s'il ne s'agit que d'un palliatif.

Si aucune solution n'est trouvée pour un incident, il se peut qu'il soit nécessaire de rencontrer plusieurs fois ce dysfonctionnement avant d'identifier un problème.

Planification et mise en œuvre

La mise en place d'un processus de gestion des incidents ne peut se faire sans la présence d'un centre de services. Mais au-delà de ce centre, la mise en place des autres processus de support, comme la gestion des problèmes, la gestion du changement et la gestion des configurations, est indispensable. Cependant, la gestion des incidents est le processus qui offre le meilleur retour sur investissement, ce qui est loin d'être négligeable lorsque son implantation donne lieu à quelques grincements de dents. La mise en place d'un centre de services et de la gestion des incidents peut prendre plusieurs mois. Aussi on aura tout intérêt à prévoir la création de ce centre dès le début d'un gros projet informatique, afin que l'importance du centre croisse avec celle du projet, avant de revenir à un équilibre raisonnable.

Améliorations

Des améliorations peuvent être obtenues par la formation des techniciens « classiques » dans le but de leur faire prendre conscience de leur rôle auprès des utilisateurs.

Des améliorations peuvent également provenir de la mise à jour régulière de la base de gestion des configurations (CMDB), et de la base de données des connaissances, permettant de recouper les informations concernant les erreurs connues, leurs résolutions et les solutions de contournement.

Une application informatique de gestion des incidents est indispensable. Il existe désormais des outils de support automatiques et efficaces disposant de systèmes experts pour la classification des incidents, mais également de procédure d'escalade automatique, de base de connaissances sur les incidents et leurs solutions.

Mesures et contrôles

Les métriques que l'on peut mettre en place pour valider l'efficacité du processus proviennent essentiellement du centre de services et concernent le nombre et la durée des incidents, leurs impacts sur le système d'information, et le ratio entre incidents résolus au premier niveau et ceux qui ont été transférés vers les supports de niveaux 2 et 3.

Documents et rapports de gestion

À l'instar des rapports du centre de services dont ils proviennent, les rapports de gestion doivent s'adresser à plusieurs publics tels que les responsables des directions fonctionnelles, les membres de la direction générale, les responsables de l'informatique, mais également les représentants des utilisateurs eux-mêmes.

Conséquences

Les conséquences générées par la gestion des incidents sont multiples et agissent sur plusieurs niveaux de l'entreprise. D'un point de vue général, on constate une réduction de l'impact des incidents par la rapidité de la résolution, ainsi que par la détection proactive de ces incidents, ou par les améliorations qui devraient être appliquées afin de les éviter. De plus, on dispose à présent d'informations plus orientées gestion et portant sur les niveaux de SLA qui vont permettre par la suite de valider l'efficacité du processus et son adéquation avec le métier de l'entreprise. Au niveau de l'organisation de support, les avantages sont plus liés aux gains en efficacité de l'équipe technique du fait de l'utilisation plus rationnelle des ressources, de la capitalisation de l'expérience de chacun, mais également par la réduction des interruptions individuelles des techniciens sollicités en direct dans les couloirs. On constate également une nette diminution puis l'élimination totale des pertes de demandes des utilisateurs, ce qui se produisait inévitablement lors de la génération Post-it !

Mais ces avantages sont également liés à la qualité des informations qui composent désormais la base de connaissances du service (CMDB), ce qui

permet sans nul doute de valider plus efficacement les éléments communiqués par l'utilisateur lors de la déclaration de l'incident, puis d'accélérer la recherche d'information sur la configuration incriminée. Cette base de connaissances procure ensuite une documentation indispensable à la capitalisation de l'expérience des techniciens.

Enfin, et c'est certainement le plus important, de tout ceci découle une plus grande satisfaction des utilisateurs.

Malheureusement, avant d'arriver à cette situation idyllique, plusieurs écueils sont fréquemment rencontrés. Le plus classique d'entre eux est sans nul doute la résistance au changement qui montre systématiquement son visage dès l'installation d'un nouveau processus. Dans le cas de la gestion des incidents, cette résistance au changement est fortement liée à l'implantation du centre de services. La conséquence immédiate peut s'exprimer par une désaffection des utilisateurs qui refusent d'utiliser le service en essayant de contacter directement les techniciens. Mais cette situation peut aussi naître au sein du personnel informatique qui décide d'ignorer le processus et de continuer à agir comme auparavant.

Un contrat de services (SLA) non exprimé, traduit un manque de clarté dans l'expression des besoins.

Le manque d'engagement de la direction entraîne souvent un manque de moyen (ressources humaines, formation, outils). Ce manque se traduit invariablement par un niveau insuffisant de la capacité du processus.

Il existe encore des entreprises dont le seul outil informatique de gestion des services informatiques est une feuille de calcul. Dans le cas d'une PME, cela peut éventuellement suffire, mais en réalité, ce type de solution n'est pas suffisant, car il ne fait que calquer une organisation de type formulaire papier et n'apporte pas les fonctions indispensables comme la gestion des configurations, la gestion des connaissances ou autre. Évidemment, il faut éviter d'équiper une petite structure d'un logiciel et d'un matériel hors de coût, car cela rendrait difficile la justification du retour sur investissement. Cependant, un minimum « vital » est indispensable.

Outils

Le processus de gestion des incidents étant très fortement lié au centre de services, ses outils le sont également. L'application de gestion du centre de services est utilisée comme point de départ à toutes les interventions nécessaires à la résolution des incidents. Pour s'assurer de l'efficacité du processus, on peut simplement mettre l'accent sur certains points.

Un premier type d'outil simple à mettre en place concerne l'escalade automatique qui doit s'activer en fonction d'un délai au-delà duquel l'équipe n'a pas apporté de réponse.

La détection automatique d'incident et l'envoi d'alertes concernant les ordinateurs, réseaux, applications et services du système d'information, sont également très efficaces, puisqu'ils permettent d'être averti d'un problème très rapidement, et au moins en même temps que l'utilisateur.

La recherche et l'extraction des données de la base de connaissances et de configurations CMDB doivent être systématiquement réalisées vers la fiche d'incident, afin d'apporter le plus d'information au technicien.

Enfin, l'accès banalisé et rapide à l'application de gestion des incidents (exemple : accès client Web/intranet) permet au technicien de remplir ses rapports d'intervention immédiatement, et d'accéder à sa file d'attente d'incidents sans avoir à revenir à son bureau.

Rôles et responsabilités

Responsable

Dans la plupart des entreprises, le responsable de la gestion des incidents est très logiquement le responsable du centre de services. Son premier rôle est de gérer l'équipe technique et en particulier la répartition des tâches au sein de cette équipe. Il doit également mesurer l'efficacité de son organisation et proposer des améliorations. Enfin il doit concevoir et produire les rapports destinés à la direction et aux utilisateurs.

Du point de vue de ses compétences, il s'agit là d'une personne méthodique, aimant le contact humain et la gestion d'une équipe sous pression, et dotée d'un sens aigu de la diplomatie. En fonction de l'importance de l'équipe, la compétence technique n'est pas indispensable, mais constitue un atout utile dans l'animation et le management de l'équipe.

Équipe

Les membres de l'équipe de support ont pour rôle de traiter, résoudre puis clôturer les incidents qui leurs sont soumis, le plus rapidement possible. Si l'incident n'est pas de sa compétence ou la dépasse, le technicien doit être en mesure d'identifier la personne appropriée afin de rapidement lui affecter l'incident ou, à défaut de le transmettre au niveau supérieur adapté.

Méthodique, techniquement compétent, appréciant le contact humain et sachant garder son calme, le profil du technicien de support n'est pas toujours simple à trouver. Faire l'impasse sur ce genre de recrutement n'est pas une bonne méthode pour assurer l'efficacité de la gestion des incidents. De plus, il faut garder à l'esprit que cette équipe est souvent le principal interlocuteur entre le service informatique et les utilisateurs. La perception que ces derniers ont des techniciens contribue largement à l'impression globale que donne le service informatique et par conséquent à son image auprès de la direction.

GESTION DES PROBLÈMES



LA GESTION DES PROBLÈMES, C'EST L'IDENTIFICATION DE LA CAUSE FONDAMENTALE D'UN INCIDENT, PUIS LA PROPOSITION D'UNE SOLUTION DÉFINITIVE OU DE CONTOURNEMENT.

La gestion des problèmes

Les incidents se succèdent, toujours les mêmes. Des petits désagréments la plupart du temps, mais qui finissent par pourrir la vie. Toute l'équipe informatique se mobilise pour régler ces dysfonctionnements, mais malgré l'efficacité de ses membres, le niveau de service ne s'améliore pas ! Les utilisateurs manifestent leur mécontentement... La révolte gronde !

Vue d'ensemble

Le but de la gestion des problèmes est de minimiser les conséquences des dysfonctionnements qui se produisent sur le système d'information en identifiant les causes sous-jacentes afin d'éviter qu'ils ne se reproduisent. À la différence de la gestion des incidents qui agit pour résoudre le plus rapidement possible ou trouver un palliatif, la gestion des problèmes doit s'attacher à identifier les causes réelles des dysfonctionnements, puis à proposer les changements éventuels qui permettraient de les corriger.

Le processus de la gestion des problèmes permet de trouver des solutions aux problèmes issus d'incidents déjà signalés au centre de services : c'est son côté réactif. Mais il présente également un côté proactif, puisqu'il permet d'identifier des problèmes potentiels et de les résoudre avant qu'ils ne se produisent. Malheureusement, ces objectifs peuvent donner lieu à quelques conflits de priorité puisque nous avons d'une part un souci de rapidité, et d'autre part un souci d'exhaustivité.

But et mission

La mission principale de ce processus est de résoudre définitivement et si possible rapidement les problèmes et en particulier ceux qui provoquent des incidents récurrents. Mais on comprend bien par ces mots que l'objectif

de la gestion des problèmes est d'identifier les causes plus que de rétablir la disponibilité du service. De ce point de vue, il ressort que la vitesse d'identification des causes et la proposition des solutions ne sont pas limitées par le temps. Cela a évidemment des conséquences sur la disponibilité du service et peut entraîner la rupture du contrat de niveau de service, mais cela permet également d'empêcher qu'un incident ne se reproduise une fois la solution mise en œuvre.

Le travail de fond mené lors des investigations permet aussi d'identifier et de résoudre des problèmes ou des erreurs connues avant qu'ils ne provoquent de nouveaux incidents. Un disque dur défaillant sur un serveur peut, par exemple, être la cause de multiples pertes de fichiers pour les utilisateurs. Dans ce cas, la technologie peut aider en signalant la future défaillance du disque avant que les pertes ne soient signalées par les utilisateurs. Mais là, on comprend bien que c'est l'action du processus de gestion des problèmes qui peut repérer ce genre de situation, la gestion des incidents devant uniquement rendre de nouveau disponibles les fichiers perdus.

Le rôle de la gestion des problèmes prend en compte les priorités qui correspondent aux besoins de l'entreprise.

Identifier les causes réelles d'un incident permet de réduire le volume des incidents, et en particulier les incidents récurrents, en proposant une solution définitive. Cela permet également aux techniciens de la gestion des problèmes, comme à ceux de la gestion des incidents, de gagner en compétence par la capitalisation des expériences de chacun, et permet ainsi d'entrer dans un cycle d'amélioration continue de la qualité du service informatique.

Une autre conséquence intéressante pour le centre de services est que l'on constate une amélioration des résolutions d'incidents dès le premier niveau.

En revanche, ne pas implémenter de gestion des problèmes peut entraîner des conséquences plus diffuses, mais désastreuses, pour l'image de l'équipe informatique. En effet, une organisation uniquement basée sur la réactivité n'a pas toujours le temps d'isoler les causes réelles d'un incident récurrent. En conséquence, les utilisateurs perdent confiance devant le peu d'efficacité de l'équipe informatique à éradiquer les causes de ces incidents. Ce manque de confiance se manifeste également au sein des membres de l'équipe technique et on voit naître une perte de motivation de l'équipe informatique.

Concepts

La gestion des problèmes est destinée à réduire le nombre et l'impact des incidents qui se produisent sur le système d'information et perturbent le fonctionnement de l'entreprise. Mais la valeur ajoutée de ce processus réside pour beaucoup dans la documentation créée par la recherche et l'identification des causes et de leurs solutions. Cette documentation doit être

accessible et compréhensible par des techniciens non-spécialistes, ainsi que par les membres du centre de services afin de leur permettre de résoudre un grand nombre de dysfonctionnements dès le premier appel.

Les problèmes et erreurs connues peuvent être identifiés par l'analyse des incidents lorsqu'ils se produisent (mode réactif), ou lors de l'analyse d'un ensemble d'incidents afin d'en retirer des tendances ou des modèles (mode proactif). L'analyse de l'infrastructure du système d'information, ainsi que l'étude des rapports fournis par la gestion des incidents, donnent également d'excellents résultats dans ces investigations. Sans oublier la mise en place d'une base de connaissances qui permet de recouper des événements et des symptômes communs à plusieurs incidents successifs.

Afin de trouver des solutions définitives aux problèmes, plusieurs étapes peuvent s'avérer nécessaires. La première d'entre elles consiste à faire évoluer un problème en erreur connue par l'identification de l'origine du dysfonctionnement sans pour autant trouver de solution définitive. La seconde étape correspond à la découverte d'une solution qui peut parfois donner lieu à une demande de changement ou RfC (*Request For Change*). Celle-ci doit être justifiable au niveau budgétaire. En effet, une solution de contournement peut devenir définitive si le changement envisagé pour corriger le problème ajoute un coût trop important au système.

La gestion des problèmes est très étroitement liée à la gestion des incidents dont elle reprend un grand nombre d'informations concernant l'incident. Parmi ces données, on retrouve en particulier les éléments de configuration (CI) impliqués dans l'incident. Ceci permet, par exemple, de déterminer si ces éléments ont des liens avec des erreurs connues impliquant le même type d'élément. La coopération entre les deux processus ne se limite pas à cela puisque la solution au problème sera communiquée au centre de services, et donc à la gestion des incidents, lorsqu'elle sera identifiée.

La nécessité de prévenir les incidents avant qu'ils ne se produisent implique l'utilisation de méthodes de répartition et d'organisation des tâches et l'utilisation d'une planification rigoureuse.

Périmètre

Les activités principales de la gestion des problèmes sont le contrôle des problèmes, le contrôle des erreurs, la prévention des problèmes, l'identification des tendances, la production d'informations de gestion à destination du centre de services, et la tenue de réunions de revue des problèmes majeurs.

Le contrôle des problèmes (figure 6-1) correspond à l'étape d'identification et d'enregistrement du problème, à sa classification (type, priorité, etc.), puis à la recherche de la cause du dysfonctionnement. Il s'agit de l'évolution du problème en erreur connue.

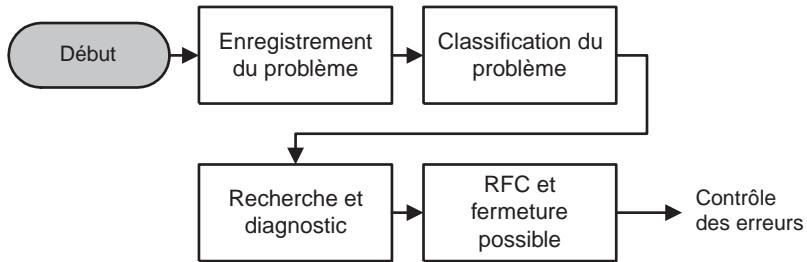


Figure 6-1 : Schéma simplifié du contrôle des problèmes

Le contrôle des erreurs (figure 6-2) correspond, quant à lui, à l'étape d'identification et d'enregistrement, d'évaluation, puis de résolution de ces erreurs. Une communication de la solution vers le centre de services est engagée afin de pouvoir renseigner les détails dans la base de connaissances CMDB.

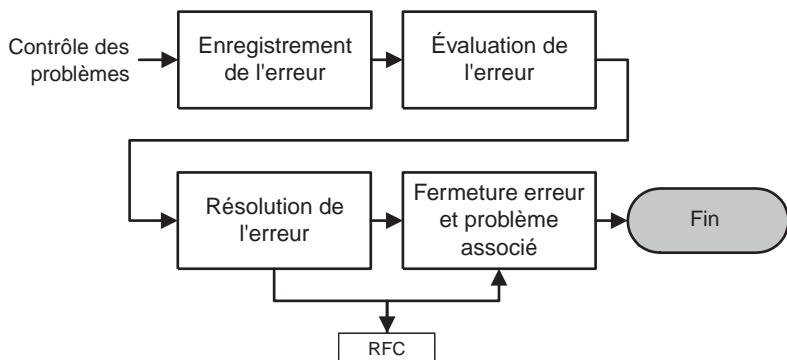


Figure 6-2 : Schéma simplifié du contrôle des erreurs

La prévention des problèmes est une conséquence des recherches de résolution des problèmes précédents, des analyses de tendance, des outils d'alerte proactive qui indiquent le potentiel de panne d'un équipement, et de l'analyse de l'architecture du système d'information, et en particulier des informations concernant le matériel, le logiciel, l'architecture et les services, c'est-à-dire les éléments de configuration (CI).

Terminologie

Un problème est la cause sous-jacente inconnue d'un ou plusieurs incidents. Il devient une erreur connue lorsque la cause à l'origine de ce problème est connue et une solution de contournement provisoire ou permanente a été identifiée. (voir : Gestion des incidents)

Description du processus

Flux du processus

Malgré les progrès réalisés par la technologie, les défaillances aléatoires qui se présentent sur certains équipements informatiques sont inévitables. Néanmoins, on s'aperçoit qu'un grand nombre des dysfonctionnements que subit un système d'information ne sont pas tous aléatoires, mais proviennent bien d'erreurs situées quelque part dans l'architecture complexe du système d'information. Le constat est évident, il est indispensable de mettre en place un processus de recherche et d'identification de ces problèmes afin de leur apporter une solution définitive.

Comme on peut le voir sur la figure 6-3, le processus de gestion des problème est divisé en trois activités principales. Le contrôle des problèmes et le contrôle des erreurs qui représentent un aspect plus réactif et enfin la gestion plus proactive qui tente de prévenir l'apparition de dysfonctionnements.

Le contrôle « réactif » des problèmes doit identifier les causes d'un problème révélé par un ou plusieurs incidents. Le but étant de fournir le plus rapidement possible une solution à mettre en œuvre afin d'éviter les futurs incidents. Le contrôle des problèmes correspond à trois phases qui sont l'identification et l'enregistrement du problème, sa classification, et enfin la recherche proprement dite de la solution.

Le contrôle plus « proactif » des problèmes réside essentiellement dans l'analyse des données des incidents. Elle permet d'identifier la récurrence de certains d'entre eux ou le fait qu'ils n'aient pas encore fait l'objet d'investigations permettant de les rapprocher de problèmes existants ou d'erreurs connues. Cette étude des données doit être complétée d'une analyse de l'infrastructure informatique.

Il est important de signaler que les membres de l'équipe de gestion des problèmes ne sont pas les seuls à pouvoir les identifier. Certains dysfonctionnements ou non-respect des engagements de service peuvent être identifiés par d'autres processus tels que la gestion de la capacité, la gestion de la disponibilité, etc.

En dehors des informations spécifiques à l'utilisateur, les données que l'on stocke dans la base CMDB lors de l'enregistrement des problèmes, sont très similaires à celles des incidents. Cela facilite alors la mise en place de liens entre le problème et les incidents qui s'y rapportent. On y retrouve en particulier les données sur les éléments de configuration (CI).

La classification des problèmes est une fonction de plusieurs paramètres parmi lesquels on trouve notamment, le type de problème (logiciel, matériel, service, etc.), l'urgence, l'impact de ce problème sur le système d'information et donc la priorité associée, mais également l'évaluation des efforts à fournir pour identifier l'élément (CI) impliqué dans ce problème ainsi que l'effort pour le remettre en fonctionnement.

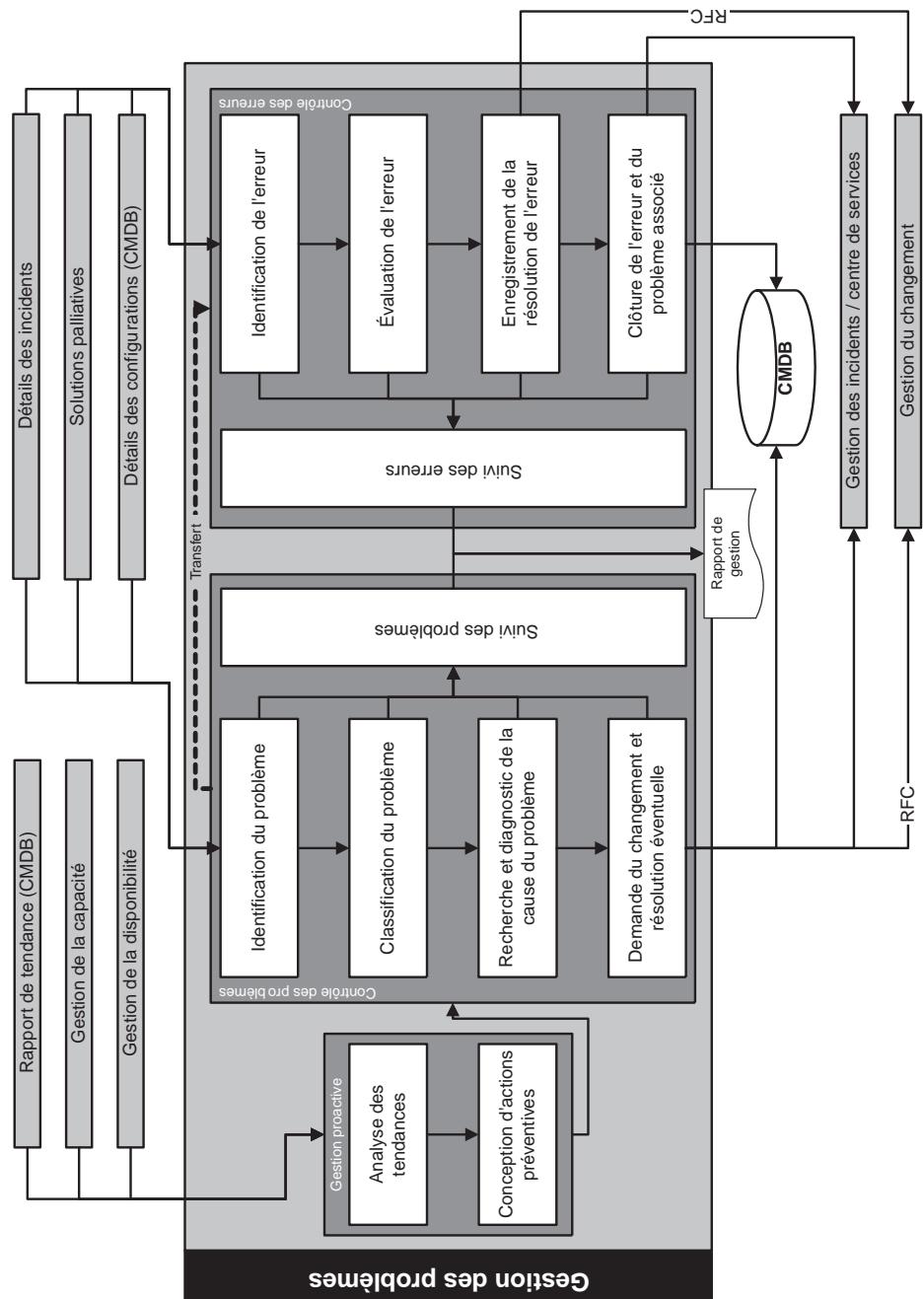


Figure 6-3 : Activités du processus de la gestion des problèmes

À l'instar de la gestion des incidents, les relations et les dépendances entre les différents éléments qui composent le système (CI) prennent toute leur importance lorsque l'on veut déterminer l'impact du problème. La CMDB démontre une fois de plus son importance dans la perception des problèmes dans leur globalité, et dans l'évaluation de l'impact sur le système d'information.

Le caractère d'urgence est vu dans une perspective différente de celle de la gestion des incidents. Comme ici, le but n'est pas de rendre le service opérationnel, la pression du chronomètre n'est pas la même. Il est clair que l'existence d'un correctif temporaire ou d'une solution de contournement relativise largement l'urgence d'un problème. C'est donc ailleurs qu'il faut chercher les critères composant le caractère d'urgence de la résolution d'un problème. Parmi ces critères se trouvent notamment la possibilité d'intervention planifiée sur le système d'information, la précarité de la solution de contournement et également l'impact sur l'activité économique.

La recherche de l'origine d'un problème peut faire apparaître différentes causes à la situation. Dans certains cas, le problème ne met pas en cause un des éléments de configuration (CI) du système, mais plus une erreur dans la mise en place de cet élément ou dans l'application d'une procédure. C'est le cas, par exemple, lorsque la mauvaise version d'un logiciel est installée. Cependant, si ce cas peut être complexe à identifier, la solution semble assez simple à trouver. Mais il existe de nombreux cas où un des éléments (CI) est impliqué lorsque le problème est créé. Dans ce cas, la procédure d'investigation doit se poursuivre jusqu'à trouver une solution.

Les divergences d'intérêt entre la gestion des incidents et la gestion des problèmes tournent régulièrement autour du classement des priorités. C'est par exemple le cas lorsqu'un incident se produit et entraîne un blocage de la production. Le rôle de la gestion des incidents est de rendre le service disponible le plus rapidement possible. Malheureusement, la recherche des informations nécessaires à l'identification du problème exige de disposer d'un peu de temps pour recueillir les données issues du dysfonctionnement (exemple : vidage mémoire du serveur en erreur). Dans ce cas, la gestion des incidents va demander de relancer le service au plus vite, alors que la gestion des problèmes demande de conserver l'incident en état.

Il existe plusieurs méthodes permettant de structurer l'analyse des problèmes. Parmi celles-ci, ITIL recommande l'utilisation d'outils et de méthodes assez classiques comme l'approche de Kepner et Tregoe¹, ainsi que l'utilisation

1. **L'approche de Kepner-Tregoe** – du nom de ses créateurs en 1958 - est destinée à faciliter la résolution des problèmes et la prises de décisions par l'analyse des causes fondamentales d'un événement (*Root Cause Analysis*). C'est une approche formelle et systématique qui permet de résoudre les problèmes ou de prendre des décisions en écartant le plus possible les éléments subjectifs.

de diagramme Ishikawa¹, et la formalisation par des diagrammes de flux. L'utilisation d'équipes multidisciplinaires dans le cadre de réunions de type *brainstorming*, est une approche particulièrement efficace pour la résolution de problèmes complexes faisant intervenir plusieurs domaines.

Pour faciliter les recherches, il faut disposer des documentations du système, des applications, des services, de l'architecture, et du réseau. De plus, il faut disposer évidemment de la liste des changements récents effectués sur le système afin de valider qu'aucune régression n'est à l'origine du problème.

Il arrive fréquemment que les techniciens spécialistes soient impliqués dans les deux processus de gestion des incidents et des problèmes. Les responsables des deux domaines doivent s'entendre pour attribuer un ratio de participation à chacun des processus afin d'éviter que le processus de gestion des incidents n'utilise cette ressource qu'en mode « pompier ».

Planification et mise en œuvre

Du fait des relations étroites qui existent entre la gestion des problèmes et celle des incidents, le projet d'implantation de la gestion des problèmes gagnera à être mis en œuvre le plus tôt possible. Cette mise en œuvre pourra éventuellement être menée en parallèle avec la gestion des incidents, étroitement liée à la gestion des problèmes, ou immédiatement après la mise en œuvre de la gestion des incidents. Si les projets sont conduits en parallèle, un manque de ressource peut éventuellement être compensé en se concentrant sur le contrôle des problèmes et des erreurs en mode plus réactif et en remettant à plus tard la gestion proactive des problèmes. Lorsque l'ensemble des actions de contrôle du service sont en place et si les données de base sont présentes, le mode proactif peut être activé sans contrainte sur le processus.

De plus, et toujours dans le cas de ressources limitées, on peut sans conséquence grave se concentrer sur les problèmes les plus fréquents (top 10)

-
1. **Le diagramme d'Ishikawa** – du nom de son créateur japonais en 1943- ou diagramme en arête de poisson, est la représentation graphique des causes d'une erreur. Celles-ci sont représentées d'une manière hiérarchique. Au niveau supérieur on distingue cinq "domaines standards" de causes (5M), puis chacun de ces niveaux est développé jusqu'au niveau des causes élémentaires. Cette technique est utilisée pour comprendre un phénomène, un processus ; par exemple, les étapes de recherche de panne sur un équipement, en fonction du ou des symptômes.

La recherche des causes peut se faire selon les 5M: Main d'œuvre, Matière, Méthode, Machines (équipement), Milieu (environnement). On peut y ajouter deux autres « M » (7M) qui sont le Management et les Moyens financiers. Ces derniers constituent des facteurs intéressants, notamment dans les domaines immatériels comme les services, la gestion de projets ou le développement des logiciels.

L'utilisation de ce diagramme n'apporte pas directement de solutions, elle permet néanmoins de bien poser le problème.

qui sont souvent les plus pénibles pour l'entreprise. En effet, on retrouve souvent le ratio de 20 % des problèmes causant 80 % de la détérioration des services !

Attention cependant au fait que les bénéfices de la gestion des problèmes peuvent être atténués par l'absence de contrôle de la gestion des incidents et par l'absence des données qui en proviennent. Si ces dernières sont absentes, de mauvaise qualité ou en nombre trop restreint, l'identification du problème risque de se compliquer.

Améliorations

Les activités que nous avons pu décrire jusqu'à présent sont essentiellement réactives. Pour gagner en efficacité, l'équipe de gestion des problèmes doit s'attacher à traiter les problèmes de façon proactive. Plusieurs méthodes sont utilisables conjointement ou non pour parvenir à cet objectif. La première d'entre elle correspond à l'analyse des tendances sur la fiabilité des éléments de configuration (CI). Ces informations proviennent en grande partie des différents rapports techniques que l'on peut retrouver dans la CMDB, ou issus de la gestion de la capacité, de la gestion des incidents ou de la gestion de la disponibilité. Cette analyse permet d'identifier les éléments fragiles assez simplement et donc d'en déduire des comportements à l'échelle du système d'information. De cette analyse, on peut ensuite proposer des améliorations de l'architecture et des modifications de matériel. L'analyse des incidents récurrents sur un élément de configuration (CI) ou un même type d'élément, permet également d'arriver aux mêmes conclusions, et lorsque le maillon faible a été identifié, il convient alors de le changer globalement. Mais pour ce faire, il est nécessaire de passer d'abord par une demande de changement (RFC) qui doit être avalisée par la gestion du changement.

Cette méthode permet d'ailleurs d'améliorer encore la gestion des problèmes puisqu'elle permet d'identifier les régressions après un changement.

L'analyse des informations liées aux incidents et aux problèmes permet également d'identifier le besoin de formation des utilisateurs, qui représente une des causes les plus fréquentes d'incidents récurrents.

L'analyse des données provenant de la gestion des incidents n'est pas tout. Désormais, de nombreux composants informatiques sont en mesure de communiquer leur état et même les défaillances internes (exemple : disque dur et raid). Mais on trouve également des informations très pertinentes dans les forums sur Internet, comme des rapports de bug ou des failles de sécurité sur un module logiciel.

L'analyse des tendances permet également d'identifier des domaines ou des technologies qui posent plus de problèmes dans le système d'information

et demandent donc plus de support et de ressources et donc des coûts plus importants.

On peut ainsi calculer la « valeur » d'un problème. En l'associant avec les notions d'urgence et d'impact, on peut ensuite déterminer l'ordonnancement des problèmes à résoudre. C'est également le critère idéal pour valider si un problème doit ou non être traité, et s'il est économiquement justifiable qu'il fasse l'objet d'une demande de changement.

Ce raisonnement permet d'éviter de se concentrer sur un problème qui prend en compte de nombreux incidents n'ayant qu'un impact réduit sur l'entreprise au détriment d'un problème moins « médiatisé » mais plus coûteux.

Une fois la solution identifiée, la gestion des problèmes doit encore proposer une demande de changement qui doit être validée. Elle doit également proposer un ensemble de modifications dans la documentation et dans la base CMDB concernant les changements envisagés. Il faut également prendre en compte l'éventuelle formation complémentaire qu'il convient de dispenser aux utilisateurs.

Mesures et contrôles

Les métriques utilisables dans la publication des rapports de gestion sont essentiellement issues de l'historique des interventions de la gestion des incidents et des problèmes. Elles permettent d'obtenir des statistiques assez fines concernant la qualité de service et l'efficacité du processus.

À l'image de la gestion des incidents, les indices qui seront utilisés ici reprennent des informations telles que le nombre de problèmes et d'erreurs identifiés, le nombre de demandes de changement exprimées et les corrections effectivement réalisées, et si possible, une estimation du gain en terme de disponibilité du système d'information, et éventuellement une estimation des coûts liés.

Documents et rapports

L'objectif des documents et rapports de ce processus est de fournir des informations sur les problèmes identifiés, les erreurs connues, et les demandes de changement afin d'évaluer les progrès réalisés dans le traitement de ces dysfonctionnements. Il s'agit donc de fournir des informations destinées au management afin d'évaluer l'efficacité du processus, mais également en vue de présenter des rapports de gestion vers les directions métier et les utilisateurs. Ces informations peuvent être communiquées vers le centre de services afin que celui-ci traite les informations et les utilise dans ses propres communications vers les utilisateurs.

Les rapports de gestion doivent donner des détails sur les ressources utilisées lors de la recherche, l'identification et la résolution des problèmes, ainsi

que d'éventuelles informations sur la progression de la résolution des problèmes en cours d'investigation. La communication des détails concernant les palliatifs, les corrections, ou les demandes de changement à destination du centre de services, est impérative afin que celui-ci puisse tenir l'utilisateur et le management au courant de la progression de la résolution.

La distribution de cette information aux différents destinataires est le rôle du centre de services. Le responsable du processus de gestion des problèmes doit uniquement fournir ces informations et le moyen de les interpréter.

Conséquences

L'implantation d'un processus de gestion des problèmes présente de nombreux avantages. Le premier qui vient à l'esprit est l'amélioration de la qualité de service. De plus, par effet boule de neige, grâce à l'apport de solutions permanentes, cette amélioration va aller en augmentant et va entraîner une réduction du volume d'incidents.

Cerise sur le gâteau, ces avantages profitent également à la gestion des incidents et au centre de services en permettant un meilleur taux de résolution des incidents dès le premier essai.

Enfin, ce type de gestion permet de ne plus agir dans l'urgence, et permet de se concentrer sur les événements réellement importants en prenant en compte les besoins de l'entreprise ainsi que les contraintes budgétaires.

En revanche, il ne faut pas éluder certains risques tels que le fait que ce processus soit perçu comme un « service support bis » qui dévalorise le rôle du centre de services et des membres de l'équipe de gestion des incidents. En effet, la présence de spécialistes au sein de l'équipe de gestion des problèmes peut faire naître un sentiment de hiérarchie entre les deux processus.

Pour finir, il faut prendre garde à ne pas relâcher l'attention concernant la saisie d'information et la maintenance de la base CMDB.

Rôles et responsabilités

Le responsable de la gestion des problèmes a pour rôle de développer et de maintenir le processus, tout en optimisant son efficacité, et de proposer des évolutions éventuelles pour améliorer son fonctionnement. Il doit également produire des informations de gestion destinées au centre de services et utiles à la mise en place de l'activité de production des rapports du centre. Ces informations sont également destinées à la direction du service et à la direction générale et servent à valider l'efficacité du processus.

Il a bien évidemment la responsabilité de gérer l'équipe technique d'un point de vue planning, allocation des ressources, etc.

Il est recommandé que le responsable du centre de services, qui est souvent le responsable de la gestion des incidents, n'assume pas en plus le rôle de responsable de la gestion des problèmes en raison des conflits d'intérêts¹.

1. Lorsqu'un serveur subit une défaillance qui provoque un long vidage de la mémoire sur le disque, le processus de gestion des incidents va demander d'interrompre ce *dump* mémoire en redémarrant la machine pour accélérer la reprise du service, alors que la gestion des problèmes souhaite que le vidage mémoire soit finalisé pour une analyse ultérieure...

GESTION DES CONFIGURATIONS



LA GESTION DES CONFIGURATIONS FOURNIT UNE IMAGE LOGIQUE
DE L'ÉTAT DU SYSTÈME ET PERMET DE LA MAINTENIR À JOUR.

La gestion des configurations

Dans une architecture informatique classique comprenant serveurs, périphériques, équipements réseaux, postes de travail et logiciels divers, qui peut dire en un instant quelle version du logiciel système est installée sur tel poste, ou de combien de mémoire dispose ce serveur, ou si la mise à jour de ce matériel réseau entraîne un risque pour le système d'information ? Personne ! Sauf le gestionnaire des configurations et sa base de données...

Vue d'ensemble

La gestion des configurations est le processus de documentation indispensable, utilisé par tous les autres processus d'ITIL, depuis la gestion des incidents, des problèmes et des changements en passant par la gestion de la disponibilité ou la gestion financière. En tant que base de référence, son but est de fournir la représentation la plus fidèle possible du système d'information et en particulier de son infrastructure en identifiant, en contrôlant, en maintenant à jour et en vérifiant les versions de tous les éléments de configuration existants.

Pourquoi ?

On imagine sans peine les difficultés que rencontre une entreprise qui ne gère pas son infrastructure ou même simplement le sous-ensemble que constitue son parc micro-informatique. Le simple ajout d'un équipement réseau peut rapidement tourner au cauchemar et que dire de la mise à jour du plus banal logiciel bureautique. Mais si l'on essaye de rechercher les causes d'un problème récurrent, cela devient impossible. La gestion des configurations facilite la réponse à cette problématique. En répertoriant les biens informatiques installés au sein du système d'information de l'entreprise

dans le but de fournir des informations précises, ce processus renseigne les autres processus de la gestion des services. Imaginons maintenant un système où chacun peut à loisir installer les logiciels et les matériels de son choix. Inutile d'expliquer les conséquences d'une telle politique sur la stabilité du système d'information de l'entreprise. Inutile même d'évoquer le risque que fait courir à l'entreprise une personne qui installe un logiciel piraté sur sa machine, engageant la responsabilité pénale du chef d'établissement ou du PDG...

La fourniture d'une production informatique de qualité au moindre coût exige le contrôle de l'infrastructure. La gestion des configurations peut en limiter la dérive et offrir une base solide à la gestion des incidents, des problèmes, des changements et des mises en production, puis permettre de vérifier les enregistrements des équipements dans la base par rapport à l'existant afin de corriger les anomalies.

Concepts

La gestion des configurations est une condition de l'efficacité de la gestion des changements grâce à la connaissance rapide de l'impact d'une évolution sur l'infrastructure. La mise en place de ce processus passe par un certain nombre d'activités de base dont il est préférable de ne pas faire l'économie.

La planification et la rédaction du cahier des charges du projet sont ici particulièrement importantes. C'est le moment où l'on va décider de l'ampleur que l'on souhaite donner à la base de connaissance du système d'information. La conséquence la plus importante de ces décisions concerne la granularité des informations associées à chaque élément de configuration ou Composant de l'Infrastructure (*Component Item : CI*). C'est également le moment où les procédures ainsi que les rôles de chacun seront édictés.

Nous verrons d'ailleurs par la suite qu'il faut éviter de se donner des objectifs trop ambitieux ou difficiles à suivre. Il ne faut pas trop attendre de la gestion des configurations au début, car le risque est grand de se décourager devant l'ampleur du travail pour aussi peu de résultat. Une des décisions importantes pour la suite est la définition du niveau de détail à trouver, ce qui correspond à l'équilibre entre la quantité d'information et la complexité de gestion. Le principe général pour définir le bon niveau est d'avoir le maximum de contrôle sur les éléments avec un minimum d'enregistrements. Ceci étant, la granularité des informations doit correspondre à ce qui apporte de l'information aux différents processus de la gestion des services, ainsi qu'à ce que l'on est en mesure de gérer. Il semble par exemple tout à fait inutile de noter les numéros de série des barrettes mémoires. En revanche connaître le nombre de barrettes dans une machine peut apporter des informations sur la capacité ou l'évolutivité de cette machine... Ceci dit, il faut pouvoir aller vérifier régulièrement que le nombre de barrettes

enregistré dans la base correspond bien au nombre de barrettes installées sur la machine.

Cet inventaire des composants de l'infrastructure (CI) est à faire une bonne fois lors d'une campagne de documentation du système puis à enregistrer dans la base de données. Enfin chaque enregistrement de ces CI fera l'objet d'une revue au cours des interventions sur les équipements. Ces revues de contrôle se font également au cours des demandes de changement où l'on peut valider l'exactitude des informations stockées au regard des informations de terrain et conserver l'historique de l'évolution d'un composant et son statut dans le système (en développement, en test, en production ou en stock).

Le travail d'identification des CI consiste à sélectionner les composants que l'on désire documenter, puis à les classer et les étiqueter, puis à référencer dans la base de gestion des configurations CMDB (*Configuration Management DataBase*) les informations importantes telles que leurs « propriétaires », leurs relations et leurs documentations.

La phase de vérification et d'audit a pour mission de valider l'existence physique des CI au sein du système d'information et de valider les informations stockées dans la CMDB et les librairies. Ceci comprend la validation des documentations livrées avec la nouvelle version d'un CI et les documentations de configuration avant la mise en production.

Périmètre

La gestion des configurations doit assurer l'enregistrement et la restitution des informations concernant chaque composant de l'infrastructure (CI) telles que la version, les détails de configuration, la capacité, le fabricant et les relations qui l'unissent aux autres composants.

Un CI peut être un matériel ou un logiciel et sa documentation, c'est-à-dire un actif du service informatique. Il peut également s'agir d'une procédure, d'un document de l'organisation, comme les accords de service (SLA), ou d'un contrat de sous-traitance.

Cependant même si l'on parle d'actif dans la gestion des configurations, il faut garder à l'esprit que ce processus n'a pas pour but de se substituer à la gestion des immobilisations (Asset Management). Ces deux disciplines sont liées, mais il faut noter des différences importantes. Tout d'abord, la gestion des immobilisations intègre des données financières sur les composants les plus coûteux que l'on désire amortir dans le temps, ce qui n'est pas nécessairement le cas de la gestion des configurations, qui elle, intègre une information complémentaire représentant les relations entre les composants. La gestion des immobilisations que l'on retrouve parfois dans les logiciels de gestion de parc informatique peut donc être un point de départ pour la mise en place d'une gestion des configurations.

Terminologie

La base de données des configurations (Configuration Management Database : CMDB)

La base de données des configurations ou CMDB constitue le cœur de ce processus. Avec la complexité croissante des systèmes d'information, il est impensable d'envisager la gestion des configurations sans un outil digne de ce nom. Cet outil doit apporter une grande capacité de stockage, le moyen de retrouver l'information rapidement, et un système de classement, tri et répartition efficace ainsi que la possibilité de stocker électroniquement et physiquement (média) les logiciels, applications et documentations référencés. Cet outil est évidemment constitué d'une base de données moderne et d'un logiciel servant d'interface permettant d'interroger simplement la base.

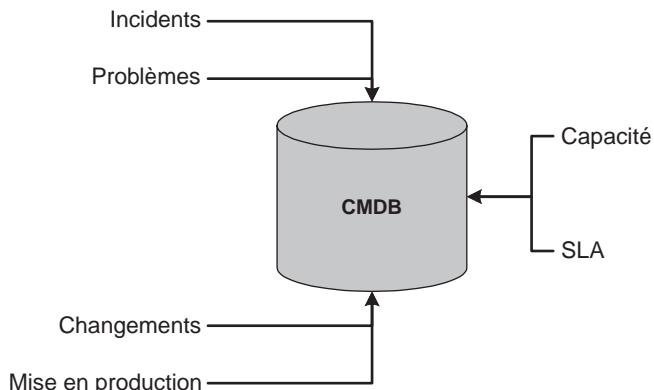


Figure 7-1 : Base de données des configurations : CMDB

Le coût initial de la création de la base CMDB peut être réduit par l'utilisation de l'information existante qui peut se trouver sous différentes formes telles que tableaux, bases de données, documentations diverses, que ce soit sous forme papier ou électronique. Mais la technique la plus efficace sera la récupération d'une base provenant de procédures automatiques d'alimentation que l'on retrouve dans certains logiciels d'identification des matériels et de cartographie du réseau. La comparaison de cette base avec les données provenant de la gestion des immobilisations comptables peut également être d'un grand secours. Ces outils de détection des équipements peuvent également diminuer le coût de mise à jour de cette base avec des recherches, des comparaisons et des mises à jour régulières.

La CMDB doit aussi contenir des informations sur les détails d'inventaire de chaque composant tels que fournisseur, coût, date d'achat, date de

renouvellement d'une licence, ou détails sur les contrats de licence et de maintenance associés, mais doit également contenir les informations d'historique sur le CI et en particulier les incidents, les problèmes et les changements (voir figure 7-1).

La bibliothèque logicielle des versions définitives (*Definitive Software Library : DSL*)

La DSL est une zone de stockage physique sécurisée dans laquelle sont stockées les versions définitives et validées de tous les composants logiciels du système d'information. Pour plus d'information, voir le chapitre 9 « La gestion des mises en production ».

La réserve de matériel de rechange (*Definitive Hardware Store : DHS*)

La DHS est une zone de stockage physique sécurisée dans laquelle sont stockées les pièces de rechange homologuées, utilisées lors des demandes de changement afin de remplacer un composant défectueux. Pour plus d'information, voir le chapitre 9 « La gestion des mises en production ».

Point de comparaison des configurations (*Configuration Baseline*)

Ce point de comparaison est un instantané de la configuration d'un produit ou d'un système à un instant donné. Il permet de conserver l'image figée de la structure et des détails pour le comparer aux évolutions ultérieures, c'est-à-dire entre un état passé donné et l'état actuel d'une partie de la configuration. C'est également le point de départ des discussions lors des demandes de changement. La configuration de base représente le type de configuration que l'on va rencontrer sur site. Cette configuration peut bien sûr être modifiée pour faire naître une nouvelle configuration de base.

Description du processus

Flux du processus

La figure 7-2 reprend les principales tâches et activités de la gestion de configuration et les relations qu'elles tissent les unes avec les autres.

Déterminer la granularité

La première tâche qui doit être réalisée dans le cadre de ce processus concerne la définition du niveau de détail que l'on souhaite utiliser dans la base CMDB. Ce niveau correspond globalement à déterminer l'entité insécable, on peut même dire atomique, que l'on doit prendre en compte lors d'un changement.

Cette mise en place de la granularité est suivie de l'identification des différents types de CI que l'on souhaite intégrer à la base, tels que les matériels

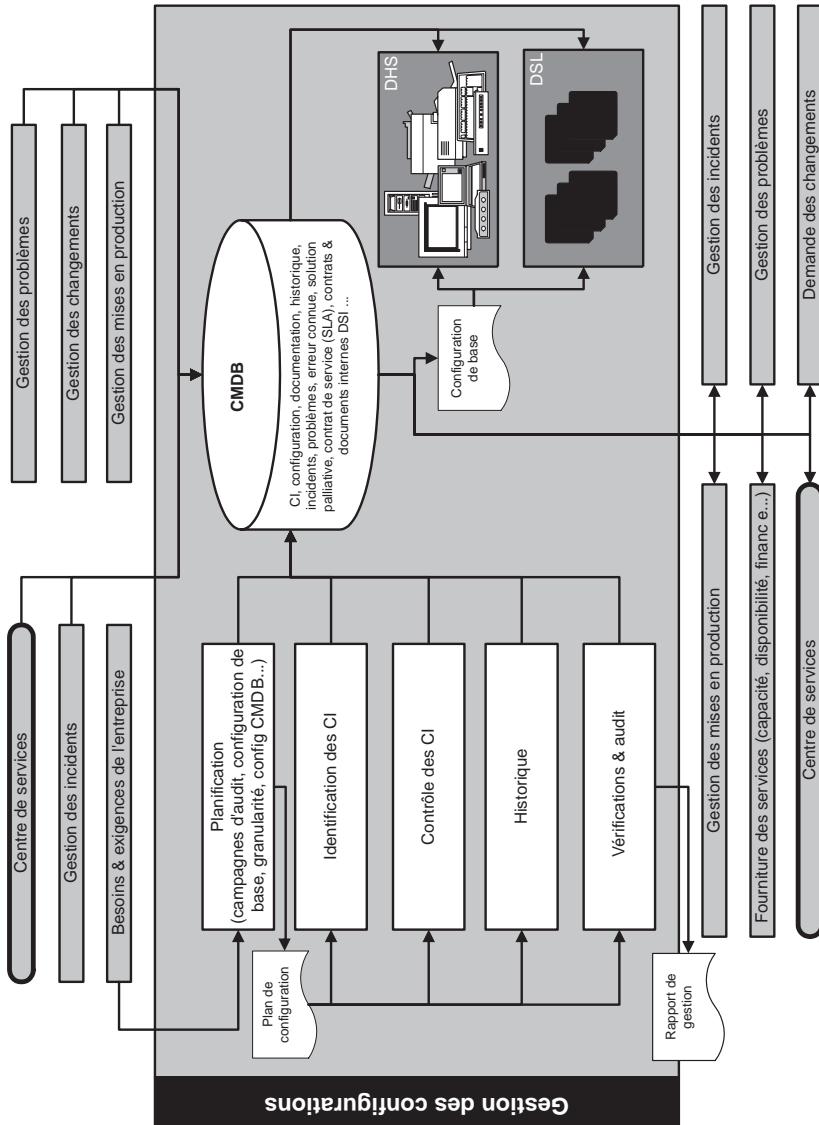


Figure 7-2 : Schéma des activités de la gestion des configurations

(ordinateur, réseau, imprimante, etc.), les logiciels (système d'exploitation, base de données, bureautique, applications métier développées en interne ou par un fournisseur, etc.), la documentation de configuration (documentations système, licences, contrats de maintenance, engagements de niveaux de service ou SLA) et autres documents (procédures internes, plan de configuration, plan de reprise d'activité, etc.).

On peut même envisager d'inclure des informations telles que les incidents et les problèmes relevés sur le CI dans la CMDB. Ceci permet alors en interrogeant un CI de connaître non seulement les relations qu'il entretient avec d'autres CI, mais également de disposer d'informations sur sa fiabilité, et sur l'historique des dysfonctionnements qu'il a subis.

On peut s'interroger sur la bonne granularité du CI. Par exemple, comme on peut le voir sur la figure 7-3, doit-on définir un CI ordinateur ou alors détailler les éléments qui le composent tels que processeur, espace mémoire, type et taille des disques, carte réseau, carte graphique, etc. ?

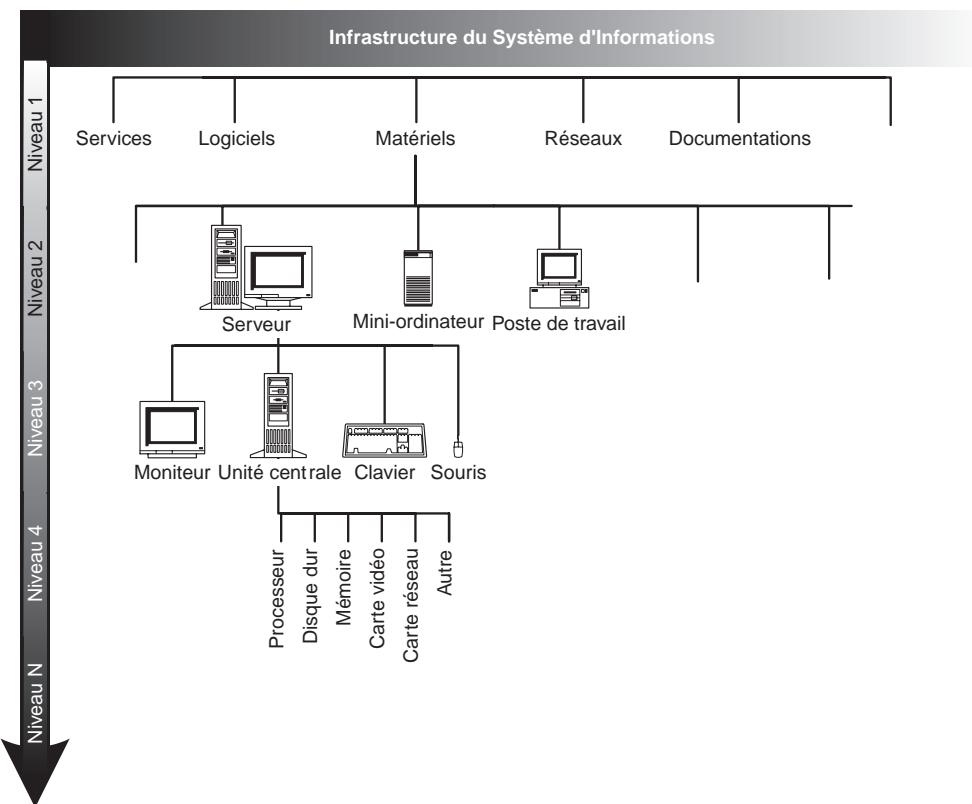


Figure 7-3 : Niveau de granularité des informations dans la CMDB

La réponse à cette question n'est pas triviale et dépend essentiellement de la difficulté et du coût de collecte de l'information, puis de l'effort de mise à jour régulière. Les outils de gestion de parc modernes tendent de plus en plus à collecter ces informations sur le matériel de manière automatique. Ceci ne veut pas dire pour autant que les informations seront pertinentes, utilisables et utilisées, mais tout au moins que le coût de leur collecte ne devient pas un point central de la décision.

Identifier les composants de l'infrastructure

Chaque CI présent dans la CMDB doit posséder des informations permettant de l'identifier rapidement et de le classer en catégories distinctes afin de pouvoir faire des tris.

Sur le terrain, cette identification doit être tout aussi efficace dans l'hypothèse de vérifications et d'audits réguliers. Chaque CI matériel doit disposer d'une étiquette visible et inamovible qui peut reprendre un code de couleur, un numéro de série ou un système de code-barres.

Une convention de nommage doit être mise en place et appliquée à l'identification des CI, des documents de configuration et des changements. Ces conventions doivent être uniques et tenir compte de l'existant de l'entreprise ou de celle du fournisseur.

Mais certains critères ne proviennent pas du CI lui-même, mais plus des relations qu'il entretient avec le reste du système d'information.

Structures de la configuration (arborescence et liens) et sélection des composants

La mise en place d'une structure taxinomique arborescente permet de placer chaque CI au sein d'une catégorie qui définit le CI lui-même et les relations qu'il entretient avec les autres CI du système d'information. Le CI doit être choisi en appliquant un processus de décomposition à l'article de plus haut niveau utilisant certains critères pour le choix du CI. Un CI peut appartenir à un ou plusieurs autres CI en même temps. On peut utiliser plusieurs types de taxonomies distinctes dans la base. Mais les trois plus fréquentes sont le découpage technique de l'infrastructure (réseau, serveur, base de données, système, etc.), le découpage plus géographique qui concerne la localisation du composant dans les locaux de l'entreprise, et la répartition par service au sens organisation du terme (service client, marketing, production, etc.). Le critère de mise en place de l'une ou l'autre de ces taxonomies ou de plusieurs d'entre elles est que la recherche d'un CI particulier soit la plus rapide possible lors des actions de support.

Relations entre éléments

Il existe un grand nombre de liens entre les composants de l'infrastructure, mais quatre grandes familles représentent l'essentiel des relations. Pour

les trois premières, il s'agit des liens d'inclusion, des liens de connexion et des liens d'utilisation.

La quatrième famille représente davantage l'historique associé aux CI. Elle peut faire référence aux incidents, problèmes et erreurs connus attachés à un CI défaillant, mais également aux évolutions apportées à celui-ci lors des demandes de changement et des mises en production.

Un CI peut posséder un lien, en général unique, de type inclusion (parent/enfant) avec un autre CI. Mais ce CI peut également posséder plusieurs autres liens de différents types, et en particulier concernant la connexion ou plus souvent l'utilisation.

Une base de données peut être hébergée par un serveur (inclusion) mais peut être utilisée par plusieurs applications, un service, etc.

Les relations entre les éléments sont stockées dans la CMDB avec l'information associée ce qui représente une des différences majeures avec la gestion des immobilisations (*Asset Management*) qui ne s'occupe que du volet financier.

Cycles de vie des CI

Les CI peuvent également être classés par cycle de vie (succession d'états : enregistré, installé, retiré, etc.) avec le processus qui gère chaque changement d'état (voir figure 7-4).



Figure 7-4 : Cycle de vie des composants du système d'information

Contrôle des éléments de configuration

L'objectif du contrôle de la configuration est de valider la conformité des informations contenues dans la CMDB par rapport à la situation réelle et de s'assurer que seuls les CI dûment autorisés sont enregistrés dans la CMDB. Dans le cas contraire, le processus de contrôle doit permettre l'enregistrement et la mise à jour des nouvelles informations détectées si celles-ci sont conformes à la politique de gestion des configurations de l'entreprise.

En plus de l'ajout ou de la modification des informations, comme le changement d'état, la modification des attributs ou la détection de nouvelles versions, le processus de contrôle peut également ajouter des liens avec les enregistrements d'incidents, de problèmes, ou de demande de changements sur les CI concernés.

- Les liens d'inclusion représentent le cas où un CI est une partie d'un autre CI : par exemple, un disque dur dans un ordinateur.
- Les liens de connexion sont utilisés pour décrire la liaison entre deux équipements : par exemple, un modem et un serveur.
- Les liens d'utilisation définissent la relation entre un composant qui demande la présence d'un autre pour fonctionner : par exemple, une bibliothèque dynamique « DLL » et une application métier.

Le contrôle des CI est extrêmement important dans la politique de sécurité de l'entreprise et en particulier lorsqu'il s'agit d'éviter l'installation sauvage de matériel réseau passant outre les sécurités anti-intrusion ou lorsqu'il s'agit d'empêcher l'utilisation de logiciels piratés.

Mise à jour de la CMDB après la découverte d'un nouveau CI

Le processus de contrôle doit également assurer la suppression ou la désinstallation du composant lorsque celui-ci est arrivé en fin de cycle de vie ou lorsque, après sa détection, il s'avère non autorisé sur le système d'information. Dans ce cas, l'équipe ou la personne qui découvre le CI doit communiquer l'information au centre de services puis, en fonction de ses autorisations, peut mettre à jour directement le CI, le marquer comme enregistrement erroné, ou signaler un incident avec une demande de changement. Le responsable de la gestion de configuration doit ensuite tracer l'origine de chaque CI non enregistré et proposer des actions pour enregistrer, corriger, ou supprimer le CI.

Vérifications et audits

Les vérifications et audits peuvent être réalisés physiquement lors des interventions, lors d'un inventaire annuel, ou à l'aide d'un outil d'inventaire automatisé. La mise en œuvre de ces vérifications peut se faire dans le cadre d'un planning précis et défini à l'avance comme c'est le cas de l'inventaire annuel, grâce à des outils automatiques, ou dans les cas de changements majeurs apportés à l'infrastructure. Dans ce cas, l'ensemble de l'infrastructure ou des catégories d'éléments de configuration sont visés plus particulièrement. Il existe cependant des cas où seule une partie de l'infrastructure sera auditée. Il s'agit par exemple de valider le retour à une situation normale après une bascule sur un site de secours, ou encore la validation d'un ensemble d'équipements en réponse à la détection d'un ou plusieurs composants non autorisés. Dans ces deux cas, l'audit ne portera certainement que sur un ensemble bien déterminé de CI à valider se trouvant dans une procédure appropriée.

Sauvegarde, archivage et maintenance de la CMDB

L'application d'interface et le SGBD qui héberge la CMDB doivent être considérés comme des composants sensibles de la production informatique au même titre que n'importe quelle autre application métier. Mais dans l'hypothèse où cette base détient toutes les informations qui permettront de reprendre l'activité en cas de désastre, il semble important d'appliquer les mêmes méthodes de gestion que celles que l'on applique à une application utilisateur avec plan de sauvegarde et archivage régulier hors site des bandes.

Planification et mise en œuvre

L'implantation de ce processus passe plusieurs étapes qui représentent essentiellement des phases de conception et de mise au point. La première d'entre elles concerne l'expression des besoins provenant de la direction informatique, mais qui doivent rester cohérents avec ceux de l'entreprise.

Ce cahier des charges global comprend les objectifs de la gestion des configurations, le périmètre du processus, les priorités associées et le plan de mise en œuvre en phase avec les objectifs métier.

C'est également à ce moment que l'on décide de la granularité des CI, ainsi que des politiques logicielles et matérielles à mettre en œuvre pour ce plan de configuration, sans oublier de négocier les budgets.

Une fois le plan validé, l'étape suivante doit proposer un échéancier de mise en place du processus, comprenant le planning d'installation de la base, l'estimation de la durée de la campagne de recensement des systèmes et des composants existants et la période de saisie de ces informations afin de disposer d'une date de début d'utilisation de la CMDB.

Les étapes de conception validées, vient le moment du stockage des informations. Cette étape nécessite la mise en place d'une solution informatique de gestion des configurations basée sur une plate-forme matérielle et logicielle pour stocker la CMDB. Cette solution doit pouvoir supporter au minimum l'import de données provenant de fichiers séparés ou de bases locales sans avoir à ressaïsir les informations.

L'étape suivante, qui correspond à la campagne d'identification des CI, permet de réaliser plusieurs objectifs. Le premier d'entre eux est de référencer tous les services informatiques (*IT Services*) et tous les composants d'infrastructure. C'est-à-dire d'identifier, d'étiqueter et d'enregistrer les noms et les versions ainsi que les relations existant entre ces composants.

Ensuite, il faut contrôler et stocker les documentations, les logiciels et les applications maison validées au sein de la DSL.

Cette campagne d'identification peut se faire en plusieurs phases calquées sur l'organisation de l'entreprise par service ou selon la répartition géographique des locaux ou tout autre critère de répartition qui permet de segmenter la période de recherche. Il est également bon de mettre en place une hiérarchie dans la recherche en partant du niveau le plus haut du système d'information (serveurs, mainframe, etc.) jusqu'au niveau le plus bas (les postes de travail, en passant par le réseau, les bases de données, les applications et tout autre composant de l'infrastructure).

Dans l'idéal, l'état des CI ne devrait pas être modifié pendant la campagne initiale de saisie de la CMDB. Dans le cas contraire, tout élément déjà saisi dans la CMDB passe sous le contrôle de la gestion des changements à chaque modification.

Enfin, par souci d'efficacité et de diplomatie, il semble préférable de commencer le remplissage de la CMDB par des domaines où le contrôle est perçu comme important ou comme générateur d'économies, afin d'éviter la lassitude de l'équipe ou le désintérêt du management, classique dans ce genre de projet.

Mesures et contrôles

Étant donné la forte évolutivité des données stockées dans la CMDB et la croissance régulière des volumes considérés, il est nécessaire de revoir périodiquement le processus.

Le choix de la période peut être donné par certains indicateurs comme le nombre de divergences entre la configuration relevée en production et celle présente dans la CMDB, ou le nombre d'incidents et problèmes causés par une régression ou un changement mal contrôlé.

Enfin, il est urgent de réévaluer rapidement le processus si l'on constate un accroissement du temps moyen d'approbation et d'implémentation des changements.

Coûts

Les dépenses de mise en œuvre de la gestion des configurations sont essentiellement composées du logiciel de base de données et du nombre de personnes qui devront l'utiliser, des formations et des salaires du personnel lors de l'étape d'identification et de renseignements des éléments de configuration.

Il faut noter que les dépenses d'exploitation seront certainement plus importantes au départ qu'une fois le processus rodé. En effet, outre la classique période d'apprentissage des procédures par le personnel, il faut ajouter à ce délai la durée de stabilisation de la base de données. Cette durée correspond à la saisie et au contrôle de la qualité des informations et peut être très influencée par la granularité choisie, la qualité des informations disponibles, et le nombre de personnes affectées à la tâche lors de l'identification des éléments de configuration.

Documents et rapports

Les rapports de la gestion de la configuration servent essentiellement à obtenir un instantané de la configuration à un moment donné. Ils permettent en particulier de connaître la configuration, la capacité, la localisation ou l'état actuel du CI. Le rapport doit également comporter des informations telles que le nombre de CI répartis par type d'élément, et la localisation. Les rapports générés doivent comporter les résultats des audits de configuration et donner des informations sur les erreurs relevées dans la base ou lorsqu'un élément repéré dans le système n'est pas présent dans la base.

Ces rapports sont utilisés en général lors de l'identification des tendances. C'est la raison pour laquelle tous les processus de résolution des dysfonctionnements trouveront des informations pertinentes dans les rapports

telles que les relations entre les éléments de configuration ou le taux de changement appliqué à un CI qui donne globalement sa fiabilité.

En transférant les informations concernant la valeur des CI au processus de gestion financière, la gestion des configurations permet de calculer le coût de l'infrastructure.

Conséquences

Le bénéfice le plus important que l'on attend de la gestion des configurations est de fournir des informations précises et pertinentes sur les CI aux autres processus de la gestion des services et en particulier aux processus de support. Ces informations vont permettre par exemple, d'identifier rapidement le CI touché par un incident ou d'analyser les tendances qui lui sont associées lors de la recherche de la cause d'un problème. Ensuite, l'analyse d'impact facilite la planification des changements et diminue les risques de perturbation suite à ces changements.

La gestion de configuration est indispensable dans le support des mises en production et permet de connaître les modifications apportées sur les composants. On constate souvent une amélioration de l'intégrité de l'infrastructure par le contrôle des versions des composants, ce qui procure une protection contre les changements malveillants ou involontaires, et facilite la définition des plans d'urgence. En effet, la CMDB et la DSL facilitent la restauration des services en cas d'urgence. La gestion de configuration permet également de contrôler qu'aucun logiciel non autorisé n'est utilisé (contrôle des licences).

Enfin, la gestion des configurations assiste la gestion financière dans le calcul des coûts de la maintenance, des licences logicielles, etc.

En revanche, malgré tout le soin apporté, il existe de nombreux risques dans la mise en place du processus. Tout d'abord, une définition trop détaillée des informations des CI risque d'entraîner un travail inutile des équipes et risque de ne pas correspondre aux besoins de l'entreprise. Ensuite, un manque d'engagement de la hiérarchie, par méconnaissance de l'intérêt de ce processus, peut entraîner une lassitude de l'équipe qui le gère, et une perception trop bureaucratique ou trop rigoureuse de ce processus. Ceci peut conduire certains à court-circuiter les étapes afin d'aller plus vite ce qui annule tous les bénéfices obtenus précédemment.

Mais le risque principal se présente lorsque le contrôle sur les configurations est incompatible avec l'organisation de l'entreprise, en particulier lorsque les utilisateurs peuvent commander eux-mêmes leurs matériels ou leurs logiciels, puis en faire l'installation, empêchant ainsi le contrôle de l'infrastructure et la constitution d'une base unique disposant de toutes les informations sur les éléments qui la constituent.

Outils

La CMDB contient les détails des attributs et l'historique de chaque CI ainsi que les relations entre les CI. Idéalement, la CMDB devrait être liée avec la DSL et d'autres bibliothèques de logiciel. Souvent, plusieurs outils doivent être intégrés pour fournir une solution entièrement automatisée de recherche d'informations à travers toutes les plates-formes de l'infrastructure informatique (exemple : outils de cartographie réseau et gestion de parc avec agent sur le poste local).

En règle générale, la solution de gestion des configurations est une base de données qui offre une sécurité et un contrôle d'accès par utilisateur, un langage de requête simple permettant de soumettre ses recherches, un système de saisie très simple des informations concernant les CI, un système d'affichage des relations et de la hiérarchie entre les CI, et en résumé, tout ce qui peut faciliter la vie du gestionnaire du processus et des équipes de support.

Rôle et responsabilités

Le responsable du processus doit établir les objectifs principaux du processus en accord avec les besoins de la direction informatique, donc ceux de l'entreprise, concernant la politique de gestion des configurations sous la forme d'un plan de configuration. Ce document contient la politique globale, les règles de gestion, le planning, la définition des CI, ainsi que le contenu des informations associées aux CI. Il doit ensuite communiquer ce document à l'équipe informatique puis en faire la synthèse à l'ensemble du personnel. Il doit concevoir, mettre en œuvre, évaluer et améliorer le système de gestion des configurations de l'entreprise. Le responsable doit également évaluer et planifier le travail et les ressources impliquées dans la mise en place de la CMDB.

Enfin, le responsable du processus doit conduire des audits réguliers de la base CMDB afin de valider son adéquation avec l'existant, puis produire des rapports sur l'état des CI dans le système, l'impact des changements sur les CI et l'état et l'efficacité du processus lui-même.

Le responsable de la base est le concepteur et le responsable des données stockées dans la CMDB concernant les CI en fonction. Il doit assister le responsable du processus lors de la création du plan de configuration. Il s'occupe également du stockage de toutes les copies des logiciels ainsi que de leurs documentations au sein de la DSL. Il doit contrôler la réception, l'identification, le stockage de tous les CI et communiquer des informations sur les

CI aux processus qui les demandent. Afin de mener cette mission à bien, il doit maintenir à jour la base de données des CI.

La gestion des configurations exige une équipe qui adoptera une approche minutieuse et prêtera attention aux détails. Compte tenu du fait qu'il s'agit là d'une équipe de logisticiens et de documentalistes, plus que d'une équipe de techniciens, en dehors des PME/PMI, cette équipe doit être dédiée à ce processus.

GESTION DES CHANGEMENTS



LA GESTION DES CHANGEMENTS PERMET D'ÉVALUER L'IMPACT D'UNE MODIFICATION ET DE PLANIFIER SA MISE EN ŒUVRE.

La gestion des changements

Une des grandes lois de la nature que l'on a vu se vérifier dans le monde de l'économie est que tout ce qui ne s'adapte pas à son environnement finit par disparaître. Ce qui est vrai pour les dinosaures l'est donc également pour le système d'information de l'entreprise. L'évolution rapide des technologies liée à une demande de réactivité du métier implique que le changement soit partie intégrante du cycle de vie du système d'information des entreprises. Ceci implique qu'une décision de figer ce système pour le rendre plus sûr, le rendrait rapidement obsolète et inutile... sûr mais inutile !

Vue d'ensemble

Le système d'information est soumis à l'impact d'événements intérieurs et extérieurs. Lorsqu'ils proviennent de l'intérieur, ces événements sont issus des incidents et des problèmes, ou représentent les optimisations que l'entreprise souhaite apporter en vue d'une amélioration du service ou d'une réduction des coûts. Lorsqu'ils se manifestent depuis l'extérieur, il s'agit de modifications réglementaires et légales ou bien d'évolutions du marché. Dans tous les cas, il convient de s'adapter pour réagir face à l'événement afin que le système d'information puisse continuer à fonctionner. Mais ces modifications doivent être contrôlées afin de ne pas perturber le fonctionnement de ce système. La gestion du changement permet de répondre à ces événements en validant qu'un changement réalisé sur le système d'information ne risque pas de le déstabiliser, ou de provoquer un impact négatif sur les engagements de niveau de service (SLA). L'objectif principal de la gestion des changements est donc de s'assurer que des méthodes et des procédures standards sont utilisées lors de l'évaluation de ces changements.

Le but poursuivi est alors d'éviter une régression consécutive à l'implémentation de ces changements ou, dans le pire des cas, de minimiser l'impact des incidents qui en découlent.

Pourquoi ?

Les changements dans l'infrastructure informatique sont inéluctables et répondent à des problèmes présents dans le système d'information ou à des exigences imposées par l'extérieur, qu'elles soient d'ordre légal, pour aligner l'entreprise sur le marché ou pour améliorer son efficacité et son rendement.

Mais tout changement expose l'entreprise à un risque supplémentaire lors de sa mise en œuvre. C'est pourquoi la gestion des changements réalise une étude préalable à tous les changements afin de faciliter leurs implantations et maintenir l'équilibre délicat entre la nécessité du changement et son effet potentiellement négatif.

Concepts

Que ce soit à la demande du processus de gestion des problèmes, suite à une contrainte légale ou à une nouvelle application, une évolution du système d'information doit tout d'abord être programmée, puis faire l'objet d'une évaluation des risques qu'elle génère sur le système d'information par sa mise en œuvre. Un système stable qui remplit son rôle ne devrait pas avoir à subir de modification. Mais la réalité est toute autre, et pour assurer l'utilité d'un système d'information, il est primordial de trouver un équilibre entre la nécessité d'un changement et l'effet qu'il produit.

Cette lourde tâche revient au processus de la gestion des changements qui doit assumer la décision d'accepter ou non un changement sur le système d'information. Et parfois, lorsque la décision n'autorise pas le changement, elle rencontre la vindicte des utilisateurs, de la direction métier, et quelquefois de la direction générale. Fort heureusement, ce processus n'est pas seul devant l'ampleur du travail. Il est étroitement épaulé par les processus de gestion des configurations, de gestion des mises en production, et par certains processus de la fourniture des services, comme la gestion de la capacité, la gestion de la continuité de service et la gestion financière. Il peut également travailler avec les équipes projet assurant le développement d'applications internes, dans la mise en place des plannings.

Périmètre

Le processus de gestion des changements est globalement moins technique que les autres processus de la gestion des services, mais il leur est très lié, ainsi qu'aux différentes gestions de projet (gestion des développements, gestion d'infrastructure TIC, etc.).

Le processus de gestion des changements peut s'appliquer à l'ensemble des processus métier de l'entreprise, et c'est déjà le cas dans un certain nombre de domaines (production, comptabilité, finance, etc.), même si ce n'est pas toujours aussi poussé que dans le cadre d'ITIL. Cependant, cela impliquerait pour ces autres services de l'entreprise, un fort investissement en temps pour un gain peu probant alors que le besoin de ce processus de gestion des changements s'impose dans le domaine informatique afin d'empêcher un système complexe constitué de multiples composants de s'effondrer sur lui-même à chaque modification. En conséquence, la gestion des changements s'applique à tous les matériels informatiques, réseaux et télécoms de l'entreprise, aux logiciels systèmes, réseaux et bases de données, aux applications métier en production, ainsi qu'aux documentations et aux procédures d'exploitation, de support et de maintenance du système d'information.

En ce qui concerne les applications métier développées en interne, la gestion des changements et le service des études doivent être étroitement liés lorsque les changements proviennent d'une évolution ou même d'une nouvelle application, afin que ces applications ne suivent pas le processus de gestion des changements, mais qu'elles l'intègrent dès la phase projet.

La gestion des changements n'a pas la responsabilité de l'identification des composants affectés par le changement, ni de la mise à jour des enregistrements dans la base CMDB. Il s'agit plus d'actions se trouvant dans le périmètre de la gestion des configurations qui doit également s'assurer que toutes les informations de configuration sont fournies.

La gestion des changements n'a pas non plus pour rôle l'implantation de modifications ou les ajouts de nouveaux composants, ce qui est plutôt du ressort de la gestion des mises en production.

Le processus est placé sous l'autorité du CAB, c'est-à-dire le comité consultatif des changements (*Change Advisory Board*). Ce comité est composé de représentants de plusieurs autres fonctions de l'entreprise, et de plusieurs membres de l'équipe informatique provenant d'autres processus. Même si le gestionnaire des changements assume la gestion quotidienne du processus, c'est bien le CAB qui approuve les demandes de changements importants.

Dans l'absolu, un changement est un processus qui doit permettre de passer d'un état stable vers un état stable modifié. Son rôle est donc de garantir la réussite de l'implantation, ou dans le cas contraire, de minimiser les conséquences de la régression.

Concernant les changements demandés pour résoudre un incident ou un problème, il faut garder à l'esprit que cette issue n'est pas systématique. En effet, un grand nombre de problèmes ne nécessitent pas de changement pour leurs résolutions. Ce changement est nécessaire lorsque la résolution d'un problème passe par une modification du système, c'est-à-dire un changement d'état de la configuration.

On doit se rappeler qu'un changement au sens ITIL concerne l'évolution d'un CI du système d'information. Dans le cas d'une demande de changement d'un mot de passe d'un utilisateur, il est clair que cela n'a pas d'impact sur le système d'information, et n'est donc pas de la responsabilité de la gestion des changements... Sauf si le mot de passe en question est codé en dur dans plusieurs applications. Mais ça, c'est mal !

Le but étant bien évidemment de réduire l'impact du changement sur le système d'information et sur la disponibilité de celui-ci, le CAB aura à cœur de planifier l'implantation du changement sur une période ayant le moins de conséquences possibles pour les utilisateurs. Exemple : remplacement d'un serveur pendant le week-end.

Attention également à faire la différence entre une demande de changement qui est de la responsabilité de ce processus, et une demande de service qui doit être traitée par le centre de services. Il ne faut pas hésiter à utiliser les autres processus de la gestion des services sous peine d'aboutir à une gestion des changements débordée par des demandes ne la concernant pas.

Enfin, l'un des rôles de la gestion des changements étant de limiter l'impact sur la disponibilité du service, le retour à la situation antérieure, ou le retour arrière, doit être systématiquement prévu lors de la phase d'évaluation du changement, c'est-à-dire avant son implémentation, et non pas lorsqu'un problème consécutif au changement se présente.

Terminologie

Un changement représente toute modification de l'infrastructure, d'une application ou d'un service, et plus généralement du système d'information. Un changement entraîne l'évolution du statut d'un ou plusieurs CI.

Cette évolution doit donner lieu au préalable à une demande de changement (Request For Change : RFC) dont l'impact sur le système et la faisabilité doivent être évalués avant son implantation.

La demande de changement est évaluée par le comité consultatif du changement (Change Advisory Board : CAB) qui est composé de plusieurs membres de l'entreprise et de la direction informatique. Le CAB évalue et approuve l'implantation d'un changement sur le système d'information.

Le CAB communique au client la liste des différents changements autorisés dans un document de planification, le FSC (Forwarded Schedule of Changes), qui contient les détails de tous les changements approuvés et planifiés pour l'implémentation.

Ce document est accompagné d'un second document de planification, le PSA (Projected Service Availability), qui indique la disponibilité de service prévue en regard des interruptions de service qui seront nécessaires à l'implantation et en regard de l'impact éventuel sur la disponibilité des services des changements planifiés dans le FSC.

Une fois l'implantation du changement terminée, le CAB se réunit pour faire une revue d'implémentation finale de la mise en œuvre de ce changement qui porte le nom un peu pessimiste de PIR (Post Implementation Review).

Description du processus

Flux du processus

Le processus de gestion des changements est le garant de la stabilité du système d'information dans un environnement instable. Grâce aux méthodes

et aux procédures employées, le processus peut évaluer les conséquences, bonnes ou mauvaises, que l'on peut attendre d'un changement. Comme tout processus, la gestion des changements attend un certain nombre d'éléments en entrée et produit des résultats en sortie. En entrée du processus, on trouve essentiellement les demandes de changement exprimées par les clients, les utilisateurs et d'autres processus, ces demandes étant parfois accompagnées d'une date d'implantation souhaitée, ou d'une précision sur le caractère d'urgence estimée. On trouve également les informations concernant les éléments (CI) touchés par le changement en provenance de la gestion des configurations (CMDB).

Comme on peut le voir sur la figure 8-1, le processus complet se décompose en trois grandes parties au cours desquelles plusieurs autres processus peuvent être impliqués. Il s'agit de l'évaluation, l'implantation et le bilan du changement. Une quatrième partie concerne la gestion de l'urgence et regroupe les trois parties ci-dessus mais avec des contrôles et des procédures allégés.

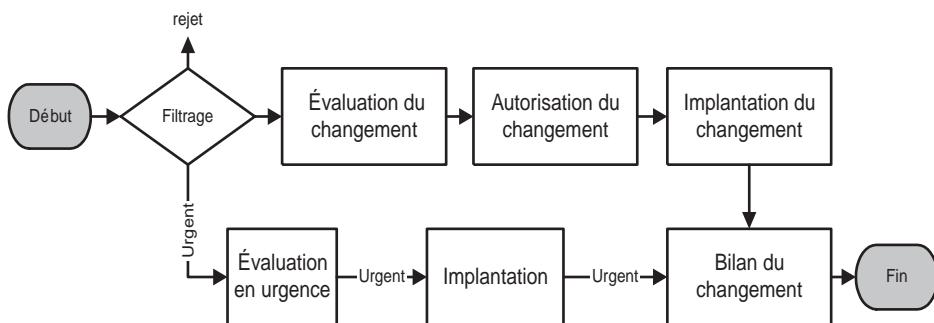


Figure 8-1 : Flux simplifié de la gestion des changements

Concernant la partie implémentation, l'essentiel du travail est assumé par les processus plus techniques et par la gestion de l'infrastructure. Les activités du processus de gestion des changements sont donc essentiellement composées : de l'évaluation des demandes du point de vue de l'intérêt pour l'entreprise et de l'impact sur le système d'information ; de la mise en place et de la tenue du comité consultatif des changements (CAB) ; de la réalisation du bilan et de la clôture des changements lors de la revue post-implémentation (PIR).

Enfin, le processus produit plusieurs éléments en sortie dont le plus important est la décision, accord ou refus, d'un changement accompagnée de la date éventuelle de mise en production de ce changement. Le processus produit également des rapports de compte rendu des actions du CAB, ainsi que des rapports de gestion sur l'efficacité de son fonctionnement.

Planification et mise en œuvre

Évaluation du changement

On trouve tout d'abord le cycle de décision qui intervient après la demande de changement. Durant ce cycle, le CAB va se réunir pour évaluer les informations provenant en particulier de la gestion des configurations, afin de déterminer l'impact du changement sur le système d'information. Selon la décision du CAB, le changement peut être ou ne pas être approuvé. Ce comité est un groupe composé de spécialistes, d'utilisateurs, de clients, dont le rôle est d'évaluer et d'approuver les changements. Si aucun consensus ne se dégage de la réunion, c'est-à-dire que le CAB n'est pas d'accord avec une recommandation, la décision finale appartient à la direction informatique.

Le choix des membres du CAB doit garantir que chaque demande de changement soit analysée et évaluée correctement sur des critères d'activités de l'entreprise et sur des critères techniques. Bien évidemment, le CAB évolue selon les demandes en fonction des changements à analyser. Dans tous les cas, il doit ou peut être composé des personnes ou du représentant d'un groupe de personnes touchées par le changement. On trouve donc :

- le gestionnaire des changements ;
- le client et l'utilisateur touchés par le changement ;
- les développeurs de l'application si nécessaire ;
- les experts techniques ;
- le représentant de la production informatique (qui peut éventuellement provenir d'une entreprise tierce comme une société d'infogérance) ;
- enfin les gestionnaires d'autres processus comme la gestion des niveaux de services, les autres processus de la fourniture des services, mais également la gestion des mises en production.

Comme on peut le voir sur la figure 8-2, une des premières actions du CAB consiste à évaluer la priorité de la demande et son bien-fondé. Certaines demandes peuvent parfois être inutiles ou sans rapport avec un besoin de l'entreprise. Certaines demandes peuvent également être traitées à d'autres niveaux comme c'est le cas pour un simple changement de mot de passe. Dans ce cas, les changements mineurs peuvent être délégués au centre de services. Ensuite, le CAB doit estimer la priorité associée au changement. Il s'agit d'une décision commune entre l'utilisateur, le client et le CAB.

Après la phase d'évaluation de la priorité du changement vient celle de l'étude de son impact. Cette phase est celle qui permet d'évaluer le gain espéré de ce changement en regard des conséquences qu'il risque d'impliquer pour le système d'information. La plupart des informations utilisées à ce moment proviennent de la gestion des configurations et concernent les CI touchés par le changement, ainsi que les relations que ces CI entretiennent avec d'autres CI.

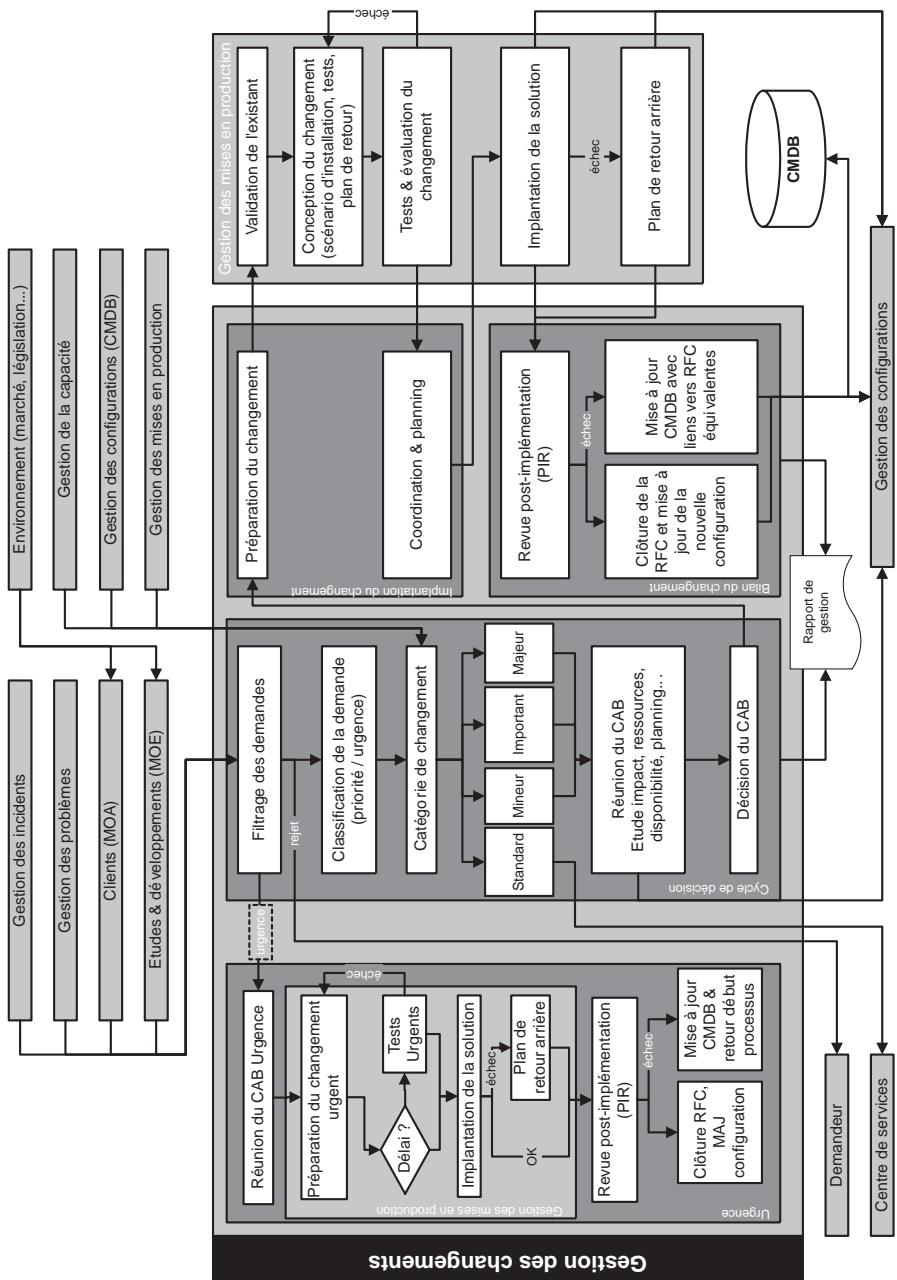


Figure 8-2 : Activité et relation du processus de gestion des changements

L'analyse des risques a une importance cruciale sur cette étape et doit être menée avant l'approbation du changement. Les contraintes prioritaires dans l'établissement du planning de mise en place des changements sont les contraintes métier plutôt que celles provenant de la production informatique. La catégorisation de chaque changement permet d'attribuer des priorités, mais permet également de déléguer certains changements.

Si un changement est placé dans la catégorie « impact métier mineur », alors les ressources et le risque financier associés à ce changement seront faibles. Dans ce cas, le changement peut aisément être validé par les administrateurs système.

En revanche, si un changement est placé dans la catégorie « impact métier significatif », les ressources associées à ce changement seront beaucoup plus importantes, et un risque non négligeable apparaît. Dans ce cas, le changement doit être validé par le CAB.

Enfin, si un changement est placé dans la catégorie « impact métier majeur », les ressources et le budget associés à ce changement seront très importants, et un risque majeur se présente pour l'entreprise. Dans ce cas, le changement doit être validé par le CAB et approuvé par la direction générale.

En associant la catégorie du changement à l'urgence (bas, moyen, haut, urgent) le CAB est en mesure de déterminer la priorité et les ressources nécessaires à un changement.

Les conséquences du changement peuvent être multiples et toucher le système d'information dans plusieurs domaines sans pour autant avoir un impact sur le niveau de disponibilité. Par exemple, il est possible que le changement entraîne des coûts supplémentaires ou une augmentation de la complexité du système. Ceci implique que le CAB doit disposer de l'autorité et des compétences suffisantes dans de multiples domaines pour approuver les changements. Parmi ces domaines, il est indispensable que le CAB dispose de la capacité de valider la dimension financière d'un changement, que celui-ci reste dans les limites du budget ou qu'il faille parfois envisager un dépassement. Il faut également que le CAB dispose de la capacité d'approuver une modification sur l'infrastructure technique. Enfin, le CAB doit obtenir l'accord du client du service touché par le changement, dans l'hypothèse où celui-ci est bénéfique pour l'activité métier.

La planification des mises en production est alors validée par les clients concernés ainsi que par le centre de services et la gestion des niveaux de services (SLA), puis publiée dans le but d'être accessible à tous les utilisateurs et les clients sous forme de deux documents qui sont le calendrier prévisionnel des changements (FSC) et le rapport de prévision de la disponibilité (PSA).

Ces réunions représentent un coût important en temps ainsi qu'en ressources et doivent donc être préparées avec attention. Mais même si la plupart des changements sont à traiter par voie électronique, dans les cas plus complexes, il est nécessaire de tenir une session formelle du CAB. Cette réunion peut avoir lieu périodiquement, comme tous les six mois, ou lors de la livraison des projets majeurs.

Implémentation du changement

Lorsque la demande de changement est approuvée par le CAB, une planification de sa mise en œuvre doit être proposée. Dans l'idéal, chaque changement devrait se faire individuellement, mais dans la réalité, il est souvent nécessaire de faire plusieurs changements simultanément. Si cette solution permet de réduire les coûts immédiats et surtout de réduire la durée d'indisponibilité du système, elle implique également un plus grand risque. Dans l'optique d'un déploiement de plusieurs changements simultanés, il est conseillé de créer un groupe de taille raisonnable et cohérent des changements à déployer en une seule fois et à considérer comme un seul changement, avec un retour arrière global en cas de problème.

Il n'est pas économiquement envisageable de tester tous les composants dans un système d'information et toutes les interactions entre ces composants. La conformité aux standards et aux normes du marché est déjà un premier moyen de valider un changement. Le second moyen le plus simple est de réaliser l'implantation sur une maquette ou sur un site pilote avant le déploiement. Les équipes techniques sont donc en charge de cette implantation pilote, puis de la mise en place sur le site de production, et éventuellement du retour arrière s'il s'avère qu'un problème se présente.

Bilan du changement

Après l'implantation d'un ou plusieurs changements, il est nécessaire de faire un bilan de l'impact et de la réussite de cette évolution du système. Ce bilan peut éventuellement se faire après une période de temps prédéfinie permettant de valider l'impact dans le temps. Ce bilan doit estimer l'effet réel du changement sur le système en le confrontant avec l'hypothèse de départ, et valider qu'aucun effet de bord n'est à redouter. Il doit également établir si le changement a été mis en place dans les temps et les coûts prévus initialement.

En tout état de cause, le bilan doit s'assurer de la satisfaction des utilisateurs et des clients après la mise en place du changement, ou dans le cas contraire, si le scénario de retour arrière s'est réalisé correctement.

Les procédures d'urgence

Lorsqu'un problème majeur se présente et que l'urgence ne permet pas la mise en place d'une réunion plénière, un comité d'urgence du CAB (CAB/EC)

se réunit pour agir rapidement. Il est composé des personnes ayant les pouvoirs nécessaires pour prendre des décisions urgentes. Mais même si les changements urgents sont essentiels pour répondre à certains impératifs métier et techniques, ils doivent être réduits au strict nécessaire car ils entraînent une prise de risque plus importante, avec un risque d'échec non négligeable. Les procédures de gestion d'urgence doivent être conçues et préparées à l'avance dans le but de gérer de telles situations. La mise en place d'un changement urgent peut s'affranchir de certains formalismes et de certains contrôles, mais les scénarios de retour arrière restent indispensables dans le cas d'une régression du système et ce malgré l'urgence de la situation. Si les contraintes de délai l'imposent, la gestion des changements doit s'assurer, en collaboration avec les responsables des autres processus, que les ressources sont suffisantes quitte à s'associer aux équipes d'autres processus. De plus, même dans ce cas, l'approbation du changement reste un pré-requis indispensable.

Le caractère d'urgence est en général associé à la prise de décision, puis l'implémentation du changement. Cela n'empêche donc pas par la suite de suivre le processus classique de gestion du changement. Une fois celui-ci validé, il est indispensable d'effectuer la mise à jour des enregistrements de la CMDB, même si cela n'est pas réalisé en temps réel.

Mesures et contrôles

Les métriques à mettre en place dans le but de contrôler le processus doivent être examinées méticuleusement. En effet, il est facile de mal interpréter les informations provenant de la gestion des changements. Par exemple, si on relève un nombre élevé de changements dans le système d'information, cela n'implique pas nécessairement la présence d'un grand nombre de problèmes, ou que le processus de gestion des changements n'est pas efficace, mais peut-être que l'activité de l'entreprise exige un alignement régulier du système vers les objectifs métier. Le gestionnaire doit donc garder à l'esprit que son objectif ne doit pas être la réduction du volume de changement et donc la réduction des coûts associés, mais bien l'adaptation à l'activité de l'entreprise.

Certains indicateurs de performance sont néanmoins tout à fait pertinents dans l'évaluation de la qualité du processus. Parmi ceux-ci on trouve notamment la mesure de l'impact négatif sur la qualité de service, la mesure du nombre d'incidents consécutifs à l'implémentation des changements, la mesure du nombre de retours arrière sur les changements, ainsi que le nombre de changements urgents. Toute diminution de ces valeurs implique un accroissement de la qualité du processus.

Enfin si l'on peut démontrer l'absence de changement mis en place en dehors de la gestion du processus et si l'estimation des ressources, des

coûts et des plannings nécessaires à l'implémentation des changements correspond à la situation réelle, on peut estimer que le processus est efficace.

Coûts

Les dépenses les plus importantes de la gestion des changements proviennent des coûts en personnel et des coûts des outils logiciels.

Les premiers sont générés par l'équipe de gestion du processus, mais surtout par la présence de membres de plusieurs équipes au sein du CAB (gestion des configurations, gestion des mises en production, gestion de la disponibilité, différents utilisateurs et clients).

Ces dépenses seront bien sûr rentabilisées par les bénéfices qui découleront de la gestion des changements. De plus, de nombreuses entreprises occupent déjà un certain nombre de personnes qui mettent en œuvre des changements, même si ceux-ci ne sont pas contrôlés par un processus de gestion formel. Enfin, bien que les recommandations d'ITIL semblent induire une augmentation du temps consacré aux changements, en pratique, on constate que le temps passé sur l'évaluation des changements est plus faible que le temps qui est nécessaire à la correction des conséquences lorsque les changements ne sont pas contrôlés.

Le coût des outils logiciels est en partie assumé par d'autres processus d'ITIL. Bien sûr, tous les processus ne nécessitent pas une implantation simultanée, mais certains processus gagnent à rester associés à d'autres. C'est le cas par exemple de la gestion des changements et de la gestion des configurations qui partagent largement le logiciel qui les supporte, ou encore de la gestion des problèmes et du centre de services. Ainsi le coût du logiciel est partagé par plusieurs processus.

Documents et rapports

Des rapports réguliers permettent aux clients et aux utilisateurs de se faire une idée de l'ampleur des changements apportés au système. Ils permettent également à la direction d'évaluer l'efficacité du processus. Ces rapports doivent présenter différents niveaux de lecture plus ou moins détaillés selon l'interlocuteur. Ils doivent comporter des informations comme le nombre de demandes de changement (RFC) et les raisons de ces demandes, ou encore le nombre de changements implémentés réussis ou avec retour arrière au cours d'une période donnée, bref tout ce qui peut permettre d'évaluer l'activité du processus.

Conséquences

La gestion efficace des services exige la mise en place d'un processus permettant de faire évoluer le système d'information de manière structurée en

minimisant les erreurs. On peut donc espérer de ce processus une meilleure visibilité de l'impact des changements et donc une analyse plus fine des conséquences. Par contrecoup, on peut penser que l'impact d'une éventuelle défaillance du changement causera moins de perturbations sur la qualité de service et donc sur l'engagement de niveau de service (SLA).

Une autre conséquence bénéfique que l'on peut attendre de la mise en place de ce processus, concerne l'amélioration du soutien des services (incidents, problèmes) par la bonne connaissance des changements mis en place sur l'infrastructure et la diminution des retours arrière.

Enfin, la gestion des changements permet également d'obtenir une meilleure analyse des coûts des changements proposés avant qu'ils ne soient mis en place, ainsi qu'une meilleure capacité à absorber de grands volumes de changements, ce qui permet une nouvelle fois de gagner en contrôle sur les dépenses de la direction informatique.

Pour ce qui est des inconvénients, il faut signaler quelques petites difficultés. Comme toujours dans ITIL, l'implantation de la gestion des changements doit rester réaliste et pragmatique. Le processus à mettre en place doit être adapté à la taille de l'entreprise sous peine d'être perçu comme trop bureaucratique, ce qui risque d'encourager les actions parallèles et de réduire l'efficacité.

Des efforts de communication et de persuasion sont nécessaires afin de convaincre les utilisateurs, les clients, les autres directions, et parfois même les membres de l'équipe informatique, que chaque composant de l'infrastructure a un impact important sur les autres composants. Ainsi, tout changement apporté à un composant peut entraîner une conséquence grave pour l'ensemble du système. La solution qui permet d'éviter ces conséquences passe par une coordination des actions du changement.

Outils

Le logiciel utilisé dans la gestion des changements est le même outil que celui qui est utilisé dans la gestion des configurations. Basé sur la CMDB, il permet de connaître rapidement l'impact d'un changement en identifiant les composants touchés ou ceux qui sont en relation avec la modification.

Rôles et responsabilités

Pour que le processus fonctionne correctement, le rôle du gestionnaire des changements doit être impérativement défini et formalisé. Ce poste de gestionnaire doit être occupé par un responsable qui en assume la charge. Le niveau de responsabilité et la charge de travail justifient souvent un

poste à part entière, même si la personne qui l'occupe peut assumer un autre processus d'ITIL.

Responsable

Le responsable du processus de gestion des changements reçoit les demandes de changement (RFC), les enregistre, les classe et leur attribue une priorité en accord avec l'auteur de la demande. Il doit ensuite planifier l'étude de ces RFC lors d'une prochaine réunion du CAB et convoquer les participants à qui il fait circuler les informations concernant ce changement. C'est également lui qui prépare et convoque les éventuelles réunions d'urgence. Il doit également présider chaque réunion du CAB.

Outre ce rôle de coordinateur et d'animateur de réunion, le responsable de la gestion du changement doit également assurer l'interface avec les processus qui vont mettre en place le changement considéré. Il s'assure que les phases d'implantation, le planning, et les tests demandés sont bien réalisés.

Une fois le changement réalisé, il doit ensuite valider son résultat au sein d'une réunion de revue réalisée après l'implémentation des demandes, puis faire la clôture des demandes.

Enfin, le responsable doit produire des rapports réguliers sur l'activité et l'efficacité du processus.

Comité

Le comité consultatif des changements doit se réunir régulièrement et pour des objectifs déterminés. Les membres de ce comité doivent disposer des compétences et de l'autorité nécessaires pour l'évaluation et l'approbation des changements qui lui sont soumis. Dans ce but, le comité doit être composé du responsable de la gestion des changements, qui agit en tant que président du comité, et peut être assisté du responsable de la gestion des configurations. Siègent également au comité les membres d'autres processus comme la gestion de la capacité, la gestion financière et la gestion de la disponibilité, qui apportent chacun leur vision du changement envisagé. On trouve également le représentant des équipes techniques chargées de la mise en place du changement ainsi que les éventuels représentants des développeurs. Enfin, et c'est le plus important, on trouve au sein du comité, les représentants des clients et des utilisateurs affectés par le changement.

Le CAB doit évaluer toutes les demandes de changement qui lui sont soumises afin de déterminer leurs impacts probables sur le système d'information, ainsi que les détails concernant la technique, les ressources à mettre en œuvre et les coûts associés à ces changements.

Enfin, en dehors de leurs compétences propres qui leur vaut de siéger à ce comité, aucune compétence particulière n'est exigée des membres qui composent le CAB.

GESTION DES MISES EN PRODUCTION

AVEC
 CETTE INSTALLATION,
 VOTRE VOITURE
 VA RENAÎTRE !

TU ENTENDS ÇA CHÉRIE ?
 ON MET EN PRODUCTION
 UN NOUVEAU MODÈLE !

AH...
 ET BIEN MOI
 AUSSI J'AI
 FAIS UNE
 MISE EN
 PRODUCTION...
 DES JUMEAUX !



BD

LA GESTION DES MISES EN PRODUCTION PERMET D'AVOIR UNE VUE
GLOBALE PRENANT EN COMPTE TOUS LES ASPECTS D'UNE
MODIFICATION AFIN DE RÉALISER SA MISE EN CEUVRE.

La gestion des mises en production

« Avanie et Framboise sont les mamelles du destin », disait le poète. Dans notre cas, et c'est tout de même moins joli, c'est plutôt changement et configuration qui font office de mamelles à la mise en production.

Vue d'ensemble

Quelle que soit la complexité du système d'information, un changement entraîne des répercussions, bonnes ou mauvaises. Pour que les conséquences de cette implantation ne soient que bénéfiques, le processus de gestion des mises en production n'intervient qu'après la décision d'approbation d'une modification par la gestion des changements, qui elle-même n'intervient qu'avec l'aide de la gestion des configurations. En conséquence, le premier objectif de la gestion des mises en production est de s'assurer que seules les versions autorisées et testées des logiciels et matériels sont mises en production. En ayant une vision globale du changement apporté au système d'information, ce processus permet de s'assurer que tous les aspects d'une mise en production matérielle ou logicielle, aussi bien techniques que non techniques, sont pris en considération, et permet également d'assurer la traçabilité de ce changement.

Pourquoi ?

Le but de ce processus est de protéger l'environnement de production, et ses services, des mises en production sauvages, en utilisant des procédures formelles et en mettant en place des vérifications lors de l'implémentation des changements.

Pour y parvenir, les trois processus de la gestion des changements, des configurations et des mises en production doivent travailler de concert. Cette étroite collaboration permet de s'assurer que la base CMDB et la DSL sont mises à jour et reflètent les changements implémentés par les mises en production.

Bien que chaque processus ITIL soit indépendant, il est vrai que dans le cas présent, la mise en commun de ces trois processus va beaucoup apporter au contrôle du système d'information.

Du point de vue de la gestion des mises en production, ce travail en commun va permettre de planifier et de superviser les mises en production des logiciels et des matériels plus efficacement, afin de s'assurer que ces changements sont traçables, et que seules les versions testées et autorisées sont présentes sur le système d'information.

Concepts

Un déploiement correspond à un ensemble de changements autorisés au même instant sur l'infrastructure (corrections de problèmes techniques et fonctionnels, et nouvelle version). Il peut comporter des modifications logicielles et matérielles simultanées.

Un déploiement peut être considéré comme mineur lorsqu'il s'agit de quelques ajouts ou modifications fonctionnelles légères tant logicielles que matérielles. Souvent, ce type de déploiement annule et remplace les correctifs urgents passés depuis le dernier déploiement majeur ou mineur. Le but de ce déploiement est de consolider une situation qui a pu être corrigée dans l'urgence.

Les déploiements plus importants sont considérés comme majeurs dès lors qu'ils concernent des ajouts fonctionnels importants ou des correctifs qui modifient le comportement du système d'information. À l'instar des déploiements mineurs, ce type de mise en production écrase toutes les modifications antérieures.

Le dernier type de déploiement correspond au traitement d'une situation d'urgence qui peut être solutionnée par la mise en production d'un correctif urgent sur le logiciel ou le matériel. Ce déploiement contient en général la correction d'un problème connu très localisé ou d'un très petit nombre de problèmes.

Un groupe de déploiements concerne un ensemble de CI qui ne peuvent être mis à jour indépendamment ou lorsqu'il est plus pratique ou économique de remplacer le groupe entier. Dans ce cas, le changement d'un CI entraînera le changement de tous les CI du groupe.

C'est par exemple le cas lorsque après une situation de crise où la gestion du changement a autorisé la mise en production d'un correctif urgent de sécurité, la situation est stabilisée par la mise à niveau des logiciels des autres configurations système.

C'est le cas des installations d'une nouvelle version du système d'exploitation ou le remplacement d'un serveur par un nouveau modèle.

C'est le cas d'un correctif logiciel répondant à une alerte de sécurité sur une faille précise.

Une fois déterminé le type de mise à jour que l'on peut qualifier d'impact, il convient de définir sa catégorie que l'on peut associer à son ampleur. On distingue trois catégories de déploiement.

- La première concerne la mise en production complète des composants d'un assemblage (*full release*). Ceux-ci sont conçus, validés, distribués et installés ensemble. Ce mode d'installation est assez consommateur de temps et demande des tests de non régression sur l'interface entre les composants à mettre en production et le reste du système.
- La seconde catégorie correspond à un déploiement différentiel (*delta release*) où seuls les composants concernés par la modification sont déployés. S'il est un peu plus rapide, ce mode d'installation entraîne plus de risques et demande donc non seulement des tests de non régression entre les composants et le reste du système, mais également entre les composants eux-mêmes.
- La troisième et dernière catégorie représente les mises en production groupées sous forme de paquets plus globaux (*package release*). Ce mode d'implantation peut se faire après un test exhaustif des éléments qui le composent, mais permet de garantir que tous les éléments sont à niveau (attention cependant à la taille du paquet réalisé). Ce mode de mise à jour est en général basé sur un calendrier. Il est donc recommandé lorsqu'il est possible de différer les déploiements afin de ne pas trop perturber la production. On peut également utiliser le déploiement groupé lorsque l'on souhaite uniformiser au même moment des systèmes sur lesquels des déploiements complets ou différentiels ont été réalisés.

La conception d'un plan de mise à jour permet de préparer et de planifier les implantations des nouvelles versions de CI. Cette politique qui doit être connue des membres de l'équipe informatique et des développeurs, ainsi que des clients et des utilisateurs, doit définir une nomenclature et une numérotation pour les versions à planter. Ces noms et ces numéros uniques doivent ensuite être gérés au sein de la CMDB par la gestion des configurations. La politique de mise à jour doit également prévoir la fréquence des déploiements en production et le niveau de détail minimal au-dessous duquel le déploiement n'est pas géré.

La conception d'un déploiement doit respecter des procédures strictes, et en ce qui concerne les logiciels, le déploiement doit être le plus automatisé possible.

La phase de validation avant mise en production permet de tester le changement en situation de pré-production. Dans la mesure du possible, ces tests doivent se dérouler dans un environnement proche de celui de la production, tant d'un point de vue matériel que logiciel. Cette validation peut comporter des aspects fonctionnels et techniques et porter sur l'intégration au système d'information ainsi que sur les performances.

Exemple : changement d'un PC complet, alors que la modification ne porte que sur le lecteur de CD-Rom.

Exemple : Pour être sûr que tous les correctifs qui ont été déployés sur l'infrastructure pendant un laps de temps précis sont bien présents sur l'ensemble du système d'information, on regroupe tous ces correctifs dans un seul déploiement groupé pour l'implanter à coup sûr.

Dans le cas de diffusions fréquentes ou massives de logiciels, l'utilisation d'outils spécifiques de télé-distribution est idéale.

Un scénario de retour arrière doit être établi dans l'éventualité d'un échec du déploiement. Ce scénario permet de documenter la restauration du système dans l'état précédent le déploiement. Dans cette optique, la gestion doit fournir un scénario de retour arrière pour chaque changement validé, alors que la gestion des mises en production doit fournir un scénario global de retour arrière, qui cumule les scénarios de retour arrière de tous les changements implémentés par le déploiement. Si des points de contrôle ou points d'arrêts ont été prévus dans le déploiement, il est envisageable de construire un scénario de retour arrière partiel, c'est-à-dire d'estimer à quel moment le déploiement est en échec, et de revenir à la situation précédant l'échec. Dans le cas contraire, c'est-à-dire si le déploiement est indivisible ou si aucun point de contrôle n'existe, le scénario de retour arrière doit permettre une complète réversibilité du déploiement.

Périmètre

Le processus de gestion des mises en production est responsable de la planification, de la conception et de la validation des matériels et logiciels destinés à être déployés en production. Ce planning doit être communiqué aux différents intervenants qui sont alors susceptibles de demander une formation pour assumer cette mise en production. Les membres de l'équipe de déploiement doivent contrôler, le cas échéant par un audit, la faisabilité de cette implantation, puis mettre en œuvre le déploiement lui-même. Enfin, le déploiement terminé, l'équipe doit transmettre les informations nécessaires à la mise à jour de la CMDB et de la DSL.

Le processus de gestion des changements est responsable du contrôle de tous les logiciels utilisés en interne, qu'il s'agisse d'applications développées en interne ou par des sociétés tierces, ainsi que des logiciels externes (système, SGBD, bureautique). Le processus est également responsable des changements de matériel au sein du système d'information. En revanche, l'installation d'un nouveau poste de travail est plutôt du ressort du centre de services.

Terminologie

À l'instar de la gestion du changement, la gestion des mises en production utilise beaucoup la base CMDB de la gestion des configurations, ainsi que les bibliothèques DSL et DHS.

La bibliothèque logicielle des versions définitives (Definitive Software Library : DSL)

La DSL est une zone de stockage physique sécurisée (une salle, une armoire, etc.) dans laquelle sont stockées les versions définitives et validées de tous les composants logiciels du système d'information, qu'ils soient produit en interne ou en externe. Sa mise à jour est strictement contrôlée par la

gestion des changements et la gestion des mises en production, ce qui permet de suivre et de contrôler les logiciels installés dans l'entreprise.

Outre cette zone de stockage physique, l'entreprise doit définir la politique de gestion des logiciels utilisés dans le système d'information en ce qui concerne le cycle de vie des produits, les licences, les contrats cadre, les achats groupés passés avec les éditeurs, et enfin, les contrats de maintenance et d'assistance sur les logiciels.

Cette politique concernant les logiciels constitue une charte qui doit être communiquée aux clients, aux utilisateurs et aux équipes installant ces logiciels.

La réserve de matériel de rechange (Definitive Hardware Store : DHS)

La DHS est une zone de stockage physique sécurisée (une salle, un entrepôt, etc.) dans laquelle sont stockées les pièces de rechange homologuées qui sont utilisées lors des demandes de changement afin de remplacer un composant défectueux.

Ces matériels doivent être maintenus au même niveau que ceux que l'on trouve en production.

Le contrôle d'accès à cette zone doit être efficace afin d'éviter les disparitions de matériel.

Description du processus

Flux du processus

L'essentiel des échanges que l'on peut trouver dans le cadre de la gestion des mises en production provient des interactions entre ce processus, la gestion des changements, et la gestion des configurations. On constate également que les liens les plus fréquents concernent les renseignements issus de la base CMDB.

Les principaux flux internes que l'on retrouve sont essentiellement la préparation logistique, la validation du contenu et de la méthode de ce déploiement, ainsi que sa planification très précise et exhaustive (voir figure 9-1).

Après cette période de préparation très importante, l'étape suivante concerne le lancement des tests en pré-production, puis l'implantation du déploiement en réel.

Une fois cette étape franchie, des tests doivent être réalisés afin de décider d'un éventuel retour arrière. Cette étape est également l'occasion de mener un bilan post-implantation et une mise à jour de la CMDB.

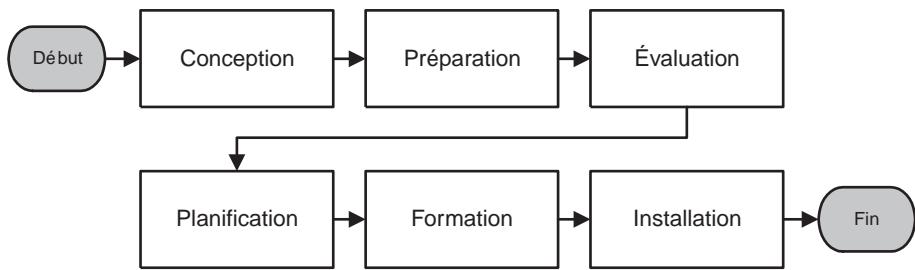


Figure 9-1 : Flux simplifiés de la gestion des mises en production

Planification et mise en œuvre

Comme on peut le voir sur la figure 9-2, la mise en production d'un ensemble de CI comporte plusieurs phases : phase de validation, phase de planification et phase de préparation logistique. La validation permet de vérifier les composants inclus dans le déploiement, ainsi que la méthode de déploiement (découpage envisagé, ressources nécessaires, répartition des rôles, etc.). Cette phase permet également de valider que la situation des matériels et logiciels en production est bien celle prévue. C'est également lors de cette phase qu'est conçu le plan de retour arrière.

La phase de planification permet de définir précisément les étapes du déploiement dans le cas d'un découpage par localisation, par service, par métier, etc. Cette étape permet de produire un calendrier des mises en production dont les dates doivent être validées en accord avec les disponibilités des utilisateurs, des clients et des équipes techniques chargées du déploiement.

En parallèle de ces deux phases, se déroule la préparation logistique du déploiement qui permet de préparer les différents composants impliqués dans le déploiement. C'est la période pendant laquelle on engage les négociations avec d'éventuels fournisseurs pour l'achat de suppléments en matériel, logiciel et service, prévus lors du déploiement.

Cette phase produit un plan de test détaillé et les critères de validation du déploiement lors de la phase maquette en pré-production. Elle permet en particulier de valider la qualité de l'élaboration et de la configuration du paquet à déployer. L'intérêt de cette étape est clairement de déterminer les difficultés possibles lors du déploiement final en vérifiant par exemple les instructions de mise en place des composants, les scripts et les manuels d'installation, ainsi que la présence des procédures d'exploitation et des procédures de retour arrière. L'autre intérêt important est de vérifier que tous les éléments du déploiement (logiciel, documentation, procédure d'exploitation, etc.) seront disponibles pour un stockage dans la DSL.

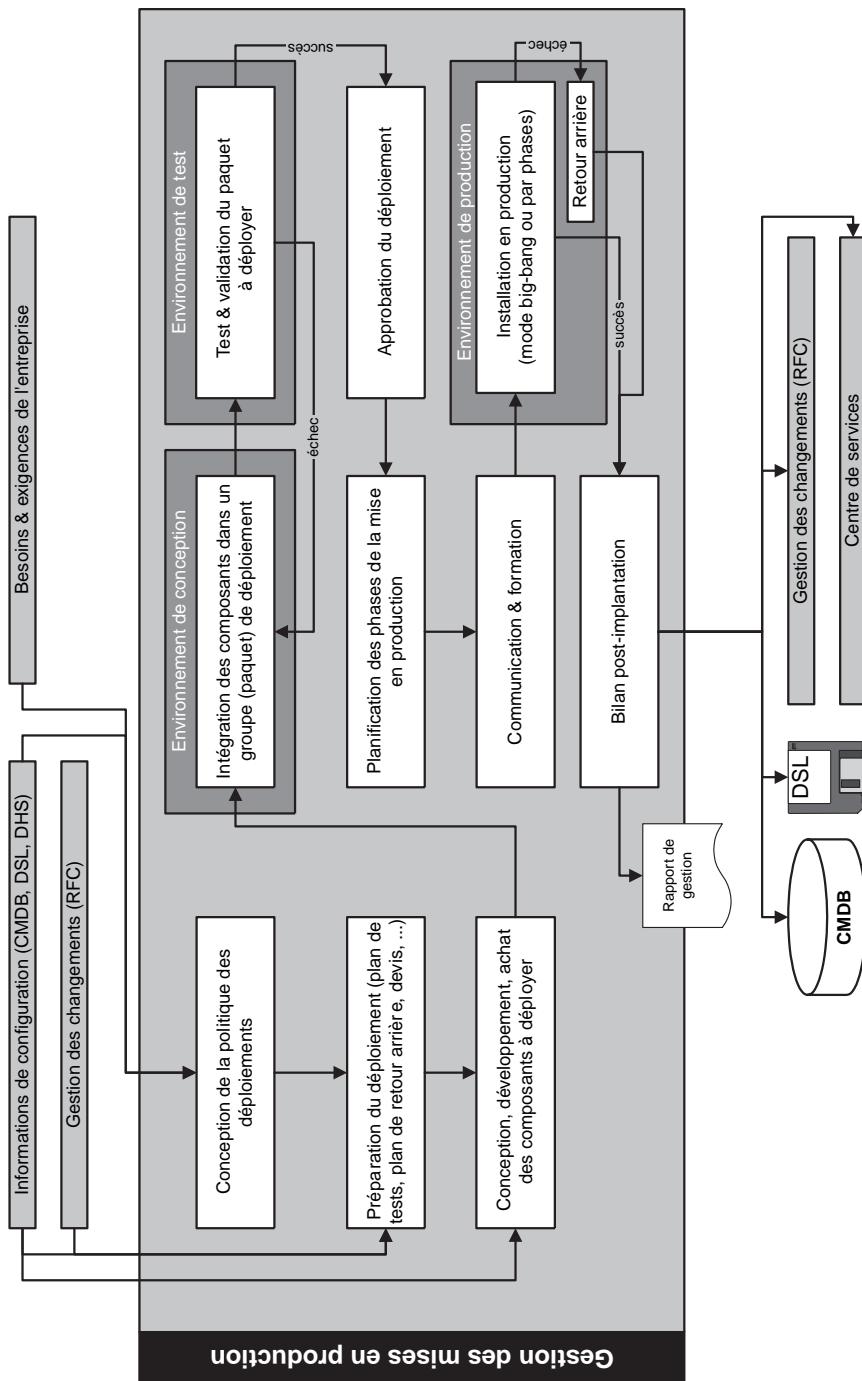


Figure 9-2 : Activités et relations internes de la gestion des mises en production

La validation du paquet de déploiement doit se faire dans la mesure du possible dans une salle de pré-production séparée et à l'aide d'une équipe indépendante à la fois de celle qui a produit les composants à installer, et de celle d'exploitation, qui assumera les CI en production informatique. Cette phase doit prendre en compte les tests techniques (installation, performances, fiabilité, etc.) mais également les tests fonctionnels avec l'aide des utilisateurs. À l'issue de ces tests, un rapport de validation doit être rédigé. Si le résultat est positif, alors le déploiement peut être mis en œuvre. Dans le cas contraire, le rapport est transféré à l'équipe ayant conçu le changement afin que ses membres puissent corriger le dysfonctionnement. Le déploiement est alors reporté et renvoyé pour une nouvelle planification à la gestion du changement.

Une fois testé en pré-production, le déploiement peut rentrer dans la phase d'implantation réelle.

Le mode de déploiement dépend essentiellement des critères vus précédemment, et en particulier de l'impact sur le système d'information et de l'ampleur des installations à réaliser. En fonction de ces critères, il peut être décidé de mettre en place le déploiement en une seule fois dans un mode dit de *full release* ou en plusieurs étapes (déploiement par phases avec site pilote puis implantations locales). Le premier mode peut s'avérer plus coûteux en regard du nombre de techniciens qu'il faut aligner pour le mettre en œuvre, mais la mise en production par phase n'est possible que si l'environnement de production peut supporter d'exploiter simultanément deux versions différentes de la même application.

Mesures et contrôles

Certains indicateurs de performance du processus peuvent être mis en place pour en contrôler l'efficacité. On trouve notamment le taux des déploiements créés, testés et mis en production qui respectent les délais et les budgets prévus.

Un indice important concerne le taux de retours arrière dus à des erreurs non détectées en phase de validation de pré-production. Ce taux qui doit évidemment être très faible est un indicateur de la qualité du processus, mais est également révélateur de l'efficacité des processus de gestion du changement et des configurations, ainsi que de la communication entre ces trois processus.

Les métriques à proposer dans les rapports de gestion concernent le nombre de déploiements majeurs, mineurs et urgents par période, le nombre de composants nouveaux, modifiés et supprimés par déploiement, ainsi que le nombre de déploiements terminés dans les délais prévus, et enfin, les choses qui fâchent, le nombre de problèmes liés à une mauvaise préparation ou à une mauvaise validation.

Exemple vécu : « Oh ! Oh ! On a installé le mauvais fichier ! » ou « Ce n'est pas le bon câble ! ».

Coûts

La mise en place de ce processus entraîne un certain nombre de dépenses. Parmi celles-ci, une part importante est représentée par les investissements en matériel (matériel de rechange, matériel en salle maquette pour les tests de pré-production, etc.), en logiciels (outils de télédistribution, utilitaire de création de paquet logiciel, etc.), et en espace de stockage pour la DSL (armoire des logiciels) et la DHS (zone de stockage du matériel).

Le deuxième poste particulièrement important concerne les coûts de personnel comme le temps passé à développer les méthodes et les procédures des mises en production, puis celui passé à former les équipes.

Mais le problème principal des coûts liés à ce processus est qu'ils sont souvent budgétés par les grands projets alors qu'ils devraient être intégrés dans les coûts d'exploitation courants. Cela implique que le coût des mises à jour est rarement budgété lors de la phase projet et il est alors attribué à tort au processus de gestion des mises en production, au lieu d'être imputé au projet lui-même.

Néanmoins, dans la plupart des cas, les dépenses associées à l'implantation du processus de gestion des mises en production sont moindres que les bénéfices qu'il apporte. En effet, sans contrôle adapté des installations de logiciel et de matériel, l'entreprise s'expose à des risques tels que la fraude informatique, les virus et autre logiciel malveillant, ou tout simplement, à la corruption des applications par négligence. Les dégâts causés par ce type de problèmes peuvent dépasser de loin les dépenses initiales.

Documents et rapports

En plus des rapports de gestion classiques que l'on peut attendre du processus, plusieurs documents sont indispensables dans le cadre de la gestion des mises en production. L'essentiel des ces documents correspond aux différents plannings qui doivent être fournis aux autres équipes de gestion des services, au centre de services, ainsi qu'aux utilisateurs et bien sûr aux clients. Ces plannings prendront évidemment en compte non seulement les dates et les durées des interventions de déploiement, mais devront également signaler les interruptions de service envisagées lors de ces interventions. Cependant, il faut se souvenir qu'une grande partie de cette planification est déjà réalisée par la gestion des changements.

L'autre grand type de documents indispensables correspond aux documents qui formalisent la politique de déploiement des nouvelles versions et des correctifs au sein du système d'information. Ils apportent des précisions sur la granularité, le type (impact) et la catégorie (volume) du déploiement et indiquent les fréquences de mise en production. De plus, ces documents doivent être adaptés aux besoins exprimés par les clients en terme de disponibilité, donc de SLA. Ils doivent signaler clairement les

périodes durant lesquelles une mise en production n'est pas envisageable en raison du risque qu'elle peut faire courir à l'activité de l'entreprise.

Conséquences

En combinant les processus de gestion des changements, des mises en production et des configurations, on obtient très rapidement des bénéfices tangibles, comme un meilleur taux de réussite lors des déploiements et une diminution du risque d'incompatibilité entre les CI lors de changements importants sur l'infrastructure. De plus, le corollaire est que l'on gagne en stabilité de l'environnement de production, ce qui entraîne une baisse des problèmes récurrents, et donc une baisse des demandes de changements.

En revanche, outre la classique résistance au changement que l'on trouve lors de l'installation de chaque processus, plusieurs écueils sont envisageables. Le plus fréquent des problèmes rencontrés concerne la vision d'un processus bureaucratique et lourd qui incite les utilisateurs, et parfois les membres du service informatique, à contourner la gestion des mises en production afin de réaliser des « installations sauvages », ou même à utiliser la procédure de déploiement en urgence afin d'installer les nouvelles versions plus rapidement. On retrouve d'ailleurs cette situation dans la demande fréquente d'outrepasser l'environnement de test pour accélérer la mise en production d'une nouvelle version.

Un manque d'engagement de la direction sera souvent associé à un manque de moyens. Cette situation se traduit alors par des ressources insuffisantes ou une plate-forme d'homologation pas assez puissante ou non représentative de la configuration de production.

Outils

La gestion des mises en production peut utiliser un grand nombre d'outils de la gestion des changements. Un bon système permettra de suivre les changements individuels ainsi que les déploiements associés, et doit permettre à l'équipe technique de déclencher, si possible électroniquement, les diverses phases de la mise en production. Pour cette raison, les membres de l'équipe doivent disposer des autorisations nécessaires pour la mise à jour du statut des CI dans la base CMDB. D'autres types de logiciels seront utilisés avec profit par les membres de l'équipe de gestion des mises en production. En ce qui concerne les développements internes, on trouve en particulier les logiciels de contrôle de version (*versionning*), qui permettent de suivre et de retrouver toutes les versions d'un logiciel ou des briques qui le composent, pendant et après un développement.

Dans le cas de logiciels internes ou externes que l'on souhaite implanter sur de nombreuses machines, les logiciels de télédistribution permettent

de préparer un scénario de déploiement automatisé d'une même version, sur un grand nombre de postes simultanément.

Enfin les outils d'interrogation à distance du système et du matériel, qu'il s'agisse d'un poste de travail ou d'un serveur, permettent de réaliser un audit logiciel et matériel à distance indiquant la configuration exacte et les capacités de la machine considérée, comme la charge processeur, la consommation mémoire et la place disque restante. De plus ces outils permettent souvent de prendre la main à distance ou proposent un langage de script, afin de faire exécuter des actions à distance ou pré-programmées.

Rôles et responsabilités

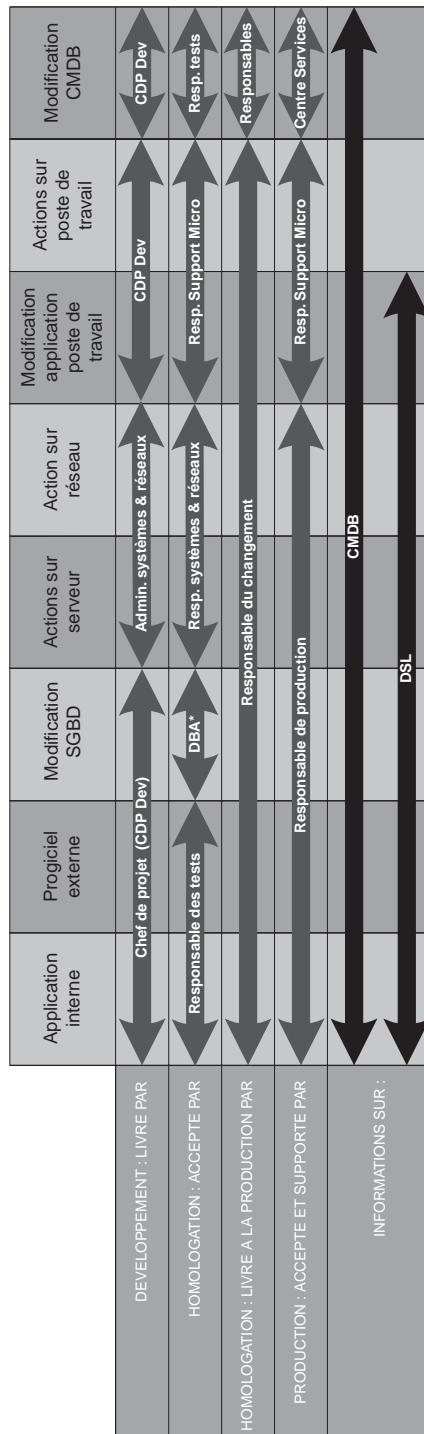
Le processus de gestion des mises en production fait intervenir plusieurs types de responsables. Les plus importants sont le responsable des changements, le responsable des déploiements et le responsable des tests et des validations.

Dans certains cas, le recours à ces responsables n'est pas indispensable. Par exemple, il n'est pas nécessaire de faire appel à la gestion des changements lors des installations de poste de travail. En général, les installations standards, prédéfinies et approuvées, sont plus du ressort du centre de services.

Comme on peut le voir sur la figure 9-3, voici par exemple la répartition des rôles et des responsabilités dans une refonte :

Le responsable de la mise en production doit disposer d'un « minimum vital » de connaissances techniques et doit au moins bien comprendre l'infrastructure et les services qu'elle fournit. Il doit également avoir une bonne connaissance des outils utilisés lors des mises en production. Des expériences de gestion d'équipe et de gestion de projet seraient les bienvenues. D'un point de vue plus fonctionnel, il doit bien connaître les actions des processus de gestion du changement et de gestion des configurations, dont il peut d'ailleurs assumer les fonctions dans le cas de petites sociétés. Enfin, il doit être sensibilisé à la stratégie et aux objectifs de l'entreprise. Voici par exemple la répartition des rôles et responsabilités dans une refonte (figure 9-2).

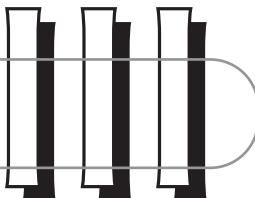
L'équipe de mise en production doit essentiellement disposer de compétences techniques et de connaissances des outils logiciels utilisés dans les mises en production. Les membres de l'équipe doivent évidemment disposer d'une vision claire de l'infrastructure et des services de l'entreprise.



* DataBase Administrator : Gestionnaire de base de données

Figure 9-3 : Rôles et responsabilités dans la gestion des mises en production

PARTIE



Fourniture des services informatiques

Au sein d'ITIL, le livre couvrant la fourniture des services correspond aux activités de conception et de prévision à plus long terme que l'on peut qualifier de « stratégiques » et qui permettent de répondre aux demandes des clients du système d'information en particulier sur les niveaux de services rendus. Le respect de ces niveaux de services exige la maîtrise des solutions permettant de garantir la fourniture des services du système d'information (disponibilité, performance, continuité de service...), mais demande également un contrôle efficace des aspects financiers. Ces processus sont évidemment orientés vers le développement de plans d'amélioration de la qualité des services informatiques livrés.

Dans cette partie, vous trouverez des détails sur chacun des processus de la fourniture des services.

Vous trouverez en particulier :

- Chapitre 10 – La gestion des niveaux de service
- Chapitre 11 – La gestion de la capacité
- Chapitre 12 – La gestion de la disponibilité
- Chapitre 13 – La gestion de la continuité de service
- Chapitre 14 – La gestion financière des services

GESTION DES NIVEAUX DE SERVICE



LA GESTION DES NIVEAUX DE SERVICES PERMET DE NÉGOCIER ET DE FORMALISER LES ENGAGEMENTS.

La gestion des niveaux de service

Depuis quelques années, les DSI sont confrontées à la concurrence acharnée que les grandes sociétés de services informatiques se livrent entre elles et parfois avec leurs clients. De plus en plus, les services proposés par ces SSII incitent les entreprises à gérer leur informatique comme un partenaire externe fournisseur de service. Mais que cette externalisation soit bien réelle ou seulement virtuelle n'empêche pas de traiter cette relation à l'image d'un lien commercial entre la DSI et l'entreprise. Comme toute relation d'affaire, la formalisation des accords entre les deux parties est indispensable et permet par exemple de préciser les objectifs à atteindre, les règles de négociations, et pourquoi pas, comment régler les litiges. La formalisation de ces accords au sein d'un document contractuel est le but de ce processus.

Vue d'ensemble

Dans une optique de maintien et d'amélioration de la qualité des services informatiques, il est indispensable de valider formellement les besoins et les exigences des clients (SLR). La gestion des niveaux de service (SLM) est responsable de cette formalisation par le biais d'accords de niveaux de service (SLA) qui permettront de maintenir et d'améliorer la qualité des prestations et des services informatiques dans un cycle permanent d'accord, de suivi et de rapport sur l'atteinte des objectifs et sur les actions menées pour les atteindre.

Pourquoi ?

Avant de s'engager sur la fourniture d'un service, il semble indispensable de s'entendre sur le contenu de ce service, c'est-à-dire ce qu'il faut livrer (le fond), mais également sur les contraintes liées à ce service et sur la façon

de présenter ce service (la forme). Combien d'applications dignes de ce nom pourraient être développées sans recourir à la rédaction d'un cahier des charges ?

Pour répondre à ce besoin, la mise en place de la gestion des niveaux de service (*Service Level Management* : SLM) permet de déterminer ces niveaux des services à fournir dans le but de supporter les métiers de l'entreprise. Le SLM permet de valider que les niveaux demandés ont été atteints et fournit les éléments indispensables permettant d'identifier les raisons d'un éventuel accord non atteint.

Concepts

Dans le but de comprendre et de définir les besoins de niveaux de service exprimés par les utilisateurs, le processus de gestion des niveaux de service propose de rédiger des accords écrits engageant le client sur ce qu'il attend et le fournisseur sur ce qu'il délivre. Sous la forme d'un cycle permanent, à l'image de la roue de Deming, le processus SLM permet l'élaboration, la coordination, la signature et le suivi des accords de niveaux de service (SLA). Cette revue permanente des SLA permet de s'assurer que la qualité de service nécessaire et financièrement justifiable est maintenue et améliorée régulièrement.

La qualité d'un service peut se mesurer par des critères objectifs et mesurables, mais la perception qu'un utilisateur en a n'est pas toujours à l'image de ces mesures. Ce processus permet de générer ces indicateurs objectifs dans le but de contrôler et d'améliorer le niveau du service rendu, mais surtout d'améliorer la perception de ce service par les utilisateurs, qui désormais connaissent précisément ce qu'ils ont demandé et ce à quoi la direction informatique s'est engagée.

Ce qui est important dans le terme SLA est l'accent qu'il faut s'attacher à mettre sur le mot « accord » : celui-ci ne doit pas être utilisé comme moyen de pression de l'une des deux parties sur l'autre, sous peine d'obtenir l'effet inverse, et de monter les protagonistes l'un contre l'autre. Un mode de fonctionnement basé sur le partenariat permet d'être bénéfique aux deux parties. Optimiser l'équilibre délicat entre les exigences des clients et des utilisateurs d'une part, et les engagements de la direction informatique en terme de capacité, de disponibilité et de coût d'autre part, exige que chacun connaisse et comprenne bien les conséquences des décisions à prendre. Le processus de gestion des niveaux de service permet de mettre en place le dialogue nécessaire dans la relation client/fournisseur afin d'y parvenir.

Périmètre

Comme l'illustre la figure 10-1, la gestion des niveaux de service (SLM) concerne tous les éléments composant le système d'information. Elle

comprend la mise en place des accords de niveaux d'un point de vue fonctionnel (SLA) entre le client (entreprise, utilisateurs, etc.) et le fournisseur interne, représenté par la direction informatique. Ces accords sont ensuite transposés en obligations techniques et représentent les accords de niveaux opérationnels (OLA ou *Operational Level Agreements*). Enfin les éventuels contrats sous-jacents ou contrats de sous-traitance qui concernent les fournisseurs externes, sont définis dans des documents complémentaires (UC ou *Underpinnings contracts*).

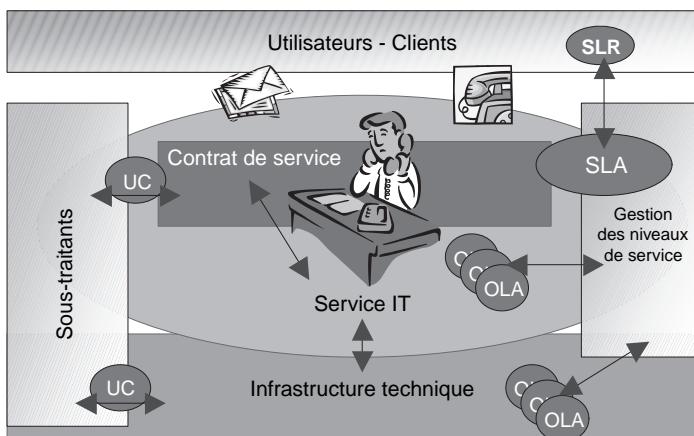


Figure 10-1 : Les différents contrats et engagements de la gestion des niveaux de service

Terminologie

SIP

À l'image de la roue de Deming, le SIP (Service Improvement Program) correspond au programme d'amélioration permanente de la qualité des services informatiques. Il se déroule dans un cycle ininterrompu de mise en action, de contrôle, de validation et de modification.

SLR

Le SLR (Service Level Requirement) correspond globalement à l'expression des besoins des clients et des utilisateurs. Il s'agit peu ou prou du cahier des charges de ce qui est attendu dans le but de soutenir l'activité de l'entreprise.

CS

Le catalogue de services définit les services informatiques disponibles au sein du système d'information (messagerie, bureautique, outils de gestion divers, ERP, sauvegarde, anti-virus, etc.). Il documente les principales

caractéristiques de ces services (disponibilité horaire, performance, capacité, coûts, etc.).

SLA

L'accord de niveaux de service est un document écrit qui définit des objectifs précis et spécifiques à ce service. Il engage les deux parties (clients et fournisseurs) sur les niveaux à atteindre en termes de disponibilité, de capacité et de coûts, et permet l'évaluation des performances de l'organisation informatique lors de la fourniture et le support de ce service.

OLA

Un OLA est la déclinaison en termes technique de la convention de niveaux de service signée par les utilisateurs. Ce document permet de placer les ressources techniques (humaines, matérielles, logicielles, etc.) en regard des demandes exprimées dans le SLR et validées dans le SLA.

UC

Les contrats de sous-traitance (*Underpinning Contract*) associés aux services doivent également être documentés dans le cadre de la gestion des niveaux de service. Ils doivent être régulièrement ré-évalués afin de valider qu'ils remplissent bien le rôle qui leur est attribué dans l'atteinte des objectifs du SLA.

Description du processus

Flux du processus

Toujours dans l'optique d'amélioration de la qualité, le processus de gestion des niveaux de service reprend le concept de la roue de Deming. Cette mise en œuvre d'un processus cyclique permet de revoir continuellement les tâches à accomplir en ayant des mesures objectives et concrètes provenant du fonctionnement du processus.

Les principaux interlocuteurs du processus en entrée sont les clients et les utilisateurs. Ce sont les personnes qui expriment leurs besoins et pour qui le service est délivré.

Plusieurs autres processus d'ITIL participent également, et en particulier pour les entrées. Les principaux sont la gestion de la capacité, la gestion financière, la gestion de la disponibilité, la gestion de la continuité de service, mais également la gestion des configurations, ou la gestion du changement, qui doivent s'assurer que les niveaux de service ne sont pas perturbés par leurs interventions.

Comme on peut le voir sur la figure 10-2, les différentes activités liées à la gestion des niveaux de service comprennent quatre grandes familles qui sont la planification, la réalisation, la validation et enfin l'amélioration des contrats de service.

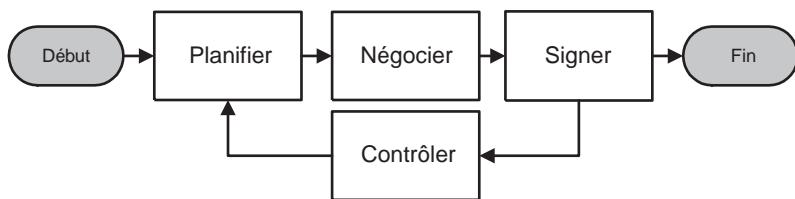


Figure 10-2 : Flux simplifié de la gestion des niveaux de service

Planifier

La phase de planification correspond globalement à la production du catalogue de services. Ce recueil exhaustif des services délivrés par la direction informatique doit permettre ensuite de proposer le brouillon de SLA aux utilisateurs. Mais avant de lancer le processus complet, une évaluation et/ou une mesure de la satisfaction des clients envers les services semble indispensable.

Une fois terminé, le catalogue doit être publié le plus largement possible vers les utilisateurs et son accès doit être le plus simple et le plus complet possible.

Réaliser

La phase de réalisation débute par le recueil des demandes exprimées par les utilisateurs (SLR) en réponse à la publication du catalogue des services. Après analyse de cette demande, il faut entreprendre la rédaction d'un projet du SLA, puis la négociation de ce projet avec les clients et les utilisateurs. Cette phase de négociation doit évidemment permettre de s'accorder sur les engagements de chacun, puis être formalisée dans le document définitif. Cette négociation est également l'occasion de valider l'adéquation de ce SLA avec les OLA et les UC.

Tant dans le catalogue de services que dans le SLA, les termes employés doivent être aisément compréhensibles par les utilisateurs. On évitera évidemment le jargon technique, les acronymes et les sigles incompréhensibles et tout autre terme abscons cher à l'informaticien moderne... Si l'utilisation de ce type de langage semble naturelle dans une conversation technique entre professionnels, il est réellement de nature à rebouter tout utilisateur peu au fait de la technologie employée. Ce type de situation peut d'ailleurs

conforter l'impression persistante de l'informaticien dans sa tour d'ivoire qui refuse de s'abaisser au niveau des utilisateurs...

Au-delà de l'aspect technique du vocabulaire utilisé, les termes employés ne doivent pas laisser la place à l'incertitude ou au doute. Chaque service doit être défini sans ambiguïté, ce qui est le garant d'une parfaite compréhension des engagements de toutes les parties, afin d'éviter des litiges éventuels liés à l'interprétation des contrats. Dans le cas d'entreprises multinationales, il est indispensable de traduire les SLA et autres documents dans la ou les langues les plus parlées dans l'entreprise et prendre en compte la dimension multiculturelle qui peut parfois conduire à des interprétations différentes.

Valider

La phase de contrôle et de suivi de la gestion des niveaux de service permet d'identifier les éventuels dysfonctionnements dans le processus. Cette phase permet également d'obtenir les informations et les métriques nécessaires au pilotage efficace du processus ainsi qu'à la production régulière de comptes-rendus. Le but de cette validation cyclique est d'obtenir des pistes d'amélioration de la qualité du service rendu.

Améliorer

La phase d'amélioration permet de boucler le cycle. C'est au cours de cette période que l'on peut revoir le SLA qui a été signé en fonction des mesures de son efficacité, et proposer des améliorations.

Planification et mise en œuvre

Avant la mise en place du SLA, il est important de mesurer ou d'évaluer la satisfaction actuelle des clients envers le service proposé. Comment annoncer une amélioration de la qualité de service si l'on ne sait pas d'où l'on est parti ?

Comme on peut le voir sur la figure suivante (figure 10-3), les quatre phases de planification, de négociation, de contrôle puis d'amélioration peuvent se diviser en étapes distinctes au cours desquelles seront élaborés les différents documents formels engageant l'un à l'autre, la direction informatique et ses clients.

Catalogue de services

Au cours du temps, les multiples ajouts au système d'information et les évolutions des solutions proposées par la direction informatique compliquent singulièrement la perception des services aux yeux des utilisateurs. L'élaboration d'un catalogue permet d'obtenir une vue précise et synthétique des services proposés par le système d'information.

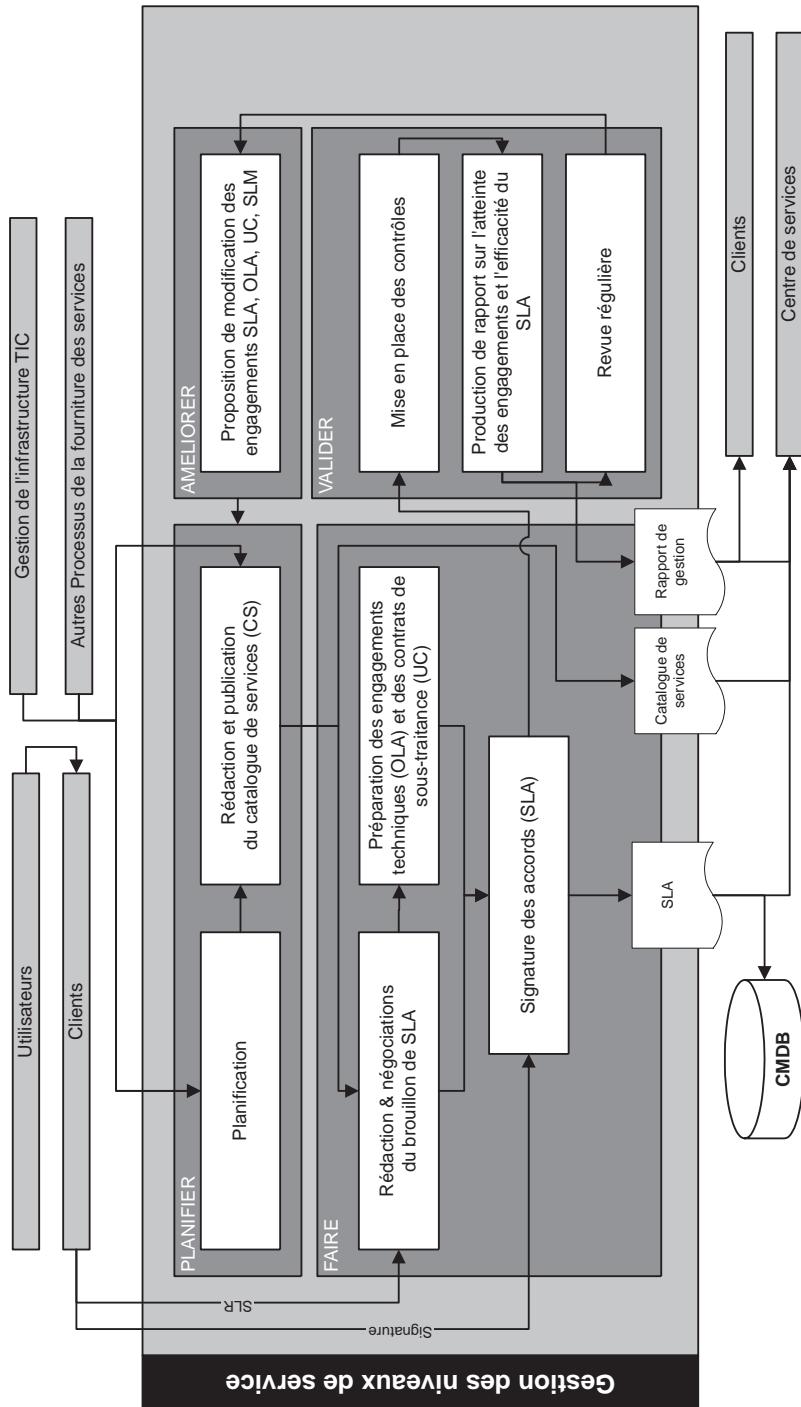


Figure 10-3 : Relations entre les activités du processus de gestion des niveaux de service

Le recensement des services proposés au sein du système d'information peut être grandement facilité par la consultation de la CMDB. C'est le cas par exemple du service de messagerie qui peut être composé d'un service de courrier électronique, du réseau, d'un anti-virus, d'une sauvegarde régulière, d'un stockage personnel sur disque, etc. C'est également le cas avec un service de transfert de fichiers entre deux sites qui, en plus du matériel et du logiciel, fait intervenir une procédure de réalisation de l'envoi des fichiers.

Comme dans le cas de la taxinomie des configurations, la documentation des services peut donner lieu à des répartitions basées sur des critères techniques, métier, organisationnels, géographiques, etc. Un service au sens utilisateur peut éventuellement être composé de plusieurs autres services qui peuvent être informatiques ou non. C'est-à-dire que ces services peuvent être composés de matériels, de logiciels ou même de procédures diverses.

La répartition des services peut se faire selon une organisation en service métier (c'est-à-dire vue par le client), en infrastructure, en application, mais en règle générale, il peut être très efficace de demander aux clients les services qu'ils utilisent et comment ceux-ci participent à leurs activités.

Catalogue de services et CMDB

Le catalogue de services peut être utile dans plusieurs autres processus de la gestion des services. Il peut par exemple servir de base à l'analyse de l'impact sur l'activité de l'entreprise (BIA ou *Business Impact Analysis*) au cours de la préparation du plan de continuité d'activité des services informatiques (*IT Service Continuity Planning*), ou sur les besoins en capacité (*Capacity Management*). Pour faciliter la réutilisation de ce catalogue de services par d'autre processus ITIL, il est recommandé de stocker ce catalogue dans la CMDB.

D'un point de vue fonctionnel, les clients peuvent obtenir ce qui est en accord avec les objectifs de l'entreprise et qu'ils peuvent justifier financièrement. Dans le cas d'une demande irréaliste ou sans rapport avec l'activité, la direction de l'entreprise doit intervenir directement.

Expression des besoins des clients (SLR)

Après avoir proposé un catalogue de services disponibles aux clients, il faut valider que ces services répondent bien aux demandes des utilisateurs. Cette partie, plutôt sensible, gagnera à être traitée selon un mode itératif. Sans aller trop loin, ce qui peut placer les clients devant un fait accompli, la production d'un modèle de document standard reprenant les informations du catalogue de services permet de générer une première ébauche et donc de gagner du temps. Ce document de travail permet en plus de poser un ensemble de questions auxquelles on ne pensera peut-être pas immédiatement en débutant les discussions avec une page blanche.

La première étape peut être celle de la mise en place de la structure de base des accords (SLA) afin de les calquer soit à l'organisation, soit aux services.

L'étape suivante consiste à interroger les clients sur les éléments qui leur semblent les plus importants dans les services dont ils ont besoin. Il faut définir les horaires et les conditions de disponibilité, les capacités nécessaires

dans le cadre d'une activité normale ainsi qu'en cas de service dégradé suite à une défaillance du système.

Une fois définie la structuration des accords, un premier document doit être ébauché sur lequel on peut revenir lors des prochaines itérations. Impliquer les clients dès le début de ces itérations va permettre de mieux cerner leurs besoins, et d'éviter leur sentiment de se voir imposer quelque chose qui ne répond pas à leurs attentes.

Conception du SLA

Le processus de gestion des niveaux de service doit concevoir la structure de SLA la plus appropriée pour s'assurer que tous les services et tous les clients sont couverts. Les structures les plus évidentes sont alors liées au client ou au service.

Dans le cas d'un accord basé sur le client, le SLA couvre tous les services qu'il utilise. Ce type d'accord est idéal pour le client qui n'a plus qu'un seul interlocuteur identifié.

Dans le cas d'un accord basé sur le service, chaque SLA couvre tous les utilisateurs d'un unique service. Ce cas est plus complexe à gérer, puisqu'il regroupe des besoins différents par groupe d'utilisateurs, et parfois des contraintes supplémentaires liées aux infrastructures ou à l'implantation géographique. L'avantage de cette solution réside dans le fait qu'elle est directement calquée sur le catalogue de services.

On peut évidemment envisager une solution basée sur une combinaison des deux types d'accord, mais en prenant garde de ne pas créer de doublons dans les contrats.

Pour certains services, et donc certains SLA, on peut envisager la mise en place d'accords répartis selon différents niveaux dans l'entreprise. Par exemple, on peut envisager un SLA de « niveau entreprise » qui couvre les services et niveaux de service communs à l'ensemble des clients. Le second niveau ou « niveau client » couvre tous les services et niveaux de service spécifiques à un groupe de clients. Enfin le troisième « niveau service » qui couvre un service utilisé par un client spécifique.

Lors de la rédaction du SLA, le niveau entreprise s'applique par défaut à tous les services, sauf si des conditions particulières sont définies aux niveaux suivants.

Le document final du SLA doit contenir un certain nombre d'informations. Les éléments communs à tous les SLA concernent l'introduction du document qui décrit brièvement le contexte et précise la date de signature, de revue, de début et de fin de l'accord.

Les chapitres suivants doivent annoncer le périmètre de l'accord, les responsabilités du fournisseur de service et des clients, et décrire chaque service couvert par ce SLA. On trouvera en particulier l'horaire de disponibilité

« normale » du service ainsi que les possibilités d'extensions de couverture. Les horaires spéciaux et jours fériés doivent évidemment être stipulés, surtout dans un contexte international où chaque pays dispose de jours chômés différents.

Concernant la disponibilité et la fiabilité du service, l'engagement pris par la direction informatique doit également être décrit sous forme d'un pourcentage sur les heures de service et un nombre maximum de ruptures de service, ou le temps moyen de disponibilité du système (MTBF), ou le temps moyen entre deux incidents (MTBSI). Les aspects sécurité, et notamment les obligations des utilisateurs dans ce domaine, doivent être stipulés dans le contrat afin que nul ne puisse en invoquer la méconnaissance. Cependant, cela ne fait pas double emploi avec la publication de la politique de sécurité de l'entreprise, ainsi qu'avec une éventuelle charte qui peut être annexée au contrat de travail.

Les informations portant sur le support du service et l'accès au centre de services doivent être précisées. On doit y trouver en particulier les heures d'ouverture du support, les jours fériés, le temps maximum de réponse et de résolution des incidents.

Le détail des objectifs de performance des services doit être indiqué clairement, c'est-à-dire de façon compréhensible pour les utilisateurs. Ces indications doivent fournir des informations de performance en situation normale (les niveaux de débit du réseau, le temps de réponse d'une application, le temps de réponse d'une transaction, le nombre d'accès simultanés, etc.), et indiquer les mêmes informations en mode dégradé, par exemple lors du fonctionnement sur le système de secours.

Concernant le volet financier du SLA, si la facturation des services auprès des directions métier est envisagée, les détails concernant la périodicité et les formules de calcul doivent être annexés au document final. Ce chapitre concerne également l'éventualité de pénalités suite au non-respect de l'accord dont les éléments (règles de calcul, motifs et seuils de franchissement, etc.) doivent être totalement clairs pour tous les signataires du contrat.

Négociations et signature du SLA

Une fois que les besoins des clients ainsi que les moyens de l'entreprise ont été pris en compte, et que les documents contractuels de SLA ont été rédigés, arrive le temps des signatures. Outre le côté formel de la chose, cette étape apporte le petit côté officiel qui permet souvent une prise de conscience du sérieux de l'engagement. D'ailleurs, c'est parfois à ce moment que la situation se complique et que plus aucun signataire ne souhaite s'engager...

Pour les clients, il faut tout d'abord identifier le bon interlocuteur, c'est-à-dire celui qui représente vraiment les intérêts de l'entreprise et de sa direction, et non pas une personne trop éloignée des utilisateurs ou qui ne représente

que son propre intérêt ou celui d'un trop petit nombre d'utilisateurs. L'idéal est de « recruter » les signataires parmi les éventuels représentants officiels des clients, s'ils sont proches des préoccupations des utilisateurs. Enfin, le niveau hiérarchique du signataire donnera un message clair sur l'importance et l'engagement que l'entreprise accorde au SLA... Dans un sens, comme dans l'autre !

Pour le fournisseur du service qu'il soit interne ou externe (infogérant, maintenance, personnel en régie ou autres), la signature de l'accord permet de valider, par le biais de son représentant, que l'engagement qu'il prend est réaliste, atteignable et financièrement acceptable. Dans le cas contraire, le contenu de l'accord doit être renégocié jusqu'à l'acceptation de toutes les parties.

Un des objectifs prioritaires de la gestion des niveaux de service est de communiquer vers les utilisateurs. Dans ce cadre, il semble particulièrement important de présenter les accords de SLA au plus grand nombre d'utilisateurs de ce contrat. Après la signature du SLA, l'accord doit donc être publié et diffusé vers les utilisateurs, les clients, et évidemment les membres de l'équipe informatique, afin que chacun puisse y faire référence en ayant connaissance de son existence et de son contenu.

Le centre de services peut jouer un rôle important dans cette étape de diffusion. De part sa position d'interlocuteur privilégié des utilisateurs, il peut être engagé très tôt dans le processus de gestion des niveaux de service et devenir ainsi un relais efficace de ces accords pris entre les utilisateurs et la direction informatique.

En revanche, laisser le centre de services en dehors des négociations ou ne pas le tenir au courant des contrats de service, sera sanctionné immédiatement par une perte de confiance rapide de la part des utilisateurs.

Contrôle du SLA

Une fois mis en place l'accord de niveaux de service, la mesure de l'atteinte de ces niveaux par le service doit être effective. Cette métrologie est souvent complexe, et son interprétation peut parfois être à l'origine de conflit.

Pour éviter ce désagrément, il faut tout d'abord aligner les dimensions de l'accord avec les moyens techniques disponibles dans l'entreprise. Si l'on ne peut pas mesurer quelque chose, mieux vaut ne pas s'engager sur cette chose, sous peine de voir apparaître une source inépuisable de conflit. De plus, ces outils et méthodes de métrologie doivent être définis en même temps que la rédaction des accords afin de faire valider cette partie par les signataires. Enfin, s'il n'existe pas encore de données provenant de mesures précédentes, il est recommandé d'utiliser un SLA provisoire tant que les mesures n'ont pas confirmé la faisabilité de la fourniture du service et donc la signature du contrat.

Débuter avec des problèmes simples pour obtenir un succès rapide !
Lors de la négociation puis la mise en œuvre du premier SLA, il est recommandé de le démarrer en tant qu'accord pilote. Dans cette optique, il semble assez « stratégique » de bien identifier des clients enthousiastes et moteurs pour le projet, et surtout de choisir un domaine simple ne générant pas de problèmes importants ou permettant d'obtenir des résultats rapides. Un sondage préalable sur la perception des services et de l'efficacité de l'équipe informatique peut aider dans le choix des clients pilotes.

Imaginons un SLA portant sur la performance d'un service de messagerie. Tout délai de livraison qui dépasse le seuil fixé doit être signalé. Mais dans ce cas, s'agit-il d'un problème réseau, d'un problème du poste client, d'un problème du serveur, d'un virus ?

Concernant les mesures utilisées lors du contrôle du SLA, aligner l'accord avec la perception des services qu'en a l'utilisateur ou le client est le plus important, mais c'est aussi le plus difficile. La surveillance de différents composants de la chaîne ne garantit pas la disponibilité du service du point de vue du client. En effet, il est souvent impossible, car très coûteux, de surveiller tous les éléments situés entre l'application sur le serveur et l'application sur le poste client. Entre ces deux extrémités s'intercalent un grand nombre d'équipements de l'infrastructure, de matériels et de logiciels, qu'il est parfois impossible de contrôler.

Certains logiciels permettent de valider cette vision de bout en bout en simulant le comportement d'un utilisateur dans le lancement de transaction, puis en mesurant le temps de réponse. On peut également faire appel au centre de services dans la surveillance de la perception du service par les utilisateurs. Dans ce cas, il est nécessaire que ces derniers signalent immédiatement les dysfonctionnements qu'ils rencontrent pour aider au diagnostic. D'ailleurs, le centre de services est déjà mis à contribution dans la mesure du temps de réponse de l'équipe informatique ou du sous-traitant lors de la résolution des incidents et des problèmes.

Le SLA n'est pas le seul élément qui nécessite un contrôle. Les documents qui en proviennent doivent également être revus régulièrement. Les OLA qui sont la transcription opérationnelle des SLA doivent détailler niveau par niveau, ou équipe par équipe, les objectifs des accords des niveaux de service. Chaque OLA doit faire l'objet d'un contrôle afin de valider que la réponse technique est adaptée à l'engagement pris dans le SLA. Ces contrôles réguliers sont l'occasion de valider les contrats de sous-traitance (UC) et l'adéquation de ce type de réponse aux besoins du client. En effet, il ne suffit pas de valider que le fournisseur fait correctement son travail, mais également que ce travail a encore un sens dans le système d'information de l'entreprise.

Mesures et contrôles

Les SLA doivent être revus périodiquement. Les rapports de gestion et les réunions de suivi doivent être définis dans le document de SLA signé par les clients. Afin de juger de l'efficacité du processus, plusieurs indicateurs de performance sont utilisables. On trouve notamment la proportion des services couverts par des accords (associés ou pas à des OLA et des UC), ou le pourcentage d'objectifs atteints, ainsi que le nombre et la gravité des éventuelles ruptures de service. Plus simplement, le rapport de contrôle du processus doit inclure des informations concernant le suivi des SLA et les rapports réguliers qui sont produits à cette occasion.

L'analyse des tendances comme l'augmentation du nombre d'objectifs atteints, la diminution des coûts de production à fonctionnalité identique,

ou l'amélioration de la perception globale des clients, sont autant de révélateurs qu'il convient de prendre en compte.

Coûts

Les coûts associés à l'implantation du processus de gestion des niveaux de service concernent essentiellement les dépenses de personnel (salaires, formation, consultants extérieurs, etc.) et les outils logiciels de support du processus (création de rapport, surveillance, etc.). Certaines solutions logicielles permettent de gérer les SLA au sein d'une application plus générique incluant la prise en charge d'autre processus ITIL. En conséquence, le coût de ce type de logiciel est partagé par l'ensemble de ces processus.

Mais une fois encore, il faut voir cette dépense comme un investissement à valeur ajoutée plutôt qu'un simple coût dans un tableau financier.

Documents et rapports

Outre les classiques rapports de gestion destinés au contrôle de l'efficacité du processus, les documents sont essentiellement contractuels comme les SLA, OLA et UC, qui seront signés par différents interlocuteurs et niveaux hiérarchiques dans l'entreprise, ou parmi les fournisseurs.

Conséquences

Si le processus est correctement amené, les bénéfices que l'on peut attendre de l'implantation de la gestion des niveaux de service sont multiples.

Tout d'abord, le gain le plus important de ce processus est certainement l'amélioration de la communication entre la direction informatique et ses clients. Cet aspect que l'on ne doit pas négliger, peut faire sourire, s'il n'existe encore autant d'entreprises où l'informatique n'est vue que comme une boîte noire qu'il suffit d'alimenter en énergie, c'est-à-dire en finance, pour qu'elle produise le résultat escompté. C'est oublier un peu vite qu'une voiture sans chauffeur reste un tas de ferraille !

Ensuite, puisque l'élaboration des services du système d'information est alignée aux besoins définis dans les accords passés avec les clients, cela entraîne une amélioration des relations et de la satisfaction des clients. Désormais, les deux parties ont une vision claire de leurs rôles et de leurs responsabilités. Le SLA permet en particulier d'identifier les objectifs spécifiques à atteindre pour chaque service, ainsi que les métriques, le mode de contrôle et de compte-rendu associé. Un suivi permanent peut être réalisé grâce à ces mesures afin d'identifier les points faibles du système d'information et de concentrer les efforts de l'équipe informatique sur les domaines définis comme essentiels par les directions métier.

Enfin, les gains d'efficacité liés à cette implantation produisent une amélioration permanente de la qualité de service ainsi qu'une diminution des interruptions de service. La conséquence induite est une substantielle économie budgétaire, sans compter l'éventuelle facturation interne qui peut en découler, et permettre l'équilibre financier du budget de la direction informatique.

Cependant, ne soyons pas naïfs. Les gains envisagés dans le cadre de ce processus sont à la hauteur des problèmes potentiels. Le plus important d'entre eux est sans nul doute la possibilité que le contrat de services soit envisagé comme un paravent pour chacun des intervenants. Dans ce cas, les contrats de service ne sont vus que comme un système d'arbitrage des situations conflictuelles. Si ce document doit ensuite servir à monter les utilisateurs contre la direction informatique, ou que celle-ci l'invoque systématiquement pour échapper à ses obligations de production, il y a fort à parier que l'antagonisme entre les utilisateurs et les informaticiens ne cesse d'empirer.

Le premier écueil qu'il faut éviter concerne la définition du catalogue et des contrats de service lors de la phase d'analyse. Ceci permet en particulier d'éviter de signer des objectifs irréalistes ou qui ne soient pas basés sur des objectifs réels de l'entreprise.

La formalisation et la rédaction des documents sont également très importantes. Si les documents sont trop longs ou trop confus, si les termes employés sont trop techniques ou ambigus, ou si les responsabilités sont floues, cela peut entraîner des situations non prévues nécessitant un arbitrage qui peut remettre en cause l'autorité du responsable du processus.

Rôles et responsabilités

Le processus de gestion des niveaux de service doit être assumé par un responsable, qui sans être nécessairement dédié, doit pouvoir y consacrer un temps non négligeable. C'est la raison pour laquelle ce rôle ne peut être assumé par le responsable d'un processus de type « pompier » comme c'est le cas pour la gestion des incidents, ou encore pour la fonction de support du centre de services.

De plus, le rôle demandant de fréquentes négociations à différents niveaux de l'entreprise, le responsable doit disposer de l'autorité et de la vision nécessaires ainsi que du soutien de la direction de l'entreprise.

Rôle

Le rôle du responsable du processus est lié au concept de l'amélioration continue de la qualité du service rendu. Dans ce but, le responsable du

processus devra régulièrement reprendre et évaluer les différents éléments et documents utilisés dans le processus. Le processus exige également un niveau important de compte-rendu et de publication des résultats aux utilisateurs.

Du point de vue de la gestion pure, il doit proposer et entretenir une structure de SLM appropriée pour l'entreprise puis y inclure la structure des SLA, OLA, et contrat de sous-traitance (UC).

Il doit donc créer et maintenir un catalogue des services existant dans le système d'information, puis négocier le SLA avec les utilisateurs, en partant de l'expression de leurs besoins (SLR), sans oublier de négocier les OLA avec le service informatique interne, et les UC avec les fournisseurs externes. Ensuite, et au moins une fois par an, l'ensemble de ces documents doit être revu afin de valider leur adéquation avec les besoins de l'entreprise.

Compétences

Le responsable du processus doit posséder une bonne compréhension des services informatiques et des facteurs qui affectent la fourniture de ces services aux clients. Dans cette optique, il doit disposer d'une bonne compréhension du métier des clients et comprendre comment l'informatique contribue à ses activités.

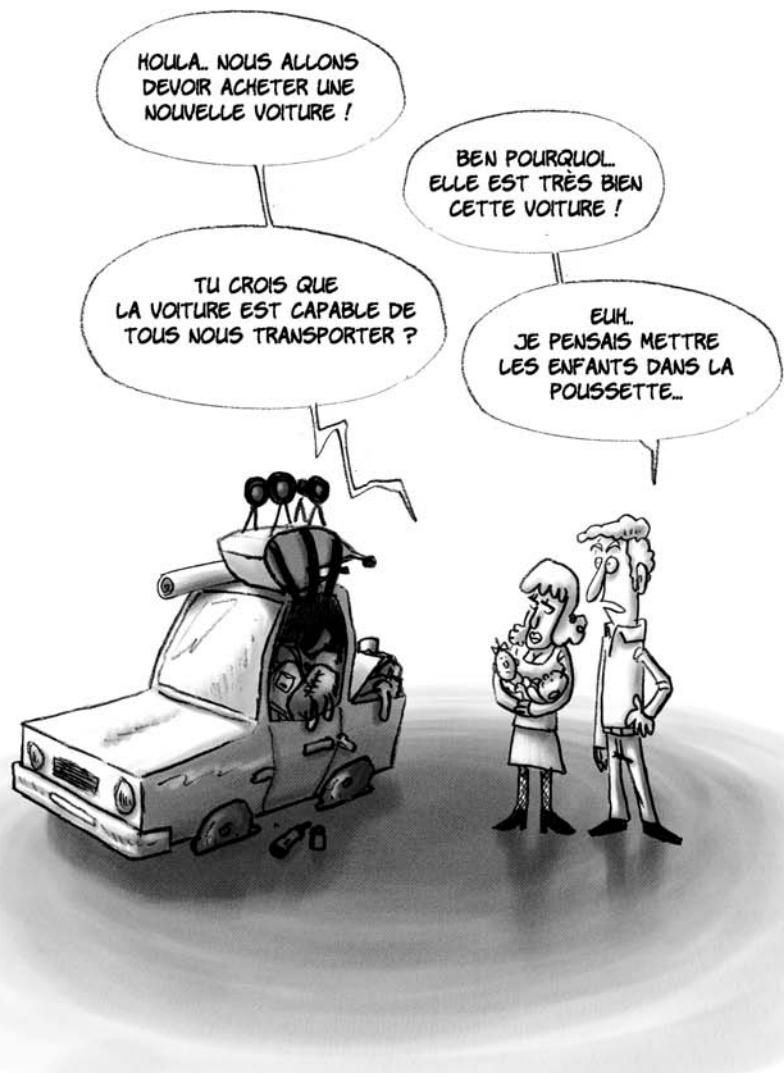
Dans l'hypothèse de négociations fréquentes, il doit posséder une grande capacité d'écoute et de synthèse, mais surtout une bonne résistance au stress, une bonne dose de patience, et un zeste d'endurance. Ses capacités de communication écrites et orales associées à son sens de la négociation seront déterminantes dans ce domaine.

Il doit également disposer d'un minimum d'expérience dans la manipulation des contrats ainsi qu'une expérience de la gestion de personnel.

La négociation peut faire intervenir de nombreux acteurs. Le responsable du processus doit donc pouvoir intervenir et dialoguer à tous les niveaux de l'entreprise, tant du coté utilisateur que du coté informatique, ce qui implique de pouvoir adapter son langage en fonction de ses interlocuteurs. Ceci implique d'avoir une compréhension raisonnable des technologies sous-jacentes, et la capacité à transmettre les concepts et les impératifs techniques en termes métier facilement compréhensibles par les utilisateurs et vice-versa.

Enfin, l'analyse de nombreuses sources d'informations, susceptibles de produire de volumineux rapports de mesure, implique une bonne compréhension des principes d'analyse et des outils statistiques, dans le but de présenter régulièrement des comptes-rendus et de publier des résultats.

GESTION DE LA CAPACITÉ



LA GESTION DE LA CAPACITÉ, C'EST ANTICIPER L'ÉVOLUTION DES BESOINS AFIN DE PROPOSER LE JUSTE NIVEAU DE RESSOURCES.

La gestion de la capacité

Un monde en évolution. Un marché et un environnement mouvants. Des fusions et des acquisitions, des licenciements et des embauches. Un système d'information en changement permanent et des besoins de plus en plus importants (espace de stockage, puissance de calcul, vitesse de communication, etc.). Les performances informatiques représentent désormais un facteur différentiateur pour l'entreprise et permettent des gains de part de marché... Qui peut encore espérer se passer de la gestion de la capacité ?

Vue d'ensemble

La gestion de la capacité est le processus responsable d'assurer que la capacité de l'infrastructure du système d'information est en mesure de répondre aux demandes de l'entreprise. Par capacité, on entend la performance de traitement, le volume de stockage ou le débit des liens de communication, au sein du système d'information. Le but du processus est donc de s'assurer que les ressources matérielles, logicielles et organisationnelles sont adaptées aux besoins actuels et futurs de l'organisation, tout en restant financièrement justifiables.

Pour assurer cette mission, la gestion de la capacité doit tout d'abord mettre en place un suivi des performances, des volumes, et des débits, pour l'ensemble des services et des composants de l'infrastructure. Ce suivi va d'ailleurs permettre d'évaluer les options sur lesquelles il faut jouer pour optimiser l'utilisation des ressources existantes. Ces informations sont à l'origine d'une meilleure compréhension des futures demandes en ressource informatique. En définitive, tout ceci doit permettre de produire le plan de capacité du système d'information, en gardant à l'esprit que le principe de ce processus est que la capacité achetée est justifiable en termes de besoins métier, mais également qu'elle est utilisée de manière optimale.

Pourquoi ?

Avec l'évolution des systèmes d'information qui sont passés de systèmes centralisés monolithiques à l'informatique distribuée que nous connaissons actuellement, où les serveurs, les postes de travail et les moyens de communications sont parfois répartis sur plusieurs pays, on a pu observer une chute des prix vertigineuse. Cependant, il ne faut pas oublier que cette réduction du prix unitaire est largement compensée par les volumes considérés. Alors qu'il fallait auparavant s'équiper d'un gros ordinateur central (mainframe), il faut désormais aligner plusieurs dizaines de serveurs pour répondre aux attentes des utilisateurs.

D'un point de vue financier, il faut donc tenir compte non seulement des économies d'échelle envisageables sur les achats en volume de ce type de matériel, mais également sur le coût de la main d'œuvre nécessaire pour administrer ces équipements de plus en plus nombreux. De ce point de vue, la gestion de la capacité procure les informations indispensables permettant de bonnes négociations avec les fournisseurs.

Malheureusement, en règle générale, on constate que les achats informatiques sont justifiés sur une base individuelle ou au coup par coup, et non sur les besoins globaux de l'entreprise. Cette absence de projet d'investissement à l'échelle de l'entreprise implique que les prévisions d'évolution de la demande métier, qui sont pourtant un préalable à la mise en place des budgets, ne seront pas prises en compte. La conséquence est des plus simples : la gestion des capacités des serveurs ou des réseaux se fait essentiellement en réaction aux événements (incidents) signalés par le centre de services, ou au pire par les utilisateurs. Le problème est que le cycle de choix, de décision, d'approvisionnement et d'installation de ce type de solution matérielle est plutôt long. Cela implique qu'un délai parfois important s'écoule entre la découverte de la sous capacité et la mise en place de la réponse. Et le pire est que parfois, alors que la réponse technique vient d'être installée, le délai de mise en place a rendu obsolète cette solution, obligeant à reprendre l'ensemble du processus, mais en laissant les utilisateurs mécontents. Quant à la gestion des capacités du poste de travail, elle est la plupart du temps inexistante et le renouvellement du poste personnel est uniquement envisagé en termes financiers (amortissement, location, plan de financement).

Il est donc nécessaire de définir en amont une politique claire de renouvellement des différents types de matériels. La gestion de la capacité fournit justement les données nécessaires pour mettre en place cette politique. Elle définit entre autres ce qu'il faut remplacer (CPU, disques, réseaux, logiciels, etc.), quand cela est nécessaire, et combien cela va coûter.

Un exemple flagrant provient de l'espace disque disponible sur le système d'information. La gestion de la capacité permet de valider les besoins en stockage. Mais actuellement le coût du stockage est très faible et la tentation

est forte d'acheter plus que nécessaire en éludant ainsi l'indispensable gestion du cycle de vie des informations. En effet, il semble bien plus économique de ne pas gérer l'espace disque utilisé par les données de l'entreprise et par les utilisateurs. Lorsqu'un besoin d'espace se fait sentir, il suffit d'acheter de nouveaux disques et le tour est joué. On économise ainsi le temps de gestion de l'espace et on satisfait des utilisateurs qui insistent pour obtenir de la place supplémentaire. Mais le problème est loin d'être réglé, puisque cet espace héberge des données qu'il convient d'administrer, de sécuriser, de sauvegarder, etc. Autant de matériels en plus, d'heures de sauvegarde et de personnels dédiés à ces tâches... Donc autant de coûts supplémentaires induits par l'absence de gestion des volumes de données en amont.

Enfin, il faut comprendre que plusieurs autres processus d'ITIL risquent de manquer d'informations si la capacité du système d'information n'est pas gérée. Par exemple, comment la capacité risque-t-elle d'être affectée par le prochain changement ? La mise en place d'un nouveau service sera-t-elle possible avec la capacité actuelle ? Et enfin, la signature de ce SLA est-elle cohérente en regard des performances demandées ?

Concepts

Les principaux concepts liés à ce processus sont donc la compréhension des besoins de l'entreprise et la transcription de ces besoins en capacité informatique, puis l'assurance qu'il existe toujours une réserve de cette capacité informatique disponible et justifiable financièrement.

Périmètre

En dehors de la gestion quotidienne ou de la prise en compte des incidents, tous les aspects liés à la capacité et aux performances du système d'information sont de la responsabilité de la gestion des capacités. Cela concerne donc les différents matériels, serveurs, postes de travail, équipements réseaux et périphériques divers (baies de disques, sauvegardes, imprimantes, etc.). Cela concerne également les différents logiciels présents sur le système d'information, comme les systèmes d'exploitation et réseaux, les bases de données, les messageries, les applications développées en interne, et les logiciels achetés à l'extérieur. Il peut également arriver que le processus signale un manque de personnel pour assumer une opération dans le respect du SLA.

Terminologie

BCM

La gestion de la capacité métier (*Business Capacity Management*) permet de s'assurer que les besoins futurs de l'entreprise sont pris en compte et repris dans le plan de capacité de l'entreprise.

SCM

La gestion de la capacité des services (*Service Capacity Management*) concerne l'évaluation et le contrôle des performances sur lesquelles la direction informatique s'est engagée dans le SLA.

RCM

La gestion de la capacité des ressources (*Ressources Capacity Management*) se focalise sur les composants de l'infrastructure du système d'information.

CDB

La base de données de gestion de la capacité (*Capacity DataBase*) est une base de données « virtuelle » qui regroupe les informations en provenance de plusieurs sources de mesures distinctes. Elle sert de base lors de l'élaboration des rapports de gestion de la capacité.

Description du processus

Flux du processus

Les sources de données du processus sont multiples. On trouve évidemment les besoins des clients sous la forme de deux plans (plan de stratégie de l'entreprise et plan financier) sur lesquels s'est aligné le plan informatique et ses budgets internes. Une autre source d'informations importante provient des processus de gestion des incidents et de gestion des problèmes, qui signalent les événements liés à des performances limitées ou peu adaptées au contexte, ou qui signalent dans le cas d'un SLA, si les performances ne sont pas à la hauteur de l'engagement. La gestion du changement est également une source d'informations puisqu'elle indique les changements envisagés prochainement ainsi que leur impact sur la capacité de l'infrastructure. Enfin, ne négligeons pas l'importance des fournisseurs de technologie qu'il faut prendre en compte lorsqu'une évolution majeure est annoncée, pouvant apporter de réels progrès et améliorer les capacités du système d'information à moindre coût, ou au contraire remettre en cause la validité de l'infrastructure et ajouter l'obsolescence aux problèmes de performances.

En interne, la gestion de la capacité est composée de trois sous-processus qui ont des activités communes mais des rôles très différents.

D'un point de vue prospectif, le BLM (gestion de la capacité métier) permet de déterminer les tendances de la consommation de ressource et, grâce à des modélisations et aux prévisions d'évolution de ces besoins, de s'assurer que les ressources nécessaires seront prévues et mises en œuvre en temps voulu.

La fourniture opérationnelle de la capacité est plus du ressort du SCM (gestion des capacités services) et permet de piloter les performances des services à l'aide d'un suivi permanent associant mesures et analyses, afin d'assurer l'équilibre entre les engagements du SLA et les performances livrées.

La prise en compte de la technologie sous-jacente de la capacité est l'objectif du RCM (gestion des capacités ressources), qui s'assure par le biais de mesures et de modélisations des performances, que tous les composants de l'infrastructure qui ont des ressources finies sont suivis, mesurés et analysés. L'objectif du RCM est également d'analyser l'évolution des tendances technologiques.

Dans chacun de ces sous-processus, on retrouve un ensemble d'activités qui vont encore une fois se succéder dans un cycle de Deming avec la surveillance, l'analyse, l'optimisation et l'implémentation.

Chacune de ces activités va produire un ou plusieurs éléments en sortie. En premier lieu, les données collectées par les sous-processus BCM et SCM sont utilisées en interne par le sous-processus RCM pour déterminer ce qu'il faut remplacer et quand cela doit être fait. Par la suite, plusieurs processus de la gestion des services utilisent des données en provenance de la gestion des capacités, comme la gestion des niveaux de service qui s'engage sur des performances, ou la gestion financière qui utilise ces données pour la mise en place des budgets et la prévision des achats.

D'un point de vue plus général, le processus de gestion de la capacité va également produire un ensemble de mesures et d'analyses qui vont permettre de fixer les seuils utilisés ensuite par plusieurs processus du support des services (incidents, problèmes) afin d'identifier si un dysfonctionnement provient d'un problème de capacité ou non.

Toutes ces informations sont stockées de manière plus ou moins centralisée dans la base de données des capacités (CDB) qui contient toutes les informations nécessaires aux sous-processus et héberge leurs résultats afin qu'ils puissent être exploités par les autres processus.

Enfin, le processus doit produire un plan de capacité qui présente le niveau d'utilisation des ressources actuelles et détermine les besoins futurs en capacité.

Planification et mise en œuvre

L'objectif prioritaire de la gestion des capacités est de s'assurer que les besoins actuels et futurs en matière de services informatiques seront pris en compte, prévus et mis en œuvre en temps voulu (BCM). Pour cela, il faut mettre en œuvre un certain nombre d'activités qui associent le suivi, l'analyse et le contrôle des services (SCM), mais également le suivi des ressources, de leur capacité individuelle et de leur disponibilité (RCM) (voir figure 11-1).

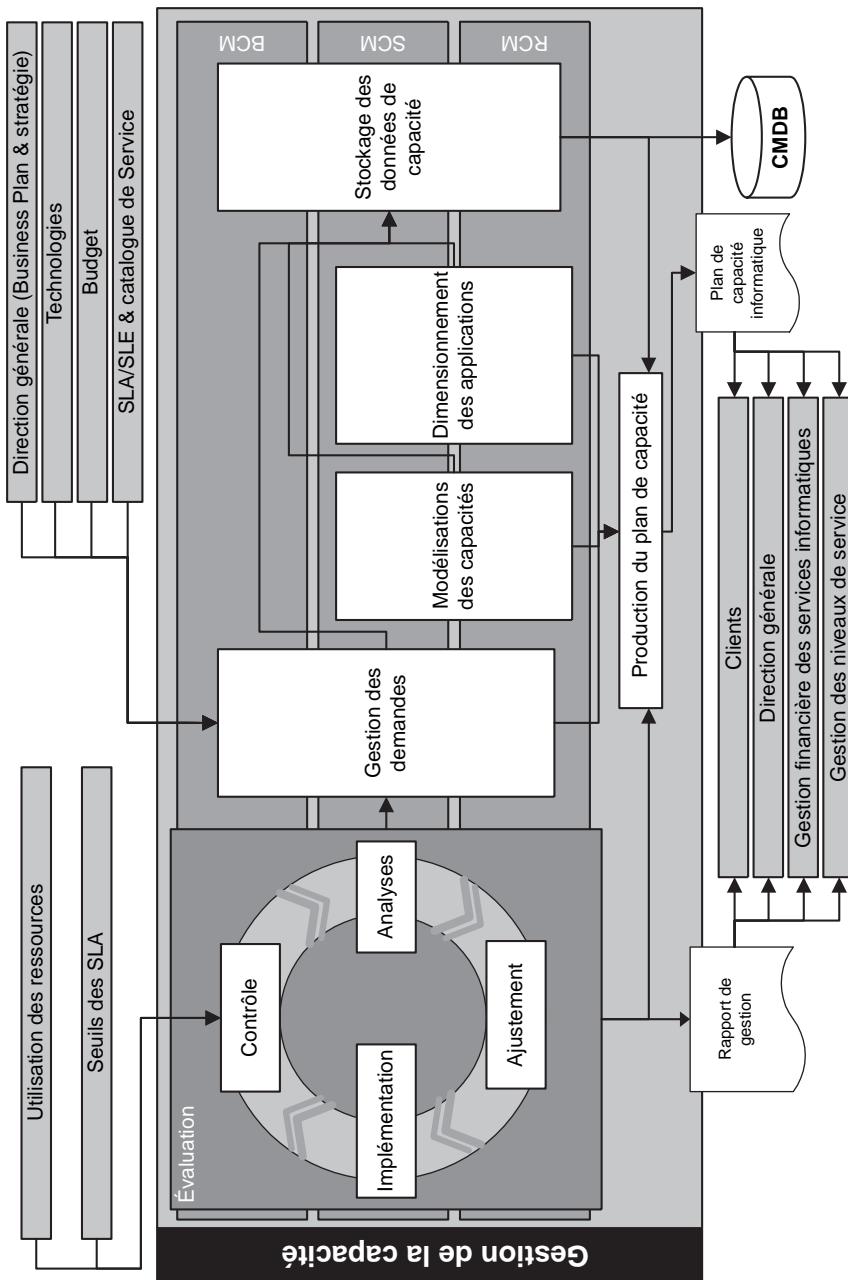


Figure 11-1 : Flux et activités internes de la gestion de la capacité

Ces trois sous-processus reposent sur plusieurs activités réactives ou pro-actives dont certaines doivent être menées cycliquement à l'image de la roue de Deming.

Parmi les activités itératives, on trouve notamment la surveillance du système d'information dans le but de suivre l'utilisation des ressources et des services. Pour surveiller le système, il faut tout d'abord mettre en place des outils afin de mesurer le taux d'utilisation des ressources (CPU, mémoire, disque), les débits réseaux, ou plus généralement le temps de réponse global d'une application. Il faut ensuite définir les seuils maximaux au-delà desquels une alarme est déclenchée et un rapport est généré, conformément aux SLA.

Après la surveillance, arrive l'analyse. Cette seconde opération itérative utilise les informations collectées précédemment dans le but d'identifier les tendances. Par mesure régulière et par comparaison avec des situations de référence, cette activité permet d'identifier les goulets d'étranglement, les applications mal conçues entraînant une consommation excessive de ressources, l'utilisation inefficace de la mémoire, et en règle générale, toutes les situations génératrices de problèmes.

Une fois ces problèmes identifiés lors de la phase d'analyse, l'étape suivante du cycle consiste à proposer des améliorations dans la configuration du système d'information afin d'augmenter les performances des services (*tuning*).

Le cycle est bouclé lors de l'implémentation des améliorations proposées lors de l'étape précédente qui fait alors appel aux processus de gestion du changement et de mise en production.

Certaines activités du processus se produisent plus ponctuellement. Parmi celles-ci, on trouve la gestion des demandes, la modélisation des ressources et le dimensionnement des applications.

La gestion des demandes a pour but d'arbitrer la demande en ressources informatiques à court et long terme. À court terme, lors de situation de pénurie, elle permet d'établir les priorités entre les services (en fonction des objectifs métier) et d'identifier ceux qui peuvent être stoppés pour permettre à d'autres de profiter de la ressource informatique rendue disponible. À plus long terme, elle permet d'optimiser l'utilisation des ressources afin de permettre au système de continuer de fonctionner malgré l'impossibilité d'investir dans une ressource supplémentaire, qui n'est pas justifiée financièrement. Il s'agit dans ce cas de limiter l'utilisation de la ressource en interdisant l'accès à certains utilisateurs ou en stoppant certains services, tout en restant bien sûr dans les limites imposées par le SLA, afin de ne pas nuire à l'activité de l'entreprise, ni à la réputation de la direction informatique.

Exemples d'améliorations.

Utilisation de systèmes d'équilibrage de charge sur le réseau, mise en place de disques parallèles (RAID 0), mise en place de zone tampon (*proxy*), optimisation de la stratégie de verrouillage des données de la base de données, augmentation de la mémoire vive pour éviter le swap (fait d'utiliser une partie d'un disque dur comme de la mémoire vive) sur disque, etc.

Exemple d'information sur un commutateur réseau dans la CDB.

L'entreprise va créer une nouvelle direction produit avec 150 utilisateurs supplémentaires. Le temps de réponse actuel des applications est rallongé par un commutateur trop chargé. La norme de charge de ce type de commutateur est de 40 % avec 400 utilisateurs. La charge actuelle du commutateur est proche de 48 % en continu avec 450 utilisateurs. L'achat du précédent commutateur est totalement amorti et un nouveau système financier permet de louer le matériel.

Exemple : place disponible sur le disque de stockage des utilisateurs inférieure à l'engagement pris dans le SLA.

Les différentes méthodes de modélisation des ressources informatiques telles que l'analyse de tendance, la modélisation analytique et la modélisation par simulation, permettent de connaître et d'anticiper le comportement des services dans des situations diverses de charge et de volume.

Le processus de gestion de la capacité est également d'une grande aide dans le dimensionnement des applications. Il permet d'estimer les ressources nécessaires au support d'une application dans le cadre des engagements du SLA. Ce dimensionnement est partie intégrante du cycle de développement et doit être intégré dès la phase de conception des applications, ou par une maquette dans le cas des logiciels achetés.

Les activités de stockage des données de gestion des capacités doivent être menées en continu. La base de données CDB (*Capacity Management Database*) est un élément fondamental de la réussite de la gestion de la capacité. Elle contient des données diverses portant sur les demandes métier (prévision de charge), l'utilisation des services (temps de réponse), le comportement technique normal (norme de temps de réponse), l'utilisation des ressources (charge unitaire et consolidée) et la dimension financière.

La base de données CDB permet en particulier de produire un ensemble de rapports sur le mode et le taux d'utilisation des ressources et des services. Elle permet également d'identifier un dépassement du seuil fixé sur une ressource, afin d'anticiper les problèmes que l'on peut rencontrer sur les SLA.

Enfin, le processus doit proposer de façon régulière un plan de capacité présentant les niveaux d'utilisation des ressources existantes, et les besoins futurs permettant de supporter l'évolution des services. Ce plan doit inclure des recommandations sur les technologies à prendre en compte pour la fourniture des ressources et sur les bénéfices que l'on peut en attendre, mais également sur l'impact de leurs mises en place et sur les coûts supplémentaires que cela va engendrer. La publication de ce plan doit être régulière et selon une période prédéfinie (annuelle, semestrielle, etc.) ou alignée sur un cycle de projets métier ou sur des budgets.

Mesures et contrôles

Le contrôle de la qualité du processus passe par l'analyse des indicateurs clés de performance. Ici, l'indicateur idéal semble être la faculté de la direction informatique à fournir la capacité nécessaire et suffisante à tout moment, pour atteindre le niveau de service convenu avec les clients. Mais plusieurs indicateurs plus spécifiques à ce processus sont utilisables. Parmi ceux-ci on peut signaler le nombre des incidents, des problèmes, et celui du non-respect des engagements du SLA causés par des mauvaises performances du système, ou encore la véracité des prévisions d'évolution de la demande en performance en regard de l'évolution métier.

D'un point de vue plus financier, la réduction du nombre d'achats en mode panique est un indicateur précieux de l'efficacité du processus. La justesse des prévisions et de la planification des dépenses représente également un bon indicateur.

Du point de vue purement technologique, l'efficacité du processus est jugée sur sa capacité à mesurer les performances des ressources et des services, puis à publier régulièrement ses mesures et les analyses qui les accompagnent, et enfin sur son aisance à identifier les nouvelles technologies en adéquation avec les besoins métier.

Le fait que le plan de capacité soit produit à temps et accepté par les directions métier est également un indicateur de la confiance de l'entreprise dans ce processus.

Coûts

Les coûts induits par la gestion des capacités proviennent essentiellement de l'achat et de la maintenance des outils logiciels et matériels utilisés pour la présentation des données, la modélisation et l'analyse de ces données, ainsi que la surveillance de l'infrastructure (réseaux, serveurs, applications, etc.). À ces coûts, s'ajoute celui de la base de données (CDB), qui regroupe les informations provenant de tous ces outils.

Les coûts en personnel sont une nouvelle fois produits par les dépenses en gestion de projet et les dépenses en formation, mais surtout par les salaires et les frais de recrutement et de conseil.

Documents et rapports

Outre les rapports de gestion concernant l'efficacité du processus, un ensemble de rapports incluant des mesures et des analyses sur la consommation des ressources et l'utilisation de la capacité doit être livré. Enfin, un plan de capacité doit permettre d'identifier la disponibilité des ressources et les prévisions d'achats.

Conséquences

Les bénéfices que l'on peut attendre de la mise en place de ce processus sont liés en premier lieu aux économies financières, mais également dans une large mesure à une amélioration du service rendu aux utilisateurs sous forme de performances adaptées aux besoins au moment opportun.

Le principal bénéfice que l'on peut attendre de ce processus est la diminution, voire la disparition, des changements urgents pour augmenter les capacités. Les achats planifiés permettent de négocier les prix et de faire d'éventuelles économies d'échelle sur les achats groupés. Cela coûte évidemment

moins cher que les achats panique durant lesquels le coût du produit à approvisionner est contrebalancé par les pertes d'activité ou de productivité. Dans ce cas, peut importe le prix du nouveau matériel du moment que les utilisateurs peuvent reprendre le travail.

L'évaluation concrète des besoins en performance permet de valider qu'un matériel va bien répondre à un besoin des utilisateurs et surtout que ce besoin est bien prévu à court ou moyen terme. Cette temporisation des achats offre la possibilité de reporter les budgets sur d'autres dépenses, peut-être plus urgentes, ou même parfois, après analyse, de s'apercevoir que le besoin était inexistant ou déjà couvert par ailleurs dans le cas d'une évolution de la technologie.

Ce contrôle centralisé des achats permet également la fourniture de service au meilleur prix grâce à l'alignement des capacités sur les besoins métier et leurs évolutions. Il n'est alors plus nécessaire de maintenir en réserve un excès de capacité inutile.

Le développement des applications est fortement influencé par l'infrastructure qui les héberge et donc par les performances de cette architecture. La gestion des capacités permet de prendre en compte les éléments de capacité très tôt dans le cycle de développement afin de ne pas les « découvrir » au moment de la mise en production. Le processus permet également de réduire les risques d'apparition de problèmes de performance grâce aux prévisions et aux modèles. C'est en particulier le cas pour l'utilisation d'applications existantes ou nouvelles, pour lesquelles le dimensionnement des ressources peut être optimisé et planifié.

En revanche, concernant les problèmes potentiels, les équipes techniques évaluent la charge d'une application sur un serveur et en tirent très souvent un indice de performance pour l'utilisateur. Cela ne suffit pas. La gestion de la capacité ne doit pas uniquement prendre en compte les aspects serveurs centraux mais bien l'ensemble de la chaîne de production, c'est-à-dire les aspects réseaux et les parties clientes des applications. S'il existe des goulets d'étranglement, la valeur de la chaîne sera celle de son maillon le plus faible.

Lorsqu'on écoute les vendeurs de solutions tant matérielles que logicielles, on découvre toujours de nouveaux produits qui surpassent les précédents et dont on se demande comment on a pu s'en passer auparavant. Mais n'oublions pas de valider toutes ces promesses de performance des fournisseurs par des vérifications chez des clients déjà installés ou par la mise en place de simulations et de maquettes. Dans le même ordre d'idée, il faut faire très attention aux promotions alléchantes qui cachent souvent un produit en fin de vie. Cela n'a parfois pas d'importance si la technologie en question est suffisamment ouverte pour pouvoir fonctionner avec les nouvelles générations de produits, mais peut entraîner de grosses difficultés

si ce n'est pas le cas, ou lorsque le fournisseur ne souhaite plus assurer la maintenance du produit.

Enfin, il est clair que les délais de mise en production se réduisent de plus en plus sous la pression du marché, ce qui rend difficile l'évaluation des besoins. Mais le manque d'information des directions métier est réellement préjudiciable pour la mise en place de prévision d'évolution des capacités.

Pour finir, bien qu'il ne s'agisse pas d'un problème, mais peut-être plus d'une opportunité qui est donnée à la gestion des capacités, il faut veiller à maîtriser les demandes et les attentes des clients. Ces derniers ont parfois des espérances excessives dans la technologie à mettre en place ou n'associent pas les performances qu'ils demandent au surcoût que cela engendre. La gestion de la capacité doit alors passer du temps à expliquer puis à ajuster la demande en fonction des besoins réels et bénéfiques à l'entreprise.

Outils

Les outils utilisés par la gestion de la capacité sont nombreux, puissants, et permettent d'obtenir un nombre impressionnant d'informations, de mesures et d'analyses prédictives. Le revers de la médaille est qu'ils sont souvent complexes à interpréter et à mettre en œuvre et surtout excessivement chers.

Parmi ces outils on retrouve évidemment la panoplie de sondes logicielles ou matérielles que l'on dispose sur les équipements du réseau ou sur les serveurs, afin d'obtenir des informations, des mesures et des alertes, en provenance des applications ou des services. Ces outils peuvent être complétés par un ensemble d'outils de remontée d'alerte et les grands « frameworks » des éditeurs.

Certains de ces outils permettent des analyses très fines des débits réseaux, des protocoles en place, et parviennent même à identifier les zones de contentions. D'autres outils permettent grâce à des systèmes experts d'identifier les tendances et de produire des simulations de l'évolution de la consommation des ressources.

Parmi les outils de simulation on trouve également des outils capables de simuler un groupe d'utilisateurs exécutant une ou plusieurs transactions vers une application afin de valider les temps de réponses.

Enfin, tous ces outils permettent la production de rapports détaillés avec graphiques et analyses statistiques à la clé.

Méthodes

Parmi les méthodes utilisées dans la gestion de la capacité, la modélisation des performances est une activité qui peut donner d'excellents résultats.

L'exemple le plus simple est celui de l'estimation de l'espace disque nécessaire dans le futur en fonction de l'évolution actuelle de la place disque. Si on constate une diminution de l'espace disque disponible de 10 % par mois, on peut estimer qu'il faut dix mois pour consommer l'ensemble de l'espace restant et en déduire la taille des disques à acheter dans un avenir proche.

Pour ce genre de simulation, on peut utiliser des outils dédiés qui vont simuler la saisie d'une même transaction par un grand nombre d'utilisateurs afin de valider le temps de réponse de l'application.

À partir des mesures réalisées sur l'infrastructure et d'estimations basées sur l'expérience, on peut déduire des comportements type à partir des composants. L'analyse de ces mesures puis la mise en place de prototypes et de bancs d'essai (*benchmarks*) permettent d'affiner ces modèles. L'utilisation de méthodes mathématiques et statistiques permet par la suite de produire des projections de ces modèles.

- L'analyse de tendance

Elle est obtenue à partir des données observées par le sous-processus RCM que l'on place ensuite dans un outil de calcul classique (par exemple, un tableur) disposant de fonctions statistiques (interpolation, régression, etc.). Signalons tout de même que ce type d'analyse ne donne que des estimations des futurs besoins.

- La modélisation analytique

Les modèles analytiques reposent sur l'utilisation de méthodes mathématiques (graphes, files d'attente, algorithmes de routage, etc.) afin de représenter le comportement d'un système informatique. On utilise en général un outil logiciel permettant de modifier certains paramètres, et qui donne une estimation du comportement du composant modélisé, que l'on compare avec les observations d'un cas réel afin de valider le modèle.

- La modélisation par simulation

La modélisation par simulation consiste à valider le comportement d'un système sur un événement ponctuel en appliquant plusieurs fois de suite un scénario de tests à cet événement. Bien qu'assez consommatrice en temps et en moyens, cette technique de simulation est particulièrement adaptée à l'évaluation des ressources nécessaires à une nouvelle application ou lors de changements.

Rôles et responsabilités

Le responsable de la gestion de la capacité doit s'assurer que la capacité informatique nécessaire et suffisante aux activités de l'entreprise est présente à tout moment. Il doit également prodiguer des conseils aux responsables de la direction informatique permettant de remplir les engagements de service pris envers les clients et les utilisateurs. Pour cela, il doit s'assurer de la mise en place du suivi des ressources informatiques existantes, de l'enregistrement et de l'analyse de ces données.

Le responsable du processus effectue une veille technologique sur les nouveautés qui peuvent procurer des gains financiers ou des gains de performance. Il supervise la réalisation de tests et de prototypes sur les nouveaux matériels. Cette évaluation permet de dimensionner les solutions

techniques en regard des demandes des utilisateurs, tant du point de vue des performances que du coût.

Il conduit les audits nécessaires à l'identification des carences en ressource et propose les optimisations de configuration des systèmes. Il conserve la trace des futures demandes de service informatique et évalue l'impact de ces demandes sur les niveaux de service actuels. À ce titre, il est présent au comité consultatif des changements (CAB) afin de valider l'impact des changements sur les capacités du système, mais également pour valider qu'un changement est possible en fonction des ressources disponibles.

Enfin, en plus des traditionnels rapports de gestion incluant les mesures, les tendances et les analyses de l'utilisation des ressources qu'il doit diffuser largement, le responsable du processus doit produire régulièrement un plan de capacité en phase avec le plan d'activité de l'entreprise. Ce plan identifie les besoins et reprend le planning des achats.

En plus des traditionnelles compétences techniques dont le responsable doit disposer, il est préférable qu'il pratique régulièrement les outils mathématiques et statistiques nécessaires à l'analyse et à la modélisation.

GESTION DE LA DISPONIBILITÉ



LA GESTION DE LA DISPONIBILITÉ, C'EST ANTICIPER LES INCIDENTS PROBABLES, PUIS IDENTIFIER ET METTRE EN OEUVRE LES SOLUTIONS DE SECOURS.

La gestion de la disponibilité

Système d'assistance respiratoire, contrôle aérien, assistance au pilotage et électronique embarqué, distributeur automatique de billets, logiciel de gestion d'entreprise, site de commerce électronique... Ces exemples de la vie quotidienne illustrent bien le caractère parfois vital de la disponibilité des systèmes. Cette problématique se présente dans les mêmes termes dans le cas de l'entreprise. En effet, les progrès continus de la technologie et les gains de performance qui y sont associés ont considérablement modifié notre utilisation de l'informatique. Malheureusement, cela nous rend également de plus en plus dépendants de cet outil. En conséquence, la disponibilité de ces services est désormais un facteur économique différentiateur. Si une entreprise ne peut répondre aux commandes de ses clients, elle perd son marché.

En corollaire, on comprend aisément qu'une bonne gestion de la disponibilité a un impact non négligeable sur l'image du service informatique, ainsi que sur la satisfaction et la confiance des utilisateurs... Par extension, cela conditionne également l'image de l'entreprise sur le marché, ainsi que la satisfaction et la confiance de ses clients.

Vue d'ensemble

Ce processus est responsable de l'atteinte des objectifs négociés dans les contrats de service (SLA), c'est-à-dire qu'il a pour mission d'assurer un niveau de disponibilité compatible avec les impératifs métier tout en restant rentable financièrement.

Pour atteindre ce but, il est indispensable de déterminer précisément les besoins métier, ou « business », et en particulier ceux qui couvrent les fonctions vitales de l'entreprise. À ces *Vital Business Functions*(VBF), identifiées au sein du SLA, doit correspondre une réponse technique et organisationnelle.

La démarche de mise en place de ce processus passe donc par une optimisation de l'infrastructure informatique et du support du service.

La mise en place de ce processus dépend dans une large mesure de la qualité et de la complexité de cette infrastructure existante (fiabilité, redondance, maintenance, etc.), mais également, et surtout, de la qualité et de la maîtrise des processus et des procédures utilisés par les services informatiques.

Périmètre

Ce processus est responsable de la conception, de l'implémentation et du contrôle de la disponibilité des services informatiques.

En conséquence, il doit être appliqué à tous les services pour lesquels un SLA a été signé, qu'il s'agisse d'un service existant ou à venir. Dans le cas d'un nouveau service, la réflexion sur la disponibilité doit être menée dès le départ afin de minimiser l'impact de ce coût sur le service.

Par extension, le processus de gestion doit également être pris en compte pour des services dépourvus de SLA, mais dont le caractère critique au niveau informatique, peut entraîner des conséquences négatives pour le SLA d'autres services ou pour l'ensemble de l'entreprise. On peut citer par exemple le service de résolution de nom DNS qui, s'il est défaillant, peut gravement perturber l'accès à l'ensemble des ressources TIC de l'entreprise.

En revanche, ce processus n'est pas responsable de la gestion de la continuité de service du métier, ni de la résolution des incidents après un désastre majeur. Cependant, il fournit des éléments importants aux processus de gestion de la continuité de service, de gestion des incidents, ainsi qu'à la gestion des problèmes.

Une gestion de la disponibilité efficace peut faire la différence et sera reconnue comme pertinente par les directions métier si son déploiement au sein de l'organisation informatique est en phase avec les besoins du métier et des utilisateurs.

Trois grands principes doivent rester à l'esprit en permanence :

- La disponibilité est au cœur du business et de la satisfaction du client.
La course à l'innovation dans les services ou les produits amène parfois le service informatique à se focaliser sur la technologie. Il risque alors de perdre de vue qu'il a pour but de satisfaire les besoins métier de l'entreprise.

En conséquence, peu importe la technologie sous-jacente. Elle est inutile si les utilisateurs ne peuvent accéder à leurs données.

- Quand les choses vont mal, il reste toujours la possibilité de satisfaire le client et de remplir ses obligations.

Pour le service informatique, c'est le moment de vérité, et la manière de gérer et de résoudre la crise est l'élément principal qui sera retenu par les utilisateurs et la direction de l'entreprise pour juger de la qualité de leur organisation informatique.

Il est évident que la durée de la panne n'est qu'un élément de la réponse de l'organisation informatique. Il est vrai que cette valeur est un révélateur de la vitesse de réaction de l'organisation, mais elle doit être pondérée par son impact sur le métier.

- L'anticipation de la panne et l'utilisation de solutions de contournement identifiées et testées au préalable sont également des critères importants dans la vision que le métier retiendra de l'efficacité du service.

Améliorer la disponibilité ne peut se faire sans comprendre comment l'informatique supporte le métier.

La gestion de la disponibilité du système ne se limite pas à la compréhension technique de chaque élément du système, mais bien à sa relation avec le processus métier.

L'optimisation de l'infrastructure informatique et de son support ne doit se faire que dans le but de délivrer le niveau de disponibilité requis par le métier.

Terminologie

La terminologie utilisée dans le processus de gestion de la disponibilité est présentée dans le tableau 13-1, où un système peut représenter le matériel, le logiciel, le service ou un composé des trois.

Disponibilité (Availability)

Indique la capacité d'un système à remplir son rôle pendant un temps donné. Cette valeur s'exprime le plus souvent sous la forme d'un pourcentage de temps pendant lequel le système est disponible par rapport à l'horaire de service négocié lors du SLA.

Fiabilité (Reliability)

Correspond à l'aptitude d'un système à fonctionner durablement avec un minimum d'incidents ou d'interruptions.

Capacité de maintenance (Maintainability)

Représente le potentiel de maintenance externe et indique la capacité d'un fournisseur externe à remettre un système en état de fonctionnement normal. La maintenabilité d'un composant particulier peut être décomposée en 7 étapes distinctes :

- l'anticipation de la panne ;
- la détection de la panne ;

- le diagnostic de la panne ;
- la résolution de la panne ;
- le retour à la normale après une panne ;
- la restauration des données et du service ;
- le niveau de maintenance préventive appliqué pour prévenir cette panne.

Résilience (**Resilience**)

Correspond à la faculté d'un système à continuer de fonctionner même si une partie des éléments du système est défaillante.

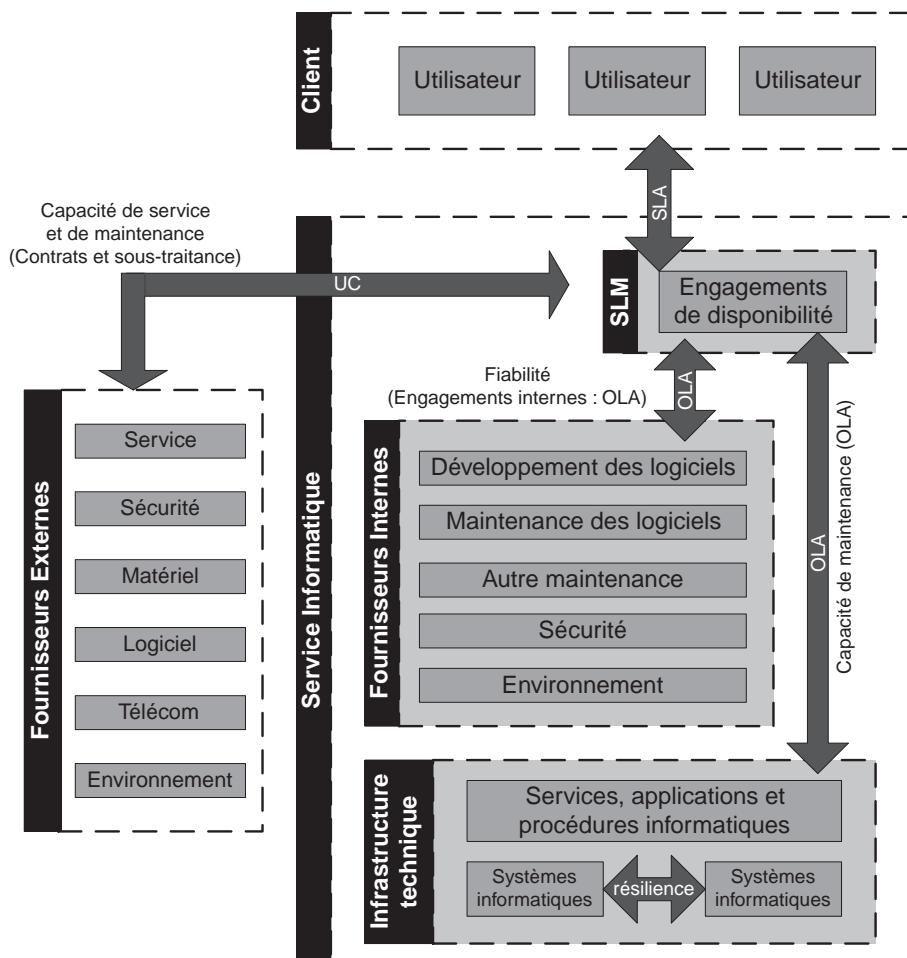


Figure 12-1 : Relations avec les organisations de support

Capacité de service (Serviceability)

Représente le potentiel de service externe et indique le niveau de service que l'on peut trouver auprès des fournisseurs tiers pour certaines parties de l'infrastructure informatique (exemple : contrat de support, contrat de maintenance).

Sécurité (Security)

Correspond à la mise en œuvre de contrôles visant à assurer un service continu en respectant des paramètres sûrs, à savoir :

- la confidentialité (interdire les accès non autorisés) ;
- l'intégrité (garantir la validité des données) ;
- la disponibilité (permettre l'accès aux données).

La disponibilité d'un élément de l'infrastructure informatique qui procure un service au métier et aux utilisateurs est influencée par :

- la complexité de l'infrastructure informatique et du service ;
- la fiabilité des composants et de l'environnement de l'infrastructure ;
- la capacité de l'organisation informatique à maintenir et à supporter cette infrastructure ;
- le niveau et la qualité de la maintenance apportée par les fournisseurs ;
- la qualité et l'étendue du déploiement des procédures.

Le service informatique est responsable devant le métier de la fourniture du système d'information. Cela implique que le niveau de disponibilité de chaque service doit être formalisé dans le SLA. De plus, ainsi que l'illustre la figure 12-1, les relations avec chaque fournisseur de service extérieur doivent également faire l'objet d'une documentation formelle.

Un moyen mnémotechnique comme un autre pour s'en souvenir : confidentialité (C), intégrité (I), disponibilité (A)... A pour Availability

Description du processus

La gestion de la disponibilité débute aussitôt que les exigences métier pour un service sont formalisées. C'est un processus permanent, se terminant uniquement lorsque le service disparaît ou n'est plus utilisé.

Flux du processus

Le flux interne du processus doit prendre en compte un nombre important d'informations en entrée, et fournir un volume également très important d'informations en sortie.

Mais globalement, la mission de la gestion de la disponibilité peut se résumer à définir les besoins exprimés par les directions métier, évaluer les risques et proposer des solutions y répondant, puis formaliser un engagement opérationnel, qui doit servir à la rédaction du SLA pour le service évalué (voir figure 12-2).

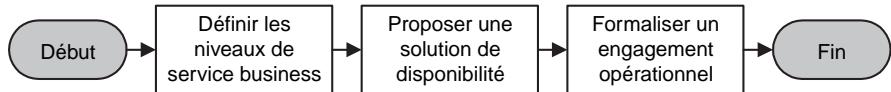


Figure 12-2 : Flux simplifié de la gestion de la disponibilité

Le périmètre de la gestion de la disponibilité couvre la conception, la mise en œuvre, la mesure et la gestion de la disponibilité de l'infrastructure. Cela implique qu'il existe un nombre important de liens entre ce processus et les autres processus ITIL. De plus, ces informations sont extrêmement diverses, ce qui complique largement la tâche du responsable de ce domaine, en lui imposant de disposer de compétences très différentes.

Parmi ces entrées, on trouve notamment des documents exprimant les besoins du métier et les risques associés à chacun de ces besoins. On trouve également un ensemble de rapports d'incident et de rapports de performance qu'il convient d'analyser avec attention. Enfin, s'ajoute à cela la connaissance fine de l'architecture, des technologies employées et des conséquences d'une défaillance technique sur un environnement métier.

La figure 12-3 reprend dans le détail les principales actions à prendre en compte dans le processus de gestion de la disponibilité.

La complexité relative de ce processus provient pour l'essentiel du nombre d'informations en entrée et en sortie interagissant les unes avec les autres.

De plus, il ne faut pas oublier qu'un lien fondamental a été retiré du diagramme afin d'en faciliter la lecture. Il s'agit de la boucle indiquant que ce processus est en perpétuelle réévaluation.

En résumé, les tâches que l'on peut identifier pour ce processus sont l'étude et la conception, l'implémentation et l'exploitation, et enfin le contrôle et la gestion.

La tâche d'étude et de conception regroupe les actions suivantes :

- analyser le besoin en terme de disponibilité, c'est-à-dire :
 - définir les besoins métier ;
 - définir les conditions optimales de disponibilité.
- analyser les tendances et les solutions proposées ;
- analyser les pannes fréquentes (gestion des problèmes) ;
- élaborer le plan de disponibilité (*Availability Plan*) ;
 - établir les niveaux de disponibilité convenus ;
 - établir les objectifs de chaque niveau ;
 - établir les plannings des interruptions (*DownTime*).
- rédiger les procédures et les documentations.

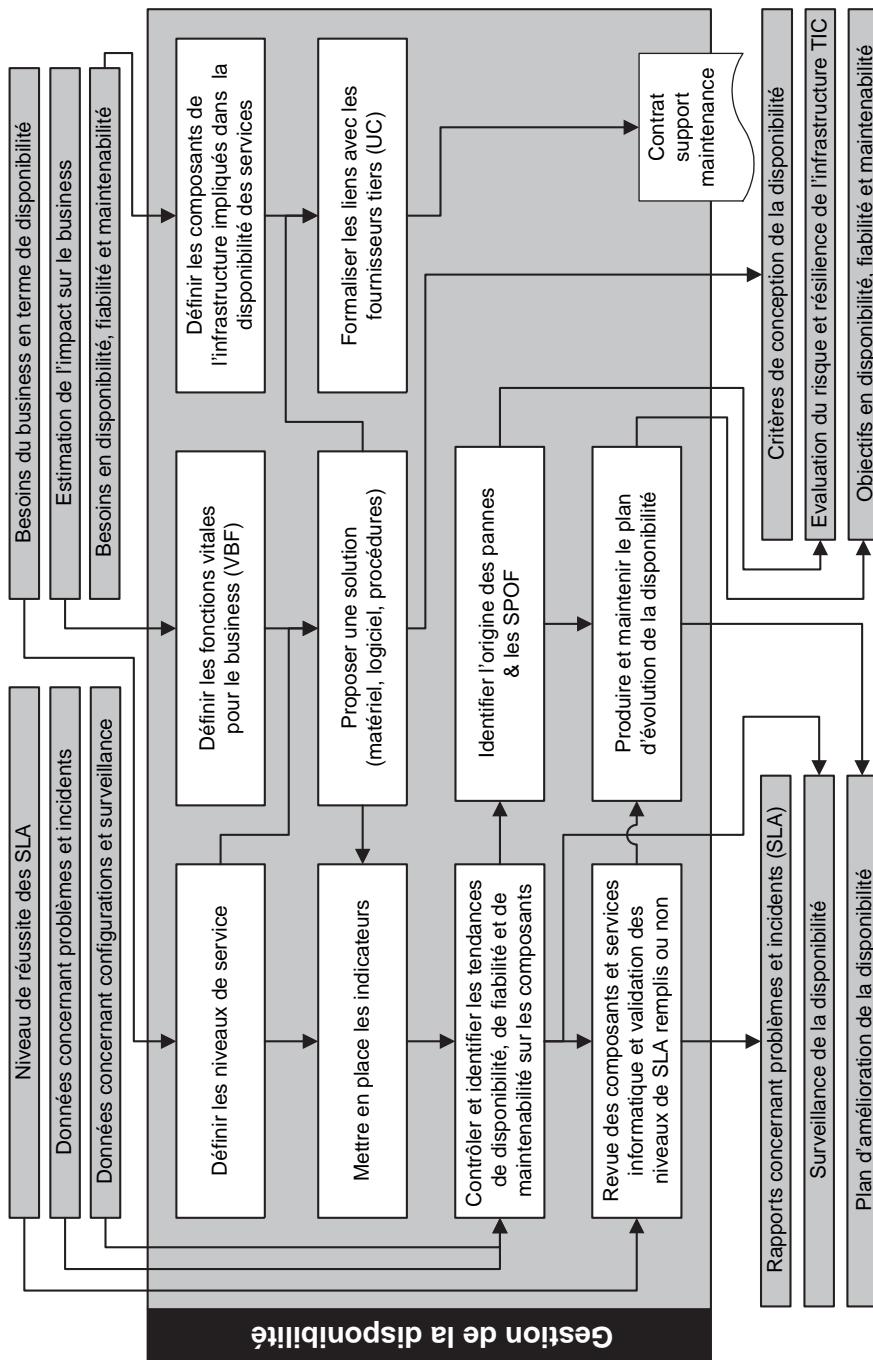


Figure 12-3 : Relations internes des activités du processus

La tâche d'implémentation et d'exploitation comprend les actions suivantes :

- assurer et optimiser les niveaux attendus de disponibilité en surveillant les éléments essentiels ;
- évaluer les options techniques et les procédures de retour au niveau précédent l'arrêt ;
- rechercher et éliminer les points uniques de panne (*Single Point Of Failure* ou SPOF) ;
- gérer la capacité de maintenance et de service.

Enfin, la tâche de contrôle et de gestion comprend les actions suivantes :

- s'assurer que les niveaux de service sont atteints par comparaison du réalisé avec les valeurs des SLA, et surveiller le respect des objectifs des OLA et les performances des fournisseurs tiers en matière de service (utilisabilité) ;
- collecter, analyser et maintenir à jour les données de disponibilité et produire des rapports sur ces données ;
- réexaminer et améliorer continuellement la disponibilité.

Documents

Le plan de disponibilité

Le plan de disponibilité (*Availability Plan*) correspond à une planification sur le long terme des buts, des objectifs et des documents de ce processus.

Ce planning définit les étapes et les moyens envisagés, tels que les ressources humaines, les processus, les outils et les techniques, dans le but d'améliorer de façon proactive la disponibilité des services informatiques tout en respectant les contraintes de coût imposées.

Comptes-rendus sur la partie disponibilité du SLA

Il s'agit de produire les tableaux, les mesures, les rapports, les commentaires et les explications sur les niveaux de SLA en exploitation.

Critères de disponibilité

Ces critères représentent des documents et des « normes » de conception à prendre en compte dans le domaine de la disponibilité et du « retour à la normale » lors de la mise en place de nouveaux services ou la modification de services existants.

Améliorer la disponibilité

La capacité du processus de gestion de la disponibilité est fortement influencée par la gamme et la qualité des méthodes et des techniques disponibles pour son déploiement et son exploitation.

Dans l'absolu, il convient d'appliquer des méthodes simples pour y parvenir. On peut tout d'abord réduire le temps d'arrêt (*downtime*) en procédant aux actions suivantes :

- réduire le temps de détection par la supervision du système et la mise en place d'alarmes ;
- réduire le temps de réaction par la gestion des incidents et la mise en place de procédures ;
- réduire le temps de réparation en disposant de configurations standards, de dossiers système à jour et de matériels de rechange disponibles (*spare*) ;
- réduire les temps de restauration (procédures, sauvegardes, données d'origine, etc.).

On peut ensuite réduire la fréquence ou l'impact des incidents par les actions suivantes :

- investir dans des systèmes à tolérance de panne (améliorer la résilience) ;
- réaliser des maintenances préventives permettant d'éviter un grand nombre d'incidents (gestion de la capacité, gestion des configurations, etc.) ;
- mettre en place la duplication des services ou des environnements, de façon synchrone ou asynchrone en fonction de la criticité du service.

Enfin, pour réduire les arrêts de service on peut : planifier les interventions préventives en dehors des horaires de service (gestion du changement, gestion des mises en production).

Il existe plusieurs techniques et méthodes associées à la gestion de la disponibilité. Parmi celles que préconise ITIL, on trouve notamment les méthodes suivantes :

- CFIA : évaluation de l'impact de la défaillance d'un composant.

La CFIA peut être utilisée pour prévoir et évaluer l'impact sur le service résultant de la défaillance d'un ou plusieurs composants de l'infrastructure, et en particulier pour identifier les endroits où une infrastructure redondante permettrait de réduire au minimum cet impact.

- FTA : analyse d'arbre des fautes.

La FTA est une technique qui peut être utilisée pour déterminer la chaîne des événements qui entraîne une rupture des services informatiques. En conjonction avec des méthodes de calcul, elle peut offrir les modèles détaillés de disponibilité.

- CRAMM : méthode de gestion et d'analyse du risque.

CRAMM est utilisé pour identifier de nouveaux risques et fournir les contre-mesures appropriées lors de l'évolution des besoins de disponibilité exprimés par le métier.

- SOA : analyse des défaillances système.
SOA est une technique conçue pour fournir une approche structurée à l'identification des causes sous-jacentes d'interruption de service.

Mesures de la disponibilité

Disponibilité des applications vs disponibilité des données.

Il est intéressant de noter que selon le métier ou la fonction que l'on considère, l'importance que l'on accorde à la disponibilité des applications/services est plus ou moins forte. Il en est de même pour la disponibilité des données.

Exemple : la disponibilité des données transportées est moins importante que la disponibilité du service dans le cas de la voix sur le protocole Internet, où on accepte de perdre quelques paquets. En revanche, l'indisponibilité d'une application comptable est moins critique que l'impossibilité d'accéder aux données, ou le fait que celles-ci soient altérées... Tout cela est à prendre en compte lors de l'établissement du SLA.

Les comptes-rendus destinés au service commercial ne peuvent pas être les mêmes que ceux qu'utilise en interne le support informatique. Afin de satisfaire ces différents points de vue, il est nécessaire de proposer un ensemble de métriques qui reflètent ces perspectives concernant la disponibilité des composants et des services informatiques. Tant sur le fond que sur la forme, les informations présentées sur le rapport doivent être adaptées au public visé.

Le modèle de mesures de la disponibilité informatique (ITAMM, IT Availability Metrics Model) regroupe un ensemble de métriques et de perspectives, qui peuvent être utilisées dans la réalisation des mesures de disponibilité, puis dans la publication des rapports associés.

Il est nécessaire de déterminer ce que l'on désire inclure dans ce type de rapport en fonction du destinataire de ce document. La liste suivante présente les paramètres importants à prendre en compte dans la mise en place de ce modèle.

- Fonctions métier critiques (VBF)
Mesures et rapports démontrant les conséquences (contribution et impact) de la disponibilité du système d'information sur les fonctions métier importantes d'un point de vue opérationnel.
- Applications
Mesures et rapports concernant la disponibilité des applications ou des services nécessaires au fonctionnement opérationnel du métier.
- Données
Mesures et rapports concernant la disponibilité des données nécessaires au fonctionnement opérationnel du métier.
- Réseau
Mesures et rapports concernant la disponibilité du réseau et sa capacité de transport effective.
- Composants clés
Mesures et rapports concernant la disponibilité, la fiabilité et la capacité de maintenance des composants de l'infrastructure TIC fournis et maintenus par le support informatique.
- Plate-forme
Mesures et rapports concernant la plate-forme qui supporte le fonctionnement des applications métier.

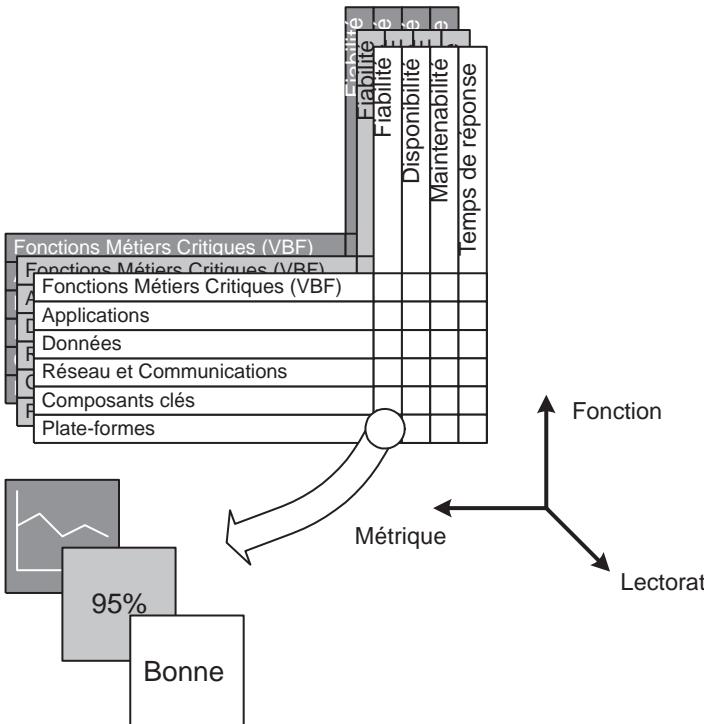


Figure 12-4 : ITAMM, modèle de mesures de la disponibilité des technologies de l'information

Comme l'indique la figure 12-4, chaque case à l'intersection d'une ligne et d'une colonne représente une métrique du modèle ITAMM. En fonction du public visé, chaque métrique peut être représentée comme une valeur discrète communiquée sous la forme d'une moyenne, d'un pourcentage (80 %), ou d'une appréciation globale (très bonne/bonne/moyenne...). Cependant, elle peut également être présentée sous la forme d'un sous-tableau ou d'un graphique plus complet mais moins rapide à lire et à interpréter. Le modèle ITAMM représente donc une mesure de disponibilité à trois dimensions qui sont la fonction, la métrique et le lectorat visé par la mesure.

Pour fournir une vue équilibrée et significative de la disponibilité d'un service ou d'un composant, le rapport doit, pour chaque élément évoqué ci-dessus, considérer les dimensions suivantes :

- Disponibilité.

Mesures et rapports exprimant le taux de disponibilité en fonctions des objectifs du SLA.

- Fiabilité.

Mesures et rapports exprimant la fréquence des pannes.

- Maintenabilité.
Mesures et rapports exprimant la durée des pannes (c'est-à-dire le temps de reprise total depuis la détection jusqu'au retour du service pour l'utilisateur).
- Temps de réponse.
Mesures et rapports exprimant le niveau de performance du système d'un point de vue utilisateur.

Calcul de la disponibilité

Du point de vue technique, la mesure de la disponibilité s'établit sur la base du ratio entre les temps des disponibilités réelles et convenues sur une période donnée (annuelle, mensuelle, hebdomadaire, etc.) :

$$\text{Disponibilité (en pourcentage)} = \frac{(\text{AST} - \text{DT})}{\text{AST}} \times 100$$

AST = *Agreed Service Time* = temps de service convenu.

DT = *Down Time* = durée d'interruption du service.

Exemple : soit un SLA indiquant une période de disponibilité de 8 heures sur 5 jours sur le service A.

Si A est indisponible pendant 4 heures sur la semaine, la disponibilité est $d(A) = (40 - 4) / 40 _ 100 = 90 \%$.

Cela semble simple mais en réalité tout dépend de ce que l'on mesure et comment on le mesure. En effet, si on envisage que l'indisponibilité du service ci-dessus ne s'est manifestée que sur une dizaine d'utilisateurs parmi 1 000 personnes, doit-on toujours considérer une disponibilité de 90 % pour l'ensemble de l'entreprise ?

De plus, et en dehors de toute recherche de responsabilité, il convient de valider que la valeur publiée correspond bien au « ressenti utilisateur » et pas uniquement à une mesure issue d'un calcul.

C'est le cas, par exemple, quand une application distante n'est plus accessible du fait d'une panne de télécommunication dont la responsabilité ne se trouve pas au sein de l'équipe informatique interne. Pour l'équipe interne, tout se déroule bien, alors que l'utilisateur ne peut plus travailler.

Un service informatique est indisponible pour un client lorsque la fonction requise à un horaire et en un lieu ne peut être utilisée dans les termes du SLA.

Dans la situation où plusieurs composants liés sont impliqués dans une indisponibilité, le calcul doit prendre en compte l'aspect séquentiel ou parallèle des ressources sur l'ensemble de l'infrastructure concernée.

Prenons le cas d'un service commercial réalisant des commandes par téléphone. Une base de données est hébergée sur un serveur distant, et une application de saisie est présente sur les postes de travail. Pour atteindre

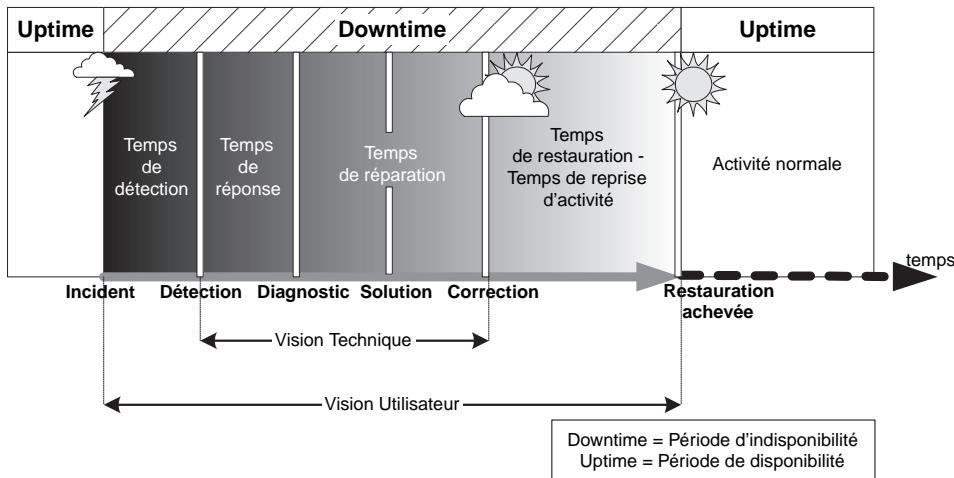


Figure 12-5 : Perception des différentes étapes de la panne

le serveur depuis le poste de travail, l'application transite via le réseau. C'est le cas typique d'une chaîne de traitement en série.

Si le serveur affiche un taux de disponibilité de 95 % mais que le réseau n'atteint en revanche que 90 % alors la disponibilité de l'ensemble ne représente plus que $0.95 \times 0.90 = 85,5\%$. Sur une semaine, dans le cadre d'un SLA réclamant une disponibilité de 8 heures sur 5 jours, le serveur est indisponible moins de 2 heures, alors que l'utilisateur ne peut travailler pendant près de 6 heures... Une journée de perdue.

Encore une fois, on comprend que la qualité d'une chaîne est celle de son maillon le plus faible. Ce qui explique l'importance de ce concept dans le ressenti de l'utilisateur, et qui permet d'insister sur la prise en compte de la disponibilité de chacun des éléments de la chaîne dans la vision de la disponibilité globale du système pour l'utilisateur.

Afin d'améliorer la disponibilité du service, une des solutions consiste à dupliquer certaines ressources afin de paralléliser les accès. Imaginons que la ressource réseau soit désormais équipée d'un système de secours qui propose un second passage. La disponibilité des deux équipements n'est pas parfaite, mais nous obtenons à présent 95 % pour le premier et 90 % pour le second. Dans ce cas la règle de calcul est obtenue par la durée de l'indisponibilité globale, ce qui donne :

Disponibilité du système complet = $1 - \text{indisponibilité du système A} \times \text{indisponibilité du système B}$.

On obtient alors un taux de disponibilité de $1 - (1 - 0.95) \times (1 - 0.90) = 99,5\%$.

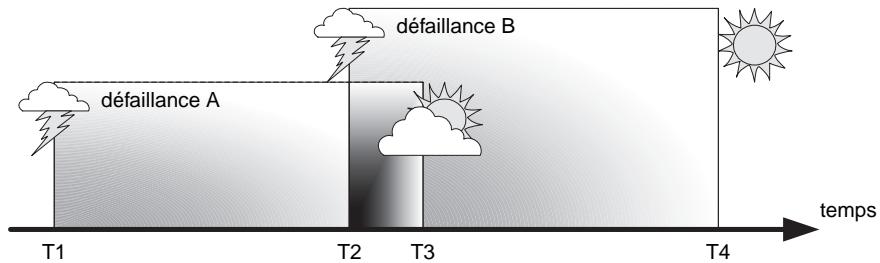


Figure 12-6 : Défaillance conjointe de deux équipements redondants

Attention, nous ne prenons pas en compte le fait que les deux équipements peuvent subir une défaillance simultanément ou en léger décalage. Dans ce cas, ce calcul est incorrect.

Dans l'exemple de la figure 12-6, on constate que l'équipement A subit une défaillance à T1, mais que le service est toujours disponible puisque l'équipement B prend le relais. Malheureusement, à T2, l'équipement B tombe également en panne alors que A n'est toujours pas disponible puisque la restauration des données se termine à T3...

Dans ce cas, le calcul de disponibilité du service d'un point de vue technique est sensiblement différent des deux calculs précédents. En effet, on peut considérer que pendant les phases T1 à T2 et T3 à T4 les équipements se portent secours mutuellement. Pendant ces périodes, le calcul des systèmes en parallèle s'applique. Mais durant l'intervalle T2 à T3, où plus aucun service n'est disponible, c'est bien le calcul des systèmes en série qui s'applique.

Il est aisément de comprendre qu'un rapport qui présente des taux de disponibilité sans autres explications et dans lequel ne sont pas précisées les règles de calcul, ne présente pas un grand intérêt. De ce point de vue, l'idéal est de fixer ces règles de calcul et d'interprétation dans le SLA.

D'un point de vue présentation, la méthode utilisée et les chiffres retenus ont également leur importance.

Si nous considérons un service stratégique pour l'entreprise et sur lequel un SLA de disponibilité à 99 % est signé, nous avons trois possibilités de présentation de la valeur mesurée :

- Pourcentage de disponibilité : 98,8 %.

Ce chiffre, qui doit être le plus grand possible, donne le pourcentage de temps où le service est disponible durant la période considérée. Souvent assenée comme une vérité absolue, cette valeur peut induire en erreur et donner un sentiment de confiance excessive chez le personnel informatique. La différence entre 98,8 et 99 % ne semble guère importante.

C'est oublier bien vite que pour certaines entreprises, un dixième équivaut à des millions d'euros de pertes.

- Pourcentage d'indisponibilité : 1,2 %.

Cette valeur qui met l'accent sur l'indisponibilité semble plus efficace dans la prise en compte par l'équipe informatique. Paradoxalement, le besoin d'une baisse de la valeur de quelques dixièmes de cet indice est mieux vécu par les personnes chargées de sa mise en œuvre que le besoin d'une hausse dans le cas précédent.

- Durée de l'indisponibilité : 105 heures par an en moyenne ; 9 heures par mois en moyenne ; 2 heures par semaine en moyenne.

Cette méthode de publication est de loin la plus intéressante pour les utilisateurs à qui elle « parle » vraiment. En effet, il est facile de mettre un coût en face de cette durée d'indisponibilité.

Cependant, pour les utilisateurs, l'indice de disponibilité le plus pertinent est une valeur composée de trois facteurs qui sont la fréquence, la durée et l'ampleur de la panne ou l'impact sur le métier.

C'est d'ailleurs l'impact qui doit être utilisé dans une communication de la disponibilité vers la direction générale ou les directions métier. Cet impact est plus complexe à calculer et est en partie fonction de l'importance que l'on donne à la disponibilité d'un service dans un métier (exemple : disponibilité de l'outil CRM de prise de commande dans un service commercial).

La valeur de l'impact de la disponibilité doit être communiquée en positif, et on parle alors de valeur ajoutée ou de création de valeur, ou en négatif, dans le cas où le niveau de SLA n'est pas atteint.

Enfin, il est indispensable de déterminer correctement les périodes à prendre en compte dans l'évaluation du taux de disponibilité. En effet, les événements tels que l'indisponibilité planifiée pour la réalisation d'une maintenance, ou le délai de débordement post-maintenance utilisé pour terminer les actions planifiées précédemment, sont des périodes que l'on doit distinguer de la période classique d'indisponibilité, c'est-à-dire la durée pendant laquelle un service défaillant n'est plus disponible.

Coûts

La gestion de la disponibilité est en permanence confrontée au dilemme entre le coût de l'investissement et le coût associé au risque en cas de défaillance du système d'information.

À l'image d'une police d'assurance que l'on peut souscrire ou non, il est du ressort de la direction de l'entreprise de décider de la somme qu'elle est prête à consacrer à la sauvegarde de son activité. Après avoir évalué les pertes potentielles, il est théoriquement assez simple d'estimer de quel budget peut disposer le processus de gestion de la disponibilité dans l'entreprise.



Figure 12-7 : Le fragile équilibre entre le coût des investissements et le coût du risque

Le coût de la disponibilité

Puisque le taux de disponibilité d'un système équivaut à la disponibilité de son maillon le plus faible, la méthode la plus classique pour augmenter ce taux est de fiabiliser chaque maillon en le dupliquant ou en appliquant une procédure de fiabilisation adaptée. On réduit ainsi le nombre de SPOF (points sensibles) du système. Le revers de la médaille est que l'on risque fort de doubler le coût de l'infrastructure. On peut également appliquer des procédures spécifiques permettant de s'affranchir de la défaillance d'un composant quelconque du système d'information. C'est le cas des procédures palliatives dans lesquelles sont expliquées les méthodes de contournement.

Mais, en observant la figure 12-8, on constate qu'au-delà d'un certain seuil, l'investissement supplémentaire n'est plus autant valorisé que dans les débuts de la courbe. Celle-ci, de forme logarithmique, nous indique que passé

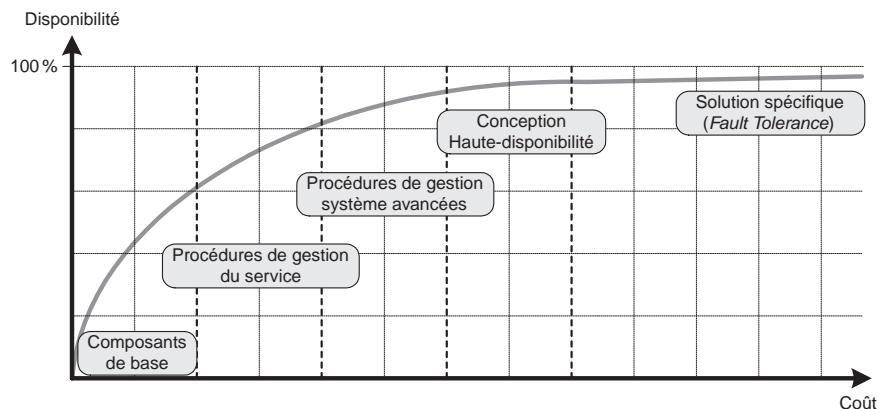


Figure 12-8 : Relation entre coût global et niveau de disponibilité

un certain niveau (le palier) chaque dixième de point de disponibilité gagné le sera au prix d'un investissement matériel ou humain de plus en plus important.

Cependant, cette courbe a aussi un grand intérêt. Elle confirme que l'investissement de base permettant d'atteindre une bonne disponibilité est loin d'être inaccessible. Cela implique qu'avec un peu de bon sens dans la conception de l'infrastructure et en mettant en place des procédures adaptées le plus tôt possible, tout système d'information peut atteindre des taux de disponibilité très respectables, sans investissement excessif par ailleurs. Rappelons également que le coût de la disponibilité est moindre lorsque l'étude et l'implantation se font en début de projet.

Le coût de l'indisponibilité

Les données du coût de l'indisponibilité sont calculées à partir des informations provenant de la gestion de la continuité de service qui détermine les fonctions vitales pour le métier, de la gestion des niveaux de service qui exprime les besoins métier de disponibilité sur ces fonctions vitales, et la gestion financière qui valorise ces demandes en termes monétaires.

L'indisponibilité du système engendre des coûts divers qui peuvent être des coûts immédiats et tangibles, mais également diffus ou différés, et par nature intangibles.

Coûts tangibles

Les coûts tangibles sont ceux que l'on peut calculer aisément. Ils représentent une part importante des pertes provoquées par une indisponibilité du système :

- perte sur les salaires des employés qu'il faut verser alors que ceux-ci ne produisent plus ;
- perte de productivité des utilisateurs qu'il faut bien rattraper par la suite ;
- perte de revenus directe si l'activité touchée génère un revenu immédiat ;
- perte de matière première ;
- pénalités de retard ;
- pertes financières sur les fluctuations du cours de l'action.

Coûts intangibles

Les coûts intangibles sont bien plus complexes à évaluer. Mais il n'en reste pas moins qu'il s'agit de sommes importantes en termes de manque à gagner. Il est fondamental de ne pas faire l'impasse sur ces coûts « cachés » :

- perte de confiance des clients envers une société à la fiabilité douteuse ;
- perte de confiance des analystes et des marchés financiers ;
- perte directe des clients qui se dirigent alors vers la concurrence ;

Les pertes de revenus directes se produisent par exemple dans les caisses des magasins de détail, ou dans celles de la restauration. Les pertes de matière première concernent les matières périssables, l'industrie plastique et chimique, l'imprimerie, etc.

- perte d'opportunités, de marchés, de contrat, etc. ;
- problème de réputation à long terme sur le marché ;
- perte de confiance des utilisateurs envers le service informatique.

Scénario

L'ERP d'une entreprise industrielle de 1 500 salariés réalisant un CA annuel de 200 millions d'euros est indisponible pendant 5 heures. La production est stoppée, les commandes ne passent plus, les livraisons ne peuvent pas partir à l'heure et sont retardées de plusieurs jours... Le salaire moyen dans l'entreprise est de 20 €/heure. Le CA horaire moyen par employé est de 83 €.

Les pertes directes en salaire sont de 150 k€, alors que les pertes en CA représentent plus de 620 k€.

Ces données issues d'un cas réel sont édifiantes. N'oublions pas qu'elles ne représentent qu'une partie des pertes potentielles, puisque les pertes en matières premières ne sont pas indiquées et que les pertes intangibles sont également à prendre en compte, dont notamment l'impact sur la confiance des clients.

Ces 770 k€ (ou au moins une partie) ne seraient-ils pas mieux employés dans le budget de la gestion de la disponibilité ?

Conséquences du processus de gestion de la disponibilité

Les conséquences du processus sont multiples. Mais ce que l'on attend en premier lieu de ce processus est bien une amélioration en terme de satisfaction client ou tout du moins, que la disponibilité des services ne soit pas un facteur d'insatisfaction.

Avantages

Parmi les conséquences de la mise en place de la gestion de la disponibilité, les avantages sont nombreux et parfois gratifiants.

En premier lieu, cela officialise un point unique de responsabilité pour cette lourde tâche. Jusqu'alors, chaque responsable d'application, d'infrastructure ou de service devait assumer la responsabilité de la mise en place de la disponibilité. Ce qui est loin d'être simple et n'est pas nécessairement dans les compétences de la personne. Mais le pire est qu'ensuite, le suivi et la responsabilité de cette disponibilité incombaient au responsable de l'exploitation qui n'avait souvent pas participé à l'élaboration du service...

En second lieu, ce processus permet de répondre aux besoins élémentaires exprimés par le métier en termes de disponibilité. Ce qui implique que la vision de son implantation évolue d'un point de vue technique vers une vision plus centrée sur le métier. La conséquence est que les services sont conçus et gérés pour répondre de manière optimale sur le plan financier à des besoins spécifiques de l'entreprise.

De plus, on découvre rapidement une évolution de l'esprit du personnel informatique, d'une attitude réactive à une attitude proactive avec en corollaire la réduction de la fréquence et la durée des « pannes » informatiques.

L'organisation informatique est alors perçue comme « apportant de la valeur » au métier.

Problèmes possibles

Les principales difficultés de ce processus proviennent essentiellement du volume et de la complexité des informations en entrée.

Le problème le plus fréquent est la difficulté à déterminer les besoins en disponibilité du métier et du client, c'est-à-dire traduire sur le terrain l'expression d'une demande en architecture, en procédures et en métriques. Malheureusement, cela s'accompagne inévitablement par la conception d'une infrastructure décalée en regard de l'attente du client, entraînant parfois des surcoûts inutiles. Mais cela peut également produire des mesures de disponibilité qui ne présentent pas d'intérêt pour le métier ou pire, une absence totale de mesure concernant la fourniture du service en question.

Le second problème réside dans la difficulté à trouver les moyens nécessaires à la mise en place du processus, tel, que les personnes qualifiées et expérimentées, ou les logiciels appropriés. Cela peut d'ailleurs entraîner une certaine dépendance vis-à-vis des fournisseurs avec d'éventuelles conséquences sur la qualité de leur service, comme la fiabilité et la maintenabilité.

Enfin, lorsque le processus n'est pas correctement expliqué ou interprété, la justification des dépenses auprès de la direction semble être le « souci » le plus fréquent et s'accompagne inévitablement d'un manque d'engagement de celle-ci.

Rôles et compétences du responsable du processus

Le rôle principal de ce responsable est de définir et de déployer la gestion de la disponibilité dans l'entreprise. Pour cela, il doit s'assurer que les services informatiques sont conçus pour livrer les niveaux requis de disponibilité demandés par le métier.

Il doit identifier les procédures ou les éléments de l'infrastructure susceptibles de fragiliser les services informatiques et doit alors apporter les actions préventives adaptées.

Le responsable doit également définir les métriques indispensables au contrôle du processus.

Il doit fournir une gamme de rapports permettant en premier lieu de valider que les niveaux de disponibilité, de fiabilité et d'aptitude à la réparation sont bien remplis (SLA), mais permettant également de valider l'optimisation de l'infrastructure afin d'apporter des améliorations financièrement avantageuses pour l'entreprise.

Après analyse des informations, il doit également identifier les pannes et apporter l'action corrective visant à réduire la durée et la fréquence de ces pannes.

Enfin, il doit créer et maintenir le plan de disponibilité destiné à mettre en phase les services informatiques et les composants de l'infrastructure avec les besoins actuels et futurs de l'entreprise.

Compétences clés

Le responsable doit avoir une bonne expérience de la gestion des processus ainsi qu'une bonne compréhension des « disciplines » ITIL.

Il doit avoir une bonne compréhension de principes statistiques et analytiques.

Il doit posséder de bonnes compétences pour la communication écrite et orale, ainsi que des compétences dans le domaine de la négociation.

Il doit bien sûr avoir une bonne compréhension des concepts de la disponibilité et de ces techniques, et comprendre comment les technologies « informatiques » supportent le métier.

Enfin, il doit avoir une compréhension raisonnable de la gestion des coûts.

GESTION DE LA CONTINUITÉ DE SERVICE



LA CONTINUITÉ DE SERVICE, C'EST DÉCIDER QUI POURRA DISPOSER D'UNE SOLUTION DE SECOURS APRÈS UN SINISTRE IMPORTANT ET DONNER DES PRIORITÉS DANS LE REDÉMARRAGE.

La gestion de la continuité de service

On l'a vu, les entreprises sont de plus en plus dépendantes de leurs moyens informatiques et de leurs systèmes de télécommunication. Cette omniprésence est un atout pour les entreprises et devient parfois un caractère différentiateur face à la concurrence. Mais cet atout peut également devenir leur talon d'Achille. Toutes les statistiques le rappellent, plus d'une entreprise sur deux qui subit un désastre majeur au sein de son système informatique disparaît en moins d'un an.

Vue d'ensemble

Dans le cadre d'ITIL, la gestion de la continuité de service doit permettre de continuer à fournir un niveau de service informatique convenu en cas d'événements graves. Le processus de gestion de la continuité de service informatique (ITSCM) s'appuie sur des méthodes d'analyse de l'impact sur les métiers, sur des mesures de réduction des risques, sur la mise en place de redondance, et sur un plan de sauvegarde pour assurer cette continuité. Mais au-delà du simple problème technique qui est davantage l'affaire de la gestion de la disponibilité, la gestion de la continuité de service est avant tout une histoire d'organisation et d'engagement de la direction, qui doit bien intégrer le caractère vital de cette gestion pour son entreprise.

Implanter efficacement ce processus demande un effort continu de la part de l'ensemble du personnel de l'entreprise qui doit prendre conscience de l'importance de la chose et être formé aux concepts de la continuité de service. L'utilisation de méthodes d'analyse de risque et d'impact sur l'entreprise permet de déterminer les actions à entreprendre. Enfin, les processus ITIL de la gestion des configurations, des changements et de la disponibilité sont nécessaires pour obtenir une bonne gestion de la continuité de service.

Pourquoi ?

Lors d'un arrêt de production informatique ou lors d'un événement important qui peut parfois tourner au désastre, la fourniture des services informatiques peut être interrompue pendant un délai plus ou moins long. Pendant cette période, l'entreprise n'est plus en mesure d'assurer ses activités, ce qui peut lui causer de considérables dommages, tels qu'un arrêt des livraisons, l'impossibilité de facturer les clients, ou la perte des informations financières et comptables. En cas d'interruption importante des activités de l'entreprise, que cette celle-ci soit ou non causée par un événement extérieur à l'informatique, la DSI doit être en mesure de continuer à fournir les services informatiques permettant de soutenir les activités métier critiques à un niveau prédéterminé et justifié financièrement. L'objectif avoué de ce processus est clairement de réduire les pertes financières associées à ces interruptions des activités métier et même, en cas d'interruption longue ou critique, de permettre la survie de l'entreprise.

L'objectif de ce type de processus dépasse évidemment la responsabilité de la direction informatique et concerne l'entreprise dans sa globalité. Il s'agit donc d'un projet qui doit associer non seulement les ressources de l'informatique, mais plus largement l'ensemble de la direction, ainsi que tous les responsables métier de l'entreprise. La mise en place de ce projet passe par la production de plans qui s'appuient sur des analyses de risque et de l'impact sur l'activité. Au niveau de l'entreprise, cela concerne le plan de gestion de la continuité d'activité, nommé BCM (*Business Continuity Management*), qui prévoit les différents scénarios de reprise des activités de l'entreprise.

Concepts

Les activités métier sont de plus en plus dépendantes du système d'information. Le but de la gestion de la continuité de service est de s'assurer que les infrastructures informatiques et les services associés peuvent être restaurés après un événement grave, tout en se concentrant sur les processus métier critiques pour l'entreprise.

À l'aide de méthodes formelles et en fonction de la structure et des objectifs de l'entreprise, on va identifier les processus métier critiques, évaluer les risques potentiels sur ces processus, puis estimer l'impact de ces risques sur l'activité de l'entreprise. La gestion de la continuité de service s'appuie sur plusieurs processus ITIL, dont la gestion de la disponibilité, et exige une implication forte de la direction générale, ainsi que de tous les niveaux hiérarchiques de l'entreprise.

Une fois conçu et mis en place, le plan de continuité de service doit subir des tests réguliers afin de vérifier la coordination de l'ensemble des techniques et des procédures envisagées lors d'une interruption importante.

La gestion de la continuité de service est comparable à une assurance couvrant des risques identifiés à l'avance permettant d'anticiper les conséquences d'une éventuelle concrétisation de l'un de ces risques.

Périmètre

Le périmètre d'action de la gestion de la continuité de service concerne tous les métiers de l'entreprise. L'analyse ultérieure permet de définir les activités critiques pour l'entreprise afin de mettre l'accent sur les processus concernés. En plus de l'examen de l'infrastructure et des services utilisés par les activités de l'entreprise, la gestion de la continuité de service doit prendre en compte des éléments tels que, les locaux, les moyens de communication, les accès, l'environnement ou les obligations légales.

L'ampleur du sinistre à envisager peut aller de la simple indisponibilité d'un service informatique jusqu'au sinistre majeur, affectant tout ou partie de l'entreprise.

Les risques à prendre en considération par le processus dépendent de l'activité de l'entreprise, de sa taille ou de sa répartition géographique, et évoluent avec elle. Il s'agit en général :

- des risques technologiques sur l'infrastructure, qui représentent dans ce cas l'incapacité de l'infrastructure à fournir le service convenu :

- des risques dus aux catastrophes naturelles, qui peuvent occasionner des dégâts importants à l'entreprise ou à son système d'information :

- des risques dus aux actions humaines (sociales, militaires ou criminelles), qui peuvent représenter la destruction ou le simple blocage des ressources informatiques ou de l'entreprise :

Attaques par déni de service, pertes totales d'énergie électrique ou prolifération virale.

Tremblements de terre, glissements de terrains, inondations, cyclones, etc.

Mouvements sociaux, blocus militaire, sabotage, attentat, etc.

En revanche, la gestion de la continuité de service ne s'occupe pas des problèmes et des incidents mineurs qui sont en principe gérés par le centre de services et d'autres processus ITIL, ni des risques à plus long terme sur les activités métier provoqués par l'action de l'entreprise elle-même sur son marché (changement de stratégie, diversification, restructuration, etc.). Elle ne s'occupe pas non plus de l'évaluation technique de la disponibilité de l'infrastructure et des services, ce qui est le rôle du processus de gestion de la disponibilité.

Terminologie

BCM

Le BCM correspond au processus d'évaluation des risques et des dommages que peut subir une entreprise lors d'un désastre, associé aux contre-mesures que l'entreprise est prête à y consacrer pour éviter un arrêt d'activité trop important, voire fatal.

ITCSM

L'ITSCM est l'équivalent du BCM à l'échelle du système d'information. Il faut noter que pour certaines entreprises, le métier repose essentiellement sur l'outil informatique, ce qui implique dans ce cas que l'ITSCM correspond en tout point au BCM.

BIA

La BIA est une méthode d'analyse de l'impact (financier et autre) d'un désastre sur l'activité économique de l'entreprise.

CRAMM

La CRAMM est une méthode d'analyse des risques encourus par l'infrastructure et les services informatiques en fonction de différents types de menaces. En découle ensuite un ensemble de contre-mesures permettant de réduire l'impact ou l'apparition des problèmes.

Description du processus

Flux du processus

Les informations utilisées par le processus sont fournies en grande partie par les autres processus ITIL. La gestion des niveaux de service permet de comprendre les engagements pris dans la fourniture des services, alors que la gestion de la disponibilité permet de réduire les risques d'indisponibilité d'un système informatique. Les gestions des capacités et des configurations s'assurent que l'infrastructure est en mesure de répondre aux demandes des utilisateurs.

Quant au centre de services, il permet de connaître les statistiques concernant les incidents et les problèmes les plus fréquents rencontrés sur le système d'information, et peut donner une estimation de l'impact qu'ils ont causés à l'activité de l'entreprise.

Cependant, il est impossible de développer de manière isolée la gestion de la continuité de service. Ce processus doit donc être développé en harmonie avec le plan de continuité plus global de l'entreprise. Le cycle de vie du processus comporte quatre grandes étapes regroupant chacune un ensemble d'activités d'analyse, d'évaluation, et de conception (voir figure 13-1). Les quatre étapes en relation avec les aspects informatiques sont : l'initialisation du projet, l'évaluation des besoins et la conception de la stratégie, la mise en œuvre du plan de continuité, et enfin la gestion opérationnelle du plan.

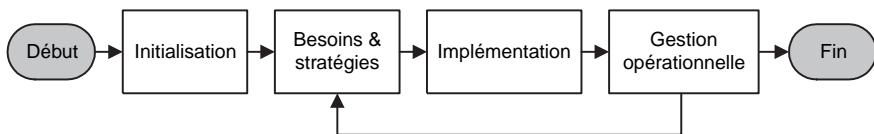


Figure 13-1 : Schéma simplifié du processus de gestion de la continuité des services informatiques

Planification et mise en œuvre

Comme nous l'avons vu précédemment, la conception d'un plan de continuité de service doit être étroitement liée à la perception du métier de l'entreprise, et surtout, à celle de la priorité attachée à chaque activité. Le processus de gestion de la continuité de service propose de réaliser quatre étapes avant de parvenir à un plan opérationnel, comme on peut le voir sur la figure 13-2.

Lancement du projet

La première étape est celle de l'initialisation du plan de continuité qui correspond peu ou prou à la mise en place d'un projet avec la définition des objectifs, des ressources, et du périmètre. Cette initialisation peut être grandement simplifiée si des documents du même type ou traitant de sujets connexes existent déjà dans l'entreprise (analyse de risque sur une activité précise, plan de bascule et plan de sauvegarde à l'informatique, etc.).

À ce stade de l'implantation, il faut définir les règles et les objectifs précis de la direction concernant le processus. Ces règles seront ensuite communiquées le plus tôt possible à tous les acteurs concernés par la continuité de service. Ensuite, le document préparatoire doit préciser les termes utilisés, le périmètre du projet, les méthodes employées, et les responsabilités de chaque responsable et de leurs équipes. La mise en place de ce processus va demander des ressources non négligeables aussi bien en matière de budget qu'en personnel. Il faut donc allouer ces ressources lors de la phase d'initialisation du projet. Ensuite, il faut définir l'organisation du projet et la structure de contrôle à l'aide de méthodes et d'outils de gestion de projet, et de préférence sous la responsabilité de la direction informatique. Enfin, les différents acteurs doivent s'accorder sur le plan projet et le plan qualité, ce qui permet à chacun de prendre la dimension de ce projet et de renforcer son adhésion.

Besoins et stratégie

La seconde étape concerne l'identification des besoins et la stratégie de l'entreprise. Cette étape fournit les bases du processus et détermine l'hypothèse de survie de l'entreprise à un désastre et les coûts que cela

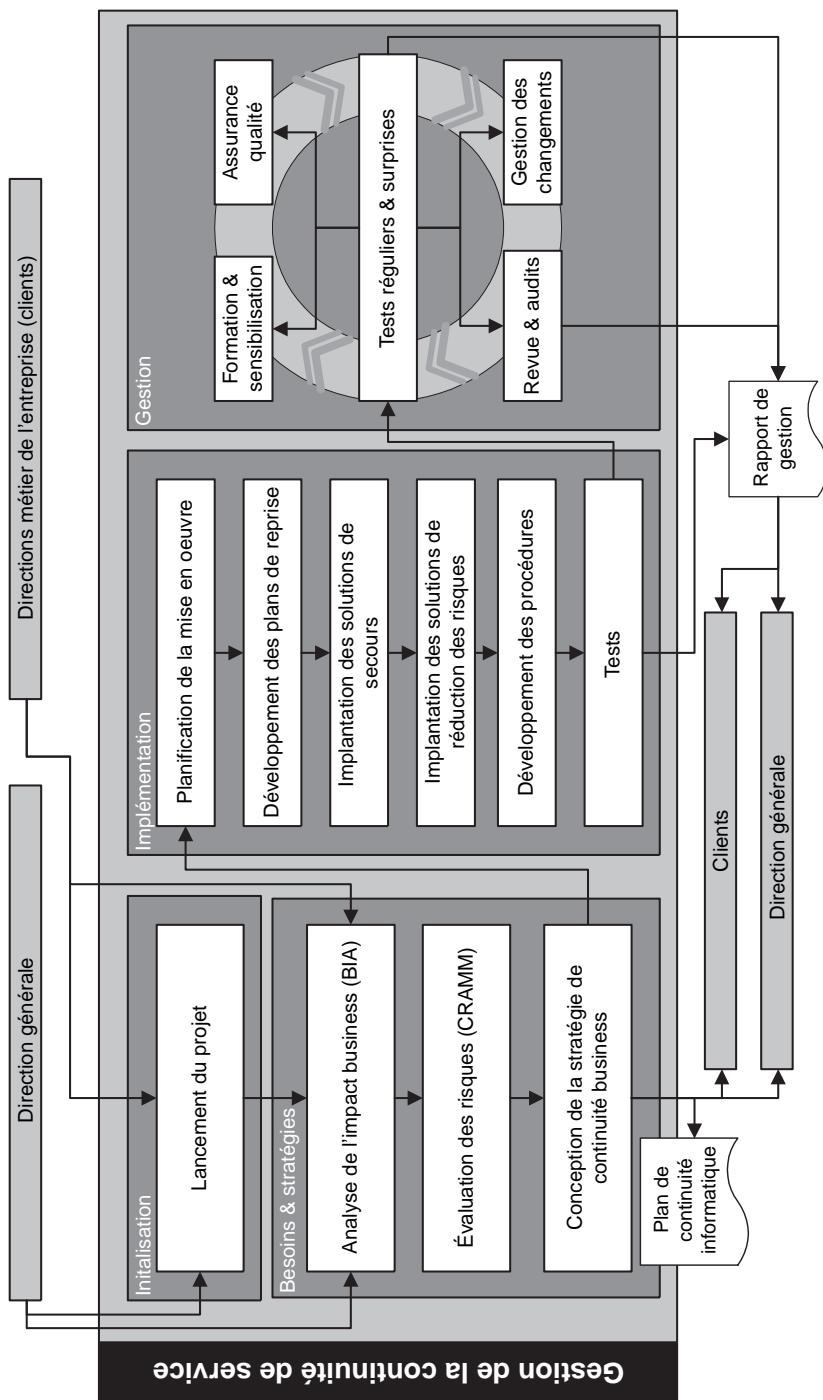


Figure 13-2 : Activités et relations internes de la gestion de la continuité des services informatiques

induira. Cette étape peut être réalisée en deux parties qui sont l'évaluation des besoins (analyse d'impact métier et évaluation des risques) et la stratégie (mesures de réduction des risques et options de reprise).

Évaluation des besoins

L'analyse de l'impact sur le business (BIA) évalue les activités métier critiques et les dommages occasionnés par une interruption de ces activités, tels que les pertes financières, les coûts supplémentaires, la perte de marchés et la perte de crédibilité. Elle identifie également les personnes, les compétences et les services nécessaires pour permettre le fonctionnement des activités métier critiques, ainsi que le délai de redémarrage au minimum, puis au complet, des activités métier critiques. En fonction de l'importance de l'impact, on choisira d'empêcher l'apparition du désastre ou au contraire de le laisser se produire tout en restaurant le service le plus vite possible.

L'utilisation d'une méthode formelle peut faciliter l'évaluation du risque. La figure 13-3 illustre la méthode CRAMM qui consiste à déterminer la probabilité d'apparition d'un désastre et le niveau de risque associé à la valeur des actifs, à l'importance des menaces, et à la vulnérabilité des actifs face à ces menaces, c'est-à-dire dans quelle mesure le service est affecté par l'apparition de la menace. Face à cette évaluation des risques, des contre-mesures sont proposées.

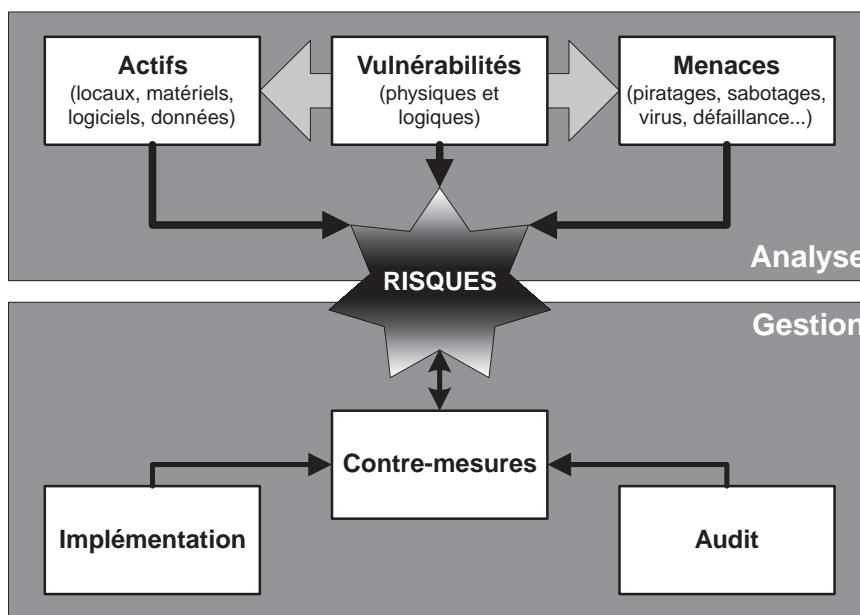


Figure 13-3 : Méthode d'analyse du risque CRAMM (Computer Risk Analysis Management Method)

Exemples de risques et contre-mesures.

Contre l'inondation : pompes, porte étanches, salle des machines à l'étage, etc.

Contre l'incendie : extincteur automatique, détecteur de fumée, etc.

Contre les pannes électriques : onduleur, groupe électrogène, etc.

Contre le sabotage : règle de sécurité, contrôle d'accès, etc.

Contre les désastres : salle de secours distante, etc.

Et bien sûr, contre tous les risques : sauvegarde et copie des bandes hors site.

Stratégie

La stratégie de continuité de service complète est un compromis entre, le coût des mesures de réduction des risques, et les scénarios de reprise permettant de supporter le redémarrage des processus métier critiques dans les délais prévus.

Mise en place de solution de redondance réseau ou serveur et élimination des SPOF.

Les informations obtenues précédemment permettent de concevoir la stratégie de continuité métier. Si l'impact est fort à court terme, on axera les actions sur la prévention, l'élimination ou la réduction des dysfonctionnements qui peuvent se produire sur l'infrastructure. Ces actions sont en général de la responsabilité de la gestion de la disponibilité et sont justifiées financièrement par les conséquences économiques d'un arrêt d'activité de l'entreprise.

En revanche, si l'impact d'une défaillance des services est faible à court terme, il sera plus efficace d'utiliser des plans de reprise ou de restauration (des services ou des données), qui sont moins spectaculaires mais bien plus économiques. De plus, comme les solutions de type redondance ne sont pas infaillibles non plus, tout risque ne peut être écarté. Le bon sens consiste donc à prévoir l'utilisation des plans de restauration dans tous les cas même si les composants sont redondants.

Ne pas oublier de vérifier quotidiennement la lisibilité des bandes de sauvegarde par un test de restauration aléatoire. Ne pas oublier non plus de stocker les bandes dans une autre pièce ou mieux à l'extérieur de l'entreprise, afin d'éviter que les données et les sauvegardes ne soient pas détruites par un sinistre.

La réduction des risques consiste à mettre au point et à tester régulièrement un ensemble de procédures destinées à garantir la disponibilité des données et des services, et de réduire la probabilité d'apparition d'erreurs (exemple : contrôle des changements). La première, et plus importante d'entre elles, concerne la stratégie de sauvegarde et de restauration.

La seconde action, qui est plus du ressort de la gestion de la disponibilité, consiste à repérer puis à éliminer les points de passage obligé non redondants, que l'on nomme également SPOF (*Single Point Of Failure*), et dont la défaillance unitaire entraîne la défaillance de l'ensemble du système (maillon faible de la chaîne).

La troisième action envisageable dans le but de réduire les risques consiste à sécuriser l'accès aux zones sensibles par un contrôle de sécurité par badge, caméra ou biométrie. Cette sécurisation physique doit s'accompagner de la mise en place de systèmes de détection des problèmes majeurs, comme les incendies et les inondations, ainsi que de la mise en place de moyens de lutte.

Les scénarios de reprise

Les scénarios de reprise d'activité doivent prendre en compte les problèmes de personnel (astreinte, éloignement, etc.), de bureaux (clés, éclairage, localisation, etc.), des systèmes et des réseaux informatiques, des services logistiques critiques (climatisation, énergie électrique, télécommunications, courrier, etc.), et enfin prendre en compte les documentations.

Les différents modes de reprises sont les suivants :

- Ne rien faire.

Cette solution semble peu envisageable actuellement, même si l'on entend parfois des nostalgiques du papier expliquer qu'ils sont capables de fonctionner sans ordinateurs... en oubliant un peu les volumes considérés désormais.

- Solutions manuelles de contournement.

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

- Arrangement réciproque.

Les entreprises qui y participent acceptent de se soutenir mutuellement en cas de sinistre en se partageant les ressources informatiques. Rarement utilisée de nos jours, cette technique a pourtant prouvé son efficacité lors de sinistres célèbres, comme lors de l'incendie d'une grande banque française.

- Reprise graduelle (*cold stand by*).

Cette solution suppose l'utilisation de locaux vides dans lesquels l'entreprise doit réinstaller son système d'information à l'aide de ses propres équipements. À utiliser lorsque l'entreprise peut fonctionner quelques jours sans informatique.

- Reprise intermédiaire (*warm stand by*).

Ce scénario est basé sur l'utilisation d'un site de repli pré-équipé en matériel (bureaux, télécommunications, systèmes et réseaux informatiques), mais non configuré. À utiliser lorsque le rétablissement des services critiques doit se faire rapidement (de quelques heures à quelques jours).

- Reprise immédiate (*hot stand by*).

Cette solution est la plus efficace mais c'est aussi évidemment la plus chère. Elle consiste à utiliser un site de repli dédié équipé de matériel préconfiguré disposant d'une copie à jour des données de production. Cette solution doit être utilisée lorsqu'il est impératif d'avoir un redémarrage immédiat des services critiques, quelques heures après le sinistre.

Dans le cas d'une situation de crise, il est important de prévoir les ressources logistiques nécessaires pour les personnes qui prendront en charge la gestion de la crise (transports, hébergement, repas, communications, etc.). Il est également important de prévoir des remplaçants pour pallier d'éventuelles absences.

Implémentation

Après toutes les étapes d'analyse et d'étude, c'est désormais l'heure de vérité. La direction informatique est en première ligne, et doit implanter l'ensemble des technologies, des procédures et des services envisagés lors de la phase précédente.

Organisation et planning

Cette étape permet de mettre en place le comité de crise et de répartir les tâches entre les différents niveaux d'action et de décision de la structure de crise (direction, coordination, exécution).

Définir les différents plans de reprise

C'est lors de cette étape que sont réalisés les différents plans de reprise d'activité. On trouve notamment au niveau direction de l'entreprise, les plans de coordination, dont les plans de réaction d'urgence, d'évaluation des dommages, de gestion de crise et de relations publiques. À un niveau plus opérationnel, on trouve les plans sur les serveurs et les réseaux informatiques, des télécommunications, de sécurité, des ressources humaines, des moyens et des services généraux, et enfin, les plans financiers et administratifs.

Il faut veiller à ce que ne soit utilisée que la dernière version de ces plans.

Enfin, chaque domaine métier critique est responsable de la définition détaillée des actions de reprise de son domaine. Le plan de reprise de la direction informatique contient pour sa part toutes les informations nécessaires au rétablissement des serveurs, des réseaux et des télécommunications lors d'une situation de crise, ainsi que les procédures de retour à la normale après cette période.

Implémenter les mesures de réduction des risques

Cette étape est souvent réalisée par le processus de gestion de la disponibilité. Il s'agit en général d'installer les équipements de redondance et de secours électrique (alimentations redondantes, onduleurs), de redondance de disques (RAID), et de systèmes à tolérance de pannes et de clusters.

Accords avec les sociétés tierces

Ces accords concernent la possibilité d'utiliser les services de secours et de reprise de sociétés tierces. (sauvegarde en ligne, sites de repli, serveurs de secours externalisés).

Rédaction des procédures

Les procédures de secours permettent aux opérateurs de procéder à la reprise d'une partie du système d'information. Le document ne doit présenter aucune ambiguïté et doit être compréhensible par une personne technique non familière de cette procédure. Enfin, il doit offrir une liste de vérification à appliquer après chaque étape importante.

Ces procédures de gestion de crise et de retour à la normale, doivent inclure les modes opératoires d'installation et de test des différents matériels, serveurs, disques, sauvegarde, et réseaux de remplacement. Elles doivent également prendre en compte la restauration des systèmes, des applications et des données, à partir d'un point de reprise cohérent commun à toutes les activités métiers.

Tests et validations

Une fois terminées la conception et l'implantation des technologies, des méthodes, des procédures et des documentations, il est impératif de tester

l'ensemble du plan le plus rapidement possible. Dans le cas contraire, le temps et l'énergie dépensés dans ce processus seront réduits à néant au premier sinistre. Le test permet en particulier de valider le fonctionnement des technologies et d'affiner les procédures utilisées, ce qui n'est évidemment pas envisageable en situation réelle de crise.

Les tests réguliers doivent être annoncés à l'avance afin d'impliquer les directions métier critiques dans des tests complets de l'ensemble du plan. Mais certains tests impromptus, impliquant certaines parties ou l'ensemble du plan, peuvent être envisagés pour valider la réactivité des équipes. Dans ce cas, la direction générale doit être avertie et donner son accord.

Gestion opérationnelle

Une fois implantées les méthodes, procédures et technologies préconisées dans le plan de continuité de service, il est nécessaire de s'assurer que le plan est maintenu à jour et aligné sur les évolutions de l'entreprise et celles du système d'information. Pour parvenir à ce résultat, toutes les personnes impliquées dans la continuité de service doivent être conscientes des implications du processus et doivent les intégrer dans leurs activités quotidiennes. Ces personnes peuvent gagner en efficacité en suivant des formations spécifiques aux métiers soutenus par le plan de continuité.

La validation du plan et des documents doit se faire en permanence ou tout au moins à chaque changement majeur. Cela permet de s'assurer que ces modifications sont reportées dans le plan de continuité et mises à jour. Il existe ensuite plusieurs solutions permettant de s'assurer que les procédures et les documents restent pertinents, même en cas de changements majeurs. La première des solutions est de mener des revues et des audits réguliers de ces documents. La seconde est d'effectuer, au moins une fois par an, un test grandeur nature.

En cas d'événement grave, si la production informatique est stoppée, le plan de continuité doit être déclenché. Cette décision ne peut souffrir aucune ambiguïté car les conséquences d'un déclenchement sont très importantes.

Cette décision doit être prise rapidement par un comité de crise (*Crisis Management Team*) composé des responsables métier et informatique. Le comité dispose d'un mode opératoire regroupant une liste d'actions, un annuaire des membres du plan de crise, et la localisation de la documentation complète.

Une fois la décision prise, il faut communiquer la situation aux principales personnes touchées au sein de l'entreprise, qui informeront à leur tour les utilisateurs de leurs entités métier.

Lors du fonctionnement en mode « crise », une certaine souplesse peut être accordée dans la gestion classique des services informatiques. Cependant, il est important de garder la trace de toutes les activités réalisées pendant la période de reprise afin de réaliser une analyse ultérieure. De plus, il est vital que les mécanismes et les contrôles de sécurité soient maintenus pendant cette période, au moins la forme dégradée prévue au plan de crise.

Concernant le personnel engagé dans la gestion de crise, il est important de bien gérer leur planning et leur temps de repos éventuels, et surtout de bien reconnaître leurs actions lors de la crise, au besoin en récompensant cet engagement une fois l'orage passé...

Mesures et contrôles

Pour ce processus, les métriques et les mesures de contrôle sont évidentes. Seuls des tests réguliers des différents plans, suivis de revues de fonctionnement peuvent valider ou non l'efficacité du processus.

Coûts

Les coûts générés par la mise en place du processus sont essentiellement composés des frais de personnel, de conseil et de gestion de projet (assez long, complexe à mettre en œuvre, et demandant de fréquentes mises à jour). Toutes les solutions permettant la redondance du matériel sont plutôt à imputer à la gestion de la disponibilité. En revanche, l'installation ou la location d'un site de secours peut représenter un coût très important, qu'il convient de justifier financièrement en regard de l'aspect critique de l'activité de l'entreprise. Mais ce qui est sûr également, c'est que le coût d'implantation de ce processus doit être mis en regard de l'hypothèse d'un éventuel arrêt total de la production de l'entreprise. Dans ce cas, c'est bien l'avenir de l'entreprise qui est en jeu.

Documents et rapports

Les documents produits par ce processus sont essentiellement représentés par les différents plans de continuité informatique et de continuité métier.

Conséquences

Les bénéfices que l'on peut attendre de la gestion de la continuité de service proviennent plus d'une absence de conséquences désastreuses, sinon fatales à l'entreprise. Parmi celles-ci, la gestion des risques permet de réduire l'impact des pannes informatiques comme des événements extérieurs. Ceci peut avoir une conséquence financière non négligeable, puisque la direction informatique démontre par ses actions proactives sa volonté de gérer les conséquences des pannes, ce qui peut permettre de négocier la prime d'assurance de l'entreprise à la baisse.

De plus, il ne faut pas oublier que certaines industries et certains services doivent assumer des contraintes légales dans toutes les situations, qu'elles soient exceptionnelles ou non. Ce processus peut permettre de respecter de telles obligations réglementaires.

La diminution ou l'élimination des interruptions de l'activité lors d'un incident participe à l'amélioration de la confiance du marché envers l'entreprise. Elle dispose ainsi d'une meilleure image (robustesse, fiabilité, réactivité, etc.) qui peut être utilisée comme élément différentiateur pour convaincre de nouveaux clients et ainsi contribuer au chiffre d'affaires de l'entreprise, mais également comme élément de fidélisation des clients existants.

Exemple : obligations FDA dans l'industrie pharmaceutique et IAS dans les banques.

Enfin, l'analyse des besoins et des priorités des activités métier passe par des relations étroites avec les directions métier. Ceci entraîne une compréhension accrue par la direction informatique des besoins métier et la rapproche des autres directions de l'entreprise.

En revanche, la mise en place de ce processus peut créer des problèmes induits par l'implantation elle-même. Le premier risque, et certainement le plus important, correspond à un manque d'implication des directions métier ainsi que de la direction de l'entreprise. Si cette dernière n'a pas intégré le caractère stratégique du processus, toute tentative d'implantation est vouée à l'échec. En effet, comment obtenir des ressources, du personnel et du temps, lorsque ce processus qui en consomme beaucoup semble ne rien apporter aux responsables de l'entreprise ? De plus cette implication n'est pas seulement nécessaire lors de la première implantation, mais tout au long de l'activité de l'entreprise.

Les coûts associés à ce processus peuvent également conduire à un échec de sa mise en place. La tentation est forte d'implanter une solution puis de la laisser en l'état sans évolution. Or, les objectifs métier font évoluer l'infrastructure ce qui peut entraîner des soucis si les plans de reprise d'activité sont mis au second plan. C'est pourquoi un message fort de la direction doit rappeler régulièrement que la pression du marché ne doit pas être utilisée comme excuse dans l'abandon du processus.

Méthodes

Il existe de nombreuses méthodes permettant de concevoir un plan de continuité d'activité, mais ITIL recommande l'utilisation de deux méthodes en particulier qui sont la BIA et la CRAMM.

BIA

La BIA (Business Impact Analysis) est une méthode d'analyse de l'impact métier qui permet d'évaluer les pertes potentielles lors d'un sinistre, informatique ou d'un désastre plus global, en identifiant les processus métier critiques et le niveau des dommages envisageables en cas d'interruption de ces processus critiques. La BIA permet également de prévoir la forme que les dommages vont prendre comme les pertes financières, la perte du stock, une perte de confiance du marché, l'altération des données ou la destruction d'un bâtiment, etc.

CRAMM

La CRAMM (CCTA Risk Analysis & Management Method) est une méthode d'analyse et de gestion du risque qui permet d'identifier les risques qui peuvent causer une altération de la disponibilité, de la confidentialité ou de l'intégrité des services informatiques. La CRAMM propose des contre-mesures dans le but de réduire la menace que représentent ces risques pour le système d'information.

Rôles et responsabilités

Le responsable du processus doit disposer d'un haut niveau dans la hiérarchie de l'entreprise, ou à défaut être épaulé par un directeur, et doit travailler en étroite collaboration avec le responsable sécurité (il s'agit parfois de la même personne).

Son rôle est de concevoir et de maintenir le plan de continuité des services informatiques de l'entreprise afin d'assurer que les objectifs de reprise d'activité après un désastre sont réalistes.

Il doit en particulier valider que les procédures, les techniques, et les tests de reprises sont opérationnels en permanence et connus des différents intervenants.

Enfin, en cas de crise, il coordonne les équipes et lance les procédures de reprise d'activité documentées dans le plan.

Compétences

Le responsable de la gestion de la continuité de service doit disposer d'une bonne expérience dans la gestion des services informatiques et doit disposer d'une expérience dans la mise en place du processus. Il doit être capable de transposer les demandes métier en spécifications techniques et doit bien comprendre l'impact qu'une indisponibilité entraîne sur le système d'information.

Enfin, il doit être capable de communiquer avec tous les niveaux de l'entreprise, et donc d'adapter son discours à ces différents niveaux.

Comité

En situation de crise, chaque employé impliqué dans la gestion de cette situation fait partie d'un « comité spécial de crise », dans le but de gérer les actions et les décisions à entreprendre pour passer la crise dans les meilleures conditions possibles.

Ce comité virtuel est en fait le reflet des rôles dont chacune de ces personnes est le dépositaire. Cette organisation de crise est constituée de plusieurs niveaux hiérarchiques, ce qui lui permet d'agir à plusieurs niveaux de l'entreprise. En fonction de la situation (situation normale ou situation de crise) chaque niveau a un ensemble d'actions à réaliser.

Situation normale	Situation de crise
Conseil d'administration et direction	
Mettre en place le processus de la continuité de service et établir la politique, les ressources et les responsabilités.	Gestion de la crise, décisions stratégiques d'entreprise, gestion des relations extérieures.
Directeurs de division et cadres supérieurs	
Gérer le processus de continuité des services, valider les documents, communiquer et former, assurer l'intégration des procédures dans l'organisation.	Coordination et arbitrage des actions, contrôle des ressources.
Cadres et responsables de service	
Analysier les processus de la continuité de service informatique, définir les documents à fournir, souscrire les éventuels contrats de services, concevoir et gérer les tests.	Déclenchement du plan, direction des équipes, gestion du site et production de rapports.
Chef d'équipe et personnel	
Développer la documentation, négocier les différents services, tester régulièrement les procédures.	Mettre en œuvre les procédures de reprise d'activité, réaliser la liaison entre les équipes.

GESTION FINANCIÈRE DES SERVICES

À LA MATERNITÉ,
J'AURAI PRÉFÉRÉ DES BONS
D'ESSENCE AU LIEU DES ÉCHANTILLONS
DE COUCHES !



LA GESTION FINANCIÈRE CONSISTE À IDENTIFIER LES COÛTS ET
À LES RELIER AUX SERVICES... POUR POUVOIR ÉVENTUELLEMENT
LES FACTURER AUX UTILISATEURS.

La gestion financière des services

Les besoins des entreprises en termes de services informatiques sont en perpétuelle croissance. Cela est certainement dû au fait que les entreprises s'approprient de plus en plus l'outil informatique pour ce qu'il est, une formidable aide à la conception, à la production et à la gestion : autrement dit, un maillon essentiel de la chaîne de valeur. Ces vingt dernières années ont vu une explosion de l'informatisation des entreprises, ainsi que des dépenses qui vont avec. Avec lassitude, les responsables des entreprises voient s'envoler ces coûts dont l'augmentation est souvent plus importante que dans les autres secteurs de l'entreprise. Mais les clients et les utilisateurs qui demandent sans cesse de nouvelles fonctions et de nouveaux services, ont-ils conscience du coût engendré par leurs demandes ? Ses nouveautés vont-elles apporter à l'entreprise un retour sur investissement justifiant leurs mises en place ? Le service informatique est-il rentable ?

Vue d'ensemble

La gestion financière des services informatiques est destinée à rendre visibles les coûts et à permettre leur contrôle au travers d'une gestion efficace des ressources informatiques utilisées dans la fourniture des services. Une fois déterminé et connu, le client et l'utilisateur peuvent être informés du coût global de ces prestations. L'objectif sous-jacent est de permettre de comptabiliser entièrement les dépenses de la direction informatique dans l'hypothèse d'une facturation éventuelle de ces coûts aux directions métier.

On peut donc dire que la gestion financière des services informatiques doit remplir les rôles suivants :

- établir les budgets annuels de fonctionnement et d'investissement de la direction informatique ;
- suivre et contrôler les dépenses du service en regard de ce budget ;

- mettre en place une éventuelle facturation des autres directions de l'entreprise en fonction des services qu'elles consomment ;
- aider à concevoir une stratégie d'investissement en fonction de l'apport des nouveautés technologiques ;
- fournir des objectifs de coûts pour la fourniture des services ;
- prendre des décisions sur le long terme à la lumière des investissements passés et de leurs conséquences sur le système d'information.

Attention cependant à ne pas générer un monstre dévorant les fruits qu'il est censé défendre. La gestion financière du système d'information peut être très complexe. Si elle est mise en place avec un niveau de détail trop fin, elle peut coûter bien plus que les réductions qu'elle souhaitait engendrer.

Pourquoi ?

Depuis des dizaines d'années, force est de constater que les coûts des services informatiques augmentent en général plus rapidement que les coûts des autres services. Ces services informatiques sont alors considérés comme trop chers ou pas assez évolutifs. Cela n'est évidemment pas le fruit du hasard. Les entreprises en cours d'informatisation sont nécessairement gourmandes en infrastructure matérielle et logicielle, ainsi qu'en service. Mais les sociétés qui disposent déjà d'un système d'information en état de fonctionnement devraient constater une diminution des coûts associés. Or, il n'en est rien, et la plupart de ces entreprises constatent même le contraire. La conséquence désastreuse est que la direction informatique ressent des difficultés à justifier ses coûts de fonctionnement et d'investissement. La réalité est en effet plus complexe qu'il n'y paraît. Comme tous les systèmes, et à l'instar de l'entreprise qui l'utilise, l'outil informatique doit vivre et évoluer sous peine de disparaître. L'obsolescence des solutions, les contraintes légales et fiscales, les nouvelles fonctions nécessaires à la compétitivité de l'entreprise, sont autant de générateurs de dépenses. Le but de la gestion financière des services informatiques est de contrôler le budget et les dépenses de la direction informatique, afin d'en optimiser le fonctionnement. Cependant, il faut comprendre que le but d'ITIL n'est pas de réduire à tout prix les coûts du système d'information mais bien de contrôler ces coûts. Si elle se produit, la diminution des coûts est uniquement une résultante du contrôle efficace qui est réalisé.

Concepts

Si les informaticiens ne veulent plus être perçus comme les paniers percés de l'entreprise, il est indispensable de changer la vision que les clients et les utilisateurs ont des services informatiques. La gestion financière permet de justifier les coûts des services informatiques lorsque ceux-ci sont alignés sur les objectifs métier de l'entreprise.

Trois processus fondamentaux constituent cette gestion financière des services informatiques.

En premier lieu, on retrouve la budgétisation, qui correspond à la prévision des dépenses dans une organisation, puis au suivi de ces dépenses afin de s'assurer que les coûts réels correspondent aux coûts prévisionnels, et d'éviter ainsi les dérapages budgétaires. Elle se réalise selon un cycle périodique (généralement annuel) constitué de demandes, de propositions puis de négociations pour définir les budgets. Au départ globales et imprécises, ces négociations débutent avec des propositions des directions métier sur un budget informatique proportionnel à leurs budgets de fonctionnement. Celui-ci est souvent réévalué en fonction de ce que la direction informatique a indiqué sur ses coûts. La négociation se termine alors par la production d'un budget global de la direction informatique regroupant les demandes des différentes directions métier.

Nous trouvons ensuite la comptabilisation des dépenses, c'est à dire la comptabilité analytique de l'informatique qui nécessite de réelles compétences comptables et financières. Elle est constituée d'une série d'activités permettant à la direction informatique d'analyser la manière dont sont dépensés les budgets (ventilation par client, par service, par activité). Cette activité d'analyse permet d'assister les responsables dans leurs décisions d'investissement. La comptabilité informatique permet également d'assister le suivi du budget, en comptabilisant l'argent dépensé dans la fourniture des services, et de calculer le coût de cette prestation fournie aux clients.

Le troisième processus fondamental correspond à la facturation. Elle regroupe plusieurs sous-processus utilisés pour imputer aux clients le coût des services qu'ils utilisent. Lorsque la direction de l'entreprise le demande, cela permet de gérer la direction informatique comme un centre d'activités (*Business Unit*) et d'influencer le comportement des utilisateurs et des clients qui perçoivent désormais l'informatique interne au même titre qu'un fournisseur classique. Cette facturation peut se faire sur une période annuelle ou mensuelle et prévoir des facturations complémentaires ponctuelles, lors de projets non inclus dans les accords du SLA (nouveaux projets, déménagements, mise à niveau imprévue du système, etc.).

Périmètre

Bien que la responsabilité de ces processus et de ces tâches puisse être assumée par la direction financière de l'entreprise, le périmètre du processus de gestion financière concerne les prévisions budgétaires, la comptabilité et la facturation des services informatiques. Mais même si la direction informatique assume la responsabilité totale du processus, il est recommandé de travailler étroitement avec le département financier et avec des comptables qualifiés.

Description du processus

Flux du processus

Le processus de la gestion financière des services informatiques est constitué de trois sous-processus fondamentaux qui sont la budgétisation, la comptabilisation et la facturation. Fidèle aux concepts principaux d'ITIL, d'amélioration permanente de la qualité, et à l'image de la roue de Deming, le lien entre chacune des trois activités est présenté dans le cycle financier de la figure 14-1.

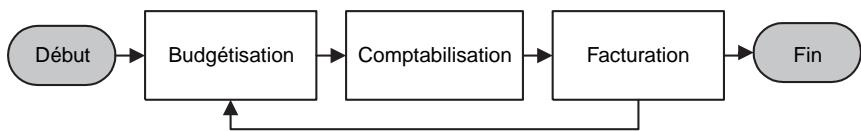


Figure 14-1 : Schéma simplifié des activités de la gestion financière

Les entrées du processus proviennent des directions métier qui communiquent leurs besoins en fonction des objectifs de l'entreprise et des moyens dont elles disposent, ainsi que d'autres processus ITIL dont les trois principaux sont :

- la gestion des niveaux de service qui demande l'estimation du coût du service attendu par les clients ;
- la gestion de la capacité dont les informations peuvent être utilisées pour estimer le coût d'un niveau de capacité de l'infrastructure ;
- la gestion des configurations qui fournit des informations sur les coûts de l'ensemble des composants des infrastructures.

Les sorties du processus sont essentiellement composées du budget, des rapports comptables et des rapports financiers concernant la consommation des ressources informatiques par les différentes directions métier.

Planification et mise en œuvre

L'implantation de la gestion financière des services repose sur la mise en place des trois sous-processus de budgétisation, de comptabilisation et de facturation. Ces trois sous-processus sont interdépendants, mais peuvent être mis en place par étape, chacune de ces étapes rentrant ensuite dans le cycle d'optimisation des finances de la direction informatique.

Le projet d'implantation de la gestion financière est, plus que tout autre projet dans ITIL, un projet d'entreprise et doit disposer d'un engagement total de la direction générale. Une équipe composée de membres de plusieurs services est constituée (directeur informatique, représentant de la direction

financière, représentant de la gestion des services informatiques, représentants des différents clients, etc.), afin de prendre en charge l'étude de faisabilité qui doit identifier les bénéfices attendus, définir les règles de facturation, mettre en place le planning, identifier les coûts et les classer, etc. L'équipe projet doit également proposer des modèles de coûts, et choisir une méthode de comptabilisation en accord avec les objectifs de l'entreprise.

Après cette étape de validation et de conception, une phase « d'évangélisation » est nécessaire afin de limiter les résistances au changement. Cette phase pédagogique consiste à expliquer les bénéfices attendus par cette gestion financière afin d'éviter que celle-ci ne soit perçue comme l'énième boulon d'une usine à gaz bureaucratique.

Enfin, et avant la mise en production totale, l'utilisation d'un site ou d'une période de transition, pour ne pas dire de site pilote, peut sans doute permettre de lever les derniers soucis dans l'identification et l'estimation des coûts, dans la comptabilisation de ces coûts, puis dans le calcul de la facturation aux clients.

Le schéma suivant (figure 14-2) illustre les différentes activités et relations du processus de gestion financière des services informatiques.

Budget

La création du budget informatique correspond à la production d'une prévision de la consommation annuelle des ressources informatiques par les directions métier de l'entreprise, associé aux prévisions de recettes provenant de ces mêmes clients et permettant d'équilibrer la balance budgétaire. Le budget permet en effet de vérifier que le financement prévu est suffisant pour assurer la fourniture des services informatiques, mais également de contrôler que les dépenses ne dépassent pas les prévisions.

Conception du budget

Le périmètre du budget de la direction informatique couvre le budget de fonctionnement ou d'exploitation, il s'agit alors de l'ensemble des dépenses courantes, ainsi que le budget d'investissement, qui concerne les nouveaux projets et les achats en matériels, logiciels et prestations du service informatique.

Le budget est composé d'un ensemble de lignes recensant de manière exhaustive tous les coûts générés par la fourniture des services informatiques durant la période budgétaire (généralement annuelle).

Lignes du budget

À la différence de la direction financière de l'entreprise, aucune contrainte réglementaire n'est imposée dans le suivi financier réalisé par la direction informatique. Le mode de répartition des composants et des coûts du système d'information importe peu tant que l'exhaustivité est garantie et que cette méthode permet d'établir des comparaisons d'une année sur l'autre.

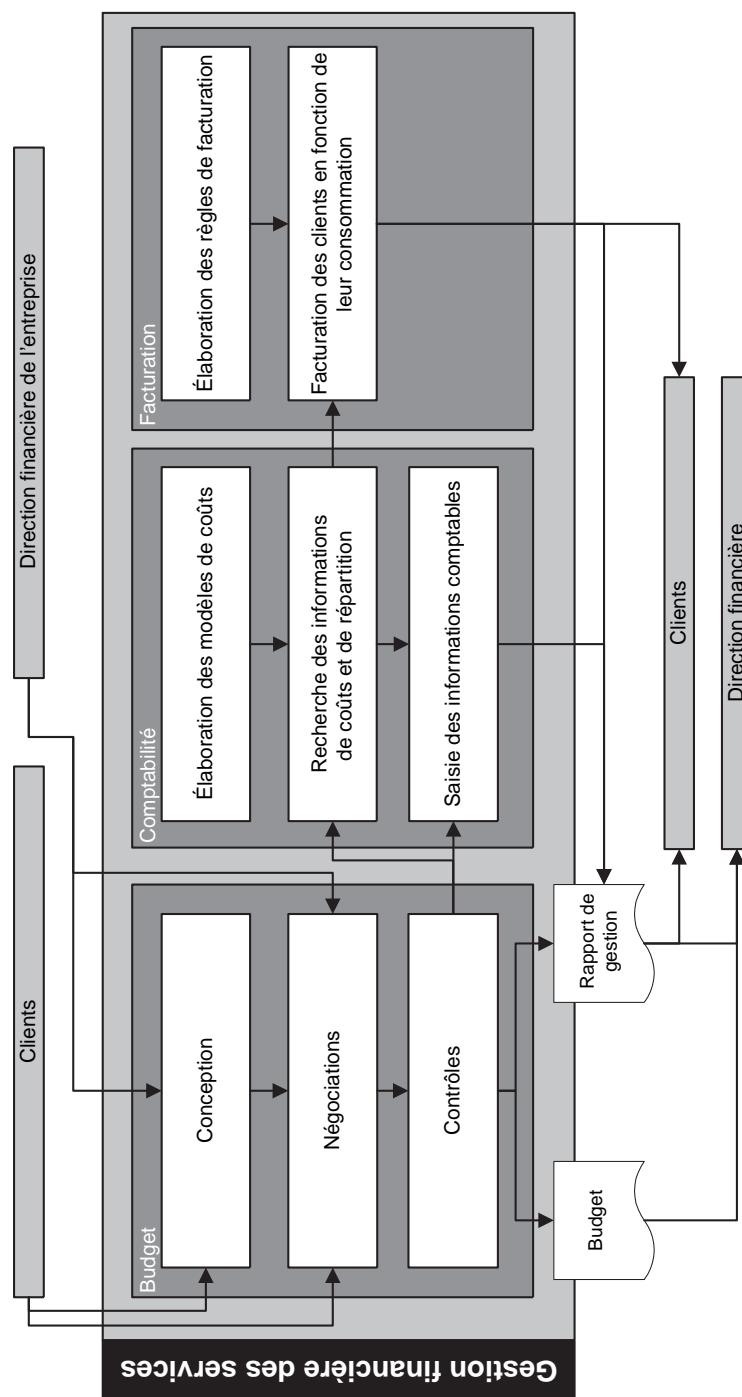


Figure 14-2 : Schéma des activités de la gestion financière des services

Le budget annuel

La méthode classique d'établissement du budget annuel est de plus en plus critiquée par certains analystes financiers qui dénoncent son caractère réducteur, pour ne pas dire destructeur. Il est vrai que cette méthode ne favorise pas la réflexion sur le bien-fondé de tel ou tel poste dans le budget. Souvent, les responsables se contentent de prendre le budget de l'année précédente, d'y appliquer un coefficient multiplicateur et de reconduire le document.

Pour éviter cela, il est conseillé de mettre en place un plan exhaustif des prévisions de recettes et de dépenses sur l'année à venir, couvrant l'ensemble des projets en cours, même si ceux-ci débordent du cadre budgétaire annuel. Il faut ensuite y ajouter un récapitulatif de l'année passée et associer les prévisions des grandes orientations et des projets importants, sur une échéance de trois à cinq ans. Bien sûr, il est souvent totalement irréaliste de s'engager sur une période aussi longue en informatique. D'une part le cycle de l'obsolescence des technologies est aujourd'hui extrêmement court, on parle actuellement de moins de sept mois ! D'autre part, les besoins et les demandes des directions métier peuvent évoluer aussi vite que les marchés auxquels elles s'adressent... Cependant, tant sur les investissements légers que sur ceux qui engagent l'entreprise sur plusieurs années, il est possible de faire des estimations financières globales. Sur les investissements plus classiques, les coûts considérés n'évoluent pas fondamentalement d'année en année. Les projets plus importants ou structurants doivent être estimés sur des périodes qui permettent l'amortissement complet de l'investissement. Enfin, lorsque l'entreprise a recours à la location de son parc informatique, le budget de fonctionnement est connu et maîtrisé. Dans le cas de notre budget sur cinq ans, la direction informatique ainsi que la direction générale peuvent infléchir ces prévisions budgétaires, afin d'aligner les coûts sur la réalité de l'entreprise. Cela peut être réalisé chaque année, et lors de la négociation budgétaire, à la lumière de la consommation de l'année précédente et de l'évolution des technologies informatiques.

Cela implique que le modèle de suivi analytique conçu puis utilisé dans le processus de gestion financière doit être réaliste et réutilisable pendant plusieurs années. Cependant, un bémol doit être apporté, puisqu'il est indispensable de respecter les règles comptables classiques qui peuvent parfois être différentes d'une ligne sur l'autre. On gagnera donc à calquer la classification des lignes budgétaires sur l'organisation retenue par le service comptabilité, c'est-à-dire basée sur le modèle de coût fixé par l'entreprise.

Contrôle du budget

Une fois le budget établi, il est de la responsabilité de la direction informatique de contrôler la consommation de ressources et de valider qu'elle correspond bien aux prévisions. Toutefois, il peut arriver que certaines estimations ne soient pas vérifiées. C'est le cas par exemple des coûts qui dépendent du volume à fournir, du nombre d'utilisateurs (licences sur les logiciels), ou des prestations extérieures. Cependant, il est possible de prévoir assez précisément ces coûts en ayant une vision claire des projets des directions métier.

Le découpage en plan analytique est un travail complexe qui dépasse le cadre de ce livre. Le lecteur intéressé peut avec profit se plonger dans l'abondante littérature sur le sujet, et en particulier celle concernant la comptabilité analytique, ou la mise en place de tableau de bord de gestion financière de l'informatique.

Comptabilité

Exemple : la durée de l'amortissement est différente sur le matériel et le logiciel, et peu utilisée sur les prestations.

En fonction de ces choix de gestion, l'entreprise peut décider de mettre en place un mode d'interprétation différent des finances de la direction informatique.

Mode de comptabilisation

L'interprétation en tant que centre de coût permet le suivi des dépenses en corrélation avec les lignes budgétaires et procure une bonne maîtrise des investissements. Cependant, elle ne permet pas de comprendre ou de maîtriser le comportement des utilisateurs, et ne donne pas d'autonomie à la direction informatique dans sa gestion financière.

La méthode intermédiaire consiste à voir la direction informatique comme un centre de gestion équilibré. Elle consiste en l'identification, le contrôle et le calcul du coût des services, puis en une imputation de ces coûts aux différents clients, suivie d'un recouvrement des sommes considérées. Cette méthode permet d'identifier clairement les coûts financiers de la fourniture des services informatiques et d'en faire prendre conscience aux directions métier.

La troisième et dernière solution consiste à voir la direction informatique en tant que centre de profit. Cette méthode de gestion est adaptée à la direction informatique qui dispose de suffisamment d'autonomie au sein de l'entreprise pour fonctionner comme une activité métier indépendante avec des objectifs fixés par l'entreprise. L'entreprise peut par exemple décider de laisser toute liberté à la direction informatique pour faire du bénéfice sur son activité, et éventuellement de vendre ce service à l'extérieur. Cette approche procure beaucoup d'autonomie mais comporte aussi de nombreux risques. En effet, la direction informatique est perçue par le client comme un prestataire extérieur, auquel il fait appel pour la fourniture de ses services informatiques. Dans ce cas, le client peut éventuellement choisir une autre société lorsqu'il n'est pas satisfait de la qualité ou des tarifs du service proposé en interne. Il est donc important d'être compétitif tant sur les prix que sur l'éventail et la qualité des prestations proposées.

Équipe interne versus externalisation

Même si elle comporte des risques pour les salariés internes, cette méthode a toujours l'avantage d'être claire sur les coûts des services. En effet, dans ce domaine, il n'est de pire ennemi que le non-dit, c'est-à-dire l'absence d'information. Certaines sociétés sont parfois tentées d'externaliser leur production informatique, au détriment de l'équipe interne, en ne connaissant pas réellement les coûts de cette production. De nombreux exemples ont démontré que l'avantage financier n'était pas systématiquement du côté de l'externalisation, et en particulier lorsque l'équipe informatique détient une connaissance non reconnue ou non identifiée par l'entreprise, et qu'aucun projet de gestion de la connaissance n'a permis de capitaliser et d'internaliser ce savoir.

Modèle de coûts

Le calcul des coûts des services informatiques demande qu'un cadre soit défini dans le but d'enregistrer et de classer les coûts connus avant de les imputer aux clients. Plusieurs types de répartitions complémentaires existent.

- La répartition en coûts directs et indirects.

Les coûts directs correspondent à des coûts clairement attribuables à un client (exemple : logiciel comptable imputé à la direction financière), alors que les coûts indirects concernent les services qui sont fournis à un groupe ou à l'ensemble des clients de manière diffuse, et pour lesquels il faut définir une clé de répartition par client (ex : réseau, messagerie, assistance utilisateur, etc.).

- La répartition en coûts fixes et coûts variables.

Ce mode de répartition permet de scinder les coûts entre ceux dont on connaît à l'avance le montant annuel (achat de logiciel, location de matériel, salaire du personnel, etc.) et ceux dont le montant est lié à un aléa tel que le volume consommé ou les évolutions saisonnières (heures supplémentaires, remplacement de personnel absent, consommables, électricité, etc.).

- La répartition en coûts amortissables et non-amortissables.

Les premiers correspondent à l'achat d'actifs qui augmentent la valeur de l'entreprise, mais dont la valeur se déprécie annuellement (amortissement) et qui correspond à la somme utilisée dans le modèle de coût.

Les seconds correspondent aux dépenses courantes (coûts opérationnels) tels que coût de personnel, d'électricité, des prestations externes, des consommables, etc.

Amortissement des actifs

L'amortissement est la mesure de la diminution de la valeur d'un actif au cours du temps d'un point de vue comptable, qu'elle soit causée par l'usure ou par l'obsolescence. Ce traitement comptable correspond à la répartition du montant de l'achat de l'actif sur une durée fixée par la direction financière en fonction de la législation locale (généralement de un à trois ans). Malheureusement, il arrive que des actifs amortis continuent à être utilisés alors que d'autres non-amortis ne sont plus utilisables.

Concernant l'amortissement des actifs matériels, trois méthodes peuvent être utilisées.

La première correspond à un amortissement linéaire durant lequel un montant fixe est déduit de la valeur de l'actif chaque année (exemple : 1/3 du prix d'achat sur 3 ans).

La seconde méthode, dite de l'amortissement dégressif, reprend la première en déduisant une somme dégressive chaque année (exemple : 50 % la première année, puis 30 % et 20 % pour les deux années suivantes).

Coûts indirects : les coûts forfaitaires.
Pour certains coûts indirects, il est très complexe de définir la répartition des sommes sur les différents clients. Dans ce cas, le plus simple est d'appliquer un coefficient multiplicateur sur l'ensemble des autres coûts, dans le but de répartir ces coûts sur chaque client et d'équilibrer les dépenses et les recettes.

La troisième et dernière méthode est relative à l'utilisation, et donc à l'usure, de l'actif. Elle permet de baser le calcul de l'amortissement sur la durée de vie estimée de l'actif (exemple : dans le cas d'une imprimante donnée pour 1 million de pages et qui imprime 200 000 pages la première année, 20 % de son prix est considéré comme amorti).

Les principaux éléments composants les coûts

Les coûts du système d'information sont composés de plusieurs types d'éléments. On peut les répartir en tant que :

- matériels (ordinateurs, imprimantes, réseaux, baies de stockage et de sauvegarde, etc.) ;
- logiciels (systèmes d'exploitation, logiciels bureautique, base de données, applications métier, etc.) ;
- ressources humaines (salaires, heures supplémentaires, frais de conseil, etc.) ;
- locaux (bureaux, salles informatiques, zones de stockage, etc.) ;
- services externes (achats de prestations externes, location de matériel, site de repli, sauvegarde externe, etc.) ;
- services internes, également appelés transferts (climatisation, sécurité aux alentours des installations, prestations internes, développement en interne, support d'autres services, etc.).

Coût total de possession (*Total Cost of Ownership*)

Le calcul du TCO est une méthode d'évaluation du coût réel d'un service informatique proposée par le Gartner Group. En plus du prix d'achat, elle prend en compte l'ensemble des coûts durant tout le cycle de vie du produit ou du service. Par exemple, le Gartner Group estime que le coût d'achat d'un PC représente à peine 6 % du coût total de possession sur 5 ans, ce coût total incluant l'achat, l'installation, la formation, le support, la maintenance, etc.

Cette méthode TCO peut également être intéressante lorsqu'il s'agit de décider d'une technologie ou d'une autre, mais des efforts pédagogiques sont nécessaires pour expliquer aux clients et aux utilisateurs les éléments de ce calcul qui surprend les clients s'il est communiqué brutalement.

Répartition des coûts

On l'a vu, le classement puis la répartition des dépenses du service informatique peut se faire par coût direct ou indirect. La question que l'on peut se poser est : comment répartir équitablement les coûts indirects aux différents clients qui consomment ces services ?

Dans l'exemple proposé ici, (figures 14-3 et 14-4) la direction « Recherches & Développements » de l'entreprise est un client de la direction informatique. Grâce à l'identification puis à la répartition des coûts, on peut identifier

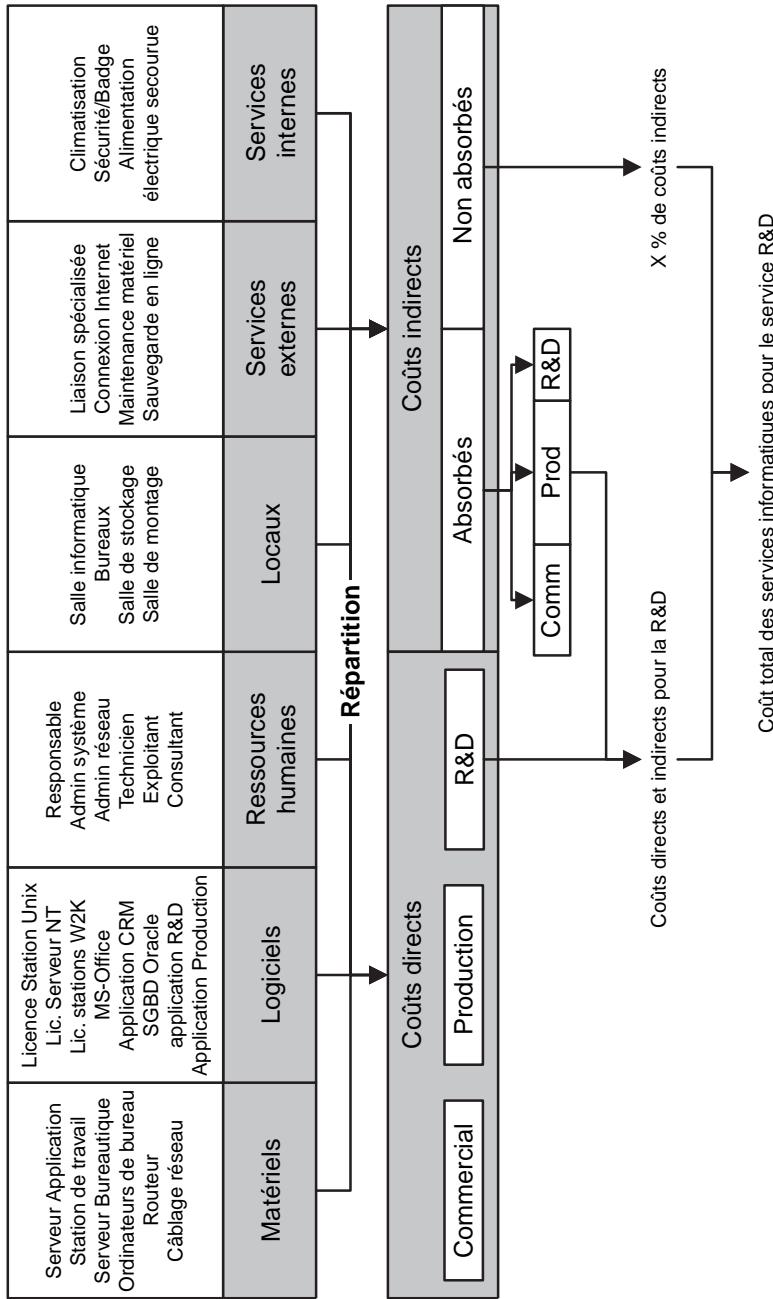


Figure 14-3 : Répartition des coûts de production des services informatiques

assez simplement les éléments que l'on peut imputer rapidement à ce client.

On peut tout d'abord repérer les coûts directs liés au métier du client. Ici, l'application de R&D et les stations de travail sont clairement des coûts directs.

Ensuite, on doit identifier les coûts indirects absorbés, c'est-à-dire les coûts qui bien que n'étant pas directement imputables à un client car mutualisés, représentent néanmoins des composants notoirement utilisés par ce client. C'est le cas ici du serveur bureautique ou du réseau. Dans ce cas, on répartira le prix en fonction du nombre d'utilisateurs dans chaque service. Pour la direction R&D cela représente 15 % des effectifs, donc 15 % des coûts indirects absorbés.

Les coûts indirects non absorbés sont représentés par les salaires, les locaux, les différents contrats, etc. La répartition de ce type de coûts peut difficilement se faire par nombre d'utilisateurs étant entendu que la consommation de chaque client peut être différente en fonction de son utilisation de l'outil informatique. Dans ce cas, le plus simple est de calculer ce qui reste à financer puis en déduire un coefficient à appliquer à tous les services afin de recouvrer l'ensemble de ces coûts de production.

Dans le tableau récapitulatif d'exemples (figure 14-4), on constate rapidement que les coûts indirects non absorbés représentent plus de 140 k€, que l'on divise ensuite par la somme du total des coûts directs et du total des coûts indirects absorbés. Cela donne alors un coefficient multiplicateur d'environ 76 % que l'on applique sur la somme des coûts directs et des coûts indirects absorbés de chaque client. Pour la direction R&D, cela donne donc 76 % de 36 k€ ce qui donne environ 28 k€. La direction R&D est donc facturée de $36 + 28 = 64$ k€.

Facturation

Confrontée à la quadrature du cercle, la direction informatique doit composer entre réduction des coûts et demande de services supplémentaires. La facturation permet de faire reconnaître les coûts engagés dans la production de services informatiques et permet également aux clients de prendre conscience des coûts des nouveaux projets. Mais la mise en place de la facturation des services informatiques est une décision de l'entreprise. Cette décision est liée au choix du mode de comptabilisation (centre de coût, de recouvrement, et de profit). Lorsqu'elle est mise en place, elle permet le recouvrement des coûts engagés dans la fourniture des services et oblige les directions métier à contrôler les demandes de leurs utilisateurs. Cependant, elle peut également avoir un effet dévastateur, et empêcher les demandes de changements ou les nouveaux projets, au détriment de l'entreprise, par crainte de se voir facturer les services.

	Nombre	Coût annuel	Type de coût	Capital (amortis)	Répartition			Comm.	Client Prod.	R&D	
Matériels											
Serveur Application	1	10 000	direct	Oui	50%	50%	100%	5 000	5 000	0	
Station de travail	3	9 000	direct	Oui				0	0	9 000	
Serveur Bureauautique	1	7 000	indirect	Oui				0	0	0	
Ordinateurs de bureau	100	90 000	direct	Oui	30%	55%	15%	27 000	49 500	13 500	
Routeur	5	2 500	indirect	Oui				0	0	0	
Câblage réseau	250	15 000	indirect	Oui				0	0	0	
Logiciels											
CD Linux	1	10	indirect	Non				0	0	0	
Licence Station Unix	3	1 500	direct	Non			100%	0	0	1 500	
Lic. Serveur W2003	1	3 000	indirect	Non				0	0	0	
Lic. stations W2000	100	6 000	direct	Non	30%	55%	15%	1 800	3 300	900	
MS-Office	40	5 000	direct	Non	60%	10%	30%	3 000	500	1 500	
Application CRM	1	12 000	direct	Non	1			12 000	0	0	
SGBD Oracle	1	10 000	direct	Non	50%	50%		5 000	5 000	0	
application R&D	1	6 000	direct	Non			1	0	0	6 000	
Application Production	1	15 000	direct	Non		1		0	15 000	0	
Ressources humaines											
Responsable	1	50 000	indirect	Non							
Admin système & réseau	1	30 000	indirect	Non							
Technicien	1	20 000	indirect	Non							
Consultant	1	10 000	indirect	Non							
Locaux											
Salle informatique	1	2 000	indirect	Non							
Bureaux	5	2 500	indirect	Non							
Salle de stockage	1	1 000	indirect	Non							
Salle de montage	1	500	indirect	Non							
Services externes											
Liaison spécialisée	2	5 000	indirect	Non							
Connexion Internet	1	1 200	indirect	Non							
Maintenance matériel	1	15 000	indirect	Non							
Support technique	1	1 500	indirect	Non							
Sauvegarde en ligne	1	2 000	indirect	Non							
Services internes											
Climatisation	1	3 000	indirect	Non							
Sécurité/Badge	1	1 500	indirect	Non							
Alimentation électrique secourue	1	2 000	indirect	Non							
Total coûts directs		164 500						53 800	78 300	32 400	
Total coûts indirects absorbés		27 510						8 253	15 131	4 127	
Total coûts indirects non absorbés		147 200		76.66%		30%	55%	15%	47 571	71 626	28 002
Total général		339 210						Total	109 624	165 057	
								Contrôle	Ok		

Figure 14-4 : Tableau de répartition des coûts de production des services informatiques

Politique de facturation

La politique de prix proposée aux clients doit être simple, compréhensible, juste et réaliste. De plus, la direction informatique doit obtenir un engagement fort de la direction générale qui doit communiquer clairement cette position à l'ensemble de l'entreprise. Il existe plusieurs modes de facturation interne :

- Prix coûtant.

Dans ce mode, le prix facturé au client est équivalent au coût de production.

- Prix avec marge.

Dans ce mode, le prix facturé au client correspond au coût de production auquel est ajoutée une marge calculée sur un pourcentage du prix de production.

- Prix comparable.
Dans ce mode, le prix facturé au client est comparable aux coûts d'autres organisations comparables (taille, activité, localisation géographique, etc.).
- Prix du marché.
Dans ce mode, le prix facturé est comparable aux prix du marché pratiqués par les fournisseurs externes.
- Prix fixe.
Dans ce mode, le prix facturé est fixé en accord avec le client pour une période donnée.

Mesures et contrôles

Pour que l'objectif de rentabilité des services informatiques soit atteint, il est nécessaire de mettre en place un ensemble de métriques permettant d'attester de l'efficacité du processus de gestion financière. Les mesures les plus évidentes de cette efficacité sont la précision du calcul des coûts et des propositions de facturation, l'équité et la justesse des charges imputées aux clients, ou également le changement de perception des services informatiques de la part des utilisateurs et des clients.

Cependant, même le modèle de coût le plus précis peut devenir incorrect en raison de changement des demandes ou du changement de comportement du client ou des utilisateurs. Il est donc certainement nécessaire de revoir ce modèle régulièrement, ainsi que le suggère ITIL dans son cycle d'amélioration permanente.

Coûts

Les coûts générés par l'implantation du processus de gestion financière sont essentiellement composés des coûts de personnel (contrôle, réalisation du budget, gestion des actifs, etc.). En effet, les logiciels de contrôle du budget et de comptabilité sont souvent achetés par la direction financière de l'entreprise ou sont issus d'applications bureautique classiques. Cependant, si un logiciel spécifique doit être acheté, son coût serait reparti entre les différents processus d'ITIL qui utilisent les autres fonctions de ce type de logiciel (gestion de parc, gestion de stock, immobilisation, inventaire, etc.).

Documents et rapports

Les documents du processus sont essentiellement composés des rapports comptables et financiers destinés à la direction générale d'une part, mais également aux utilisateurs et aux clients d'autre part. On trouve également un ensemble de documentations destinées aux utilisateurs et qui récapitulent les différents modes de facturation ainsi que les prix pratiqués par la direction informatique en fonction du service proposé.

Conséquences

Globalement, la gestion financière permet d'aligner les objectifs du service informatique aux métiers de l'entreprise. En tout état de cause, elle permet d'éviter les dérapages financiers en ne répondant qu'aux besoins réels exprimés par les directions métier. Ce processus permet également d'obtenir des informations pertinentes sur les coûts de possession (TCO) de l'infrastructure et des services, et permet ainsi d'aider les décisions d'investissements informatiques. Il en résulte alors un accroissement de la confiance que la direction générale place dans la direction informatique. Le corollaire de cet « engagement » est d'éviter la tentation que peuvent avoir certaines directions métier de monter des informatiques parallèles ou de faire appel à des prestataires extérieurs sans consulter la direction informatique.

Comme chaque sous-processus est implantable séparément, on trouve des avantages liés à chacun d'eux. Concernant la mise en place de l'activité de budgétisation, elle permet de s'assurer que les directions métier accordent les financements nécessaires à la fourniture des services qu'elles demandent, et permet de s'assurer que le niveau des services est maintenu tout au long de l'année. Elle permet également de percevoir rapidement un manque ou un excès de consommation de services et donc de budget.

Concernant la comptabilité des services informatiques, le principal avantage qui en découle est la production des informations sur le coût des services fournis afin de valider l'efficacité de la direction informatique. En effet, il est impossible d'optimiser les coûts informatiques si le coût des services fournis n'est pas connu auparavant.

Enfin, le troisième sous-processus, la facturation des services, apporte également son lot d'avantages. Le premier d'entre eux est certainement la prise de conscience des clients et des utilisateurs concernant le coût réel du service qu'ils consomment. Cela permet de mettre en balance le contenu et la quantité du service fourni en regard des besoins et des ressources du client. Il n'est pas rare alors de découvrir des services produits depuis des années, mais que personne n'utilise, et de les voir disparaître rapidement lorsqu'un projet de facturation est émis. En tout état de cause, si le client estime qu'un service fourni ne justifie pas le coût facturé, ce dernier sera interrompu ou modifié selon les besoins et les ressources du client. Concernant le formalisme du processus, celui-ci n'impose pas de mettre en place une facturation réelle, car si elle peut globalement améliorer le rapport qualité/prix du service, la charge de travail supplémentaire peut empêcher de réaliser les économies attendues.

Mais la mise en place d'un processus de gestion financière au sein de la direction informatique peut également présenter certains problèmes. Parmi ceux-ci, le premier provient de la difficulté de trouver une double compétence comptable et informatique. En effet, la comptabilité et la

facturation des services informatiques sont des activités relativement nouvelles. Il peut en résulter une connaissance limitée des règles comptables ou une mauvaise modélisation des coûts et de la facturation. Malheureusement, cela peut conduire à des systèmes erronés, trop complexes ou inefficaces, qui ne permettront pas d'atteindre les objectifs fixés, et qui au mieux coûteront plus que ce qu'ils permettent d'économiser. Dans ce cas, certaines activités doivent alors être partagées avec des équipes se trouvant en dehors du service informatique et dont ce n'est pas la priorité.

Outils

À l'exception des très petites organisations , il n'est pas pratique de mettre en place la gestion financière sans disposer d'une application appropriée. La solution minimale doit inclure la gestion de différents documents comptables classiques basés sur le modèle de coût choisi (grand livre, rapport d'utilisation de ressources, inventaire, etc.). Malheureusement, alors que ces outils existent, la plupart des directions informatiques utilisent encore des tableurs classiques pour développer leurs modèles de coût et de budget. Il est probable que ces solutions « maison » coûtent moins cher que l'investissement dans une application de gestion financière dédiée à l'informatique, mais en réalité, les données issues de ces tableurs doivent ensuite être contrôlées, puis éventuellement resaisies dans l'application comptable de l'entreprise. Au final, le coût d'exploitation et de maintenance de ce type de solution n'est pas inférieur à celui d'un système comptable complet.

Rôles et responsabilités

Certaines entreprises disposent d'un responsable des finances informatiques dédié, mais la plupart du temps, ce rôle est distribué entre la direction financière et la direction informatique, et peut être cumulé avec le rôle de responsable de la gestion des niveaux de service et de la gestion des capacités. L'important étant que les personnes qui assument ce rôle disposent des compétences et de l'autorité pour mener à bien cette mission de gestion financière.

Rôle

Quelle que soit sa position dans l'organigramme de l'entreprise, le rôle du responsable du processus est de travailler en étroite collaboration avec la direction financière afin de développer les règles budgétaires, comptables et d'imputation de la direction informatique. Il doit également assister la

direction informatique dans la conception et la mise en place des plans d'investissement.

Concernant le budget, le responsable doit préparer celui de la direction informatique et assister les clients sur la partie informatique de leur budget. Il doit également réaliser des rapports réguliers sur la consommation des services en regard des prévisions.

Concernant l'activité comptable, les tâches du responsable vont du choix de l'outil utilisé à l'analyse, jusqu'au conseil auprès des responsables des directions métier concernant les coûts des services, en passant par l'établissement des règles comptables et d'amortissement des actifs informatiques.

Enfin, son rôle dans le sous-processus de facturation est d'identifier les méthodes et les règles d'imputation envisageables, d'établir des listes de prix pour les services et de préparer les factures internes, le cas échéant.

Compétences

Du point de vue des compétences, le responsable du processus doit évidemment disposer de capacités réelles dans le domaine financier. Sa double compétence dans le domaine de la gestion des services informatiques, associée à sa compréhension des besoins des clients, lui permettent de communiquer avec l'ensemble des clients et la direction générale de l'entreprise. À ce titre, il doit disposer d'excellentes capacités de négociation. Enfin, il doit disposer d'une bonne expérience dans la production de contrats, de rapports, de graphiques et autres tableaux statistiques en utilisant les outils bureautique classiques ou les solutions de gestion financière plus élaborées.

PARTIE

IV

Mise en place d'un projet ITIL

La mise en place d'un projet ITIL au sein de l'entreprise ne peut se faire en quelques jours ou quelques semaines. Il s'agit en général d'un projet de longue haleine durant lequel de fortes oppositions sont envisageables. Dans cette partie, nous détaillerons l'implantation des différents processus et les difficultés potentielles lors de la mise en œuvre au sein de l'entreprise.

Vous trouverez en particulier :

- Chapitre 15 – Projet d'implantation d'ITIL/ITSM
- Chapitre 16 – Étude de cas
- Chapitre 17 – Justifier un projet ITIL
- Chapitre 18 – Conclusion

Projet d'implantation d'ITIL/ITSM

L'implantation d'ITIL, ou plus exactement de la gestion des services informatiques (ITSM), implique la mise en place d'un projet digne de ce nom qui va mobiliser les responsables de l'entreprise et, dans certains cas, la direction générale, les membres de la direction informatique, les ressources techniques et logistiques, et plus globalement l'ensemble de l'entreprise.

ITIL : un projet permanent !

La planification et la mise en œuvre de la gestion de service (ITSM) correspond à l'évaluation de ce qui doit être fait et à la production d'un plan pour le réaliser. Fidèles à leur concept d'amélioration continue de la qualité, les créateurs d'ITIL proposent de mettre en œuvre le référentiel dans le cadre d'un projet cyclique durant lequel les phases de conception, d'implantation, de mesure et de correction sont réalisées de manière itérative. De ce point de vue, il est peu aisé de parler de projet classique, avec un début, des objectifs, une fin et sa période de recette ; l'implantation d'ITIL demande que le cycle continue indéfiniment afin d'installer les différents processus, puis de les optimiser continuellement. Bien sûr, les ressources employées tout au long de ce projet vont évoluer, et il est clair qu'une fois certains processus mis en place, les besoins diminueront rapidement. Cependant, si l'on souhaite obtenir les améliorations annoncées, il ne faut pas envisager que ce projet ne dure que quelques mois puis se termine.

Il est évident que certaines entreprises ne souhaitent pas ou ne supporteraient pas la mise en œuvre immédiate de l'ensemble des processus. En effet, les ressources nécessaires, le coût ou tout simplement la maturité indispensable sont des freins à l'adoption intégrale d'ITIL. Une solution consiste à choisir certains processus jugés importants à planter dans un premier temps, puis de prévoir la mise en œuvre des suivants dans un second temps.

Il est donc important de prendre en compte les besoins les plus urgents et de planifier une stratégie à long terme, même si les objectifs d'amélioration doivent se situer à court, moyen et long terme.

En effet, l'adhésion des membres du projet peut se gagner simplement à l'aide de résultats rapides obtenus grâce à des objectifs proches et « faciles » à atteindre. Cet engagement du personnel actif est indispensable au projet, mais il doit en plus être totalement secondé par celui des responsables de la direction informatique et, plus largement, par celui de la direction générale. Cet engagement de chacun réduit en outre la résistance au changement qui, bien qu'inéluctable dans ce type de projet, sera largement diminuée par l'adhésion des responsables et des acteurs majeurs du projet. Cette résistance peut également être diminuée par une bonne communication, expliquant avec pédagogie les avantages que l'entreprise et la direction informatique vont tirer des processus ITIL, sans pour autant occulter les écueils envisageables.

Un autre élément important de la planification, de l'exécution et de la maintenance des processus de gestion des services informatiques (ITSM), concerne les rapports et l'analyse statistique, qui prouvent que les changements ont l'effet désiré. Il est important que, lorsque les changements de méthodes de travail n'ont pas l'effet souhaité, le programme soit modifié en conséquence. Il est également très important que, lorsque des améliorations ont été réalisées, celles-ci soient communiquées au personnel informatique aussi bien qu'aux utilisateurs et aux clients des services informatiques.

Enfin, ITIL fait souvent référence au besoin d'évaluer et de planifier les projets. S'il est effectivement important que ces tâches soient réalisées, il est également fondamental d'agir selon les actions planifiées, et de ne pas passer son temps à évaluer, à planifier et ensuite à réévaluer, sans améliorer réellement la qualité de service par la réalisation effective des actions préconisées.

En tout état de cause, l'implantation de ces processus donnera au personnel informatique l'occasion de jouer un rôle clé dans le soutien de l'activité de l'entreprise.

Les étapes du projet

Par où commencer ?

La réponse à cette question dépend du niveau de maturité de l'organisation informatique et des buts stratégiques qu'elle recherche. ITIL propose un modèle de maturité qui évalue le positionnement actuel et envisage le chemin à parcourir vers le but à atteindre. Dans cette optique, le modèle

propose l’évaluation de chacun des processus, puis les situe sur un des niveaux de maturité. En extrapolant, il est possible d’estimer le niveau de maturité global de la direction informatique.

Le niveau de maturité

Les nombreux modèles de maturité existants, tels que ceux d’ITIL ou de CMM, reprennent tous le même type de symbolique de l’escalier à gravir dans le but d’atteindre le fonctionnement optimal, comme on peut le voir sur la figure 15-1.

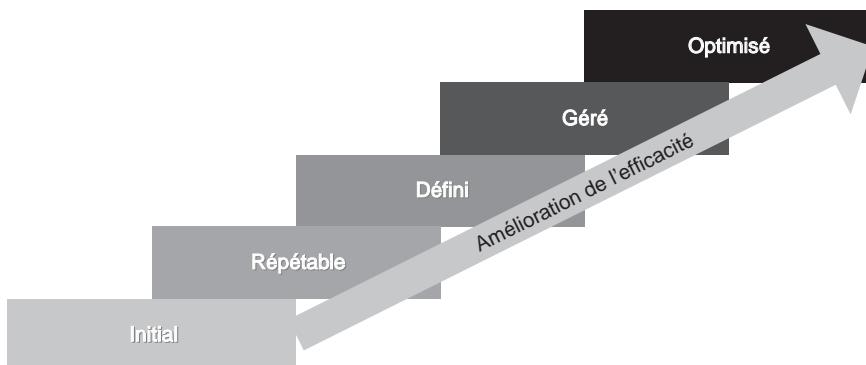


Figure 15-1 : Le modèle de maturité de l'organisation informatique

Ce schéma illustre bien les différentes étapes qu’un processus doit franchir avant de parvenir à l’optimum. Pour chaque processus de la direction informatique, il sera donc nécessaire d’évaluer sa situation actuelle et d’envisager l’effort à produire pour le faire évoluer vers le haut, sachant qu’aucun effort n’est nécessaire pour qu’un processus redescende vers le bas !

Niveau 1 : initial (parfois nommé « chaotique »)

Le premier niveau de maturité correspond à celui de l’initiation du processus. Bien que reconnu, celui-ci est inexistant ou non géré et ne dispose pas de ressources pour cette gestion.

Niveau 2 : répétable

Dans ce second niveau, l’importance du processus est reconnue et un minimum de moyens a été alloué pour sa gestion. Généralement, les activités liées à ce processus sont non coordonnées et irrégulières mais permettent d’obtenir le résultat escompté.

Niveau 3 : défini

Le troisième niveau est celui où le processus a été reconnu et est documenté. Cependant, il n’y a pas encore d’accord formel sur son rôle dans la

mise en œuvre de l'ensemble des processus. Celui-ci possède un propriétaire, des objectifs et des cibles avec des ressources allouées et il est concentré sur l'efficacité aussi bien que sur les résultats du processus. Les rapports et les résultats sont disponibles pour consultation.

Niveau 4 : géré

Le quatrième niveau décrit un processus totalement reconnu et accepté par l'ensemble de la direction informatique. C'est un processus orienté vers le service et disposant d'objectifs basés sur les besoins de l'entreprise. Il est entièrement défini, géré et il est devenu proactif. Le processus et ses interfaces sont documentés, ainsi que ses dépendances avec d'autres processus.

Niveau 5 : optimisé

Le cinquième et dernier niveau correspond à un processus optimum, dont l'intégration à l'entreprise est totale et qui met en place des objectifs stratégiques alignés sur ceux de l'entreprise. Un sous-processus d'amélioration continue est établi afin de maintenir le processus principal à l'optimum.

Le choix des processus

L'implantation de la gestion des changements ou de la gestion des niveaux de service n'a réellement aucun sens dans une direction informatique fonctionnant en mode « pompier ». Dans ce cas, le plus prudent serait de se concentrer sur un processus comme la gestion des incidents et la mise en place d'un centre d'appel ou d'un centre de services. Par la suite, la mise en place d'une gestion des problèmes, même embryonnaire, permettra de sortir du mode pompier avant d'aller plus loin.

Concernant les organisations qui ont déjà des processus opérationnels, qu'ils soient formels ou informels, elles utiliseront également les processus d'ITIL pour améliorer leurs résultats. La mise en place de la gestion des incidents aide l'équipe d'assistance à réduire le temps de résolution et de réponse, alors que la gestion des problèmes réduit le nombre d'incidents récurrents. La gestion des changements apporte elle aussi une amélioration dans le fonctionnement de la direction informatique, en diminuant la durée des changements. Chaque amélioration de ces processus aura besoin d'une base de données de configuration fiable, gérée par un processus de gestion des configurations. En tout état de cause, l'apport des processus de soutien des services est le plus intéressant pour les sociétés qui disposent déjà d'un système d'information en place.

En revanche, dans le cas où l'organisation informatique est en cours d'implantation sur une nouvelle société, il est utile de commencer par les processus de fourniture des services. De cette façon, les engagements de fourniture des services informatiques peuvent clairement être définis en

termes de fonctionnalité, de qualité, de coût et de disponibilité. Ensuite, les niveaux de service sont rédigés dans un document formel répondant aux exigences de l’entreprise. Cependant, il sera indispensable d’implanter rapidement les processus de gestion de la disponibilité et de la capacité, ainsi que le centre d’appel, la gestion des incidents et la gestion du changement.

Le cycle d’implantation ITIL

Comme on a pu le voir dans la première partie du livre, ITIL propose une mise en œuvre des processus dans un projet cyclique, désormais classique. Les phases du cycle, ici au nombre de six, correspondent toutes à une étape clé de la prise de conscience de l’entreprise, puis de l’implantation d’ITIL comme référentiel de gestion des services informatiques. Comme le montre la figure 15-2, chacune de ces étapes répond à une question fondamentale, et fixe ainsi le cahier des charges de l’implantation. Comme ce projet est continuellement remis en route par la boucle du cycle, les objectifs spécifiques de l’implantation d’ITIL sont alignés continuellement sur les objectifs plus globaux de l’entreprise.

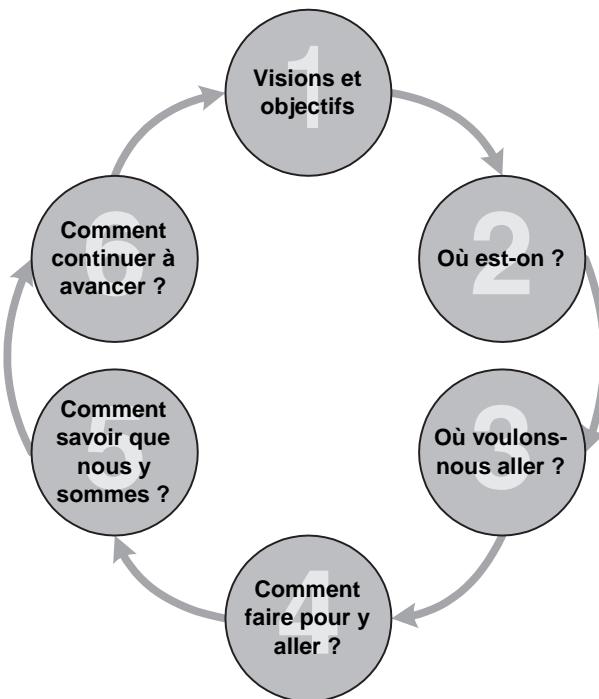


Figure 15-2 : Cycle de planification de l’implantation des processus ITIL

Quel est le but à atteindre ?

Cette étape est celle de la définition des objectifs. Répondre à cette question permet de fixer la vision et les objectifs métier idéaux aux yeux de l'entreprise, et surtout de déterminer en quoi le système d'information aidera l'entreprise à atteindre ces objectifs. Pour éviter de partir de zéro lors de cette étape, une solution consisterait à employer les processus ITIL comme modèle, et de proposer des objectifs en fonction de ce qui semble apporter le plus à l'entreprise.

Où se trouve-t-on actuellement ?

La seconde étape s'interroge sur le niveau de maturité atteint par l'entreprise en général, et la direction informatique en particulier.

Il s'agit également de comprendre en quoi l'organisation actuelle diffère de celle proposée par ITIL, et si un manque de compétence ou de ressource entraîne des difficultés. L'évaluation de ce niveau aide à quantifier l'effort à fournir pour remplir les objectifs énoncés précédemment.

C'est une étape complexe portant sur des sujets très différents comme la vision à long terme, les processus de gestion, la culture de service, les apports de la technologie, et bien sûr la dimension humaine comme la formation ou la taille de l'effectif. C'est réellement l'étape de la prise de conscience qui demande l'utilisation de techniques d'entretiens, de bancs de test (*benchmarking*), et autres audits.

Pour cette raison, une attention particulière sera apportée à la communication sur les bénéfices attendus par le service informatique et l'entreprise, par le biais de séminaires, réunions, circulaires ou journal d'entreprise.

Où voulons-nous aller ?

Cette troisième étape est l'occasion de définir plus précisément les objectifs, le rôle et les caractéristiques de l'implantation d'ITIL au sein de la direction informatique, afin qu'elle soutienne plus efficacement l'activité de l'entreprise. C'est le moment où l'on définit les objectifs de performance et les métriques du projet qui valideront les progrès accomplis.

Les objectifs annoncés permettent de concevoir chaque processus, y compris l'assistance pour celui-ci, c'est-à-dire d'élaborer son mode de fonctionnement, sa structure, ses relations par rapport à l'organisation actuelle et les besoins en formation, puis d'identifier les bénéfices attendus, les coûts et les problèmes possibles.

C'est également la phase d'évaluation des moyens à employer pour parvenir aux résultats envisagés dans les étapes précédentes. Cette étape analyse les besoins de façon détaillée, quantifie les ressources et la charge de travail, afin de produire le plan du projet d'implantation des processus, dans lequel est expliqué comment les changements vont être réalisés, où commencer et quel élément essentiel doit prendre en compte le projet.

Comment atteindre notre but ?

La quatrième étape correspond à la mise en œuvre des processus et à la mesure de leur efficacité, c'est-à-dire au moment de développer ou d'améliorer les processus, puis d'adapter ou d'installer les outils informatiques destinés à les soutenir.

Ensuite, arrivent la rédaction de documents de référence et la formation du personnel impliqué dans la mise en place des processus.

Enfin, une phase de tests, puis de validation doivent mettre à l'épreuve le bon fonctionnement des processus, et vérifier qu'ils répondent bien aux objectifs fixés par l'entreprise.

Comment savoir si le but fixé a été atteint ?

La cinquième étape consiste à identifier et à mettre en place un ensemble de métriques pour évaluer le progrès et la performance du processus.

Ceux-ci doivent être régulièrement mesurés, contrôlés et passés en revue à chaque étape du projet afin d'en assurer le succès. Il est important d'inclure des mesures qui touchent directement aux avantages procurés à l'entreprise et des améliorations de la qualité de service. Ces revues et contrôles post-implantation sont l'occasion de vérifier que les services fournissent ce que les utilisateurs attendent, en comparant les niveaux d'activité réels avec les prévisions. Cette évaluation peut également se faire lors d'une enquête de satisfaction du personnel à l'égard du service. Tout ceci permet de déterminer les bénéfices obtenus par la nouvelle organisation.

Comment continuer le cycle ?

La sixième étape, qui ne doit pas être la dernière, est la plus difficile à mettre en place, puisqu'il s'agit de l'étape de bouclage.

En effet, dans la perspective d'amélioration continue, il est nécessaire de revenir à la première étape afin de revoir ce qui a été réalisé, les difficultés rencontrées, et de réfléchir à la façon de l'améliorer. Le bouclage correspond donc à la surveillance, la révision et l'ajustement de l'efficacité du service en fonction des mesures obtenues précédemment. C'est le moment où l'on peut réviser et amender les différentes parties du projet comme les étapes et le mode de gestion du projet lui-même, mais également les processus, s'il s'avère que le mode d'implantation ou son contenu n'est pas aligné sur les objectifs.

Il faut en effet toujours se rappeler au cours de toutes les activités du processus, que le message clé est de maintenir une vision métier, où la priorité, l'impact et l'alignement sur le métier doivent être soulignés et re-soulignés, pour s'assurer que toutes les améliorations comprennent de vrais avantages pour l'entreprise.

Comment débuter un projet ITIL ?

La mise en place d'un projet ITIL s'accompagne toujours d'un grand nombre de questions auxquelles il est nécessaire de répondre. Parmi celles-ci, on trouve notamment des questions sur les besoins en formation, la communication, la structure de projet à mettre en place, les processus à lancer en priorité et, bien sûr, comment financer le projet lui-même...

Quelle structure de projet mettre en place ?

Cette question est certainement celle qui revient le plus souvent. En réalité, elle concerne la nécessité de mettre en place un projet spécifique lors de l'implantation d'ITIL ou de décider d'implanter les processus au fil de l'eau en fonction de la disponibilité des personnes...

Si la seconde solution est attrayante d'un point de vue purement financier, il s'avère que c'est également celle qui a le moins de chances d'aboutir. En conséquence, c'est certainement celle qui représente le coût le plus important.

La conclusion de ce premier point est évidemment qu'une structure projet formelle est la meilleure solution lors de la mise en place d'ITIL.

D'un point de vue purement opérationnel, il est vrai que l'organisation par les processus est souvent mal perçue dans nos sociétés, habituées à réagir à un système hiérarchique vertical (haut/bas), alors qu'ITIL fait plus intervenir des relations transverses horizontales. Il est donc particulièrement important d'expliquer largement en amont les concepts d'ITIL avant de prendre les décisions et de communiquer sur la répartition des responsabilités.

Enfin, en fonction du type et de la taille de l'entreprise, la structure sera évidemment adaptée dans le but de répondre aux impératifs de l'organisation.

Les grandes entreprises mettront en place avec profit une approche en mode projet engendrant une documentation largement partagée. L'apport des outils informatiques est souvent indispensable dans ce cadre. Concernant la répartition des rôles, chaque processus peut être distribué sur un propriétaire spécifique en fonction des rôles opérationnels.

Le pilotage du projet sera basé sur plusieurs indicateurs variés et s'appuiera sur les objectifs des processus pour mesurer le succès. Enfin, la communication entre la DSI et les clients et utilisateurs doit rester une priorité laissant recadrer le projet rapidement.

Dans les entreprises de taille plus réduite, l'approche par projet doit rester la règle, mais dans ce cas, elle peut être allégée et être éventuellement moins formaliste. Ici, le côté pragmatique doit l'emporter, tant il est vrai qu'un projet trop ambitieux peut décourager les plus résistants et mener le projet à l'abandon pur et simple. L'exemple de la documentation est le cas typique où l'on va plutôt avoir tendance à favoriser le minimum requis

sans viser l’exhaustivité. L’important dans ce cas est de s’assurer que l’on met la priorité sur les documentations les plus souvent utilisées.

La technologie doit rester ici en soutien et ne pas devenir le point central sous peine de devenir ce contre quoi ITIL se bat.

Dans le cas d’une entreprise moyenne, les différents processus pourront être distribués à des propriétaires distincts ou cumulant des responsabilités multiples.

Concernant le pilotage, ce type de situation fera plus usage d’un nombre d’indicateurs limités qui aideront surtout à valider la gestion des processus conformément au « bon sens » plus orienté sur l’historique de l’entreprise que sur les recommandations ITIL pures.

En revanche, la communication entre la DSI et les clients et utilisateurs est toujours le point sur lequel il faut appuyer.

Sur quels éléments se fonder pour lancer le projet ?

Les éléments à prendre en compte lors du lancement du projet sont essentiellement la formation (identifier le besoin en formation au sein des équipes, sensibiliser aux méthodes et référentiels). Il est également important de mettre en œuvre un plan de communication et de marketing du projet afin de s’assurer le soutien de sponsors forts en externe (direction générale) mais également en interne avec des chefs de projet et des responsables de services formés et qui s’engagent dans la promotion du projet. Le but recherché par ces deux étapes est d’éviter, autant que faire se peut, la résistance au changement qui ne manquera pas de se manifester. Il faut d’ailleurs signaler que cette résistance se retrouve dans les équipes mais également chez les responsables (toujours le problème de perception entre hiérarchie et processus).

En parallèle à cette formation, une étape indispensable d’audit doit se dérouler afin d’évaluer le niveau de maturité de la DSI et d’identifier des manques. Cet audit se fera en interne ou en externe, mais il faut garder à l’esprit que « nul n’est prophète en son pays ».

Une démarche préalable par une certification ISO 9000 apportera éventuellement les informations nécessaires et suffisantes. Néanmoins, il n’est pas indispensable d’en passer par là pour obtenir le même niveau de connaissance sur la maturité.

Une fois la structure mise en place, comment démarrer ?

Selon le contexte de l’organisation (taille, activité, structure), il faut considérer l’urgence et le besoin de mise en place des processus en fonction de la maturité. Il est ensuite indispensable d’envisager l’impact des projets sur les opérations du département TI afin de valider que le projet ITIL ne

risque pas de déstabiliser la production informatique et donc l'activité de l'entreprise.

Pour cela, il faut évaluer la charge de travail actuelle des équipes et le niveau de mobilisation.

En règle générale, il est recommandé de ne lancer que deux à trois processus en parallèle et d'éviter la surcharge des équipes opérationnelles sur le projet. Il est envisageable de recourir à de l'assistance externe en opérationnel ou en management (avec éventuellement de l'assistance maîtrise d'ouvrage ou du *coaching*).

La question se pose ensuite sur l'externalisation ou au contraire, l'internalisation de certains services. C'est en général la question que l'on se pose tout de suite pour le centre d'assistance (*Help Desk*). Attention à envisager les pertes potentielles en savoir-faire et en connaissances (KM).

Enfin, il est bon de ne pas oublier de mettre en place des relations fortes avec d'autres services tels que les moyens généraux qui seront largement mis à contribution pour les installations téléphoniques, les locaux ou les équipements divers (climatisation, onduleurs, sécurité...), qui seront souvent pris en compte dans les contrats de service sans pour autant être de la responsabilité de la DSI.

Quels processus lancer au début ?

La réponse à cette question ne peut être apportée qu'en connaissant l'entreprise concernée. En tout état de cause, on ne peut se prononcer qu'après un audit de l'existant de la production informatique.

En conséquence, cette question engendre plusieurs réponses. En fonction du niveau de maturité de l'entreprise, il est possible de débuter par des processus plus opérationnels ou plus tactiques.

Cependant, il faut garder à l'esprit que lancer un projet ITIL pour ITIL n'a aucun sens ; les projets qui réussissent sont ceux qui sont dictés par un besoin métier, c'est-à-dire exprimés clairement par les utilisateurs ou le client.

Le plus efficace est donc de commencer par les processus qui soutiennent le plus les activités informatiques, qui elles-mêmes soutiennent l'activité de l'entreprise. Une autre solution peut consister à débuter par les processus qui sont les plus visibles auprès des clients. Le principal reste de n'entreprendre que des sous-projets limités, au moins au début, en commençant par les processus produisant des résultats visibles rapidement (*Quick Wins*).

En règle générale, les processus opérationnels sont ceux qui apportent le plus au démarrage. La mise en place d'un bureau de service ou d'un simple « *Help Desk* » centralisé apporte une plus-value visible rapidement. Cette fonction doit s'accompagner le plus rapidement possible de la gestion des incidents et de la gestion des problèmes. Par la suite, les autres processus

à mettre en place sont la gestion des changements et celle des mises en production.

Enfin, la gestion des configurations, qui est un peu à part, doit débuter dans les premiers processus, mais sans viser l’exhaustivité. En effet, il s’agit ici typiquement du projet tunnel qui risque de durer indéfiniment. C’est donc un processus à initier très rapidement et qui doit régulièrement être réévalué, d’où l’importance de disposer d’un outil informatique adaptable simplement sous peine de devoir régulièrement refaire sa base de données des configurations (CMDB).

En revanche, démarrer par le processus de gestion des niveaux de service afin de générer les SLA peut être politiquement intéressant mais reste très risqué compte tenu du fait qu’aucun chiffre n’est là pour appuyer ce contrat de services. Un contrat minimum sans engagements formel est envisageable, mais il doit rapidement être étayé par les processus tactiques complémentaires (disponibilité, capacité, continuité de service, finances).

Comment faire accepter le projet ?

Faire accepter le projet ITIL revient souvent à convaincre les personnes qui vont le mettre en œuvre d’une part, mais également les personnes qui vont le financer. Nous détaillerons ce dernier point plus loin.

Le credo d’ITIL est d’adapter les services informatiques aux besoins exprimés par le client. Cette simple proposition est déjà un projet en soi. En effet, le préalable à cela consiste à faire accepter à de nombreux informaticiens que les métiers de la DSI évoluent. Avec l’évolution des technologies des dernières années, on a vu également une profonde modification des métiers.

De la « simple » fourniture d’une technologie, nous nous dirigeons désormais vers la fourniture d’un service. Si les débuts de l’informatique correspondaient effectivement à la fourniture d’une ressource de calcul centralisée (demande de calcul, *batch*, impression des résultats...), les besoins de l’utilisateur ont migré vers le poste de travail. Cette distribution de la ressource de calcul fait que le métier se transforme en profondeur, pour se rapprocher toujours plus du client.

Ce changement de mentalité au sein des populations techniques est souvent difficile et dépend pour beaucoup de la maturité de l’entreprise et des membres qui la composent.

Dans l’absolu, il est indispensable de faire comprendre aux informaticiens l’importance du métier en regard de l’aspect technique.

Un excellent moyen d’y parvenir est de faire connaître le métier de l’entreprise aux techniciens informatiques. Dans ce sens, le parcours initiatique, durant lequel le salarié doit, pendant une période brève, occuper un poste différent du sien dans l’entreprise, peut permettre de mieux comprendre le

travail du collègue et donc de communiquer plus facilement avec lui, et parfois de mieux appréhender le métier de l'entreprise.

Quelle durée consacrer à la formation ou à la sensibilisation ?

Pour répondre à cette question, il convient surtout de s'interroger sur la maturité de l'entreprise à la gestion des services informatiques, c'est-à-dire sur l'ampleur des compétences à acquérir.

Il existe plusieurs techniques de formation et plusieurs publics potentiels pour ces formations.

La première technique, la plus large, est celle du séminaire de présentation. Cette étape se déroule généralement sur une durée de deux jours maximum pendant lesquels un grand nombre de personnes sont sensibilisées. Un intervenant extérieur ou parfois de la société présente devant le groupe les grands concepts d'ITIL. Le risque de cette technique reste que les participants peuvent ne pas se sentir réellement impliqués. Le public visé est large, et couvre l'ensemble du personnel informatique, personnel d'encaissement et non-cadre. En tout état de cause, ce type de session n'est pas nécessairement limité aux informaticiens.

La seconde technique, qui est de loin la plus classique, est celle de la formation traditionnelle en groupes plus réduits. Elle est plus destinée aux personnes qui mettront en œuvre directement les processus ITIL et en particulier les responsables de services et chefs de projet. Ce type de session se déroule en général sur une période de trois à cinq jours et dépend essentiellement du niveau de compétence recherché.

Une autre technique envisageable consiste à mettre en place un système de *coaching* lors du projet. Celui-ci peut-être externe sous forme de conseil plus orienté vers les décideurs, mais également sous forme d'un *coaching* de projet ou plus opérationnel. La durée envisageable sur ce type de prestation est très variable et peut aller de quelques jours à plusieurs mois.

Comment justifier les investissements budgétaires ?

La principale justification à la mise en place d'ITIL est la maîtrise, voire la réduction des coûts liés à la production informatique. Il est dommage de n'envisager ITIL que par ce biais, mais c'est en général comme cela que sont justifiés ces projets. Les résultats sont cependant souvent là pour confirmer le bien-fondé de cette vision. En effet, les gains de productivité ou même l'amélioration de la qualité des services se traduit rapidement par des économies financières. En conséquence, ce point reste le meilleur candidat à la justification d'ITIL. Le second point qui peut être soulevé est très lié à l'aspect financier et consiste à envisager d'externaliser certains services en vue d'économies ultérieures. Attention, cette étape ne peut être

envisagée sans industrialiser auparavant le service en question dans le but de connaître le processus, ce qui explique les coûts.

Comme signalé précédemment, le Help Desk est souvent le premier service à être externalisé. Là encore, il convient de valider que l’on maîtrise la fonction. Dans le cas contraire, on risque de ne pas connaître réellement les processus mis en œuvre, et donc de ne pas savoir évaluer les coûts afférents. Dans ce cas, comment peut-on être sûr que l’on paye le juste prix pour le service rendu, et surtout comment évaluer que le service rendu est bien conforme à la qualité demandée ?

Il faut également comprendre que le Help Desk est un service difficile et ingrat (problème de *turn-over*, usure et fatigue, plage horaire importante, qualité des intervenants), qui représente néanmoins l’interface principale entre la DSI et ses utilisateurs. En conséquence, la qualité de réponse du Help Desk va conditionner la perception que l’utilisateur a de la DSI...

En tout état de cause, le SLA implique un engagement devant les clients permettant de déterminer le processus prioritaire. Si un engagement fort est pris sur le Help Desk, alors il ne faut pas l’externaliser.

En conclusion, on peut dire que pour réussir, il est indispensable de former les équipes, de formaliser les besoins, d’exprimer les besoins lors de réunions ou d’ateliers de travail entre la DSI et les directions métier puis d’identifier les niveaux de maturité des processus par un éventuel audit.

Les ressources du projet

Personnel

Beaucoup d’entreprises ont d’ores et déjà implanté un certain nombre d’activités et même parfois certains des processus exposés dans ITIL. Il existe donc un personnel compétent en interne pour mener à bien l’installation et l’exploitation de ces activités. La question que l’on peut se poser concerne le besoin de disposer de personnel supplémentaire lors de l’implantation de ces nouveaux processus. Peut-on redistribuer les tâches existantes et les rôles entre les membres de l’équipe, afin de débloquer du temps libre destiné à prendre en charge l’étude et l’implantation des processus ?

Comme on le constate sur la figure 15-3, une même personne peut assumer plus d’un rôle dans ITIL. Dans ce schéma, on voit se dessiner des « compatibilités » verticales et horizontales réunissant les rôles des responsables des différents processus. Les liens épais indiquent une synergie étroite entre les rôles, alors qu’une absence de lien indique qu’il n’y a pas de lien particulier, mais que les deux rôles ne sont pas incompatibles. En revanche, un lien en pointillés, indique une interaction fortement déconseillée.

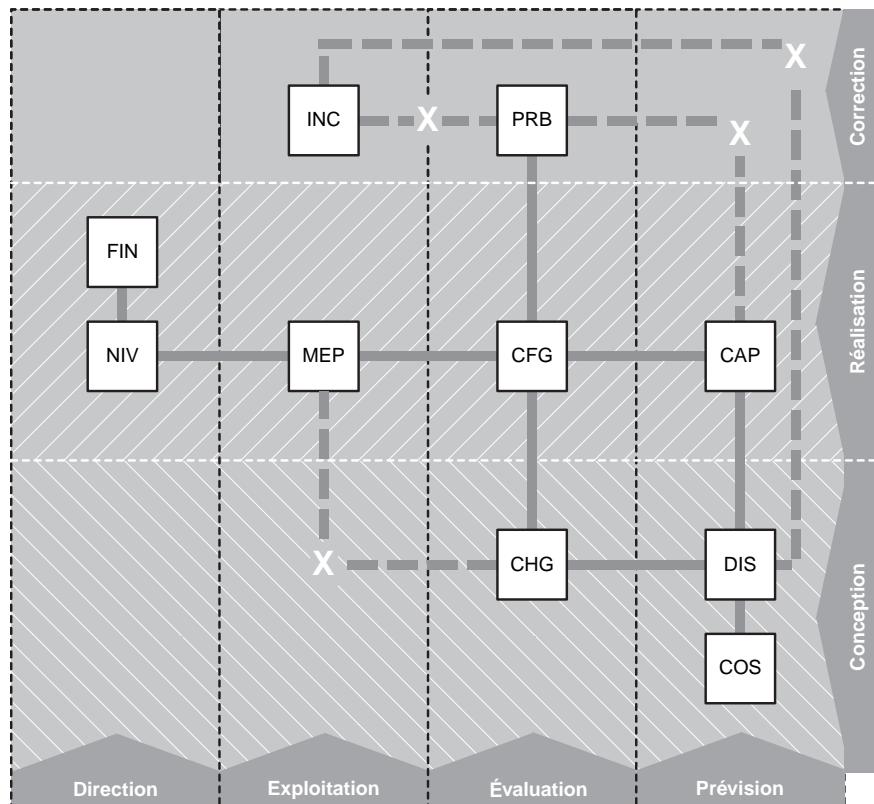


Figure 15-3 : Matrice de compatibilité des rôles ITIL

En horizontal, on trouve par exemple le type « réalisation » qui regroupe finance, niveaux de service, mise en production, configuration et capacité. En vertical, on identifie rapidement le type « prévision », qui concerne la gestion de la capacité, de la disponibilité et de la continuité de service. Cependant, certains rôles ne peuvent être cumulés. Comme on le voit dans le type « correction », il n'est vraiment pas recommandé que le gestionnaire du centre d'appel et le responsable de la gestion des incidents prennent également la responsabilité de la gestion de problème, en raison d'un conflit d'intérêt.

En résumé, on peut dire que ce graphique aide à déterminer les rôles qui peuvent être cumulés par une personne, et donc le nombre de responsables nécessaires dans la mise en place des processus ITIL (exemple : quatre responsables de type direction, exploitation, évaluation et prévision peuvent se partager les différents rôles).

Temps

La durée d’implantation des processus ITIL dépend de plusieurs paramètres dont les objectifs de l’entreprise, la maturité de l’organisation informatique, les ressources engagées, etc. Globalement, il ne faut pas espérer planter ITIL en moins de trois ans. Le tableau 15-1 reprend les délais individuels de chaque processus en fonction de la taille de l’entreprise. Ces valeurs sont évidemment indicatives, mais constituent une base de travail raisonnable.

Tableau 15-1 : Estimation de la durée d’implantation des processus ITIL

Processus ITIL	Durée de mise en œuvre	
	Informatique PME	Informatique grande entreprise
Configuration	3 à 4 mois	4 à 12 mois
Centre d’appel incident	3 à 6 mois	6 à 24 mois
Problèmes	1 à 3 mois	3 à 4 mois
Changements	1 à 3 mois	3 à 5 mois
Mise en production	1 mois	1 à 2 mois
Niveaux de service	2 à 4 mois	4 à 6 mois
Finances	4 à 6 mois	6 à 9 mois

Logiciel

De nombreux éditeurs proposent désormais des suites logicielles de gestion des processus ITIL. Certaines couvrent la totalité des processus ou une grande partie alors que d’autres préfèrent se concentrer sur un processus très précis. En général, les premiers outils proposés sont la gestion du centre d’appel et du centre de services, et la gestion des incidents et des problèmes, c’est-à-dire les premiers éléments du soutien des services.

On trouve ensuite très rapidement la gestion des configurations et parfois des solutions de gestion budgétaire et comptable de l’informatique très complètes, ou plus simplement des outils de gestion de parc et de gestion d’actifs, qui sont les briques essentielles de la gestion des configurations et de la gestion financière.

Matériel

Dans l’estimation des ressources à mettre en œuvre, il est important de considérer également le matériel supplémentaire à acquérir en vue de l’installation des applications de gestion des processus, ou destiné à délivrer des informations à ces applications. Parmi ces matériels, on trouve notamment

les serveurs dédiés en vue de l'hébergement des applications, les bases de données de configuration (CMDB) et de la gestion du centre de services. On trouve également les outils d'analyse des pannes, d'audit des configurations et autres sondes de mesure.

Formation

Points importants à ne pas négliger, la formation et éventuellement la certification de personnel aux processus ITIL semblent particulièrement importants dans le cadre d'une implantation ITIL. Tant du point de vue de la compréhension des concepts principaux que de l'acquisition d'un vocabulaire commun, la formation donne à tous les acteurs un niveau de connaissance minimal pour mener à bien ce projet d'ampleur pour l'entreprise.

Concernant les personnes à prendre en compte, il semble indispensable de faire suivre les formations aux différents responsables de la direction informatique, ainsi qu'aux intervenants principaux du centre de services.

Certaines formations sont plus adaptées à un rôle que d'autres et le vaste panel des sociétés de formation donne le choix de la session en fonction des objectifs poursuivis.

Les facteurs de succès

Avoir une vision claire

La compréhension d'ITIL est une chose. Identifier en quoi il va soutenir l'activité de l'entreprise et participer à la création de valeur en est une autre. Le but premier d'ITIL est de substituer une vision plus orientée métier à la trop classique vision technique des directions informatiques.

ITIL est un moyen, pas un but !

Malheureusement, on a vu des directions informatiques ou des fournisseurs de services informatiques se servir d'ITIL comme d'un paravent permettant de se protéger des clients et des utilisateurs au lieu d'utiliser ses principes pour résoudre les problèmes rencontrés avec ces derniers. ITIL doit donc servir cet objectif et non devenir lui-même l'objectif.

Préparer l'entreprise

Implanter ITIL suppose un projet long et parfois difficile. Le chemin est long et les résistances au changement sont rarement inexistantes.

Diffuser le message

L'entreprise doit se préparer à une modification en profondeur de ses méthodes de travail. Pour y parvenir, l'ensemble du personnel, et en particulier

les dirigeants de l’entreprise et les responsables des activités métier (les clients), doivent être sensibilisés aux enjeux et aux grands concepts d’ITIL.

Impliquer le management

Le manque d’implication des responsables du projet ou de la direction générale est rapidement perçu par les différents intervenants, avec des conséquences néfastes sur la motivation de l’équipe, ou l’apparition d’une résistance au changement. La solution passe par l’engagement sans faille du management qui doit tenir un rôle actif dans la conception et l’évangélisation de cette nouvelle culture de service.

Identifier les promoteurs

En plus de l’équipe de management, la mise en place sera grandement facilitée par l’adhésion des promoteurs du projet qui aident à le construire tout en gérant les difficultés, mais qui relaient également en permanence la vision, et maintiennent dans le temps la dynamique d’évolution vers une « culture de service ». Ces personnes qui ne sont pas issues de la direction informatique doivent être identifiées au sein de la direction de l’entreprise ou parmi les responsables des différentes directions métier; et doivent disposer de suffisamment d’influence à défaut d’autorité pour agir ou conseiller.

Identifier les propriétaires des processus

Un processus ITIL recouvre souvent plusieurs domaines alors que l’organisation classique en silos de compétences ou d’activités peut entraîner des « perturbations » hiérarchiques. Tout le monde doit comprendre qu’ITIL fonctionne selon un schéma collaboratif. La solution à ce problème est d’identifier un propriétaire pour chaque processus ITIL, dont le rôle est de se focaliser sur la gestion de ces flux transversaux.

Former les intervenants

Un des grands apports d’ITIL est de proposer un vocabulaire commun à tous les acteurs de la gestion des services informatiques. La formation de ces acteurs aux termes employés et aux principes fondamentaux fera gagner un temps considérable dans la mise en place des processus et renforcera l’adhésion des acteurs. En revanche, les propriétaires et les gestionnaires de processus devront participer à des sessions plus approfondies.

Accompagner le changement

L’implantation d’un nouveau système ou d’une nouvelle procédure entraîne systématiquement une résistance de la part des personnes qui utilisent ou produisent l’élément modifié. Cette résistance au changement est naturelle et classique, mais ne doit pas être prise à la légère. Afin de traiter ce problème, les utilisateurs comme les membres de la direction informatique doivent comprendre les buts recherchés, identifier les avantages espérés,

et partager la vision de la nouvelle organisation, afin de percevoir le changement comme souhaitable et nécessaire. La présentation de ces changements demande une approche progressive et doit conduire à leur acceptation par les différents intervenants du projet.

Prévoir une démarche progressive

Les dix processus de la gestion des services d'ITIL représentent une charge très importante lors de leur mise en œuvre et vont parfois à l'encontre de la maturité de l'entreprise. Cela peut entraîner une certaine confusion et une mauvaise intégration de l'ensemble. La solution consiste à passer par des étapes progressives qui respectent les objectifs de l'entreprise et les futures évolutions de sa maturité. Cela laisse également envisager l'implantation des processus dans une optique de résultats à court terme qui favorise leur adoption.

Respecter les priorités

Le choix du nombre et de la méthode d'implantation des processus doit se faire en fonction des impératifs fixés par l'entreprise. L'accent sera mis sur ce qui permet de développer une culture de service le plus simplement possible. En fonction de la maturité de la direction informatique, débuter par les processus d'assistance tels que la gestion des incidents ou la maîtrise des changements, semble le plus approprié. À l'aide de projets simples et rapides, les premiers résultats permettront d'asseoir la progression vers une culture du service.

Envisager un projet d'envergure...

La réussite d'un projet ITIL impose de se donner les moyens humains, technologiques et financiers à long terme. La durée objective de l'implémentation des processus s'envisage sur une période allant généralement de trois à cinq ans.

... mais éviter les projets trop ambitieux

Vouloir mettre en œuvre tous les processus en même temps représente un projet très important, long et coûteux. Le risque encouru est celui de tous les projets « serpent de mer », c'est-à-dire une rotation de personnel et une perte de motivation des participants.

Rester pragmatique

En plus du nombre de processus à planter simultanément, il faut décider du niveau de définition que l'on désire obtenir pour chaque processus. Toutes choses égales par ailleurs, la solution la plus simple est la meilleure. Le pire ennemi lors de l'implantation d'ITIL reste la recherche de la perfection et les objectifs trop ambitieux. Dans ce cas, les risques de démotivation ou de

rejet sont fort élevés. Rester pragmatique et aligné sur les objectifs de l’entreprise semble être la politique la plus sûre dans ce domaine.

ITIL doit être adopté et adapté !

Ne pas oublier les processus tactiques

Très souvent, après avoir mis en œuvre des processus opérationnels comme la gestion des incidents, la gestion des configurations et la gestion des changements, certaines directions informatiques sont tentées par l’implantation immédiate de la gestion des niveaux de service, en oubliant que ces engagements ne peuvent se prendre qu’en toute connaissance de cause. Pour parvenir à garantir la disponibilité d’un service dans un document formel, la direction informatique gagnera beaucoup à planter auparavant des processus plus tactiques comme la gestion de la disponibilité, la gestion de la capacité ou la gestion financière.

Conclusion

Les changements continuels apportés aux organisations informatiques impliquent que la gestion des services orientée processus n’est pas une activité ponctuelle à planter une fois pour toutes en espérant que le projet s’arrête là. Ces changements peuvent d’ailleurs être perçus comme des opportunités visant à améliorer continuellement la qualité du service rendu, en veillant systématiquement à s’assurer que le processus réponde bien aux objectifs de l’entreprise, et que la qualité et les coûts soient optimisés et équilibrés. Une bonne gestion du changement, une communication efficace, un engagement fort de la direction et un choix raisonné d’implantation de processus, sont autant de facteurs qui faciliteront la mise en place d’ITIL.

Étude de cas

Illustrons par une étude de cas l'utilisation de l'ensemble des processus d'ITIL lors de l'audit, puis la mise en place d'un processus pour améliorer la qualité des services dans la direction informatique d'une PME.

Présentation

Le cas que nous allons traiter est fréquemment rencontré dans le tissu industriel de type PME lorsque l'entreprise se retrouve confrontée à sa propre croissance. Il s'agit ici d'une organisation familiale centrée sur le fondateur d'origine, ce qui entraîne une gestion de l'entreprise davantage liée aux relations inter-personnelles qu'à une organisation formelle. Comme souvent dans cette situation, la priorité est donnée à la réactivité des actions au sein de l'entreprise comme facteur de différenciation, plutôt qu'à la pérennisation de l'information. Si ce mode de fonctionnement peut répondre aux besoins d'une petite structure, il ne convient plus lorsque la croissance de l'entreprise atteint un seuil trop important de salariés. Pour gérer le flux d'informations, il est alors nécessaire de changer de modèle, sous peine de voir l'organisation s'effondrer sous son propre poids. À cet instant, il est vital pour l'entreprise d'entreprendre sa révolution culturelle.

Dans notre exemple, l'influence du fondateur de l'entreprise a historiquement imposé une perception de l'outil informatique comme un passage obligé, au coût injustifié et présentant parfois un risque important, plutôt que comme un puissant vecteur d'optimisation de l'efficacité de l'entreprise. De plus, et même si ce point est fondamental pour ce type d'entreprise, alors que les moyens financiers sont loin de faire défaut, le critère de choix prioritaire pour les décideurs reste le coût de la solution. Il est évident que cette situation ne favorise pas l'investissement en moyens humains et

matériels et encore moins en évolution des procédures et des mentalités. En revanche, la méconnaissance de l'outil et de ses possibilités est un facteur bien plus insidieux et souvent plus important. En effet, cette crainte de l'inconnu, cette sensation de tomber dans un guet-apens permanent incite les responsables de l'entreprise à considérer l'informatique comme une boîte noire dans laquelle il faut injecter de l'énergie « financière » pour en sortir un résultat. Le résultat est évidemment l'inverse de ce qui était attendu et conforte la direction de l'entreprise dans son sentiment : « L'informatique, ça coûte cher et ça ne marche jamais ! ».

L'entreprise

L'entreprise considérée dans cette étude est une PME d'environ 900 personnes, réparties sur trois sites en France. Elle a rejoint un groupe industriel européen depuis quelques années, s'ajoutant ainsi à un effectif de 1 400 personnes réparties sur quatre autres sites en Europe. Le but recherché étant de mutualiser certaines ressources et compétences entre les différents établissements, le groupe a décidé de centraliser certaines directions, dont la direction informatique, au sein du site principal français (voir figure 16-1), qui est le plus important du groupe. La production industrielle se réalise sur trois pays, chaque unité étant dédiée à une ligne de produits spécifique. Les stocks de produits finis sont gérés au plus près de la zone de commercialisation, mais chaque unité de production dispose

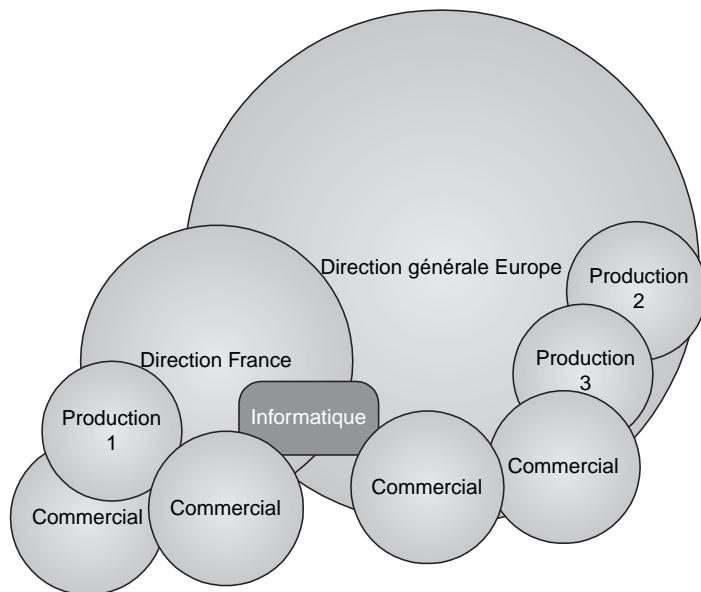


Figure 16-1 : Répartition des établissements du groupe

également de son stock pour gérer ses matières premières, et d'une zone d'attente avant expédition.

Alors que les sites européens sont davantage dédiés à la production et couvrent la commercialisation en Europe du Nord et Europe de l'Est, les sites français se partagent la commercialisation des produits sur l'Europe du Sud. Le site français le plus important est composé de deux implantations distantes de trois kilomètres qui composent l'établissement principal, cumulant des rôles de production et de commercialisation, et assumant l'ensemble des directions pour la France. Enfin, chaque site de commercialisation français couvre une zone correspondant à un tiers du territoire national. La commercialisation à l'export en Europe du Sud est réalisée par l'intermédiaire de revendeurs locaux avec lesquels l'entreprise entretient des liens forts.

Historique

L'historique de l'entreprise est jalonné de plusieurs événements charnières. Sa croissance continue sur une trentaine d'années l'a fait passer d'une PME familiale d'une cinquantaine de personnes à un groupe industriel moyen avec plus de 2 300 salariés, par des rachats successifs et des coopérations avec d'autres entreprises complémentaires, dont d'anciens sous-traitants et d'anciens revendeurs. Une croissance de ce type impose des actions et des délais entre les rachats afin de « digérer » l'ancienne structure. Malheureusement, les réorganisations indispensables à la création d'une nouvelle entité disposant d'une culture d'entreprise commune n'ont pas été menées lors des rachats successifs. Cette situation a donc entraîné certains manques et dysfonctionnements dans les méthodes de gestion et d'organisation des différentes directions. Plusieurs années après le départ en retraite du fondateur, l'entreprise, encore largement teintée par son historique familial, n'a pas encore atteint un stade véritablement industriel et les relations informelles passent souvent outre l'organigramme fonctionnel ou hiérarchique. Si cela permet parfois d'obtenir une forte réactivité, la direction a néanmoins perçu le risque d'un effondrement de la structure sous son propre poids. En effet, certains directeurs ont évoqué divers problèmes d'efficacité, des délais commencent à apparaître dans les lignes de production, certains produits présentent de plus en plus souvent des problèmes de qualité, et surtout, le contrôle de gestion vient de signaler des gaspillages importants entraînant une baisse notable de la rentabilité de l'entreprise.

Après un audit de la structure mené par un cabinet indépendant durant plusieurs mois, une vaste réorganisation de l'entreprise a été décidée.

L'organisation informatique de l'entreprise

Avec la centralisation, la direction informatique est passée de 21 à 33 personnes, essentiellement présentes sur le site principal français. Les sites

distsants disposent au mieux d'un à trois informaticiens sur place ou d'un correspondant informatique choisi parmi les utilisateurs.

À l'instar de l'entreprise, le personnel de la direction informatique est essentiellement issu du regroupement et des rachats successifs. Ces derniers ont tout d'abord apporté des systèmes d'information notoirement différents et parfois divergents. Du point de vue de l'infrastructure, l'ensemble présente désormais un état d'hétérogénéité important tant sur le matériel et les logiciels que sur les procédures. Au niveau du site central, on constate en effet l'utilisation de trois types de matériel très divergents tels qu'un petit ordinateur central (petit mainframe) en fin de vie, trois serveurs RS6000 sous AIX et un ensemble de serveurs PC fonctionnant sous Unix, Windows NT et Linux. Les postes clients sont parfois composés de différents types de terminaux passifs en mode texte et d'ordinateurs de bureau de type PC. Sur les sites distants, on dénombre trois types de matériels différents tels que l'utilisation de terminaux passifs reliés au site central par une ligne spécialisée, l'utilisation d'un serveur d'application local de type PC/Unix et enfin l'usage modéré de bureautique sur postes PC.

Pour les applications, l'usage d'un seul système de messagerie électronique a pu être imposé par la direction informatique aux utilisateurs. En revanche, plusieurs applications métier existent au sein du système d'information, chacune utilisant sa propre base de données. Il en résulte que l'administrateur des bases de données doit gérer deux SGBD (système de gestion de bases de données) différents (Oracle, SQL Server) sans compter les données présentes sur les postes de travail et utilisant un SGBD bureautique.

Concernant les membres du personnel, les âges, les niveaux de compétences, l'orientation vers le client et la motivation sont également très disparates.

Avant l'audit de l'entreprise, la direction informatique ne s'était pas réellement posé de question sur son organisation interne, tant elle était focalisée sur la résolution des nombreux problèmes techniques auxquels elle se trouvait en permanence confrontée. La multiplicité des systèmes et des logiciels imposait un combat épuisant pour maintenir l'ensemble en état de fonctionnement. Cette situation a ainsi fait perdurer une organisation assez peu efficace dans laquelle tous les services internes de la direction informatique dépendaient immédiatement du directeur. Comme on le voit sur la figure 16-2, cette organisation en « râteau » où tous les cadres du service sont en prise directe avec le directeur informatique, ne lui permettait pas de disposer de temps pour améliorer l'efficacité de son organisation afin de justifier du même coup ses budgets dispendieux.

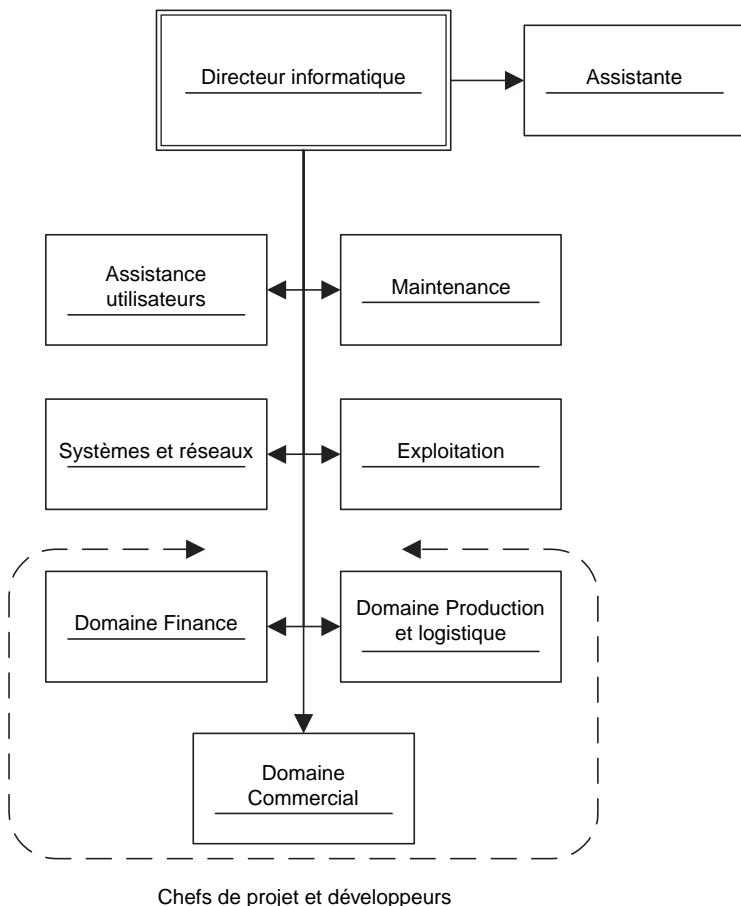


Figure 16-2 : Organigramme de la direction informatique

Situation actuelle

Les évolutions de l'entreprise et l'embauche de personnel extérieur à certains postes d'encadrement dans les directions métier ont apporté leur lot de nouveautés dans les idées et les méthodes de travail. Du point de vue informatique, l'arrivée de ces nouveaux utilisateurs a posé des problèmes en termes de capacité, mais plus généralement en termes d'assistance technique des services. En effet, les attentes de l'ensemble du personnel sont désormais liées à l'augmentation de l'utilisation de ces services par les nouveaux arrivants.

En particulier, un projet de grande ampleur a été « demandé » de manière insistant par la direction et concerne la mise en place d'un système intégré

de gestion de l'entreprise (ERP) global au sein du groupement d'intérêt économique (GIE). Même si ce système est une solution plus spécifique au métier de l'entreprise que ne le serait un ERP généraliste, il n'en reste pas moins que toutes les directions vont être touchées par cette nouvelle application, et surtout par les bouleversements organisationnels qui vont en découler.

Constat

Un cabinet d'audit a été mandaté pour évaluer l'organisation de l'entreprise puis proposer des solutions d'évolution. Après plusieurs semaines d'entretiens avec le personnel et d'analyse des documents, le constat fut sans appel. Il était indispensable de passer d'un modèle oral à un modèle plus formel, et certainement d'un modèle globalement artisanal à une organisation plus industrielle, et ce à tous les niveaux de l'entreprise. Ce besoin de documentation était d'autant plus important que de nombreux salariés et cadres approchant de la retraite risquaient d'emporter leurs connaissances avec eux.

L'audit a également mis en évidence que l'équipe interne, bien que disposant de compétences avérées, avait perdu une bonne partie de son crédit auprès des utilisateurs et, dans une moindre mesure, de la direction. Le sentiment général était que l'entreprise accordait plus sa confiance à des prestataires extérieurs qu'à l'équipe en place. Cette impression ressentie par les membres de la direction informatique participait évidemment à une lassitude et à un découragement palpables.

Le but du projet était donc de réorganiser globalement l'entreprise dans son organigramme et son mode de fonctionnement.

Du point de vue informatique, les recommandations de l'audit correspondaient essentiellement à une révolution culturelle et technologique. Elles imposaient de modifier le comportement des membres de l'équipe sur la perception du client et de ses besoins. Un effort considérable devait être apporté à la documentation des configurations et des procédures. Enfin, une vaste opération de rationalisation de l'infrastructure devait être engagée au plus vite. Pour mettre en œuvre ce vaste chantier, l'utilisation des meilleures pratiques du référentiel ITIL fut proposée.

Le projet

Nous ne nous intéressons ici qu'à la partie informatique de la réorganisation de l'entreprise, mais nous verrons que plusieurs sous-projets ont un impact direct sur certaines directions métier. Ce projet de plusieurs mois est essentiellement orienté sur la mise en place des processus d'amélioration de la qualité des services en s'appuyant sur la formation des membres de l'équipe, la réorganisation de l'organigramme et l'attribution de nouvelles fonctions.

Objectifs

Les objectifs de la direction informatique sont multiples :

- amélioration globale de la qualité de service ;
- rationalisation drastique de l'infrastructure technique ;
- réorganisation de l'assistance utilisateur en centre de services ;
- installation d'une application de gestion du centre de services ;
- adaptation des compétences de l'équipe aux besoins de l'entreprise ;
- facturation interne des services informatiques ;
- réduction des coûts liés à l'informatique à l'échéance de 3 ans.

Planification

Outre le projet de réorganisation de la direction informatique, la mise en place des processus ITIL est un projet à part entière qu'a bien intégré la direction générale et dans lequel sont placées des attentes fortes. Ce projet doit se dérouler sur trois années, découpées en grandes phases de quatre à huit mois.

Après la phase d'audit d'une durée de trois mois sur la fin de l'année, le début du projet de réorganisation fut placé au premier trimestre de l'année suivante, avec comme objectif de produire un bilan à l'été de la troisième année.

Comme on peut le voir sur le diagramme de Gantt de la figure 16-3, les cinq étapes se succèdent sur trois ans, entrecoupées de bilans intermédiaires qui constituent les jalons du projet. Il est important de placer ces périodes de bilan sur des échéances relativement proches avec des objectifs réalisables, afin d'éviter que le projet ne rentre dans un « effet tunnel » qui ne peut que décourager les participants et faire baisser la mobilisation. Chacune de ces étapes est l'occasion d'implanter un ensemble de processus ITIL, en partant des plus tactiques (assistance des services) pour aller vers les plus stratégiques (fourniture des services) :

- 1^{re} étape : structure d'assistance aux utilisateurs (*helpdesk*), gestion des incidents, gestion des problèmes ;
- 2^e étape : gestion des configurations, gestion des changements, gestion des mises en production ;
- 3^e étape : gestion de la capacité, gestion de la disponibilité, gestion de la continuité de service ;
- 4^e étape : gestion financière et gestion des niveaux de service ;
- 5^e étape : revue individuelle et amélioration des processus. Cette étape est l'occasion de faire le bilan de l'ensemble du projet, d'évaluer le retour sur investissement et de relancer la dynamique d'amélioration pour accroître l'efficacité des processus.

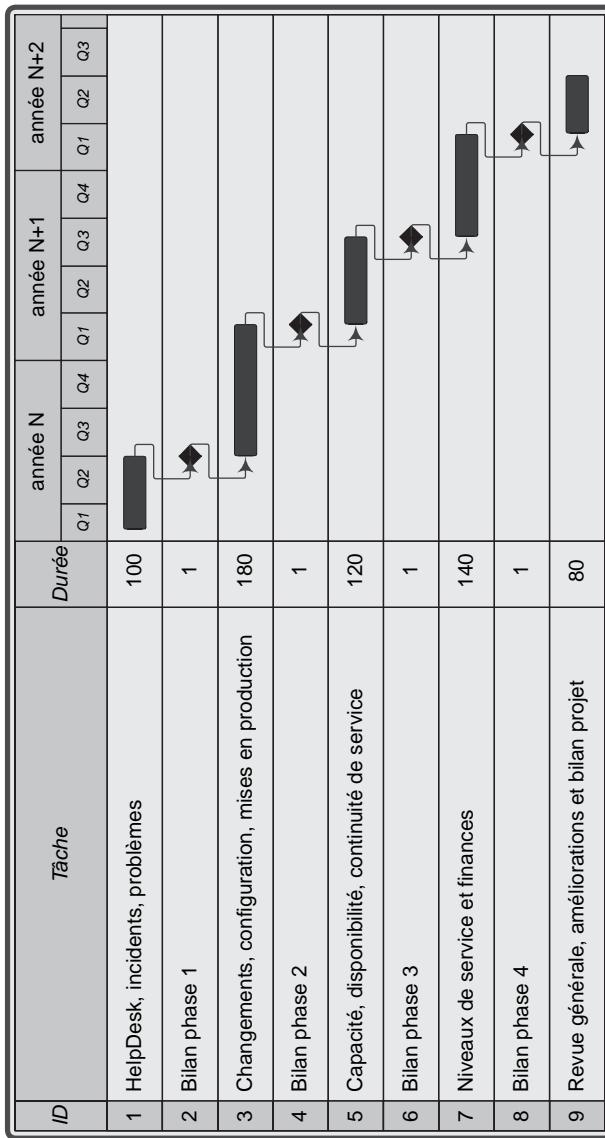


Figure 16-3 : Planification du projet sur trois ans

Les durées des étapes représentées sur le graphique ne correspondent pas à une charge continue des équipes, mais plus au délai utile à l'implantation de chaque processus incluant les périodes d'audit, de conception, de mise en place et d'évaluation.

Ressources

Les ressources utilisées durant le projet ont été de plusieurs types. En premier lieu, il faut évidemment signaler les ressources humaines. En effet, outre les ressources internes en personnel, l'entreprise a fait appel à une assistance extérieure par le biais de la présence ponctuelle d'un à trois consultants sur les différentes phases du projet.

L'organigramme des équipes informatiques ayant été bien modifié, plusieurs transferts de personnel entre les équipes ont été réalisés, en particulier entre l'équipe d'exploitation et l'équipe d'assistance aux utilisateurs.

Sur le plan logiciel, l'entreprise s'est équipée d'une solution intégrant une gestion de parc, de la base des configurations CMDB, ainsi que de plusieurs autres processus ITIL (gestion des configurations et des capacités, gestion financière, gestion du centre d'appel, des incidents et des problèmes, et gestion des changements et des mises en production).

De nombreuses formations ont été dispensées, non seulement aux membres de l'équipe informatique, mais également aux responsables d'autres services et aux principaux cadres de l'entreprise, essentiellement sous la forme de séminaires internes.

Ces formations portaient globalement sur des aspects tels que la rédaction de documentations et de procédures, mais également sur la gestion du stress, la réponse téléphonique, des notions de service et enfin l'assistance aux clients.

De plus, les responsables de l'équipe informatique ainsi que les différents responsables des directions métier ont suivi une formation ITIL pour les dirigeants. Ceux-ci ont ensuite présenté les concepts et le vocabulaire à l'ensemble de leurs équipes au cours de séminaires internes avec l'assistance d'un consultant externe.

Enfin, plusieurs formations techniques ont été suivies par les membres de l'équipe afin d'améliorer la maîtrise des technologies employées dans l'entreprise.

Réalisation

Changement d'organisation au sein de l'équipe informatique

La réorganisation de la direction informatique a débuté par des modifications importantes dans l'organigramme.

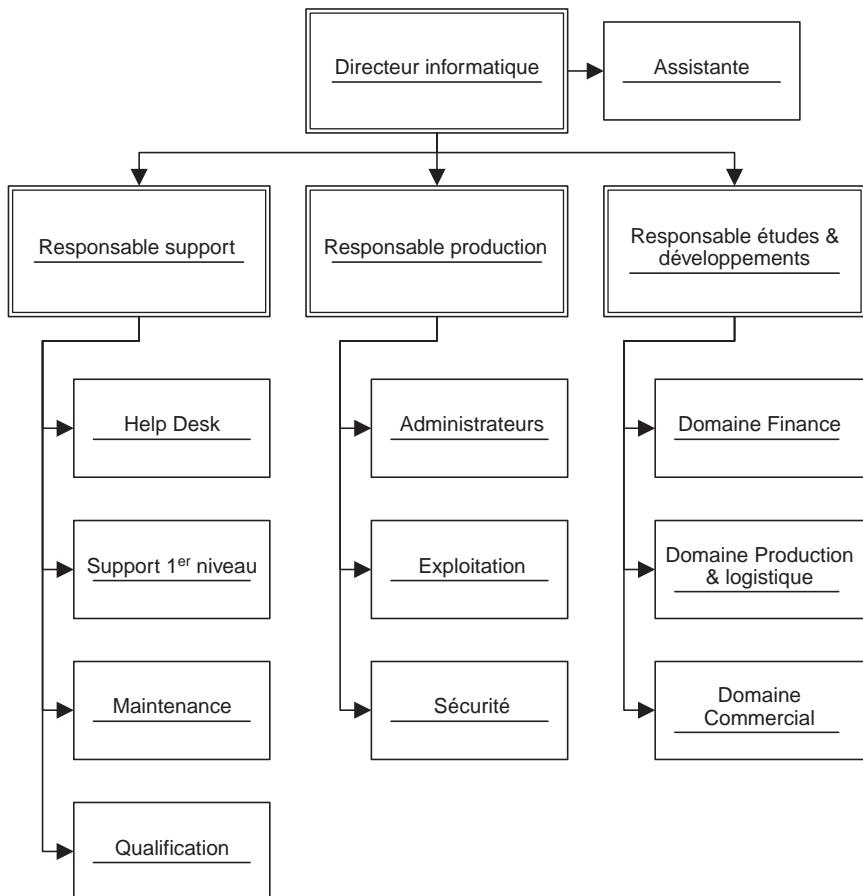


Figure 16-4 : Nouvelle organisation de la direction informatique

Comme on peut le voir sur la figure 16-4, la plus importante de ces modifications est la scission de la direction informatique en trois services distincts et la nomination ou l'embauche de trois personnes en tant que responsables de ces nouveaux services :

- Le service d'**assistance** est composé de quatre équipes : le centre d'appel, l'assistance de 1^{er} niveau assistée d'une équipe de maintenance sur site et enfin, la cellule de qualification des nouveaux produits et des changements divers.
- Le service de **production** est composé d'une équipe d'administrateurs qui prend également en charge le traitement des problèmes, ainsi que d'une équipe d'exploitation et d'une personne plus transversale qui prend en charge les questions de sécurité.

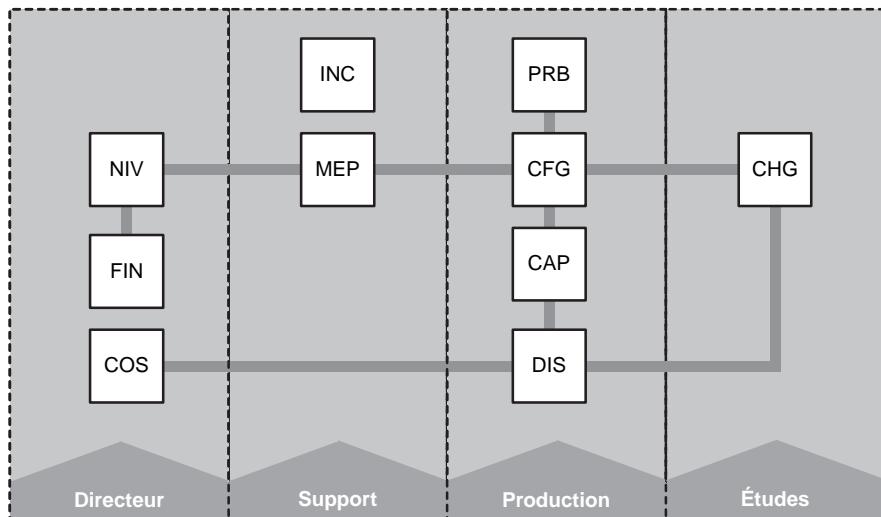


Figure 16-5 : Répartition des processus entre les responsables du service

- Le service **étude et développement** est composé de trois chefs de projet fonctionnels plus ou moins polyvalents qui assurent les grandes fonctions de l'entreprise.

Du point de vue ITIL, après les formations et les séminaires, une première répartition des responsabilités et des tâches de gestion a été réalisée. Comme on le voit sur la figure 16-5, l'accent a été mis sur la répartition de la responsabilité des processus selon le niveau tactique ou stratégique de ceux-ci. On peut également noter que la répartition des processus de gestion du changement, des configurations et des mises en production s'appuie sur les trois services. Ceci implique que chaque modification apportée au système d'information reçoit l'avis des trois responsables de service. Les mises en production sont réalisées par le service Production, mais se trouvent sous la responsabilité du service Assistance par le biais de la cellule Qualification. De même, alors que les changements seront mis en place par le service Production, c'est bien le service Étude et développements qui en assume la responsabilité et doit réunir régulièrement le CAB.

Gestion de l'infrastructure

Les changements les plus radicaux dans l'infrastructure sont essentiellement ceux qui tournent autour du remplacement de l'ordinateur central (*mainframe*) par un serveur Unix. Les quelques applications qui fonctionnaient encore sur cet environnement furent migrées vers le nouveau système dans le but d'assurer la disponibilité de l'historique en parallèle avec les nouvelles

applications, elles aussi hébergées par les serveurs Unix. En complément, la direction informatique décida de remplacer les terminaux passifs connectés à l'ordinateur central par des terminaux graphiques utilisant un protocole réseau léger.

D'importantes modifications ont également eu lieu sur les infrastructures réseaux et télécommunications, telles que le passage de lignes spécialisées vers des réseaux privés virtuels (VPN) sur des liaisons plus économiques.

Dans l'ensemble, toutes les modifications apportées à l'infrastructure l'ont été par le biais de la mise en place des processus ITIL, et en particulier par la gestion des configurations, la gestion de la capacité et la gestion de la disponibilité.

Gestion du support des services

Centre de services

Comme souvent dans ce type de projet, la mise en place d'un centre de services est certainement la plus belle réussite de l'utilisation d'ITIL dans cette entreprise. C'est bien souvent l'aspect le plus spectaculaire d'un projet de réorganisation, mais c'est également celui qui est le plus tangible pour l'entreprise.

Après une série d'entretiens avec des utilisateurs, l'audit et la réorganisation du service informatique ont mis en évidence la nécessité de mettre en place un service centralisé de prise d'appels et d'assistance. Le besoin le plus souvent exprimé était de pouvoir disposer d'un seul interlocuteur qui prenne en charge l'ensemble de la demande et en assume la responsabilité.

Durant le projet, les auditeurs ont identifié plusieurs services d'assistance au sein de l'entreprise. En effet, en ne considérant que la direction informatique, pas moins de cinq services d'assistance distincts étaient proposés, correspondant en fait aux différentes entités composant la direction. On trouvait un numéro d'appel pour l'assistance générale couvrant la bureautique et la maintenance des matériels, un pour l'exploitation et les administrateurs, et enfin un autre pour chaque équipe de développement... De plus, chaque membre des différentes équipes était sollicité directement par les utilisateurs au téléphone ou dans les couloirs... La messagerie de la machine à café !

Dans ces conditions, il est évident que l'efficacité du processus est plus qu'aléatoire. Entre la perte de temps à identifier le bon interlocuteur et les oubliés des demandes, les pertes d'informations entre la machine à café et le bureau, ou l'absence de la personne qui doit traiter le problème, de nombreuses requêtes des utilisateurs ne voyaient jamais le jour. Le mécontentement envers « l'informatique » était palpable, et certains membres de l'équipe évitaient même les couloirs.

Enfin, les auditeurs ont également identifié deux autres « centres d'appel » au sein de l'entreprise. Le premier était constitué d'un service d'assistance réalisé par les services généraux (travaux divers et maintenance du bâtiment, demandes d'entretien, commandes de fournitures, etc.) et le second par un centre d'appel destiné aux commandes des clients finaux mis en place par le service commercial.

Concernant le « centre d'appel » des services généraux, il faut également noter que plusieurs de ses actions sont très proches de la direction informatique et en particulier en ce qui concerne l'approvisionnement en certains consommables informatiques (papier pour imprimantes et photocopieurs, cartouches d'encre et de poudre d'encre (toner), disquettes et CD-Rom, etc.). Cependant, au-delà d'une simple demande de fourniture de consommables, les services généraux réalisent également la gestion de la téléphonie, des systèmes de photocopie et d'impressions en volume, du contrôle d'accès aux bâtiments, des climatisations et de l'alimentation électrique.

Le centre d'appel a nécessité l'implantation de certaines infrastructures téléphoniques et l'installation d'une nouvelle application de gestion des structures d'assistance aux utilisateurs (*helpdesk*).

Certains membres de l'équipe d'exploitation ont émis le souhait d'une évolution de carrière en passant dans l'équipe d'assistance au centre d'appel ou dans l'équipe d'assistance 1^{er} niveau. Cette proposition fut assez bien accueillie puisqu'elle permettait au service d'assistance de récupérer des personnes bilingues. En effet, un autre problème de taille fut la prise en compte des différentes langues lors du projet de centre d'appel. Comme l'essentiel des sites de production ne passe que par le correspondant local, il fut décidé de ne proposer que le français et l'anglais en réponse téléphonique, les techniciens informatiques ne parlant pas systématiquement la langue du pays appelant. Charge à l'équipe locale ou au correspondant informatique de transmettre l'information aux utilisateurs.

Le regroupement de l'assistance utilisateur d'origine avec une partie de l'équipe d'exploitation permit également d'augmenter la plage horaire en associant l'astreinte de l'exploitation à celle de l'ancienne structure d'assistance aux utilisateurs (*helpdesk*).

Toutefois, le projet le plus novateur pour l'entreprise fut de fusionner le centre d'appel dédié à l'informatique à celui des services généraux. Grâce à ce système, le centre d'appel – et ses ressources téléphoniques, messagerie et intranet – peut aiguiller les demandes de moyens informatiques, mais également les demandes de maintenances classiques ou encore l'approvisionnement et les demandes d'achats auprès des services généraux.

Gestion des incidents

Avant la mise en place des processus d'assistance, les techniciens du service informatique avaient tendance à vouloir régler chaque dysfonctionnement

dans sa totalité avant de rendre le service disponible aux utilisateurs. Ainsi, sur un problème récurrent d'imprimante dans un service, après l'appel à l'assistance technique, les utilisateurs devaient attendre que le technicien emporte l'ensemble du matériel dans son local, le répare et rapporte ensuite l'équipement à son emplacement d'origine...

Désormais, lorsque ce type d'incident se manifeste, le technicien arrive systématiquement avec du matériel de remplacement temporaire qu'il est en mesure de laisser sur place en tant que solution de contournement s'il ne parvient pas à rendre rapidement disponible le service. Comme le matériel a été largement harmonisé depuis la rationalisation de l'infrastructure, il ne lui reste plus qu'à enregistrer la modification de configuration dans la CMDB.

Gestion des problèmes

Malgré un travail conscientieux et appliqué, le technicien, qui « s'accroche à son problème » et ne veut pas s'arrêter avant d'avoir trouvé la solution, représente un risque important pour le respect des temps de remise en service qui ont été validés dans le SLA. Cette recherche des vraies causes des dysfonctionnements doit impérativement se faire sans la pression du sablier qui s'écoule inéluctablement. La solution proposée dans le paragraphe précédent est l'un des moyens permettant au technicien de rendre le service disponible après un incident pour traiter les vraies causes de son problème. Cependant, cela n'est pas toujours possible, comme dans notre exemple, où l'imprimante est facilement déplaçable et n'impose pas l'intervention de plusieurs techniciens ou administrateurs. Dans le cas du réseau par exemple, alors qu'auparavant un incident sur un segment du réseau pouvait paralyser plusieurs centaines d'utilisateurs pendant plusieurs heures, l'architecture prévoit désormais des passages redondants permettant de pallier une panne en activant le lien de secours afin que les techniciens puissent poursuivre leurs investigations plus sereinement sans pour autant affecter le travail des utilisateurs.

Gestion des configurations

L'implantation de ce processus a fait perdre quelques cheveux à la direction informatique lors de la conception de la structure de la CMDB, mais la rationalisation de l'infrastructure informatique a simplifié cette dernière en allégeant par la même occasion la taxinomie des CI.

Grâce à cet outil, mais plus généralement à l'ensemble du processus, un certain nombre d'économies ont été engendrées. Le suivi permanent des configurations a entraîné plusieurs réductions de coûts au sein de la direction informatique mais également pour les services généraux.

- Auparavant, il fallait à l'équipe de maintenance plus de deux à trois semaines pour faire l'inventaire des équipements informatiques (hors réseau et site central). L'utilisation d'un logiciel de gestion de parc a

réduit de plus de 70 % le temps consacré à cette tâche peu motivante. Grâce à un système de remontée automatique d'informations de configuration et à la mise en place d'étiquettes codes-barres, le technicien n'a plus qu'à numériser ces dernières lors de son passage dans les bureaux et valider la configuration qui lui est retournée par le logiciel. Cette solution a d'ailleurs été largement utilisée lors de la première saisie de la base de configuration dans la CMDB. Ce type d'outil permet de recenser rapidement l'ensemble du matériel et des logiciels présents sur un poste de travail.

- Toujours concernant le matériel, certaines économies ont pu être réalisées par le contrôle des locations. Plusieurs contrats ont ainsi pu être résiliés à temps, évitant le renouvellement par tacite reconduction, ce qui était arrivé à plusieurs reprises dans certains établissements. Le plus impressionnant fut l'économie réalisée sur la résiliation d'un contrat qui n'avait plus d'intérêt et qui continuait d'être souscrit inutilement depuis plusieurs années. Enfin, la rationalisation de l'infrastructure et surtout l'abandon de certains matériels et logiciels se sont rapidement traduits par l'arrêt des contrats d'assistance et de maintenance associés.
- Enfin, le suivi des consommables informatiques (CD-Rom, papier, cartouches d'encre, etc.) a accentué la maîtrise des dépenses en centralisant les demandes. Ce système permet en effet de valider les besoins d'achat en volume en relation avec des projets précis et d'obtenir ainsi des prix négociés globalement.

Gestion des changements

Au début du projet, il arrivait fréquemment que les administrateurs système reçoivent des mises à jour provenant des éditeurs, se rendent en salle des machines et appliquent les modifications... Cette attitude peut se comprendre par l'un des points suivants :

- une chance insolente qui permet d'expliquer que l'entreprise n'ait pas subi de désastre auparavant ;
- une inconscience du danger que l'on ne retrouve que chez les enfants ;
- une maîtrise totale de la technologie ou l'impression de cette maîtrise.

Ce dernier cas étant bien évidemment peu probable, il était urgent de modifier ce comportement.

Qu'il réponde à une obligation réglementaire, commerciale, d'adaptation de l'entreprise à la demande client ou à son environnement concurrentiel, qu'il soit nécessaire à la progression technologique ou pour réduire les coûts, le changement est devenu une constante : chaque fois que l'entreprise évolue, les processus de l'entreprise doivent également s'adapter. Et l'environnement informatique doit suivre et soutenir l'évolution de ces processus.

Avec la complexité croissante de son environnement informatique, et en particulier des logiciels, il était indispensable de mettre en place une gestion efficace des changements. Même s'il ne fait pas tout, un logiciel peut faciliter cette étape. Il doit d'une part permettre de conserver l'historique des changements intervenus sur un équipement ou un logiciel de l'infrastructure informatique, et d'autre part, à l'aide des informations stockées, simplifier la prise de décision lorsque le comité consultatif du changement se réunit dans le but de valider ou non une demande de modification.

Dans les premiers temps, la réunion du CAB se déroulait tous les quinze jours et était davantage une réunion de suivi des modifications que de contrôle de celles-ci. En revanche, après trois mois de mise en place du processus, les réunions ont enfin pu être productives et respecter les recommandations ITIL. Par la suite, la périodicité de ces réunions est passée à un mois.

Pour ne pas entraver le fonctionnement, la gestion du changement doit être rapide et efficace. Dans le cas contraire, elle est rapidement cataloguée comme bureaucratique. Les PME demandent une forte réactivité, mais beaucoup de personnes utilisent ce besoin comme une excuse pour ne pas documenter les actions ou pour passer outre les procédures et les contrôles. Désormais, les administrateurs et autres intervenants sur l'infrastructure doivent assister au CAB lorsqu'ils envisagent une modification et doivent la justifier.

Processus particulièrement complexe, la gestion du changement demande surtout un véritable changement de mentalité. Plus qu'un simple historique des modifications, la gestion des changements doit également prendre en compte l'impact de ces évolutions. Les outils de ce processus peuvent alors rapidement se cantonner à la diplomatie, au compromis, et parfois à la prise de risque. Il devient indispensable de faire la part des choses entre les demandes fondées, celles dont l'urgence est toute relative et surtout celles émanant plutôt d'un problème « politique » que d'un problème touchant à l'efficacité de l'entreprise.

Gestion des mises en production

La gestion de la mise en production s'inscrit dans la continuité de la gestion du changement, même si elle présente souvent moins de caractère conflictuel. Dans le cas qui nous concerne, l'équipe d'assistance a mis en place une salle maquette dans laquelle les nouveaux matériels et logiciels sont testés avant leur mise en production. Afin de limiter le coût d'une telle infrastructure, le service informatique utilise un système de plusieurs serveurs virtuels sur des ordinateurs PC musclés. Ce système permet d'émuler de multiples machines et un réseau plus ou moins complexe (routeur, pare-feu, etc.). Afin de prendre en compte la charge générée par les utilisateurs, un logiciel de simulation est utilisé pour évaluer les temps de réponse des applications et

des matériels dans une configuration proche de l'environnement de production.

La gestion des mises en production se trouve sous la responsabilité du service Assistance qui assume la cellule de qualification. Néanmoins, c'est bien le service Production qui met en place les nouveaux modules logiciels ou modifie l'infrastructure matérielle. Dans le cas d'un remplacement rapide d'une machine, le service de la production informatique a mis en place un système de télédistribution permettant une installation semi-automatique du système d'exploitation du poste et l'installation automatique des applications bureautiques en fonction du profil de l'utilisateur. Ainsi, le changement d'un poste ou l'arrivée d'un nouvel utilisateur peut être géré par un technicien non spécialiste qui n'a qu'à installer physiquement le poste puis à appuyer sur une combinaison de touches.

Gestion de la fourniture des services

Gestion des niveaux de service

La mise en place du SLA est souvent perçue comme l'aboutissement d'un projet ITIL.

Au début des négociations du SLA, la vision et les objectifs des deux parties impliquées, à savoir la direction informatique et les clients et utilisateurs, différaient considérablement. Chaque partie apportait sa part d'incompréhension du rôle de l'autre, mais également de son propre rôle. Des méthodes permettant de réduire le plus possible ces malentendus existent. L'essentiel est de parvenir à fixer les objectifs de chacun, et de parler un langage commun. La première étape de la négociation est donc souvent une affaire de dialogue et de compromis. Un bon moyen de gagner du temps lors de ces négociations consiste à préparer un plan type de SLA et à veiller à la conception d'un catalogue de services réaliste et facilement compréhensible pour des personnes non spécialistes.

Le SLA est perçu comme un document technique par les clients et les utilisateurs, alors qu'il apparaît ne refléter que les besoins exprimés pour les techniciens. Cette incompréhension mutuelle est souvent à l'origine de tension entre les parties. Certains directeurs de service reprochaient à la direction informatique de ne pas vouloir assumer ses responsabilités et d'utiliser le SLA comme un paravent. Le grand défi du SLA est donc de dépasser ce cadre technique de la fourniture d'un service pour parvenir à une compréhension des besoins de chacun...

L'élément le plus important consiste à créer un climat de confiance réciproque. Cette étape est la meilleure et parfois l'unique occasion de résoudre les divergences sur le rôle et les engagements mutuels, c'est-à-dire de concilier les attentes de chacune des parties et de s'entendre sur la façon de procéder.

Les coûts actuels de la production informatique, ainsi que ceux de la gestion des services avec l'ITIL sont connus. Cependant, la direction a souhaité attendre de mettre en place le processus de gestion des finances pour valider ces estimations et ces mesures. L'évaluation des coûts de la fourniture des services et des engagements pris par la direction informatique demandant à être validée par l'expérience, la première année n'a pas été imputée aux directions bénéficiaires des services. Ce SLA ne prend en compte pour l'instant que la bureautique et la messagerie. À l'avenir, il sera étendu à l'ERP.

La conception de chaque SLA s'est déroulée en plusieurs phases. Au début, la configuration standard est proposée par défaut selon un plan type. Une phase de négociation s'engage alors afin d'amender les engagements mutuels et d'apporter la réponse la plus proche possible des demandes des utilisateurs. Puis dans une phase pilote, le SLA est évalué en situation de production de 1 à 3 mois. À l'issue de cette période d'évaluation, le contrat de SLA est signé.

Gestion financière des services

L'implantation de la gestion financière des services a été assez longue et s'est largement appuyée sur les travaux précédents d'implantation de processus, et en particulier sur les négociations du SLA. Certaines directions étaient assez réticentes à se voir facturer un service qu'elles estimaient comme naturel ou déjà financé par leur propre activité. Néanmoins, cette facturation interne, même si elle n'est pour l'instant que fictive, a permis à chacun de bien mieux percevoir l'impact financier des décisions de chaque direction. Le plus frappant est sans aucun doute le fait qu'après avoir obtenu des chiffres moyens sur un service générique de type bureautique, certaines directions évaluèrent elles-mêmes le coût de plusieurs de leurs demandes et en limitèrent la portée. C'est ainsi que des demandes d'impression régulières ont été supprimées ou remplacées par de l'archivage électronique de document, ce qui a encore fait gagner en coût d'impression et en coût de stockage du papier.

Globalement, l'expression des besoins sur les nouveaux services a été revue à la baisse après l'annonce de la facturation et certaines demandes qui pouvaient parfois apparaître comme farfelues ont dû être justifiées auprès de la direction générale.

Gestion de la capacité

Au fil des années, les utilisateurs du système d'information ont généré un volume considérable d'informations sous la forme de fichiers bureautiques classiques (textes, tableaux, images, etc.). L'augmentation importante du nombre et de la taille de ces fichiers stockés sur les serveurs a causé quelques soucis aux gestionnaires de la capacité. Jusqu'alors, la direction informatique

ne se préoccupait pas réellement de ce problème. En achetant continuellement des disques supplémentaires, la question était éludée rapidement. Lorsque la place disponible sur les disques venait à manquer, on attendait les plaintes des utilisateurs. Lorsque celles-ci devenaient trop insistantes, un investissement rapide suivi d'une installation précipitée suffisait à calmer les esprits... temporairement. La diminution sensible des prix sur ce type de matériel tendait à donner raison à la direction informatique. Cependant, après une étude des coûts cachés, le gestionnaire de la capacité a proposé une nouvelle lecture de ce problème.

À l'aide des principes de la gestion financière des services, il réussit à démontrer que le coût de possession de ces zones de stockage devait prendre en compte plusieurs autres postes financiers. En effet, plus de fichiers sur les serveurs implique non seulement plus d'espace disque pour les héberger, mais également plus de temps pour les sauvegarder, ce qui conduit souvent à un investissement supplémentaire en nouveaux matériels et logiciels pour réaliser cette fonction : robot de sauvegarde, sous-réseau de stockage ou SAN (*Storage Area Network*), etc. De plus, il faut également envisager qu'au-delà d'un certain seuil, un administrateur de serveur ne peut assumer seul le volume de données à gérer. Cela implique un coût en personnel supplémentaire qui, ajouté au coût d'investissement, surclasse de loin le gain réalisé dans la non-gestion du problème.

Après audit des fichiers sur les différents serveurs de l'entreprise, il fut décidé d'archiver les fichiers en utilisant les fonctions de base présentes dans le système d'exploitation des serveurs bureautiques. Cette technique permet de basculer automatiquement sur des supports de moindre coût (disques durs temporaires, disques optiques, CD-Rom, stockage sur bandes ou DLT, *Digital Linear Tape*, etc.) les fichiers les plus anciens ou ayant dépassé une limite fixée. Elle a ainsi pu libérer immédiatement près de 38 % de l'espace disque utilisé sur les serveurs en conservant en accès immédiat les cinq dernières années de fichiers. Bien sûr, cela n'empêche pas de valider que les fichiers sont bien présents en exemplaire unique sur les serveurs afin de libérer encore plus de place.

Ce qui est important dans cet exemple, c'est que les utilisateurs qui pensaient au départ revenir en arrière dans la souplesse d'utilisation de la bureautique, n'ont ressenti que très peu d'inconvénients à cette solution. En effet, lorsque la limitation de l'accroissement de l'espace disque fut décidée, les utilisateurs se sont globalement opposés à cette solution. Il fallut alors démontrer par un test grandeur réelle dans l'un des services que l'archivage des fichiers était transparent pour l'utilisateur, et surtout que l'action permettant de retrouver un ancien fichier était strictement identique, en dehors du délai supplémentaire occasionné par la recherche du fichier sur bande ou disque optique.

Gestion de la disponibilité

L'implantation de la gestion de la disponibilité a été menée par un audit interne des ressources informatiques et de leur implication dans la chaîne de valeur de l'entreprise.

Le but premier est alors de réduire les points sensibles aux pannes, que ce soit par la fragilité ou l'unicité de l'élément. Concernant les communications, cette réduction des SPOF s'est réalisée en mettant en œuvre la duplication de certains passages réseau entre les deux sites principaux, mais également en proposant la duplication des accès réseau à distance (réseau privé virtuel ou VPN sur SDSL/ADSL plus VPN sur satellite, réseau numérique ou RNIS en secours). Les serveurs furent systématiquement équipés d'une alimentation redondante et d'un mécanisme de copie automatique des disques (RAID1 et RAID5). Les serveurs les plus critiques furent mis en *cluster* (architecture de groupes d'ordinateurs) dont chacun des deux membres se situait dans une salle des machines différente (voir Gestion de la continuité de service).

Cependant, la gestion de la disponibilité ne doit pas prendre en compte uniquement l'aspect site central ou salle des machines informatiques. Il est important de prendre également en compte les différents équipements présents dans les bureaux ou dans les bâtiments de production. Ainsi l'audit a-t-il mis en lumière une activité d'expédition pour laquelle deux imprimantes redondantes pouvait prendre le relais dans l'impression des bons de livraison. Malheureusement, ces deux imprimantes n'étaient reliées qu'à un unique concentrateur réseau. En cas de panne de cet équipement, l'ensemble de la chaîne aurait été bloqué.

Gestion de la continuité de service

L'implantation de la gestion de la continuité de service a consisté essentiellement en un audit des activités de l'entreprise, et des différentes étapes de sa chaîne de création de valeur. Le but étant de déterminer l'ordonnancement de la reprise d'activité globale de l'entreprise en cas de sinistre, il a été nécessaire d'évaluer avec chaque responsable métier le caractère d'urgence de son activité parmi toutes les autres. Là encore, un certain niveau de diplomatie et de pédagogie est nécessaire, puisque chacun a à cœur de « défendre » son domaine, et évidemment de le faire passer comme vital pour l'entreprise...

À l'issue de cet audit, les fonctions vitales pour l'entreprise ainsi que les applications les soutenant ont été identifiées. Grâce à ces résultats, une étude d'implantation fut réalisée dans l'optique de la mise en place d'une salle de secours à distance, hébergée par le site de production n° 2 situé à quelques kilomètres de là.

Le coût de la solution est relativement faible en regard de la sécurité qu'elle offre. En effet, la direction a décidé de n'implanter que le strict minimum

nécessaire à la reprise d'activité. Il s'agit essentiellement de quelques serveurs bureautiques et Unix hébergeant une copie synchrone de la messagerie, de certains fichiers bureautiques et des applications principales (sauvegarde et restauration, ERP, paye, finance, etc.). Concernant les télécommunications, un autocommutateur IP peut prendre le relais en cas de désastre, et un réseau minimal est en mesure d'interconnecter les sites en mode dégradé. Grâce à la sortie d'une copie des bandes de sauvegarde du site principal, le site de secours est en mesure de restaurer l'ensemble des données en cas de sinistre, même si dans ce cas, il devient nécessaire de se procurer le matériel manquant.

Gestion de la sécurité

L'implantation de ce processus a également donné l'occasion d'exploiter toutes les préconisations d'ITIL. En effet, bien que crucial, ce point était particulièrement mal exploité. L'élément le plus important, outre l'aspect technique non maîtrisé, était l'absence totale de consultation des besoins des utilisateurs en termes de sécurité. Il en résultait un ensemble de règles de sécurité excessives et, comble de l'ironie, assez peu efficaces. Aucune politique d'entreprise n'avait été mise en place, mais la direction avait souhaité limiter l'usage de la messagerie aux chefs de service pour réduire les menaces de piratage et d'attaques virales. De leur côté, les administrateurs avaient décidé de limiter la consultation Internet à certains sites Web répondant à une liste de critères plus ou moins professionnels.

Cette situation étant évidemment intenable, certains passe-droits étaient accordés oralement, sans contrôle réel des abus et des risques potentiels... jusqu'à l'inévitable problème.

L'utilisation de la messagerie électronique étant de plus en plus important pour l'activité de l'entreprise, la prise en compte par les salariés des notions de sécurité devint de plus en plus importante. Une charte d'utilisation des moyens de communication (téléphone, fax, messagerie, intranet, Internet) fut mise en place et annexée au contrat de travail des salariés.

Certaines modifications furent apportées à l'infrastructure informatique afin de sécuriser le « périmètre » logique de l'entreprise (mise en place d'une DMZ après le pare-feu, mise en place d'un serveur *proxy-mail* avec antivirus, etc.). Sur les postes de travail, les graveurs de CD-Rom et de DVD-Rom furent retirés et l'accès aux ports USB fut interdit afin d'éviter les fuites de documents et d'informations. Afin de compenser l'absence de ces graveurs sur les postes, la direction informatique proposa un service de graveur de CD-Rom accessible par réseau et capable de produire un volume considérable de copies du même média. Cette solution permet de contrôler le contenu du CD-Rom, mais également la consommation des médias vierges afin d'éviter les abus.

Enfin, une politique spécifique à la prise en compte de la sécurité dans les développements internes fut mise en place. Cette politique, qui correspond plus à un ensemble de bonnes pratiques dans les développements, ainsi qu'à certaines exigences dans les tests avant mise en production, a permis de sensibiliser plus directement les chefs de projet et les développeurs, afin qu'ils portent une attention soutenue à ce problème.

Bilan

Pour cette entreprise, le bilan est donc globalement positif. Même si certains écueils n'ont pu être évités, il en ressort tout de même une production informatique optimisée, un meilleur service aux utilisateurs, et l'hypothèse d'une future réduction supplémentaire des coûts, en particulier en mutualisant le centre d'appel du service commercial avec celui du service informatique et des services généraux.

Un projet d'implantation d'un ERP s'est déroulé en parallèle. Si cela implique une charge supplémentaire non négligeable pour l'équipe informatique et surtout pour les directions métier, cela représente néanmoins un excellent « alibi » à l'implantation des processus ITIL. C'est en effet le moment rêvé pour lancer les indispensables réflexions et réorganisations des processus internes de l'entreprise. C'est également le moment où l'entreprise va se poser des questions sur le bien-fondé de certains besoins en regard du surcoût financier qu'ils imposent. En conséquence, c'est également le moment de l'évaluation et de la validation de la pérennité de ces besoins.

En tout état de cause, l'implantation d'un ERP impose souvent certaines procédures lourdes qui seront bien mieux gérées par l'intermédiaire de processus ITIL. Il faut d'ailleurs rappeler que très souvent, l'éditeur de la solution ERP encourage ses clients à implémenter un processus de gestion et d'amélioration de la qualité.

Au bilan, on note une augmentation particulièrement encourageante des documentations et des procédures rédigées. En partant d'un état d'absence quasi total de ces informations, le service a déjà rédigé 55 % de ces procédures. Néanmoins, le naturel revient au galop, et la principale difficulté réside dans le besoin de relancer continuellement le processus, afin de terminer cette tâche et de faire vivre l'existant (gestion du changement). Même si certains soucis se présentent encore, la satisfaction des clients et des utilisateurs est également en hausse. Ceux-ci le signalent d'ailleurs fréquemment au centre d'appel. En reprenant le fameux modèle du Gartner Group, nous pouvons dire que la direction informatique vient de se hisser à la deuxième marche des niveaux de maturité – qui en compte cinq – et est passée d'un niveau technique centralisé à un niveau réactif. Enfin, concernant

les coûts de l'informatique dans l'entreprise, en faisant abstraction des dépenses liées à l'implantation de l'ERP, la direction financière estime qu'une augmentation des coûts a lieu durant les deux premières années, mais qu'une réduction de 4 à 5 % du budget a été réalisée lors de la troisième année sans réduction significative du niveau de service.

Toutefois, nous n'en sommes pour l'instant qu'à la première itération de l'implantation d'ITIL. L'entreprise doit désormais prendre en compte l'ensemble des processus mis en place et lancer leur évaluation afin d'améliorer une nouvelle fois l'efficacité de chacun d'entre eux. Il reste en effet de nombreux axes de progrès dans les domaines du support et de la fourniture des services, lesquels permettront sans doute d'accroître ses gains financiers qui, bien qu'annoncés en dernier dans la liste des objectifs, étaient certainement les plus attendus.

Justifier un projet ITIL

Comme tout projet, la mise en œuvre du référentiel de bonnes pratiques ITIL s'accompagne non seulement de coûts non négligeables mais s'envisage également sur des durées importantes. Si les entreprises sont sensibles aux perspectives rassurantes véhiculées par les différentes études relayées par la presse, il n'en reste pas moins que les attentes sont clairement orientées vers un besoin de preuve.

Quelle adoption pour ITIL ?

La mise en œuvre des bonnes pratiques de gestion de services est une initiative majeure. Elle s'étend sur plusieurs années, demande d'investir dans les personnes, les outils, la documentation et modifie profondément la culture de l'entreprise. Il est compréhensible qu'avec un tel niveau d'investissement, l'entreprise envisage une amélioration des performances et/ou un retour financier.

Les différentes études publiées confirment l'avancée d'ITIL dans les entreprises européennes, stimulée par une meilleure culture des bonnes pratiques et la nécessité d'informer plus largement les directions générales des avantages du référentiel.

Une étude menée en janvier 2007 par BMC Software auprès de 200 décideurs d'entreprises répartis sur six pays d'Europe (Allemagne, France, Grande-Bretagne, Italie, Espagne et Portugal) a fourni un panorama très instructif sur le niveau d'adoption d'ITIL.

Les décideurs informatiques sondés sur leur propre expérience au sein d'une organisation basée sur ITIL sont extrêmement positifs. Cette information est d'autant plus pertinente que 56 % des personnes de ce groupe ont personnellement implémenté certains éléments d'ITIL dans leur entreprise.

Les gains perçus

Il apparaît désormais que parmi les entreprises ayant débuté un « projet ITIL » :

- 70 % des personnes interrogées reconnaissent ses bénéfices.
- 77 % des personnes travaillant dans une organisation conforme au référentiel attestent que son implémentation a répondu à leurs attentes.
- 62 % des membres de ces organisations le recommanderaient à leurs confrères.
- 70 % des décideurs informatiques reconnaissent que les principales limites à l'adoption d'ITIL sont :
 - le temps et les ressources disponibles ;
 - la compréhension limitée de ces bonnes pratiques à l'extérieur de la DSi ;
 - la justification du ROI.

Les principaux avantages perçus de l'implémentation d'ITIL sont :

- une amélioration de l'alignement informatique/métier (54 %) ;
- un gain de productivité (51 %) ;
- l'utilisation de bonnes pratiques (53 %).

Les obstacles rencontrés

En dépit de ces avantages, les DSIs doivent convaincre les directions générales. Plus des deux tiers des sondés chargés de déployer un cadre de bonnes pratiques reconnaissent que les principaux freins à l'adoption du référentiel sont :

- la prise de conscience des avantages d'ITIL au-delà du département informatique ;
- l'accroissement des budgets consacrés aux technologies de l'information ;
- l'adhésion des instances dirigeantes et/ou du conseil d'administration.

On comprend bien que le principal frein à l'application d'ITIL reste malheureusement sa faible popularité en dehors des départements informatiques. Selon l'étude, un tiers des décideurs IT estime que cette compréhension limitée du référentiel par les non-informaticiens constitue un obstacle.

Les niveaux de mise en place des différents processus ITIL sont également plutôt disparates. Assez logiquement, la gestion des incidents est totalement intégrée ou en passe de l'être dans 26 % des entreprises de cette étude. En revanche, ce processus reste encore en cours de réflexion dans 15 % d'entre elles ou n'est même pas envisagé pour près de 60 % des cas.

La gestion des problèmes est implantée dans 24 % des entreprises et est encore à l'étude dans 15 % des cas. Les taux d'implantation des processus

suivants décroissent logiquement en fonction de leur pragmatisme et leur proximité de l'opérationnel : gestion des configurations 21 %, gestion des changements 20 %, gestion des mises en production 18 %, gestion des niveaux de service 14 %.

Une autre étude, menée par Compass MC dans onze pays européens sur des entreprises ayant débuté leurs projets ITIL depuis au moins dix-huit mois, nous apprend que près de 67 % des entreprises interrogées font confiance à ITIL dans l'amélioration des performances de l'informatique, alors que paradoxalement, près des trois quarts d'entre elles estiment ne pas pouvoir démontrer la corrélation directe entre l'adoption d'ITIL et les gains de productivité.

Les constats

À la lecture de ces études, deux constats forts peuvent être faits.

Le premier concerne le volet financier. Alors que l'une des raisons les plus souvent citées pour la mise en place d'ITIL est la réduction des coûts, il apparaît que seuls 30 % des entreprises ayant mené une implémentation d'ITIL en ont tiré des bénéfices de réduction des coûts. Fort heureusement, les entreprises interrogées reconnaissent que ce déploiement en lui-même ne suffit pas à produire un retour sur investissement immédiat mais qu'il s'agit d'une étape essentielle pour y parvenir.

Le second constat concerne le taux et le type de reconnaissance d'ITIL au sein de l'entreprise. La culture organisationnelle préalable de l'entreprise est un élément essentiel à son adoption. En effet, on constate une forte adhésion à ITIL (86 % des cas) dans les entreprises qui utilisent déjà un autre cadre de normalisation ou de gouvernance comme ISO, COBIT, Six Sigma et autres. En revanche, parmi celles n'ayant pas implanté de standard de ce type, le taux d'adoption d'ITIL n'est que de 43 %.

Ceci souligne l'écart considérable entre le perçu et le réel. Si les DSI veulent maintenir l'investissement dans ITIL et la confiance des parties prenantes de l'informatique, il est indispensable qu'ils parviennent à démontrer les avantages réels de leurs investissements dans ITIL. Pour cela, ils devront mesurer la maturité de chaque processus et démontrer que la progression de ces processus réduit les coûts et améliore les performances de l'informatique.

Gérer le changement

De nombreuses organisations estiment qu'une bonne formation à ITIL, un projet solide, accompagné de bonnes compétences en organisation et en gestion de projet suffiront à mettre en place les changements organisationnels exigés par l'adoption du référentiel.

Malheureusement, tout cela risque de ne pas être suffisant. En effet, le succès de l'adoption est plus basé sur l'implication de tous les acteurs, puis sur leur participation active au développement du processus.

Comme on a pu le voir dans le processus de gestion du changement d'ITIL, un changement « technique » se prépare en amont afin d'évaluer l'impact qu'il peut avoir sur le système. Dans le cas de changements organisationnels, la méthode est identique. Implanter un processus ITIL dans une organisation demande de comprendre comment celle-ci travaille afin d'évaluer les changements nécessaires. Ceci dit, il faut comprendre également que les changements apportés à l'organisation informatique vont toucher des personnes et la façon dont elles travaillent. Ces changements sont généralement peu appréciés et un effort de communication et d'explication sera nécessaire avant d'espérer une adhésion à la nouvelle organisation, ou au pire à une résistance au changement allégée.

Changements organisationnels

Selon John Kotter, professeur à Harvard et dont l'ouvrage *Leading Change* est considéré par un grand nombre de personnes comme la bible dans le domaine de la gestion du changement, il existe huit raisons principales pour lesquelles un projet de changement peut échouer :

- Autoriser trop de complexité dans le changement.
- Ne pas réussir à construire une coalition autour du changement.
- Ne pas comprendre le besoin d'une vision sur le projet.
- Ne pas parvenir à communiquer clairement cette vision.
- Laisser quelqu'un faire barrage à la vision.
- Ne pas planifier les résultats à court terme et ne pas les réaliser.
- Déclarer la victoire trop tôt.
- Ne pas ancrer les changements dans la culture de l'entreprise.

Pour éviter ces erreurs, John Kotter propose d'utiliser le modèle suivant des Phases de Changement. Il comprend également huit étapes qu'il est crucial de suivre :

- Créer un sentiment d'urgence.

Il s'agit là de faire comprendre aux acteurs que le changement est nécessaire, voire vital, à la bonne marche de l'organisation. La question que l'on se pose à ce moment est : « Que se passera-t-il si nous ne faisons rien ? ».

- Former un groupe puissant de guide.

Créer un groupe multi-niveaux disposant de l'autorité, des compétences, de l'expérience, du respect et de la confiance des autres ; en bref, un groupe qui ait assez de pouvoir et de crédibilité pour mener le changement.

- Créer une vision.

Le groupe de guides est en charge de créer une vision et des plans stratégiques permettant d'orienter le processus de changement. Cette vision doit préciser la direction prise par le projet et motiver les participants à suivre cette dernière. Elle doit également coordonner les actions des différents acteurs et souligner les buts de la direction générale.

- Communiquer cette vision.

La vraie mesure du changement est prise au moment de la communication de cette vision. Pour cela, il est nécessaire d'utiliser tous les médias disponibles et d'adapter son approche en fonction du public visé.

- Donner le pouvoir et la capacité d'agir selon la vision.

L'action la plus importante consiste à éliminer les barrières au changement et modifier les systèmes qui bloquent la vision.

- Engendrer des succès à court terme (*quick wins*).

Ces succès rapides aident à conserver l'enthousiasme et l'engagement dans le projet. Pour cela, il faut planifier puis mettre en œuvre des améliorations de performance bien visibles. Reconnaître et récompenser les intervenants est également un facteur d'adoption du changement par ses acteurs.

- Consolider les gains et prévoir les nouveaux changements.

Les succès rapides apportent une crédibilité supplémentaire sur laquelle il faut s'appuyer pour modifier les systèmes, les structures, les politiques qui ne cadrent pas avec la vision.

- Institutionnaliser la nouvelle méthode dans la culture.

La dernière étape est celle qui permet de faire entrer les nouveaux comportements dans l'entreprise en les associant à ces succès.

Changements culturels

Comme nous venons de le voir, l'adoption d'ITIL va également avoir des conséquences sur la culture de l'entreprise. Celle-ci peut être d'une grande aide en étant moteur du changement ou au contraire être la source d'une résistance.

La culture d'entreprise

Il est toujours surprenant de voir qu'une entreprise ne perçoit pas la gestion du changement de sa propre culture comme l'une de ces priorités. Par culture d'entreprise, on entend les idées, les valeurs, les comportements, les pratiques et les attentes partagés par les employés et les dirigeants de l'entreprise.

Les changements à cette culture affectent les personnes qui y adhèrent ainsi que les sentiments qu'ils éprouvent à son encontre. Ceci explique

pourquoi un changement proposé est parfois perçu comme une cassure entre deux parties représentées par ceux qui demandent le changement et ceux qui le subissent. Dans ce cas de figure, la réaction est souvent épidermique et correspond à une bataille que se livrent deux camps dont chacun est persuadé qu'il se bat pour la « bonne cause ».

La mise en place d'un logiciel de suivi des appels d'un bureau de service vise à fournir des statistiques sur l'efficacité du processus de gestion des incidents. Il permet en particulier de suivre quantitativement et qualitativement l'évolution des appels. Cependant, il y a fort à parier que certaines personnes impliquées dans ce changement vont le percevoir comme un outil de surveillance de l'activité salariée. Pour les individus, seul le changement « perçu » compte. Ceci implique pour ces personnes que le changement sera « subi ».

De même, le niveau du changement et le système concerné sont dépendants de la place de l'observateur et des choix qu'il peut faire.

La résistance au changement

La résistance qu'un changement peut rencontrer ne doit pas être perçue comme une simple inertie mise en travers d'une évolution. En fait, il s'agit plus d'une phase de maturation nécessaire dont on ne peut faire l'économie.

La principale difficulté rencontrée dans la gestion des changements n'est pas le changement lui-même, mais bien la transition entre les deux états. Dans le cas d'un changement dans l'organisation, il s'agit évidemment du processus psychologique par lequel les gens doivent passer pour accepter la nouvelle situation. Selon les travaux de la psychiatre américaine Elisabeth Kübler-Ross, il existe six étapes de changement que les gestionnaires doivent connaître. Ses travaux portaient davantage sur la notion de deuil que ressent chaque individu lorsqu'il perd une personne, un objet ou une situation, mais s'applique parfaitement aux changements organisationnels. Dans ces situations, la fluctuation du comportement de la personne touchée est illustrée par la courbe de la figure 17-1.

La gestion des émotions

Appliquée au changement, cette théorie décrit six étapes successives indépendantes des différences individuelles et caractérisées par une réponse émotionnelle au changement. Ce cycle vaut surtout s'il s'agit d'un changement imposé et subi.

La première étape est le déni, c'est-à-dire le refus du changement. La personne ne peut croire que cela lui arrive et peut ressentir une torpeur. Certaines personnes font comme si l'événement ne s'était pas produit et continuent d'agir comme avant, en espérant que les choses se remettront en place.

Dans la seconde étape, qui est celle de la colère et du rejet, les personnes s'opposent aux changements et peuvent aller jusqu'à utiliser un vocabulaire blessant ou à critiquer leur organisation et leurs collègues.

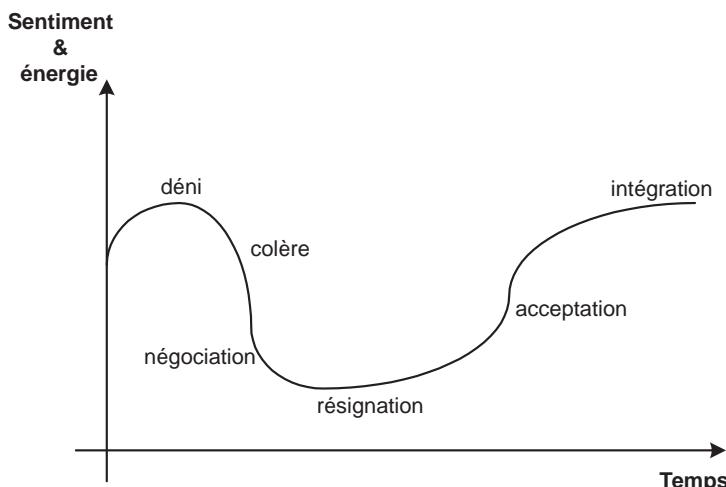


Figure 17-1 : La courbe de Kübler-Ross

Dans la troisième étape, les gens tentent de négocier et de remettre en cause le changement. L'objectif est alors de le faire disparaître, d'en être exempté ou de le rendre moins douloureux.

La quatrième étape est celle du découragement et parfois de l'anxiété. Les personnes sont tristes et découragées. C'est une étape d'affliction pendant laquelle les personnes réfléchissent et évaluent la situation.

Ces étapes critiques doivent être suivies avec attention pour éviter les réactions excessives qui peuvent naître. Dans les trois premières situations, une éventuelle réaction sera dirigée contre le changement ou ce qui l'amène. A contrario, lors de la quatrième étape, une réaction excessive sera dirigée contre la personne elle-même (démission, perte de confiance, dépression...).

Durant la cinquième étape, la personne touchée par le changement a passé le point le plus bas du cycle et reconnaît l'inévitable en cherchant la prochaine étape.

La sixième et dernière étape correspond au moment où, ayant bien accepté le changement, la personne intègre la nouvelle situation comme étant la situation normale et se fixe de nouveaux objectifs.

Évidemment, ces étapes sont très différentes selon les personnes et dépendent de nombreux facteurs. Par conséquent, la courbe peut être largement modifiée en amplitude et en durée selon les événements et l'assistance que l'on apporte aux personnes impliquées.

Les individus ont besoin de comprendre les changements qui les concernent avant d'agir en conséquence. Plus les apprentissages individuels nécessités par un changement organisationnel seront complexes, plus les résistances

au changement seront longues et difficiles à gérer pour le gestionnaire du changement.

C'est donc à lui qu'il incombe d'aider ces personnes à passer d'une étape à l'autre, c'est-à-dire à réaliser le mieux possible les transitions vers la fin du cycle plutôt qu'elles restent coincées dans l'une des premières étapes.

Vendre son projet

La préoccupation du client ne tourne pas autour d'ITIL et faire du processus pour le processus ne l'intéresse pas plus. Pour présenter le référentiel dans l'entreprise, vous devez trouver quelles sont les problématiques métier qui préoccupent la direction et comment la mise en œuvre des bonnes pratiques d'ITIL peut aider dans la prise en compte de ces questions.

Il n'est pas rare de voir une entreprise lancer un vaste et coûteux projet informatique de déploiement d'une nouvelle technologie parce qu'un concurrent a fait la même chose. Cela implique de développer un système qui n'a que peu de valeur pour le métier de l'entreprise.

Essayer de mettre en œuvre ITIL sans aucun lien avec le métier de l'entreprise consiste à améliorer un processus que personne n'utilise. Par conséquent, on retombe dans le travers qu'ITIL essaie de combattre : au lieu de se préoccuper des besoins du client, la DSI se focalise sur une technologie !

Alors, comment faire pour promouvoir les avantages potentiels du référentiel des bonnes pratiques auprès du reste de l'organisation ?

Identifier les cibles

Les organisations sont typiquement structurées autour de trois principaux niveaux, qui possèdent chacun une vision et des espérances différentes des processus informatiques :

- Stratégique.

Niveau auquel les décisions sont prises, la politique établie, les règles créées et les engagements financiers décidés.

- Tactique.

Niveau auquel la politique devient réalité, les décisions et les règles sont mises en œuvre et les niveaux financiers sont confirmés.

- Opérationnel.

Niveau où les décisions qui ont été mises en œuvre deviennent actives, en suivant la politique, les règles et les engagements financiers.

Le succès de l'adoption d'ITIL passe par plusieurs étapes :

- identification de ces niveaux dans une organisation ;

- compréhension des besoins des différents niveaux ;
- démonstration de l'apport d'ITIL pour atteindre les objectifs.

La perception que l'on a d'une organisation tend à être modelée par deux composantes. La plus évidente est l'expérience que l'on a de l'entreprise, l'autre est tirée des organigrammes. Cependant, aucune de ces perspectives ne fournit l'ensemble des éléments nécessaires permettant de préparer une promotion efficace d'ITIL dans l'organisation.

En effet, l'expérience est souvent limitée par les frontières des rôles, des responsabilités et du temps passé dans l'organisation. Dans quelques cas cela peut suffire, mais généralement la vue est limitée.

Quant aux organigrammes, ils essayent de représenter les rôles et les responsabilités, mais ne parviennent qu'à montrer les niveaux hiérarchiques.

En fait, ce qu'il est important d'identifier est lié aux niveaux de décision et d'influence de l'organisation, qui ne sont pas toujours les mêmes que les niveaux hiérarchiques.

Préparer ses plans

Vendre ITIL à la direction, puis à l'ensemble de la société n'est pas si difficile si vous êtes bien préparé. La première étape est de savoir si l'organisation est prête pour l'adoption du modèle. Les cadres dirigeants de l'entreprise doivent être conscients du besoin et de l'importance de disposer de services de haute qualité.

Un premier indicateur efficace consiste à identifier si une directive claire de l'équipe de direction reconnaît que les meilleures pratiques sont nécessaires pour améliorer l'alignement de l'informatique sur les besoins métier de l'entreprise.

Pour vendre ITIL dans l'organisation, ses partisans doivent communiquer les avantages de son adoption dans des termes que chacun comprendra. On peut notamment mettre en avant certains bénéfices potentiels d'ITIL au niveau de la DSI, par exemple une utilisation plus efficace des ressources, l'élimination de tâches superflues ou une plus grande fiabilité des services informatiques, et expliquer en quoi ils sont applicables à de nombreuses autres situations et peuvent profiter à l'ensemble de l'entreprise.

En clair, vous devez annoncer en quoi ITIL résoudra des problèmes de l'entreprise et contribuera directement à ses revenus et à ses marges.

Identifier les sponsors

Sensibiliser les cadres dirigeants implique d'apporter une description des avantages stratégiques, tactiques et opérationnels d'ITIL en termes économiques, organisationnels et métier. Il faut montrer à ces cadres comment ITIL peut aider l'organisation à livrer des produits informatiques et des services à un taux optimum et aux dépenses justifiables.

Il est très important d'inclure également les personnes réticentes ou sceptiques dans cette approche.

« L'avion ITIL » ne décollera pas avant que chacun des directeurs ou des responsables de département ne soit à bord. Si vous ne les incluez pas au projet, ils auront une occasion de ne pas contribuer et donc de peser sur ses résultats.

Il est important de comprendre que les processus d'ITIL ne représentent pas la solution miracle qui changera une infrastructure informatique défaillante en un système efficace en une nuit. Récolter des résultats va demander du temps, une planification et l'engagement des équipes. L'implication de certaines personnes clés de l'organisation est critique.

Un des facteurs clés de succès dans la mise en place d'ITIL consiste à prendre du temps pour mettre en place un haut niveau d'engagement au travers de l'organisation.

Vendre à la direction

Il apparaît désormais que la direction de l'entreprise demande fréquemment le développement d'une relation contractuelle entre les DSI et les autres directions. Cette tendance est couplée à une industrialisation des processus de production et à un mouvement d'externalisation de plus en plus affirmé. Cet alignement de l'organisation de la DSI sur les objectifs stratégiques de l'entreprise est-il une solution permettant la maîtrise des coûts informatiques ?

En clair, le modèle ITIL apporte-t-il une réponse à ces attentes ?

Il faut bien comprendre qu'ITIL est un sujet qui doit être traité par la direction informatique. En effet, pour qu'elle parvienne à aligner ses services sur les besoins de l'entreprise, il est indispensable de prendre en compte certains points indirects comme la stratégie de l'entreprise ou sa politique commerciale. Cependant, il est clair que les directions métier ne conduiront pas un projet ITIL et son adoption dans l'entreprise. Elles ont d'autres choses à faire... Il incombe donc à la DSI de communiquer, de convaincre et de justifier ses plans.

Comment vendre ITIL à la direction ?

Nous savons désormais que le référentiel ITIL est une bonne chose pour l'activité de l'entreprise... Malheureusement, le reste de l'entreprise ne le sait pas. En effet, ITIL reste avant toute chose un ensemble de processus lié à l'activité de la direction informatique, et reste donc assez obscur pour les différentes entités de l'entreprise.

Nous savons également que cette mise en œuvre va représenter un investissement en moyens, en temps, en personnes et en produits. Pour ces

raisons, il est indispensable de justifier et donc de vendre le projet ITIL à la direction de l'entreprise.

Apprendre à vendre ITIL

Pendant de nombreuses années, tout ce que l'informatique devait faire, c'était répondre aux demandes, et l'entreprise payait la facture. C'est une entente un peu bancale si l'on considère le fait que les autres départements doivent justifier leur activité et leurs projets.

Ceci implique que la seule façon de réussir à vendre ITIL à la direction est d'apprendre à vendre !

Vendre ITIL correspond à expliquer en quoi les optimisations apportées au fonctionnement de la DSI feront certainement gagner en performance informatique, ce qui à terme peut améliorer la performance globale de l'entreprise. Malheureusement, ce lien dans la compréhension entre la vision métier et celle de l'informatique est l'endroit où se produit généralement la cassure. Chacun des deux mondes a du mal à appréhender la perspective de l'autre. Alors, comment identifier les avantages que l'informatique apporte à l'entreprise dans le but de promouvoir l'utilisation d'ITIL dans le reste de l'entreprise ?

Identifier les acteurs

Dans plusieurs livres ITIL, la notion de « partie prenante » occupe une place significative dans le contenu. Le concept y est détaillé et est utilisé pour définir les différents acteurs internes ou externes à une entreprise concernés par son bon fonctionnement.

On peut alors considérer que cette partie prenante (*stakeholder* en anglais) est composée des :

- acteurs internes :
 - dirigeants ;
 - salariés ;
 - employés.
- acteurs externes :
 - clients, fournisseurs ;
 - actionnaires et investisseurs ;
 - organismes de régulation (administrations et collectivités territoriales) ;
 - Chambre de commerce et d'industrie (CCI) ;
 - intermédiaires de financement (banques, gérants de fonds...) ;
 - compagnie d'assurances ;
 - citoyens riverains de l'entreprise.

Dans le cas qui nous intéresse, cet acteur peut être n'importe quel individu ou groupe dépositaire d'un intérêt particulier dans l'informatique ou dans

Aucune direction marketing digne de ce nom ne présente un nouveau produit sans une analyse de marché et une planification formelle décrivant une étude de coûts, les bénéfices potentiels tout en s'adaptant aux besoins du marché. Enfin, ce projet est présenté et soutenu en termes métier que les représentants des autres directions comprennent.

le programme d'amélioration continue des services (CSIP). Vous connaissez certainement les acteurs (parties prenantes) classiques de l'informatique, mais avez-vous identifié les différents acteurs situés à l'extérieur de la DSi et présents dans les autres directions de l'entreprise ? Il s'agit évidemment de connaître les rôles et responsabilités des cadres dirigeants de l'entreprise, des multiples clients internes et des utilisateurs.

Maintenant, avez-vous également considéré les parties prenantes de la DSi situées à l'extérieur de la société, par exemple les fournisseurs, les concurrents, les administrations et autres organismes de régulation ?

Enfin, vous pensez généralement en premier aux acteurs ayant un impact positif sur la DSi. Cependant, vous devez aussi y inclure les autres, c'est-à-dire envisager le concept de parties prenantes en réunissant tous les acteurs internes et externes à l'informatique et à la société, qu'ils aient un impact positif ou négatif sur votre activité.

C'est dans la compréhension et la documentation de ces parties prenantes que vous trouverez les arguments les plus efficaces pour la promotion d'ITIL auprès de la direction. Vous constaterez probablement que les alliés les plus puissants pour justifier ITIL ne sont pas à l'intérieur de la DSi, ou même à l'intérieur de la société. Par ailleurs, vous verrez également que leur impact ne sera pas toujours positif.

Comme point de départ de la promotion du référentiel ITIL vers la direction de l'entreprise, voici un plan en 7 points que vous pouvez commencer à mettre en œuvre dès aujourd'hui.

1. Identifier le métier de l'entreprise et ses influences

La première étape consiste à identifier les éléments métier et les critères économiques qui influencent votre entreprise. Ces influences métier ou « leviers métier » (en anglais *business drivers*) correspondent aux influences externes ou internes qui touchent significativement les projets et les objectifs de l'entreprise. Dans le cas qui nous intéresse, il ne s'agit bien évidemment pas de repérer les éléments liés à l'informatique comme les différentes technologies utilisées, mais bien de comprendre les raisons de l'existence de l'entreprise et de sa principale activité, c'est-à-dire comprendre son métier !

Le fait d'actionner le levier correspond ici à l'atteinte des objectifs métier qui influencent l'activité de l'entreprise. Ne pas activer le levier revient donc à dire que l'entreprise n'a pas réussi à répondre aux attentes d'au moins un acteur « partie prenante » de son activité.

N'oubliez pas d'inclure les facteurs internes et externes, mais également les aspects positifs et négatifs qui affectent votre organisation. Par exemple, les règlements et les obligations légales sont des critères qui peuvent influencer largement le fonctionnement de l'entreprise. La concurrence est également un aspect important qui affecte directement les sociétés qui

vendent des produits (c'est-à-dire à peu près toutes !). La question ici sera de savoir s'il s'agit d'un aspect positif ou négatif...

D'un point de vue pratique, on utilisera un tableau à huit colonnes. Sur chaque ligne, vous inscrivez l'aspect ou l'élément qui influence le métier dans la première colonne. Notez que chaque acteur ou « partie prenante » a des raisons différentes de participer à la vie de l'entreprise et envisage des résultats sous un angle qui lui est propre. En conséquence, il est plus que probable que chaque niveau hiérarchique envisagera un même aspect ou une même influence avec une vision et des attentes différentes.

2. Identifier le responsable du levier

Une fois que vous connaissez les éléments susceptibles d'influencer l'activité de l'entreprise, ces fameux « leviers métier », essayez d'assigner le titre ou le rôle de la personne de plus haut niveau en tant que responsable de chacun de ces leviers. Par exemple, si l'un de ces éléments est en relation avec certaines attentes des actionnaires comme la communication des résultats de l'entreprise, le PDG en est clairement responsable et « possède » ce levier. Dans un autre exemple, si l'élément important correspond à la conformité d'un produit à un cahier des charges ou à une législation particulière, le responsable qualité ou le responsable de la production industrielle se verra attribuer le levier. Dans ce cas, inscrivez le titre ou le rôle de propriétaire de l'élément en question dans la seconde colonne, puis inscrivez le nom du propriétaire dans la troisième colonne.

3. Identifier les prérequis de l'audit et du contrôle

Une fois que vous aurez inscrit plusieurs des éléments qui influencent les affaires de l'entreprise ainsi que les acteurs qui en sont responsables, examinez comment votre société mesure l'accomplissement des objectifs qui permettent d'actionner les leviers en question. En clair, comment l'entreprise évalue-t-elle sa capacité à répondre aux questions posées par les actionnaires, les salariés, les organismes de régulation, et bien évidemment le marché ?

Chaque activité économique a ses propres « leviers métier » comme la conformité à une norme imposée par un organisme de régulation ou d'audit. Il peut s'agir d'obligations financières et comptables, de contraintes ou de normes de fabrication ou encore d'attentes du public et des clients potentiels. Dans tous les cas, inscrivez ces prérequis dans la dernière colonne du tableau.

Votre tableau présente désormais une vision globale des éléments critiques ou qui influencent fortement l'activité de l'entreprise. Il indique également les différentes personnes responsables des leviers et comment ces personnes mesureront l'accomplissement de leurs actions, c'est-à-dire comment savoir si les leviers sont activés ou non.

4. Identifier les liens entre les acteurs

Après avoir identifié les différents acteurs et autres parties prenantes dans l'activité de l'entreprise, essayez de les rassembler par groupes d'intérêt commun. Votre but est d'identifier les rapports entre les acteurs pour repérer les rôles et les personnes clés.

Le référentiel ITIL décrit plusieurs rôles incluant l'avocat du changement (*change advocate*), le parrain du changement (*change sponsor*), l'agent du changement (*change agent*) et la cible du changement (*change recipient*) :

- avocat du changement (AVC) : personne responsable du levier métier et cautionnant activement le changement ;
- parrain du changement (PAC) : personne patronnant le changement ;
- agent du changement (AGC) : personne menant le changement ;
- bénéficiaire du changement (BEC) : personnes affectées par le changement.

L'utilisation du mot « changement » dans ce contexte ne représente pas la demande du changement (RFC), mais plutôt le changement de mentalité ou les activités nécessaires à la motivation du département informatique.

Pour compléter le tableau, nommez les en-têtes des colonnes cinq à sept en tant que AVC, PAC, AGC et BEC.

5. Créer une carte des acteurs

Une fois que vous connaissez ce qui motive votre société, qui sont les responsables et comment ils mesurent leur succès, vous pouvez commencer à vendre la valeur d'ITIL.

Dessinez un diagramme « organisationnel » des acteurs avec leurs rapports réels, indépendamment des liens hiérarchiques.

Par exemple, un directeur peut avoir plusieurs responsables sous ses ordres sur un organigramme traditionnel ; cependant, placer son assistant(e) peut être plus pertinent ! Vous devez comprendre la vraie dynamique de l'organisation pour vendre ITIL au sommet.

6. Traduire en termes métier

L'étape finale consiste à traduire les activités d'ITIL dans des termes métier. C'est le moment où vous apprécierez de disposer de votre carte des acteurs et de votre tableau des leviers, des responsabilités et des rôles, car cette partie est certainement la plus difficile.

Par exemple, imaginons que vous deviez convaincre le directeur financier de la nécessité d'acheter un logiciel de gestion des incidents. Vous pourriez essayer de justifier cette dépense en termes informatiques en invoquant uniquement vos besoins. Cependant, équipé de votre carte et de votre tableau, vous savez que le directeur financier est responsable avec le PDG des audits financiers imposés, comme Sarbanes-Oxley. Vous savez que les auditeurs utiliseront certainement les outils du système d'information et que certains

prérequis de ces audits incluent la disponibilité et le suivi de ce système. Donc, vous placez le logiciel de gestion des incidents comme un investissement nécessaire au respect des obligations légales de ce type d'audit.

7. Boucler et relancer le cycle

Fidèle aux principes de Deming, il convient maintenant de réaliser des itérations régulières pour améliorer cette carte et ce tableau. Au cours des cycles, exécuter ce processus d'identification des parties prenantes va permettre de préciser les rôles, les personnes, les prescripteurs et les leviers métier qui formeront la carte de chaque engagement majeur de la direction informatique.

À terme, vous réussirez à aligner vos objectifs informatiques autour des besoins des acteurs en utilisant des termes qu'ils comprennent. Pour cela, abstenez-vous de placer le problème sur un plan technique et concentrez-vous sur les choses mesurables dont l'acteur est responsable.

Enfin, communiquez et produisez des rapports qui utilisent des termes et des expressions qui lient vos besoins à ceux des parties prenantes. En effet, ce que vous obtenez en aidant ces acteurs c'est de les aider à réaliser leurs objectifs métier par vos objectifs informatiques.

Cette approche peut ressembler au bon sens, mais comme en toutes choses, bien y réfléchir et planifier ses actions à l'avance permet d'obtenir des bénéfices plus cohérents. Pour enfoncer le clou, les étapes précédentes sont celles que l'on retrouve dans le plan d'amélioration continue des services (CSIP).

Si un tel plan n'est pas déjà en place, vous devriez penser à en préparer un. Une telle carte n'est bien sûr pas la justification de l'adoption d'ITIL, mais vous fournit une planification pour y parvenir. En utilisant cette carte des parties prenantes, vous pouvez planifier vos actions, décider de qui approcher, dans quel ordre et ce que vous direz et ferez à chaque étape.

Il y a encore beaucoup à faire si vous souhaitez vendre ITIL à la direction, mais ces sept étapes représentent un bon point de départ. Cet exemple se concentre sur la motivation et l'engagement des acteurs, mais vous pouvez utiliser la même approche pour n'importe quel objectif ou activité. Cette méthode vous donne des pistes dans la promotion d'ITIL.

Enfin, il n'est pas inutile de signaler qu'il existe un autre avantage réel à tout ce travail. La prochaine fois que vous vous trouverez en présence d'un de ces acteurs de l'entreprise, vous serez capable de communiquer avec lui en utilisant des termes qu'il comprend et qui le touchent directement.

Vendre aux équipes

Comment présenter un modèle dont on sait pertinemment qu'il peut être perçu comme une mode, un modèle bureaucratique ou une perte de temps et d'argent... voire les trois à la fois ?

Cette première perception, souvent négative, explique également pourquoi certaines personnes rejettent le modèle avant même de savoir ce qu'il recouvre.

Vendre aux équipes internes revient souvent à leur montrer en quoi ITIL n'est rien d'autre que ce qu'elles pratiquent souvent depuis des années de manière informelle et souvent non structurée. À l'instar de monsieur Jourdain, ces personnes font de l'ITIL sans le savoir.

En tant que consultant/formateur, j'ai eu, à plusieurs reprises, la joie de voir des visages sombres s'éclairer à mesure qu'ils découvraient que l'adoption d'ITIL ne représentait pas une révolution si importante, mais plus la professionnalisation et l'industrialisation de certaines de leurs pratiques. La crainte du changement laisse alors rapidement la place à l'acceptation. Bien sûr, tout cela n'ira pas sans quelques concessions, et les bonnes pratiques de l'un sont parfois les repoussoirs de l'autre. Néanmoins, le « bon sens » véhiculé par le modèle finit généralement par emporter les décisions. Cependant, tout ceci n'est évidemment possible que par le biais des séances de sensibilisation et de formation que doivent impérativement suivre les acteurs du projet.

Présenter ITIL autrement

J'en ai parlé au début de ce livre, faire la promotion d'ITIL dans une entreprise passe inéluctablement par une sensibilisation des équipes, puis une formation et parfois la certification de certains. En tant que formateur ITIL, j'ai eu l'occasion de rencontrer des personnes qui, dès le départ, m'annonçaient être réfractaires au contenu supposé de la session. La formation classique est basée sur une série de diapositives que l'on enchaîne sur un rythme plus ou moins rapide. Aidés d'un support de cours papier, les stagiaires peuvent suivre la présentation sans implication personnelle, et donc sans réel enthousiasme. Bien sûr, certaines formations incluent des études de cas issues de situations réelles en entreprise, mais globalement, cela reste souvent assez éloigné des attentes des participants. Certains arrivent dans ces formations en étant contraints et forcés et envisagent déjà de passer ces quelques jours en bâillant.

Le référentiel ITIL est parfois complexe à expliquer lorsque le public n'est pas acquis à la cause. Selon les auditeurs, plusieurs cas se présentent :

- Ils ne sont pas concernés directement par le référentiel.
- Ils ne comprennent pas l'intérêt d'un nouveau modèle.
- Ils ne comprennent pas l'intérêt de ce modèle.
- Ils sont rebutés à l'avance par l'arrivée d'un nouveau modèle.
- Un mélange des raisons évoquées précédemment.

La complexité et le côté conceptuel du modèle rendent parfois difficile la sensibilisation à ITIL et peuvent même provoquer une résistance à son

adoption en dehors de la sphère d'influence de la DSI. Selon le cabinet d'études Forrester, la réticence des clients internes de la DSI devant ce modèle est l'une des raisons les plus souvent invoquées pour le rejet d'ITIL.

Alors, avec un modèle ITIL difficile à promouvoir et ces concepts complexes à appréhender, comment parvenir à faire passer le message ?

Une solution alternative amusante est proposée par trois organismes de formation. Ces trois sociétés présentent des jeux de simulation dont le but est de démontrer la valeur du modèle de processus ITIL. Et il y en a pour tous les goûts. On trouve notamment une simulation d'aéroports, un voyage dans l'espace ou une course de formule 1.

Pour avoir participé à certaines de ces sessions en tant que stagiaire puis en tant qu'instructeur, je dois avouer que le concept est réellement au point. J'ai eu l'occasion de voir des groupes entiers de participants réticents se transformer au cours des simulations en joueurs amusés, puis en auditeurs attentifs et enfin en stagiaires impliqués.

La situation la plus efficace semble même être celle où se côtoient des membres de la DSI et d'autres directions plus fonctionnelles, et surtout lorsque les niveaux hiérarchiques sont également mélangés.

L'intérêt de ce type d'approche est que la personne est confrontée à un cas concret qui peut éventuellement sortir de la vie de tous les jours, mais qu'elle perçoit comme réel. Très rapidement, le stagiaire envisage les situations rencontrées par le biais de leurs implications sur le fonctionnement du jeu, et donc de l'enjeu global. Ceci implique que la découverte des processus présentés va se faire par l'expérience et non par le cours magistral. Ensuite, le formateur n'a plus qu'à « reprendre la main » pour transmettre la théorie et le contenu plus conceptuel d'ITIL, mais en ayant des exemples concrets à proposer à ses stagiaires.

Conclusion

Du bon sens...

L'implantation d'un modèle de type ITIL dans une entreprise n'est pas un petit projet. Même si les processus ITIL ne représentent que rarement des phases à plein temps, il faut envisager une durée allant de quelques mois à quelques années pour les plus gros projets.

Il ne s'agit pas non plus d'un produit que l'on peut acheter sur une étagère. Même si ce genre de solution va aider par sa puissance de traitement et de synthèse, il n'en reste pas moins que seule la mise en place de processus « audités et auditables » par des personnes formées à l'amélioration permanente de ces processus peut permettre la réussite d'un tel projet. Il est indispensable de former les personnes qui interviendront dans l'élaboration puis l'exploitation des différents processus.

En clair, l'informatique ne change rien à ce qui ne fonctionne déjà pas...

Enfin, il est impensable d'espérer gagner de l'argent immédiatement avec ITIL. La simple mise en route des processus ITIL ou l'optimisation d'un processus existant demande déjà un investissement en temps incompatible avec des gains immédiats. Les réductions de coût, lorsqu'elles se produisent, ne peuvent se présenter qu'après plusieurs mois de projet, et en tout état de cause, ne peuvent intervenir avant d'avoir franchi certaines étapes de la maturation des services informatiques de l'entreprise. En revanche, ces réductions sont réelles lorsque le projet est mené à son terme et surtout lorsque le soutien de la direction de l'entreprise est acquis au projet.

PARTIE V

Annexes

Cette partie présente un ensemble de ressources vous permettant d'approfondir votre connaissance des processus ITIL.

Vous y trouverez :

- un examen blanc de passage de la certification de base d'ITIL ;
- un glossaire français des termes ITIL ;
- une équivalence des termes anglais/français ;
- une description de la norme ISO 20000 ;
- une bibliographie non exhaustive incluant des livres et des sites Internets consacrés à ITIL.

Certification ITIL

La formation aux concepts d'ITIL permet de rencontrer d'autres utilisateurs d'ITIL afin de confronter les différentes expériences. Elle convient à tous les types de postes, du technicien de maintenance jusqu'au directeur des systèmes d'information, et à tous les niveaux de connaissance, depuis des populations ne connaissant pas ITIL jusqu'à des populations déjà sensibilisées aux bénéfices de ce référentiel. La certification est l'aboutissement de cette formation et permet de garantir un engagement et une compréhension des principes d'ITIL.

Organismes

OGC

Conçu et développé à l'origine par le CCTA (Central Computer & Telecommunications Agency), ITIL appartient aujourd'hui à l'Office gouvernemental du commerce anglais (OGC) dont l'objectif est l'évolution, la diffusion et la promotion d'ITIL dans le monde. Pour atteindre ce but, l'OGC s'est associé avec un certain nombre d'entreprises, d'organismes et d'associations. Parmi ces organisations, certaines sont davantage orientées vers le conseil et l'assistance, d'autres vers la formation et la certification autour des concepts d'ITIL.

itSMF

Le forum itSMF est une association indépendante d'utilisateurs, internationalement reconnue, dédiée à la direction des services informatiques. Elle appartient et fonctionne uniquement grâce aux adhérents. Son rôle est de promouvoir l'échange d'informations et d'expériences pour permettre aux directions informatiques d'améliorer les services qu'elles fournissent.

Ses membres organisent des séminaires, des conférences, des soirées à thèmes, et autres événements concernant des sujets courants des directions informatiques.

L'association itSMF publie également un bulletin d'informations régulier et gère un site Internet permettant le partage d'informations.

EXIN et ISEB

L'EXIN au Pays-Bas et l'ISEB en Grande-Bretagne sont des instituts d'examineurs indépendants, gérant le processus de certification professionnelle en Europe. Ce sont organisations à but non lucratif, qui coopèrent afin d'offrir une gamme complète de qualifications à trois niveaux. Ces certifications ont été mises en place en collaboration avec l'OGC et itSMF.

Certifications

Niveau de base, les fondations : « Foundation Certificate in IT Service Management »

L'objectif de la formation d'une durée de 2 à 3 jours, puis de la certification, est d'initier les participants à la gestion des services informatiques à un niveau suffisant pour leur permettre d'exprimer le but et les objectifs de cette gestion. La formation porte sur les dix processus ITIL et s'adresse à tout public. Si aucune connaissance préalable n'est officiellement nécessaire, il paraît important que le candidat dispose de certaines connaissances et d'une expérience élémentaire dans le domaine de l'informatique, des moyens d'informatisation et de leur gestion.

Cette certification démontre que la personne dispose d'une compréhension de base des principes d'ITIL, c'est-à-dire de la terminologie, des fonctions du centre de services, des dix processus ITIL, et de leurs relations internes ou avec le métier. Elle concerne essentiellement les personnes qui s'intéressent à ITIL ou qui doivent travailler dans le contexte ITIL.

La certification se déroule sous la forme d'un examen en français (ou en anglais) d'une durée d'une heure. Cet examen a lieu après avoir suivi une formation et est composé d'un questionnaire à choix multiples de 40 questions portant sur tous les processus ITIL. L'utilisation de documents, calculatrice téléphone, ordinateur et autres n'est évidemment pas autorisée. La certification est attribuée lorsque le stagiaire obtient 65 % de bonnes réponses, ce qui équivaut donc à 26 bonnes réponses dans tous les domaines de la gestion des services informatiques.

Dans le cas d'un examen sur ordinateur, un résultat préliminaire est donné immédiatement et sera ensuite confirmé par courrier. En revanche, dans le cas d'un questionnaire papier, les examens sont envoyés sur le site de correction (Grande-Bretagne ou Pays-Bas) et un délai de trois à quatre semaines sera nécessaire avant d'obtenir les résultats... ainsi qu'une éventuelle épingle verte (pin's) du plus bel effet !

Niveau de praticien expert : « Practitioner Certificate in IT Service Management »

À la différence de la certification des fondations, la formation puis la certification de praticien expert, se focalise sur un processus précis d'ITIL parmi les dix existants. L'objectif de cette formation, puis de la certification, est donc de plonger dans les détails de l'implantation et de la gestion d'un des processus de la gestion des services informatiques. Tous les processus ITIL sont disponibles en certification de praticien expert, mais malheureusement, les organismes de formations ne dispensent pas systématiquement l'ensemble des cours. Vous devrez certainement vous renseigner sur les processus disponibles afin de choisir le centre de formation adapté. Les pré-requis sont également différents, puisqu'il est nécessaire pour accéder à cette formation, d'obtenir au préalable la certification de base et de posséder une expérience professionnelle de deux à trois ans dans la gestion du processus en question.

Cette certification atteste que la personne dispose d'une compréhension approfondie du processus ITIL et est capable de gérer et d'implémenter totalement le processus au sein de son organisation. Elle concerne essentiellement les responsables de processus ITIL, les consultants et plus généralement toute personne intéressée par les détails du référentiel ITIL.

La certification se présente sous la forme d'un examen en anglais d'une durée de deux heures, composé d'un questionnaire à choix multiples de 40 questions qui portent sur le processus ITIL choisi. La certification est attribuée lorsque le stagiaire obtient 60 % de bonnes réponses, ce qui équivaut à 24 réponses correctes dans le domaine ITIL considéré.

Niveau responsable/gestionnaire : « Service Delivery certificate » et le « Service Support Certificate »

Cette certification est évidemment la plus complète et la plus poussée. Sa particularité est de couvrir tous les processus ITIL à l'instar de la certification de base. Par ailleurs, elle traite chacun des processus en profondeur à l'image de la certification du praticien expert. L'objectif de cette formation est bien de couvrir l'ensemble d'ITIL en plongeant dans les détails de l'implantation et de la gestion de tous les processus de la gestion des services informatiques. On le comprend aisément, les pré-requis sont ici très forts, puisqu'il

est nécessaire pour accéder à cette formation, d'obtenir au préalable la certification de base et de posséder une expérience professionnelle d'au moins cinq ans dans la gestion des services informatiques et de deux ans en tant que responsable.

Cette certification atteste que la personne dispose d'une compréhension approfondie de l'ensemble du référentiel ITIL et est capable de gérer un service informatique en utilisant les meilleures pratiques proposées, et d'implémenter totalement, puis d'améliorer continuellement les processus au sein de son organisation. Elle concerne essentiellement les responsables informatiques, les consultants, et les formateurs.

La certification se déroule sous la forme de deux examens en anglais, d'une durée de trois heures chacun et composés d'études de cas avec cinq questions ouvertes par examen, auxquelles il faut répondre sous la forme d'essais rédigés en anglais et qui portent sur tous les processus ITIL.

La certification est attribuée lorsque le participant obtient au moins 50 % de réussite à l'évaluation des compétences de direction dans un premier temps, et au moins 50 % de réussite à l'examen de soutien des services et 50 % de réussite à l'examen de fourniture des services, dans un second temps. L'obtention de ces deux certificats donne automatiquement la certification « Manager's certificate in IT Service Management ».

Exemple de certification de base

Chaque question de ce questionnaire est suivie de quatre propositions (A, B, C et D). À chacune de ces questions ne correspond qu'**une seule et unique réponse**.

Si vous souhaitez vous replonger dans les conditions de l'examen, ranger vos livres, documentations et brouillons, et chronométrez-vous durant l'évaluation. La durée maximum de l'examen est de 1 heure.

Questionnaire

1. Laquelle de ces méthodes n'est pas utilisée dans la gestion des capacités ?

- A – Le dimensionnement des applications.
- B – La gestion de la demande.
- C – L'équilibrage de charge.
- D – L'analyse des causes d'origine.

2. Laquelle des affirmations suivantes est de la responsabilité d'un centre de services ?

- A - Tenir les clients informés des progrès des incidents.
- B - Chercher les causes des incidents.

C - Effectuer des changements pour corriger les incidents.

D - Calculer le coût du traitement des incidents.

3. Pour procéder au déploiement d'un nouveau logiciel, quel traitement doit-on utiliser pour assurer la mise à jour de la CMDB ?

A – Le changement de gestion.

B – La gestion de la configuration.

C – La mise à jour de la configuration.

D – La gestion des niveaux de service.

4. Observez la liste ci-dessous :

1) Dimensionner les applications.

a) Gestion de la capacité.

2) Budgérer.

b) Gestion de la disponibilité.

3) Sécurité.

c) Gestion de la continuité.

4) Analyser l'impact sur l'activité.

d) Gestion financière.

Lequel de ces appariements est exact ?

A – 1b, 2c, 3d, 4a.

B – 1a, 2d, 3b, 4c.

C – 1c, 2d, 3c, 4a.

D – 1b, 2c, 3a, 4d.

5. Dans quel processus une configuration de base (*baseline*) est-elle utilisée ?

A – La gestion du changement.

B – La gestion des problèmes.

C – La gestion de la configuration.

D – Le centre de services.

6. L'analyse de Kepner et Tregoe est une technique utilisée pour ?

A – La gestion de la capacité.

B – La gestion financière des services informatiques.

C – La gestion des niveaux de service.

D – La gestion des problèmes.

7. Laquelle de ces mesures sera probablement la moins pertinente pour juger de l'efficacité du processus de gestion des changements ?

A – Le nombre total de changements effectués en un mois.

B – Le pourcentage des changements effectués dans un temps imparti.

C – Le pourcentage des changements qui doivent être recommandés.

D – La moyenne des coûts de changements.

8. Considérez les déclarations suivantes relatives à une gestion de la disponibilité efficace :

- A – La maintenabilité peut aider à éviter l'apparition de défaillance, permettant ainsi une économie financière potentielle et améliorant les niveaux de service.
- B – L'aspect sécurité de la gestion de la disponibilité repose sur trois aspects : confidentialité, intégrité et automatisation.

Laquelle de ces déclarations est correcte ?

- A – Les deux.
- B – Seulement la première.
- C – Aucune des deux.
- D – Seulement la seconde.

9. Considérez les déclarations suivantes :

- A – Facturer est obligatoire pour toutes les organisations.
- B – Budgéter permet de calculer les dépenses de l'année précédente, et de déterminer avec précision où l'argent a été alloué.

Laquelle de ces déclarations est exacte ?

- A – Les deux.
- B – Aucune des deux.
- C – Seulement la première.
- D – Seulement la dernière.

10. Laquelle de ces séquences est la plus susceptible de se produire ?

- A – Incident – Problème – Erreur connue – Changement.
- B – Problème – Incident – Erreur connue – Changement.
- C – Changement – Problème – Erreur connue – Incident.
- D – Changement – Incident – Problème – Erreur connue.

11. La gestion de la capacité est un arbitrage entre :

- A – Le coût face à la demande et la capacité face à la fourniture.
- B – La capacité face à la disponibilité et la fourniture face aux ventes.
- C – Le coût face à la capacité et la demande face à la fourniture.
- D – La capacité face au risque et la planification face à la ressource.

12. Considérez les déclarations suivantes :

- A – Les membres du CAB sont toujours membres du CAB/EC.
- B – Le directeur du changement est le seul membre permanent du CAB/EC.
- C – Le CAB voit et approuve toutes les RFC.

Laquelle de ces déclarations est exacte ?

- A – Seule la réponse 3 est correcte.
- B – Les réponses 2 et 3 sont correctes.
- C – Les réponses 1 et 3 sont correctes.
- D - Seule la réponse 2 est correcte.

13. Selon ITIL ...

- A – La gestion des problèmes est sous le contrôle de la gestion des incidents.
- B – La gestion du changement est sous le contrôle de la gestion de la configuration.
- C – La gestion des mises à jour est sous le contrôle de la gestion du changement.
- D – La gestion des niveaux de service est sous contrôle de la gestion de la continuité de service.

14. Le principal objectif du processus de gestion de la disponibilité est de...

- A – Délivrer 100 % de disponibilité au métier.
- B – Négocier avec les clients les besoins du métier en disponibilité.
- C – S'assurer que les systèmes ont la capacité suffisante pour assurer la disponibilité requise.
- D – Procurer un niveau de disponibilité à un coût justifié afin de satisfaire les objectifs du métier.

15. Parmi les éléments suivants, lesquels sont évalués dans un modèle d'évaluation des risques ayant pour but de découvrir les contre-mesures requises ?

- A – Capacité, risque, et impact.
- B – Actifs, services, et systèmes.
- C – Confidentialité, intégrité et disponibilité.
- D – Actifs, menaces et vulnérabilités.

16. Par quel processus la DSL et le DHS sont-ils contrôlés ?

- A – La gestion des mises à jour.
- B – La gestion des changements.
- C – La gestion des niveaux de service.
- D – La gestion des configurations.

17. Dans la gestion des incidents, la priorité est généralement la combinaison de...

- A – L'impact et la disponibilité.
- B – L'urgence et le temps enregistré.

C – L'urgence et l'impact.

D – La charge de travail et les ressources disponibles.

18. Les coûts indirects sont composés de...

A – Matériels et logiciels.

B – Production et ventes.

C – Coûts directs et éléments de coûts.

D – Frais généraux absorbés et non absorbés.

19. Lequel de ces éléments n'est pas un CI de PC ?

A – L'unité centrale.

B – la distribution logicielle.

C – Le numéro de série.

D – L'écran.

20. Laquelle de ces propositions n'est pas un processus de support des services ?

A – Le centre de services.

B – La gestion des problèmes.

C – La gestion des incidents.

D – La gestion des changements.

21. Observez les listes suivantes :

1) CMDB. a) Gestion des changements.

2) CFIA. b) Gestion des niveaux de service.

3) MTTR. c) Gestion des configurations.

4) CAB. d) Gestion de la disponibilité.

Lequel de ces appariements est correct ?

A – 1b, 2d, 3c, 4a.

B – 1a, 2d, 3b, 4c.

C – 1c, 2d, 3b, 4a.

D – 1b, 2c, 3a, 4d.

22. Laquelle de ces propositions n'est pas une option pour un type de centre de services ?

A – Local.

B – Global.

C – Mutualisé.

D – Virtuel.

23. Un niveau d'agrément opérationnel est...

- A – Un accord entre le service informatique et ses clients.
- B – Un contrat entre le service informatique et ses fournisseurs.
- C – Un accord entre les clients et les fournisseurs.
- D – Un accord entre les services informatiques internes.

24. Un redémarrage immédiat (à chaud) survient au bout de...

- A - 24 à 72 heures.
- B – Moins de 24 heures.
- C – Plus de 72 heures.
- D – Une semaine maximum.

25. Le centre de services a enregistré une demande d'installation de Windows® XP émanant du service financier. Quels sont les deux processus ITIL qui contrôleront et mettront en application la demande ?

- A – Le changement et la mise à jour.
- B – Le centre de services et la gestion des configurations.
- C – Le centre de services et la gestion des mises à jour.
- D – Les incidents et la gestion des changements.

26. Laquelle de ces propositions est gérée par le responsable des problèmes ?

- A – S'assurer que l'incident initial est enregistré.
- B – Monter la priorité d'un RFC pour résoudre un problème grave.
- C – Développer et maintenir un système de gestion d'erreur.
- D – Négocier l'alignement de ses objectifs avec les clients.

27. À quels processus d'ITIL les activités de planification, d'identification, de contrôle, d'enregistrements des états, de vérification et d'audit sont-elles liées ?

- A – Le centre de services.
- B – La gestion des configurations.
- C – La gestion des finances.
- D – La gestion des problèmes.

28. Un client voudrait savoir quelles sont les heures de disponibilité de l'application financière. Quel est le document susceptible de lui fournir cette information ?

- A – Le plan de capacité.
- B – Le plan de continuité d'activité.

- C – Le rapport du CAB.
- D – L'accord des niveaux de services.

29. Un incident c'est...

- A – La cause fondamentale inconnue.
- B – Un événement qui provoque une interruption dans un service.
- C – Quand la cause fondamentale sous-jacente est connue.
- D – Une demande de changement.

30. Une organisation informatique a décidé de facturer ses clients afin de récupérer ses coûts avec un profit de 5 % pour couvrir d'éventuelles dépenses futures. Laquelle de ces méthodes de rétablissement de coût est la plus appropriée pour cela ?

- A – Le coût.
- B – Le taux du marché.
- C – Le prix de détail.
- D – Le coût avec marge.

31. Qu'est ce qui décrit le mieux une mise à jour DELTA ?

- A – Les changements apportés aux CI depuis la dernière mise à jour.
- B – Tous les composants du logiciel sont mis à jour ensemble.
- C – Un groupe de mises à jour individuelles combinées ensemble.
- D – La quatrième mise à jour dans une série de mise à jour.

32. Qu'est ce qui ne peut pas être un gain lors de l'implantation de la gestion des capacités ?

- A – L'optimisation des équipements et l'élimination de la capacité inutile.
- B – La réduction de la fréquence et de la durée des pannes informatiques.
- C – Les dépenses sont reportées et les achats onéreux effectués dans l'urgence sont éliminés.
- D – La prévision des capacités nécessaires à l'organisation est plus adaptée et améliorée.

33. Quelle partie de la procédure de changement peut être omise au cours d'un changement d'urgence ?

- A – L'autorisation.
- B – Le test.
- C – L'implantation.
- D – L'analyse du changement.

34. Considérez les déclarations suivantes :

- A – Le plan de continuité du service informatique inclut le plan de continuité du métier.
- B – Le plan de continuité du service informatique assure la survie des activités métier en réduisant l'impact du désastre.
- C – Le plan de continuité du service informatique devrait être testé à la conception, après les principaux changements et au minimum tout les ans.

Laquelle de ces affirmations est vraie ?

- A – Toutes les trois
- B – Aucune des trois
- C – La première et la troisième seulement
- D – La deuxième et la troisième seulement

35. Lorsque l'on combine les rôles ensemble quelle combinaison devrait être évitée ?

- A – Le responsable du centre de services et des incidents.
- B – Le responsable des changements et des mises à jour.
- C – Le responsable des niveaux de service et des disponibilités.
- D – Le responsable des incidents et des problèmes.

36. Laquelle de ces propositions est une liste d'éléments de coûts typiques ?

- A – La capacité, la disponibilité, les équipements, le personnel, les frais généraux.
- B – Le matériel, le logiciel, le personnel, les locaux, les services externes, les transferts.
- C – Le capital, l'opérationnel, le direct, l'indirect, le fixe, le variable.
- D – Le matériel, le logiciel, le personnel, les systèmes, les véhicules, les réseaux.

37. Quel processus ITIL est considéré comme ayant une partie réactive et pro-active ?

- A – La gestion des niveaux de service.
- B – La continuité des services informatiques.
- C – La gestion des problèmes.
- D – La gestion des configurations.

38. Le centre de services a reçu les appels suivants : un utilisateur du département financier a un écran blanc ; le responsable ne peut pas accéder aux applications financières ;un autre utilisateur recherche

ses messages ; le directeur financier ne peut pas imprimer le rapport financier en cours. Qui doit établir le lien entre tous ces appels ?

- A – Le responsable des incidents.
- B – Le responsable des changements.
- C – Le responsable des problèmes.
- D – Le responsable des configurations.

39. Par quel processus sont habituellement employés les termes d'opérations « Big Bang » et « par phases »

- A – Le centre de services.
- B – La gestion des incidents.
- C – La gestion des finances.
- D – La gestion des mises à jour.

40. Observez ces affirmations :

- A – Valider l'organisation afin de prévoir les coûts requis au fonctionnement du service informatique.
- B – Réduire le risque de surcoût.
- C – S'assurer que les dépenses réelles correspondent aux prévisions.

Parmi les fonctions suivantes, quelle est celle la mieux décrite par les affirmations précédentes ?

- A – Imputer.
- B – Budgéter.
- C – Comptabiliser.
- D – Facturer.

Formulaire de réponse

Questions	Réponses			
	A	B	C	D
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				

Questions	Réponses			
	A	B	C	D
21				
22				
23				
24				
25				
26				
27				
28				
29				
30				
31				
32				
33				
34				
35				
36				
37				
38				
39				
40				

Avertissement

Les questions et réponses proposées ici sont uniquement données à titre indicatif afin d'évaluer votre compréhension et votre connaissance des processus ITIL. En aucun cas, cette évaluation ne reflète les difficultés que vous pourrez rencontrer dans la certification réelle. En conséquence, l'auteur ne prend aucun engagement sur votre éventuelle participation, ni sur votre réussite à l'examen.

Solutions du test

Questions	Réponses	Questions	Réponses
1	D	21	C
2	A	22	B
3	B	23	D
4	B	24	B
5	C	25	A
6	D	26	C
7	A	27	B
8	B	28	D
9	B	29	B
10	A	30	D
11	C	31	A
12	D	32	B
13	C	33	B
14	D	34	D
15	D	35	D
16	A	36	B
17	C	37	C
18	D	38	C
19	C	39	D
20	A	40	B

Glossaire

Vous retrouverez ici un ensemble de termes utilisés dans cet ouvrage. Classés par ordre alphabétique, vous trouverez également les acronymes, les sigles et les termes anglais utilisés dans l'abondante littérature d'ITIL que l'on retrouve sur Internet ou dans les ouvrages de l'OGC.

Termes français

Accord de niveaux d'exploitation. Déclinaison en termes technique de la convention de niveau de service signée par les utilisateurs et exprimant en particulier les ressources techniques et humaines à mettre en place.

Accord de niveaux de service. Document écrit qui définit des objectifs précis et spécifiques au service considéré. Il engage les deux parties (clients et fournisseurs) sur les niveaux à atteindre en termes de disponibilité, de capacité et coûts, et permet l'évaluation des performances de l'organisation informatique lors de la fourniture et le support de ce service.

Adaptabilité. Capacité d'un service à modifier son niveau de performance et de coûts lors d'un changement dans la demande ou dans l'infrastructure.

Alerte. Message émanant d'un système de surveillance automatique signalant qu'un seuil a été atteint, qu'une défaillance s'est produite ou est susceptible de se produire.

Amélioration continue. Principe selon lequel tous les aspects de la fourniture et du soutien des services sont régulièrement réévalués afin d'identifier les améliorations potentielles au niveau financier et en termes d'efficacité.

Amortissement. Mesure de la diminution de la valeur d'un actif au cours du temps d'un point de vue comptable, qu'elle soit causée par l'usure ou l'obsolescence.

Analyse d'impact. Identification des processus métier critiques et des pertes ou dommages potentiels pouvant être causés à l'entreprise suite à une perturbation de ces processus.

Analyse des pannes du système. Technique conçue pour fournir une approche structurée à l'identification des causes sous-jacentes d'interruption de service.

Analyse de risque. Identification de l'importance des composants de l'infrastructure (les éléments d'actifs), des menaces auxquelles ces composants pourraient être exposés, et de leur vulnérabilité face aux menaces identifiées.

Anomalie. Condition occasionnant l'impossibilité pour une unité fonctionnelle d'exécuter la fonction requise.

Assemblage. Étape finale dans la production d'une configuration utilisable à partir d'un ensemble d'éléments de configuration afin d'obtenir un paquet logiciel ou matériel à installer.

Assurance (assurance qualité). Validation de la qualité, de l'exactitude et de l'exhaustivité du plan de continuité d'activité.

Attribut. Caractéristique descriptive d'un élément de configuration enregistrée dans la base de données de la gestion des configurations (exemple : type de CI, marque ou modèle, fournisseur, etc.).

Audit. Processus d'inspection et de vérification, utilisé pour valider qu'une activité est effectuée selon un standard accepté ou selon la meilleure pratique reconnue.

Axé sur le client. Basé sur les objectifs du client.

Base de données de la gestion des configurations. Base de données regroupant les informations de configuration et d'historique de tous les éléments de configuration (CI) ainsi que les relations tissées entre ces CI.

Bibliothèque des logiciels définitifs. Zone de stockage physique où sont conservés tous les logiciels utilisés officiellement sous leur forme définitive, ainsi que les éléments de configuration associés, tels que les licences et les documentations.

Budgétisation. Cycle périodique de prévision, de négociation et de contrôle des dépenses de l'organisation informatique.

Calendrier des changements. Calendrier contenant les détails de tous les changements approuvés pour implémentation et leurs dates d'exécution proposées.

Calendrier de mise à jour. Document contenant les dates des déploiements des mises à jour dans l'environnement de production.

Capacité. Puissance, performance, débit, ou volume d'un composant ou de l'infrastructure.

Capitalisation. Augmentation du capital de l'entreprise suite à l'achat ou au développement d'un actif logiciel important afin de réduire l'impact de la dépense sur l'exercice financier.

Catalogue des services. Document produit par la direction informatique dans le but d'informer ses clients et ses utilisateurs sur les services et l'infrastructure disponibles.

Catégorie. Classification par groupe distinct des éléments de configuration, comme le matériel, les changement, les problèmes.

Catégorisation des incidents. Classification permettant de hiérarchiser les incidents.

Centre d'appel. Interface entre les utilisateurs et l'informatique dédiée à la réception des appels téléphoniques de demande d'assistance, de requêtes ou de plaintes.

Centre d'assistance/centre de services. Extension fonctionnelle du centre d'appel, le centre d'assistance ou centre de services remplit également un rôle de gestion des incidents en offrant une ressource technique de premier niveau, et prend en compte toutes les demandes, plaintes ou requêtes des utilisateurs.

Centre de coût. Mode d'organisation comptable dans laquelle une activité métier n'est perçue qu'au travers de ses dépenses.

Centre de profit. Mode d'organisation comptable dans laquelle une activité métier interne de l'entreprise est perçue comme une activité indépendante, dont les objectifs sont définis par la direction de l'entreprise mais qui est susceptible de réaliser des profits, même si ceux-ci se font aux détriments d'autres activités de l'entreprise.

Centre de recouvrement. Mode d'organisation comptable dans laquelle l'activité métier analyse ses coûts et les facture réellement ou fictivement dans le but de recouvrer et de justifier ses dépenses.

Chaîne de valeur. Succession d'activités qui crée un produit ou un service susceptible de générer une valeur marchande ou permettant à l'entreprise d'accroître son chiffre d'affaire.

Changement. Modification volontaire d'un élément de configuration ou d'un service de l'infrastructure dans le but de modifier son comportement, sa capacité ou son état.

Changement d'urgence. Modification d'un composant de l'infrastructure planifiée et mise en œuvre dans un délai très court, dans le but d'éviter un risque potentiel important ou d'en réduire l'impact pour le système d'information.

Changement standard. Modification fréquente connue et maîtrisée, disposant de procédures de mise en œuvre précises, ne nécessitant pas le passage devant le comité d'évaluation du changement.

Classification. Activité de regroupement des éléments de configuration (CI) par type (matériels, logiciels, procédures, documents, services externes).

Client. Personne qui paie pour l'obtention de services informatiques et qui en définit les objectifs, le niveau de capacité, de performance, de disponibilité et de coût. Il s'agit en général d'un responsable d'activité métier de l'entreprise qui est habilité à signer l'engagement de niveau de service (SLA).

Comité consultatif sur les changements. Groupe de personnes possédant les compétences et l'autorité nécessaires afin d'évaluer puis de valider les demandes de changement. Ce groupe est composé du responsable des changements qui le dirige systématiquement, et selon les cas, de représentants des clients et des utilisateurs, des représentants d'un fournisseur, de membres de la direction informatique et des éventuels responsables de plusieurs autres processus ITIL (finance, capacité, disponibilité, etc.).

Comité d'urgence des changements. Réunion d'urgence d'un comité consultatif des changements réduit aux membres indispensables à l'évaluation d'un changement urgent.

Comptabilité (des TIC). Ensemble des activités permettant à l'organisation informatique d'identifier, de classer et de justifier ses dépenses financières.

Configuration de base. Image figée de l'état d'un élément de configuration (CI) ou d'un ensemble de CI dans le but d'évaluer l'impact d'un changement sur l'infrastructure, ou de s'assurer que l'infrastructure peut être rétablie rapidement.

Contrat. Accord formel entre deux personnes morales, soumis aux contraintes légales en vigueur.

Contrat de sous-traitance. Contrat passé avec un fournisseur externe afin d'obtenir une prestation de services permettant la fourniture des services informatiques.

Contre-mesure. Action prise pour réduire le risque ou son impact sur le système d'information.

Contrôle des configurations. Activité qui s'assure que seuls les éléments de configuration (CI) autorisés et identifiables sont utilisés sur l'infrastructure informatique de l'entreprise.

Convivialité. Capacité d'un service, d'une application ou d'un matériel à être utilisé simplement, de façon intuitive et sans formation excessive.

Coût de transfert. Représente le coût des prestations fournies d'une division de l'entreprise à une autre.

Coût des services externes. Représente les coûts des services acquis aux fournisseurs externes.

Coût direct. Représente les coûts qui peuvent être totalement imputés à un client (exemple : application comptable imputée à la direction financière).

Coût fixe. Représente un coût qui ne varie pas avec le volume d'utilisation ou les évolutions de l'activité de l'entreprise.

Coût vindirect. Représente un coût qui ne peut pas être directement et complètement alloué à un seul client et dont la valeur doit donc être répartie entre les différents consommateurs (exemple : réseau local utilisé par l'ensemble de l'entreprise).

Coût marginal. Représente le coût de production d'une unité supplémentaire après la mise en place du système de production. Il comprend essentiellement les coûts de matière première, les coûts de main d'œuvre et le coût d'amortissement du système. L'intérêt de cette valeur est de démontrer que le coût de possession d'un équipement n'est pas simplement son coût d'achat, mais elle permet également de confirmer que le coût de production d'une unité diminue avec le volume produit.

Coût total de possession. Représente le coût cumulé de tous les éléments qui composent un service ou un équipement. Outre le prix d'achat initial, il comprend les coûts de personnel, l'entretien, la maintenance, les coûts de transfert, les matières premières consommables, etc.

Coût variable. Représente un coût qui évolue en fonction du volume d'utilisation d'un service, de matière première ou d'un produit.

Coût de fonctionnement (d'exploitation, de production, etc.). Représente les dépenses d'exploitation quotidienne d'une organisation dont les coûts en personnel, la maintenance du matériel et l'électricité.

Culture de service. Doctrine selon laquelle la satisfaction du client est la priorité la plus importante et que les activités mises en œuvre contribuent à ces objectifs.

Cycle de vie. Description des différentes étapes de la durée d'utilisation d'un produit, d'un service ou d'un processus.

Cycle de vie des incidents. Progression du statut d'un événement entraînant un dysfonctionnement du système d'information et passant par les états de l'apparition (de l'incident), de la détection, du diagnostic de l'origine, de la réparation ou du contournement de la défaillance, dans l'infrastructure opérationnelle et la restauration du service.

Cycle de vie des problèmes. Progression du statut de la cause d'une anomalie affectant le système d'information qui passe par l'identification de la cause, l'élaboration d'une solution permanente et la demande de changement éventuelle pour mettre en œuvre cette solution.

Déclenchement. Lancement par la direction générale de l'entreprise du plan de reprise d'activité suite à un sinistre.

Demande de changement. Proposition de modification de n'importe quel composant ou service de l'infrastructure informatique.

Demande de service. Demande de changement mineur n'affectant pas l'infrastructure et ne justifiant pas l'intervention du comité consultatif des changements, comme la modification d'un mot de passe ou l'installation d'un nouveau poste de travail.

Détection. Deuxième étape du cycle de vie d'un incident correspondant à la découverte de cet incident par l'équipe informatique ou le centre de service.

Diagnostic. Troisième étape du cycle de vie d'un incident pendant laquelle l'équipe informatique tente de d'identifier son 'origine'.

Dimensionnement d'application. Activité d'évaluation des ressources nécessaires à une nouvelle application, à l'ajout, ou à l'amélioration d'une application existante.

Disponibilité. Indique la capacité d'un système à remplir son rôle pendant un temps donné. Cette valeur s'exprime le plus souvent sous la forme d'un pourcentage de temps pendant lequel le système est disponible par rapport à l'horaire de service négocié lors du SLA.

Durée moyenne de réparation. Temps moyen écoulé entre l'instant où se produit l'incident et le moment où le service est rétabli.

Durée moyenne entre les défaillances. Temps moyen écoulé entre l'instant où le service est rétabli jusqu'au moment où une nouvelle défaillance se produit.

Durée moyenne entre les incidents affectant un système/service.

Temps moyen écoulé entre le début des différentes défaillances d'un système ou d'un service.

Élément de configuration. Représente n'importe quel composant de l'infrastructure informatique référencé dans la base de données des configurations (CMDB), y compris les matériels, les logiciels, les documentations ou les documents de l'organisation (contrats, engagements, formulaires, procédures, etc.).

Élément de coût. Subdivision de la répartition en type de coût (exemple : coûts matériels divisés en serveurs, postes de travail, réseaux, imprimantes, etc.).

Élément en capital. Élément maintenu en actif comptable et amorti sur plusieurs exercices financiers.

Enregistrement... Information individuelle ou composée contenue dans une base de données.

d'erreur connue. Enregistrement contenant les renseignements et l'historique d'une erreur connue.

d'incident. Enregistrement contenant les renseignements et l'historique d'un incident.

de changement. Enregistrement contenant les renseignements sur un changement, ainsi que sur les différents composants affectés par ce changement.

de mise à jour. Enregistrement contenant les renseignements sur l'historique d'une mise à jour ainsi que sur les éléments de configuration affectés par cette mise à jour.

de problème. Enregistrement contenant les renseignements et l'historique d'un problème.

Environnement. Ensemble de matériels, de logiciels, de procédures, etc., fonctionnant conjointement dans le but de fournir un service.

Environnement de test. Système informatique composé de matériel, de logiciels et de documentation, employé afin de tester les changements avant leur implantation dans l'environnement de production.

Environnement de production/opérationnel. Système informatique utilisé pour fournir le service demandé par les utilisateurs.

Erreur connue. Cause identifiée du dysfonctionnement d'un composant de l'infrastructure sans pour autant qu'une solution définitive n'ait été pour l'instant implantée.

Escalade. Opération de transmission d'une information ou d'une demande d'intervention (hiérarchique ou technique), sur un incident, un problème ou un changement.

Établissement des coûts de revient. Activité d'identification et de calcul des coûts de fourniture des services informatiques.

Évaluation des risques. Activité permettant d'analyser les risques potentiels et leurs conséquences sur le système d'information, et par extension, sur l'activité de l'entreprise.

Événement. Première étape du cycle de vie d'un incident situé au moment d'un dysfonctionnement.

Externalisation. Méthode par laquelle les services proposés auparavant par une organisation interne passent sous la responsabilité d'un fournisseur externe. Facturation

Activité de création et d'émission d'une facture dans le but de recouvrer les sommes engagées dans la fourniture d'un service.

Fenêtre de changements. Période de temps convenue pendant laquelle peuvent être introduits un ou plusieurs changements en exposant les services à un impact minimal.

Fiabilité. Correspond à l'aptitude d'un système à fonctionner durablement avec un minimum d'incidents ou d'interruptions.

Fonctions vitales pour le métier. Regroupent les fonctions supportées par un ou plusieurs services informatiques dont l'indisponibilité peut entraîner des conséquences graves pour l'activité de l'entreprise.

Fournisseur de services. Organisation interne ou externe fournissant les services ou les produits aux clients. Certaines de ces organisations peuvent héberger certaines applications de l'entreprise dans leurs locaux. Il s'agit alors de fournisseur d'hébergement d'applications (Application Service Provider : ASP).

Fournisseur interne. Unité responsable de la fourniture des services informatiques au sein de l'entreprise, indépendamment de son appartenance effective à l'entreprise.

Fournisseur externe. Tiers partie responsable de la fourniture ou du soutien d'un ou plusieurs éléments du système d'information.

Fourniture des services. Regroupement logique des cinq processus de gestion des niveaux de service, de gestion de la capacité, de gestion de la disponibilité, de gestion de la continuité des services informatiques, et de gestion financière des services informatiques.

Gestion des crises. Processus d'estimation des impacts suivant un sinistre et d'identification des modes d'action permettant d'y survivre.

Gestion de la capacité des affaires. Activité de la gestion des capacités permettant de s'assurer que les besoins futurs en matière de services informatiques sont pris en compte.

Gestion de la capacité des ressources. Activité de la gestion des capacités permettant de s'assurer que les ressources informatiques existantes sont surveillées et mesurées, et que l'apport des nouvelles technologies est pris en compte.

Gestion de la capacité des services. Activité de la gestion des capacités permettant de s'assurer que les ressources remplissent les objectifs des services informatiques signés dans les accords de niveaux de service.

Gestion de la continuité des affaires. Processus d'évaluation des sinistres et des conséquences qu'ils peuvent avoir sur les fonctions et les processus métier critiques afin de s'assurer que l'entreprise est en mesure d'y répondre de façon planifiée et préparée.

Gestion de la continuité des services des TI. Processus d'évaluation des sinistres et des conséquences qu'ils peuvent avoir sur le système d'information, et d'identification des composants de l'infrastructure pouvant être affectés.

Gestion des capacités. Processus chargé de définir et de contrôler les besoins de l'entreprise en matière de capacité informatique dans le but de fournir cette capacité au bon moment et au coût optimal.

Gestion des changements. Processus responsable de contrôler et de gérer les demandes de changements sur l'infrastructure et les services.

Gestion des configurations. Processus de planification, d'identification, de contrôle et de vérification des éléments de configuration composant l'infrastructure.

Gestion de la disponibilité. Processus responsable de la conception, de l'implémentation et du contrôle de la disponibilité des services informatiques.

Gestion des incidents. Processus de gestion des événements inattendus dont l'objectif prioritaire est de rendre le service disponible le plus rapidement possible.

Gestion des licences. Activité de contrôle et de vérification de l'utilisation des logiciels sous licence dans l'entreprise.

Gestion des mises à jour. Processus de planification, de conception, d'assemblage, de configuration et de test des mises à jour de matériel et de logiciels au sein de l'infrastructure informatique de l'entreprise.

Gestion des problèmes. Processus d'identification des causes des dysfonctionnements existants ou potentiels.

Gestion des risques. Activité d'identification des risques pouvant affecter l'entreprise et d'identification des contre-mesures adaptées et justifiées financièrement.

Gestion financière des services des TI. Processus responsable de la budgétisation, de la comptabilisation et de la facturation des services informatiques.

Gestionnaire des services informatiques. Personne responsable de la bonne exécution d'un ou plusieurs services ou processus au sein de la direction informatique. Cette personne doit s'assurer de la bonne marche

de son activité et de la production de rapports réguliers sur l'efficacité du service ou du processus. Elle peut siéger au comité consultatif des changements si ceux-ci portent sur son activité.

Heures/Horaire de service. Horaire convenu de disponibilité du service.

Heures/Horaire de soutien. Horaire convenu de disponibilité du support des services.

Historique des changements. Informations de suivi de l'initiateur, de l'origine, de la date et du contenu des changements.

Impact. Mesure des conséquences qu'un événement (incident, problème, sinistre, changement) entraîne ou pourrait entraîner, sur l'entreprise.

Imputation. Attribution des coûts de production des services informatiques en vue de leur recouvrement à un ou plusieurs clients sous la forme d'une facturation réelle ou fictive.

Incident. Correspond à un événement qui ne fait pas partie du fonctionnement normal d'un système (service, procédure, logiciel, matériel, etc.) et qui cause ou peut causer une altération de la qualité des services et de la productivité du client.

Infrastructure. L'infrastructure regroupe l'ensemble des composants (éléments de configuration) utilisés dans la fourniture des services informatiques et de télécommunication aux utilisateurs (matériel informatique et de télécommunications, logiciels, locaux, personnels, documentation, etc.).

Interface. Lien d'interaction physique ou fonctionnelle entre les éléments de configuration.

Local d'équipement informatique autorisé. Zone de stockage sécurisée des équipements informatiques de rechange.

Menaces. Causes éventuelles d'une perturbation agissant sur l'infrastructure (matériels, logiciels, services) et qui pourraient gêner la fourniture des services.

Mesure de réduction de risque. Mesure prise afin de réduire la probabilité ou les conséquences de la survenue d'une perturbation sur les activités de l'entreprise.

Mise à jour... Regroupement d'un ou plusieurs changements autorisés, testés et installés dans l'environnement de production.

complète. Mise à jour intégrale des composants d'un système (matériel, logiciel, documentations, procédures, etc.) qu'ils aient été modifiés ou non, depuis la dernière mise à jour.

différentielle (DELTA). Mise à jour qui ne remplace que les éléments de configuration qui ont changé depuis la dernière mise à jour.

groupée. Ensemble de mises à jour logicielles et/ou matérielles implantées simultanément dans l'environnement de production.

Modèle de coût... Répartition des coûts de production des services informatiques dans le but de calculer le coût total de ces services avant de les facturer aux clients.

par client. Coûts identifiés et répartis par client des services.

par service. Coûts identifiés et répartis sur les services informatiques fournis.

Métrologie de la disponibilité informatique. Ensemble de métriques utilisées dans la mesure de la disponibilité, de la fiabilité, de la maintenance et du temps de réponse des services informatiques.

Objectif de continuité des affaires. Définition du délai et du périmètre de reprise d'activité après un sinistre incluant personnel, infrastructure et service.

Objectifs de niveaux de service. Équivalent au cahier des charges d'un service, ce document correspond à l'expression des besoins des clients de l'informatique en termes de service.

Objectifs métier. Objectifs mesurables élaborés dans le but d'aider à la réalisation de la stratégie d'entreprise

Période convenue du service. Horaire de disponibilité convenu dans le SLA d'un service informatique.

Période d'indisponibilité. Période située dans les horaires de service convenus, durant laquelle celui-ci n'est pourtant pas opérationnel.

Phase d'alerte. Première phase du plan de continuité d'activité durant laquelle sont démarrées les actions d'urgence et l'évaluation des dommages.

Phase d'invocation et de reprise. La seconde phase d'un plan de reprise des activités d'affaires durant laquelle sont lancées les procédures de réparation, de restauration puis de reprise des services.

Plan... Document formel décrivant les objectifs, la planification et les ressources à mettre en œuvre dans un processus.

des capacités. Décrit les ressources nécessaires permettant d'aligner la capacité de l'infrastructure informatique à l'évolution des demandes de l'entreprise.

de continuité des activités métier. Décrit les rôles, les responsabilités et les actions nécessaires permettant de reprendre les activités métier critiques suite à un sinistre.

de continuité des services des TI. Décrit les actions et les procédures à suivre par la direction informatique en cas de sinistre dans le but de reprendre la fourniture des services critiques pour le métier.

de la disponibilité. Décrit les options permettant l'amélioration de la disponibilité de l'infrastructure informatique sur le long terme et à un coût justifié.

des déploiements. Décrit les méthodes, les plannings et les ressources nécessaires à l'implantation des mises à jour en production.

de gestion des configurations. Décrit l'organisation du processus, ainsi que les procédures de gestion des configurations d'un matériel, d'un logiciel ou d'un service spécifique.

de mise à jour. Décrit les activités, plannings, ressources et responsabilités liés à une mise à jour de l'infrastructure ou d'un service.

de la qualité des services. Décrit les objectifs internes à atteindre durant une période donnée afin d'améliorer les niveaux de service convenus et la perception qu'a l'entreprise de la qualité de ces services.

de retour arrière. Décrit les actions à entreprendre afin de rétablir le service après une mise à jour infructueuse.

Point de défaillance unique. Composant de l'infrastructure non redondant dont l'indisponibilité entraîne un impact significatif sur les activités de l'entreprise.

Politique de facturation. Ensemble de règles et de décisions de l'entreprise concernant la facturation et le recouvrement, que la direction informatique doit mettre en œuvre afin de justifier ses finances.

Potentiel de service externe. Capacité à disposer de l'assistance de fournisseurs externes afin de configurer un CI de l'infrastructure.

Potentiel de maintenance externe. Capacité à disposer des services de fournisseurs externes dans le but de maintenir un CI de l'infrastructure en état de fonctionnement afin qu'il puisse exécuter les fonctions requises.

Premier niveau d'assistance. Ressources techniques et de gestion présentes au sein du centre de services, permettant de résoudre rapidement les incidents simples.

Priorité. Valeur basée sur l'impact métier et l'urgence que l'on attribue à un incident, un problème ou un changement afin d'indiquer son importance relative dans la file de gestion de ces événements.

Prix avec marge. Coût de production auquel est ajouté une marge équivalente à un pourcentage de ce coût.

Prix du marché. Prix identique ou comparable à celui facturé par un fournisseur externe pour le même service.

Prix fixe. Prix convenu avec un client pour un service donné sur une période donnée.

Problème. Origine inconnue d'un ou plusieurs incidents existants ou potentiels.

Programme d'amélioration des services. Planification des objectifs d'amélioration continue de la qualité et de l'efficacité des services informatiques contenant les métriques, les procédures et les périodes de validation de ces objectifs.

Propriétaire du processus. Cadre de la direction informatique dont le rôle est d'assurer la pertinence des objectifs, de la conception, des métriques et, d'un point de vue général, de l'efficacité d'un processus.

Questionnaire de diagnostic. Ensemble structuré de questions employées par le personnel du centre de services pour permettre la résolution plus rapide et/ou l'attribution plus précise des incidents. Des scénarios de diagnostics seront souvent maintenus et fournis par le personnel technique en tant qu'une de leurs responsabilités au sein du processus de la gestion des incidents.

Redondance. Méthode utilisée pour éliminer les points de défaillance uniques par la duplication des éléments de configuration (CI) dont l'indisponibilité est susceptible de perturber l'activité du service.

Registre des changements. Liste exhaustive regroupant des informations sur les demandes de changement (évaluation, tests, décisions, état actuel, etc.).

Réglage. Activité visant à adapter les paramètres d'un composant de l'infrastructure ou d'un service dans le but d'obtenir une amélioration de la performance.

Relation. Interdépendance ou connexion entre les composants de l'infrastructure, les services ou les processus de la direction informatique. Permet d'évaluer l'impact potentiel d'un changement ou d'une défaillance.

Reprise... Opération de relance de l'activité suite à une défaillance regroupant les actions de réparation puis de restauration d'un ou plusieurs éléments de configuration ou d'un service.

graduelle (redémarrage à froid). Option de la continuité des services informatiques permettant la reprise de l'activité de l'entreprise dans un délai pouvant aller jusqu'à plusieurs jours après un sinistre, en réinstallant un système d'information minimal dans des locaux vides.

intermédiaire (redémarrage à chaud). Option de la continuité des services informatiques permettant la reprise de l'activité de l'entreprise dans un délai pouvant aller de quelques heures à quelques jours après un sinistre, en utilisant le système d'information minimal d'un site de repli pré-équipé mais non configuré.

immédiate (redémarrage immédiat). Option de la continuité des services informatiques permettant la reprise instantanée ou quasi immédiate des services (moins de 24 heures) dans le cas d'un sinistre, mais qui exige la présence d'une infrastructure de secours disponible en permanence dans un site de repli, et sur laquelle sont dupliquées régulièrement les données de l'entreprise.

Résilience (résistance aux pannes). Correspond à la faculté d'un système à continuer de fonctionner même si une partie des éléments du système sont défaillants.

Restauration du service. Activité de remise à disposition des utilisateurs d'un service ou des données indispensables à leur travail.

Retour à la normale. Phase du plan de reprise des activités où sont rétablies les opérations normales.

Revue post-implémentation. Réunion d'évaluation d'un changement tenue après son implémentation afin de déterminer s'il a été implanté avec succès et si les avantages prévus sont obtenus.

Risque. Évaluation de la probabilité qu'une perturbation se produise et des pertes potentielles pouvant en résulter.

Second niveau d'assistance. Groupe de personnes, disposant de compétences techniques avancées, impliquées dans la gestion des incidents et la gestion des problèmes non résolus dans un premier temps.

Service. Dans le cadre d'ITIL, un service peut prendre plusieurs sens.

Assistance. Le service correspond à l'aide, le support, l'assistance que la direction informatique apporte. C'est le service rendu.

Prestation. Il s'agit de l'ensemble plus ou moins intégré de composants d'infrastructure, de personnel et de procédures afin de satisfaire un objectif de gestion exprimé par le client.

Organisation. Le dernier sens que l'on peut donner au terme correspond à la dimension organisationnelle. C'est le service informatique en tant que division spécifique de l'entreprise.

Seuil. Niveau prédéterminé au-delà duquel une action est déclenchée.

Solution de secours. Matériels, logiciels et procédures mis en place afin d'assurer la disponibilité des composants de l'infrastructure qui subiraient une défaillance.

Solution palliative (de contournement). Solution permettant d'éviter un incident ou un problème afin de permettre au service de reprendre en utilisant une réparation provisoire ou 'une autre ressource temporaire.'

Soutien des services. Regroupement logique au sein du référentiel ITIL des cinq processus de gestion des configurations, des incidents, des problèmes, des changements et des mises à jour.

Tarification. Élaboration de la politique tarifaire et établissement des taux qui seront facturés aux clients.

Taux de résolution au premier contact. Proportion d'incidents résolus dès le premier contact entre l'utilisateur et le centre de services.

Taux en vigueur. Mode de facturation des services informatiques dans lequel les prix proposés sont comparables à ceux pratiqués par des organisations semblables.

Technologie de l'information et des communications (TIC). Ensemble des technologies du traitement et du transfert des données selon des instructions programmées afin d'en tirer des résultats. Ceci inclut les informations de types texte, image, film, son, etc.

Test d'intégration. Tester en situation identique à la production l'ensemble des composants matériels et logiciels impliqués dans un changement afin de s'assurer qu'ils fonctionneront bien ensemble.

Tolérance aux pannes. Capacité d'un service ou d'un système à continuer son activité lorsqu'une défaillance se produit.

Traitement des erreurs. Activité qui élabore une solution permanente permettant de résoudre une erreur connue (la cause) en passant éventuellement une demande de changement dans l'infrastructure.

Traitement des problèmes. Activité qui identifie la cause d'un problème et permet son passage au stade d'erreur connue.

Type d'appel. Tous les appels reçus au centre de services sont classés selon leurs attributs en fonction de leurs sujets, leurs destinations, leurs importances, etc. (exemple : demande de service, plainte, incident, etc.).

Type de coût. Afin d'élaborer un modèle de coût, les composants des services informatiques sont classés par type de composant tel que matériel, logiciel, personnel, installation, service externe, etc.

Utilisateur. Personne qui utilise tous les jours le service informatique délivré. Il est à noter qu'un client peut également être un utilisateur.

Urgence. Évaluation de la criticité de l'incident par rapport à l'activité de l'utilisateur et qui reflète la rapidité nécessaire à la résolution d'un incident.

Vulnérabilité. Faiblesse d'un composant ou d'un service de l'infrastructure qui pourra être exploitée par des menaces.

Équivalence des termes anglais/français

<i>Absorbed Overhead</i>	Coût indirect
<i>Absorption Costing</i>	Méthode de coût de revient
<i>Account Manager</i>	Responsable de compte
<i>Accounting</i>	Comptabilité
<i>Agreed Service Time</i>	Période convenue du service
<i>Alert</i>	Alerte
<i>Alert Phase</i>	Phase d'alerte
<i>Application Sizing</i>	Dimensionnement d'application
<i>ASP, Application Service Provider</i>	Fournisseur d'hébergement d'application
<i>Asset Management</i>	Gestion des actifs
<i>Assurance</i>	Assurance
<i>Attribute</i>	Attribut
<i>Audit</i>	Audit
<i>Auditing for compliance</i>	Audit de conformité
<i>Availability</i>	Disponibilité
<i>Availability Management</i>	Gestion de la disponibilité
<i>Availability Plan</i>	Plan de disponibilité
<i>Back-out Plan</i>	Plan de retour arrière
<i>Baseline</i>	Configuration de base

<i>BCM, Business Capacity Management</i>	Gestion de la capacité des affaires
<i>BCM, Business Continuity Management</i>	Gestion de la continuité des affaires
<i>BCP, Business Continuity Plan</i>	Plan de continuité des affaires
<i>Budgeting</i>	Budgétisation
<i>Business Continuity Objective</i>	Objectif de continuité d'activité
<i>BIA, Business Impact Analysis</i>	Analyse d'impact sur le métier
<i>Business Objectives</i>	Objectifs business/métier
<i>Business Value Chain</i>	Chaîne de valeur
<i>CAB, Change Advisory Board</i>	Comité consultatif du changement
<i>CAB/EC Change Advisory Board /Emergency Committee</i>	Comité consultatif du changement / Comité d'urgence
<i>Call Center</i>	Centre d'appel
<i>Call Type</i>	Type d'appel
<i>Capacity</i>	Capacité
<i>Capacity Management</i>	Gestion de la capacité
<i>Capacity Plan</i>	Plan de capacité
<i>Capital Cost</i>	Coût en capital
<i>Capital Item</i>	Élément en capital
<i>Capitalisation</i>	Capitalisation
<i>Category</i>	Catégorie
<i>Change</i>	Changement
<i>Change Control</i>	Contrôle des changements
<i>Change History</i>	Historique des changements
<i>Change Log</i>	Registre des changements
<i>Change Record</i>	Enregistrement des changements
<i>Change Slot</i>	Fenêtres de changements
<i>Charging</i>	Facturation
<i>Charging Policy</i>	Politique de facturation

CI, Configuration Item	Élément de configuration
<i>Classification</i>	Classification
CM, Change Management	Gestion des changements
CM, Configuration management	Gestion des configurations
CMDB, Management Database	Base de données de gestion des configurations
<i>Cold Standby</i>	Reprise graduelle
<i>Compliance</i>	Conformité
<i>Configuration Audit</i>	Audit des configurations
<i>Configuration Control</i>	Contrôle des configurations
<i>Configuration Management Plan</i>	Plan de gestion des configurations
<i>Continuous Improvement</i>	Amélioration continue
<i>Contract</i>	Contrat
<i>Cost Center</i>	Centre de coût
<i>Cost Element</i>	Élément de coût
<i>Cost model</i>	Modèle de coût
<i>Cost Plus</i>	Prix avec marge
<i>Cost Types</i>	Types de coût
<i>Cost-by-Customer Cost Model</i>	Modèle de coût par client
<i>Cost-by-Service Cost Model</i>	Modèle de coût par service
<i>Countermeasure</i>	Contre-mesure
<i>Crisis Management</i>	Gestion de crise
<i>Customer</i>	Client
<i>Customer Focus</i>	Axé sur le client
<i>Delta Release</i>	Mise à jour différentielle
<i>Depreciation</i>	Amortissement
<i>Detection</i>	Détection
DHS, <i>Definitive Hardware Store</i>	Local d'équipement informatique autorisé
<i>Diagnosis</i>	Diagnostic

<i>Diagnostic Script</i>	Questionnaire de diagnostic
<i>Direct Cost</i>	Coût direct
<i>Downtime</i>	Période d'indisponibilité
<i>DR, Disaster Recovery</i>	Reprise après désastre
<i>DRP, Disaster Recovery Planning</i>	Plan de reprise d'activité
<i>DSL, Definitive Software Library</i>	Bibliothèque des logiciels définitifs
<i>Emergency Change</i>	Changement d'urgence
<i>Environment</i>	Environnement
<i>Error Control</i>	Contrôle des erreurs
<i>Escalation</i>	Escalade
<i>External Service Costs</i>	Coûts des services externes
<i>Fault</i>	Faute/panne/défaillance
<i>Fault Tolerance</i>	Tolérance aux pannes
<i>Financial Management for IT Services</i>	Gestion financière des services informatiques
<i>First level Support</i>	Premier niveau de support
<i>First Time Fix Rate</i>	Taux de résolution au premier niveau
<i>Fixed cost</i>	Coût fixe
<i>Fixed Price</i>	Prix fixé
<i>FSC, Forward Schedule of Change</i>	Calendrier des changements
<i>Full Cost</i>	Coût complet
<i>Full Release</i>	Mise à jour complète
<i>Gradual Recovery</i>	Reprise graduelle
<i>Hot / Standby / Immediate Recovery</i>	Reprise immédiate
<i>Impact</i>	Impact
<i>Impact Analysis</i>	Analyse d'impact
<i>Incident</i>	Incident
<i>Incident Categorisation</i>	Catégorisation d'un incident
<i>Incident Life-cycle</i>	Cycle de vie des incidents
<i>Indirect Cost</i>	Coût indirect

Annexe C - Équivalence des termes anglais/français

<i>Information Technology Service</i>	Services informatiques
<i>Infrastructure</i>	Infrastructure
<i>Integration Testing</i>	Test d'intégration (pré-production)
<i>Interface</i>	Interface
<i>Invocation</i>	Déclenchement
<i>Invoicing/ Billing</i>	Facturation
<i>IR, Incident Record</i>	Enregistrement d'incident
<i>IT Accounting</i>	Comptabilité des TIC
<i>IT, Information Technology / ITC</i>	Technologies de l'information et des communications (TIC)
<i>IT Infrastructure</i>	Infrastructure informatique
<i>IT service</i>	Service informatique
<i>IT Service Continuity Plan</i>	Plan de continuité des services informatiques
<i>ITAMM, IT Availability Metrics Model</i>	Métrologie de la disponibilité informatique
<i>ITSCM, IT Service Continuity Management</i>	Gestion de la continuité de service informatique
<i>ITSM, IT Service Management</i>	Gestion des services informatiques
<i>KE, Known Error</i>	Erreur connue
<i>KER, Known Error Record</i>	Enregistrement d'erreur connue
<i>Known Error Classification</i>	Classification d'erreur connue
<i>Licence Management</i>	Gestion des licences
<i>Life Cycle</i>	Cycle de vie
<i>Maintainability</i>	Potentiel de maintenance externe
<i>Marginal Cost</i>	Coût marginal
<i>Market Price</i>	Prix du marché
<i>MTBF, Mean Time Between Failures</i>	Durée moyenne entre les pannes
<i>MTBSI, Mean Time Between System/Service Incidents</i>	Durée moyenne entre les incidents
<i>MTTR, Mean Time To Repair</i>	Durée moyenne de réparation
<i>Operational Costs</i>	Coûts de fonctionnement

<i>OLA, Operational Level Agreement</i>	Accord de niveau d'exploitation
<i>Outsourcing</i>	Externalisation
<i>Overheads Costs</i>	Coûts indirects
<i>Ownership</i>	Propriété
<i>Package Release</i>	Paquet d'installation
<i>Performance Management</i>	Gestion de la performance
<i>PIR, Post Implementation Review</i>	Revue post-implémentation
<i>PM, Problem Management</i>	Gestion des problèmes
<i>PR, Problem Record</i>	Enregistrement d'un problème
<i>Pricing</i>	Tarification
<i>Priority</i>	Priorité
<i>Proactive Problem Management</i>	Gestion proactive des problèmes
<i>Problem</i>	Problème
<i>Problem control</i>	Contrôle des problèmes
<i>Process Owner</i>	Propriétaire du processus
<i>Production Environment / Live Environment</i>	Environnement de production
<i>Profit Center</i>	Centre de profit
<i>RCM, Resource Capacity Management</i>	Gestion de la capacité des ressources
<i>Recovery</i>	Restauration
<i>Recovery Center</i>	Centre de recouvrement
<i>Redundancy</i>	Redondance
<i>Relationship</i>	Relation
<i>Release</i>	Mise à jour
<i>Release Management</i>	Gestion des mises à jour
<i>Release Plan</i>	Plan des mises à jour
<i>Release Policy</i>	Politique des mises à jour
<i>Release Record</i>	Enregistrement des mises à jour
<i>Release Schedule</i>	Calendrier des mises à jour

Annexe C - Équivalence des termes anglais/français

<i>Reliability</i>	Fiabilité
<i>Resilience</i>	Résilience
<i>Return to Normal</i>	Retour à la normale
<i>RFC, Request for Change</i>	Demande de changement
<i>RFS, Request for service</i>	Demande de service
<i>Risk</i>	Risque
<i>Risk Analysis</i>	Analyse du risque
<i>Risk Assessment</i>	Évaluation du risque
<i>Risk Management</i>	Gestion du risque
<i>Risk Reduction Measure</i>	Mesure de réduction du risque
<i>Roll-out Planning</i>	Planning des déploiements
<i>Running costs</i>	Coûts de fonctionnement
<i>Scalability</i>	Extensibilité
<i>SCM, Service Capacity Management</i>	Gestion de la capacité du service
<i>Second Level / Line Support</i>	Second niveau de support
<i>Service</i>	Service
<i>Service Catalogue</i>	Catalogue des services
<i>Service Culture</i>	Culture du service
<i>Service Delivery</i>	Fourniture des services
<i>Service Desk</i>	Centre de services
<i>Service Hours</i>	Horaires du service
<i>Service Manager</i>	Gestionnaire du service
<i>SOA, Service Outage Analysis</i>	Analyses des pannes du système
<i>Service Planning</i>	Planning des services
<i>Service provider</i>	Fournisseur de service
<i>Service Support</i>	Soutien des services
<i>Serviceability</i>	Potentiel de service externe
<i>SIP, Service Improvement Plan/Programme</i>	Plan d'amélioration continue

<i>SLA, Service Level Agreement</i>	Accord de niveau de service
<i>SLR, Service Level Requirement</i>	Objectifs de niveaux de service
<i>Software Environment</i>	Environnement logiciel
<i>SPOF, Single Point of Failure</i>	Point de défaillance unique
<i>SQP, Service Quality Plan</i>	Plan de qualité des services
<i>Standard Change</i>	Changement standard
<i>Stand-by Arrangement</i>	Solution de secours
<i>Support Hours</i>	Heures de soutien
<i>Test Build Environment</i>	Environnement de test
<i>Threats</i>	Menaces
<i>Threshold</i>	Seuil
<i>Transfer Cost</i>	Coût de transfert
<i>Tuning</i>	Réglage
<i>Underpinning Contract</i>	Contrat de sous-traitance
<i>Urgency</i>	Urgence
<i>Usability</i>	Convivialité
<i>User</i>	Utilisateur
<i>Variable Cost</i>	Coût variable
<i>VBF, Vital Business Function</i>	Fonction métier vitale
<i>Vulnerability</i>	Vulnérabilité
<i>Warm Standby</i>	Reprise intermédiaire
<i>Work-around</i>	Solution palliative

Norme et certification ISO 20000

L'un des leitmotivs d'ITIL étant l'adoption du modèle et son adaptation au contexte de l'organisation qui le met en œuvre, il en ressort que chaque implantation sera différente en fonction des éléments qui ont conduit à sa mise en place. Cette faculté d'adaptation d'ITIL a certainement contribué à son essor. En revanche, cela complique singulièrement la possibilité de comparer deux exemples distincts. Cela rend également difficile une éventuelle certification de respect du modèle.

Le contexte de l'ISO 20000

Avec l'essor mondial du référentiel ITIL, de nombreuses organisations souhaitent rationaliser leur gestion des services informatiques. Que ce soit pour améliorer la qualité du service rendu ou dans une optique de réduction des coûts, le but à atteindre est d'accroître l'efficacité et la capacité des entreprises à répondre à de nouveaux défis. Certaines d'entre elles ne s'y sont pas trompées et souhaitent communiquer sur leur respect des meilleures pratiques. Pour ces entreprises, en particulier les sociétés de service en informatique, cette reconnaissance est synonyme de crédibilité et parfois de parts de marché potentielles. Malheureusement, ITIL n'étant pas une norme, l'entreprise ou le produit qui se targue d'être « Compatible ITIL » ou « Certifié ITIL » fait plutôt la preuve de sa méconnaissance du domaine... ou d'une volonté d'abuser le client.

La réponse à ce type de demande ne peut se faire que par l'adoption d'un standard imposé par le marché ou par la mise en place d'une norme au niveau mondial. Jusqu'alors, cette certification d'un système de gestion de service était absente de la normalisation internationale.

Avec la BS 15000, l'organisme de normalisation britannique (BSI) est le premier à avoir proposé dès l'an 2000 une norme destinée à certifier les bonnes pratiques des entreprises concernant la gestion des services informatiques.

L'ISO/CEI 20000-1 a été élaborée à partir de cette norme du BSI et adoptée, par la procédure particulière dite « par voie express », avant d'être publiée le 10 novembre 2005.

Bien que la norme ne mette jamais en avant le fameux référentiel, et n'impose pas son utilisation, elle est largement calquée sur les recommandations d'ITIL. Dans les faits, cette norme s'appuie sur les deux concepts principaux du référentiel que sont l'approche processus et boucle d'amélioration continue de Deming (PDCA). Elle demande aux entreprises qui s'y conforment de respecter un ensemble de plus de deux cents règles et exigences qui démontrent la capacité de l'organisation à procurer des services de qualité aux clients.

Les avantages de ISO 20000

La « certification ITIL » ne concerne que les individus avec les trois niveaux de certification déjà évoqués. Le problème pour les entreprises est de faire reconnaître les efforts déployés au sein de l'organisation, et en particulier après le départ éventuel des personnes certifiées. La norme ISO 20000 propose désormais cette certification plus globale.

Garantissant le respect des règles de l'art pour les organisations informatiques, cette norme offre dès lors un avantage concurrentiel pour les structures de service et particulièrement pour celles qui proposent des solutions d'infogérance.

Comme on a pu le voir avec l'ISO 9000, il est plus que probable que l'ISO 20000 devienne dans peu de temps un pré-requis pour prétendre répondre à un appel d'offres. Cependant, à la différence d'une démarche qualité ISO 9000 très généraliste, la norme ISO 20000 offre un modèle de standardisation parfaitement dédié à la production des services informatiques. Dans tous les cas, cette certification apportera l'assurance du respect des bonnes pratiques ITIL au sein de l'organisation.

- Pour les clients utilisateurs des services, ce label sera la garantie d'une démarche qualité basée sur le respect des bonnes pratiques.
- Pour le fournisseur des services, les améliorations de la qualité des prestations et de la productivité apporteront certainement un avantage de taille dans un environnement très concurrentiel.

Le contenu de l'ISO 20000

La norme se compose de deux parties. La première est entièrement consacrée à une description formelle et définit les spécifications qui doivent être

respectées par l'entreprise qui souhaite obtenir la certification. La seconde partie correspond aux recommandations (code de bonnes pratiques) permettant d'atteindre des objectifs de la première partie. Elle dépasse la première étape de définition en apportant des conseils aux entreprises qui souhaitent atteindre les critères de la norme. Cette partie utilise le même plan que le premier volume, mais utilise un vocabulaire moins formel et plus orienté sur la mise en œuvre pratique. Concrètement, cette partie correspond à un support d'accompagnement préparant la certification ISO/CEI 20000-1.

Ces deux parties peuvent être achetées séparément auprès de l'AFNOR. Il s'agit de :

- ISO/IEC 20000-1 : 2005 Technologie de l'information – Gestion de services
 - Partie 1 : Spécifications
- ISO/IEC 20 000-2 : 2005 Technologie de l'information – Gestion de services
 - Partie 2 : Code de bonnes pratiques

Description de l'ISO 20000

Les deux documents qui définissent la norme ISO 20000 sont relativement succincts. Le premier représente seulement une quinzaine de pages et le second parvient à peine à en noircir plus d'une trentaine. Ceci dit, le fait est que la norme fait appel à des concepts de gestion des services largement documentés dans d'autres publications. Ainsi la relative légèreté du document ne doit pas faire penser qu'une certification puisse s'obtenir à la légère.

Le premier document est composé d'un avant-propos et d'une introduction suivie d'un paragraphe sur les différents domaines d'application de la norme, puis d'un mini-glossaire précisant certains termes et définitions. À partir du troisième chapitre, qui expose les exigences d'un système de gestion, le document entre dans le vif du sujet et entreprend une énumération des points importants de la norme. On y traite notamment de la responsabilité de la direction, des exigences relatives à la documentation, et enfin des compétences, de la sensibilisation et de la formation.

Le quatrième chapitre évoque la planification et mise en œuvre de la gestion des services. Ce chapitre s'appuie sur les principes du cycle de Deming (PDCA) avec la planification de la gestion des services (Planifier), la mise en œuvre de la gestion des services et de la fourniture des services (Faire), les étapes de surveillance, de mesure et de revue (Vérifier) et enfin, l'amélioration continue (Agir).

Le cinquième chapitre expose les étapes d'évolution des services avec la planification et la mise en œuvre des modifications ou création de services.

À partir des chapitres suivants, la norme reprend les treize processus de gestion des services largement inspirés d'ITIL et qui composent la norme.

Le sixième chapitre expose les processus de fourniture des services :

- gestion des niveaux de service ;
- rapport de service ;
- gestion de la continuité et de la disponibilité des services ;
- budgétisation et comptabilisation des services informatiques ;
- gestion de la capacité ;
- gestion de la sécurité de l'information.

Le septième chapitre évoque les processus de gestion des relations entre clients et fournisseurs :

- généralités ;
- gestion des relations commerciales ;
- gestion des fournisseurs.

Le huitième chapitre est consacré aux processus de résolution des problèmes. Cela peut paraître impropre dans la terminologie ITIL, mais a été généralisé dans la norme. Dans ce chapitre en effet, on traite au même niveau des incidents et des problèmes :

- contexte ;
- gestion des incidents ;
- gestion des problèmes.

Le neuvième chapitre décrit les processus de contrôle destinés à maintenir un système d'information sous contrôle :

- gestion des configurations ;
- gestion des changements ;

Le dixième chapitre est dédié au processus de mise en production.

Le dernier chapitre est une bibliographie des différentes normes liées à la gestion des services et à l'ISO 20000.

Domaine d'application de la norme

La norme ISO 20000 peut être utilisée en plusieurs occasions. Son domaine d'application couvre les aspects client et fournisseur de la gestion des services informatiques et, plus généralement, de tous les services liés aux technologies de l'information. Elle peut donc être utilisée :

- pour spécifier les critères d'un appel d'offre de sous-traitance de services ;
- pour formaliser une approche cohérente chez tous les fournisseurs de services, au sein d'une chaîne logistique ;
- par une entreprise qui souhaite évaluer sa propre gestion des services informatiques ;
- en tant que référence lors d'une évaluation des services ;
- par une entreprise qui souhaite démontrer sa capacité à fournir des services qui répondent aux besoins des clients ;

- dans une démarche d'amélioration des services par l'application de processus de contrôle et d'amélioration de la qualité.

Comme on peut le voir sur la figure D-1, la norme définit treize processus dans cinq grandes familles. On trouve notamment :

- les processus de fourniture de services :
 - gestion des niveaux de service ;
 - rapport sur le service ;
 - gestion de la capacité ;

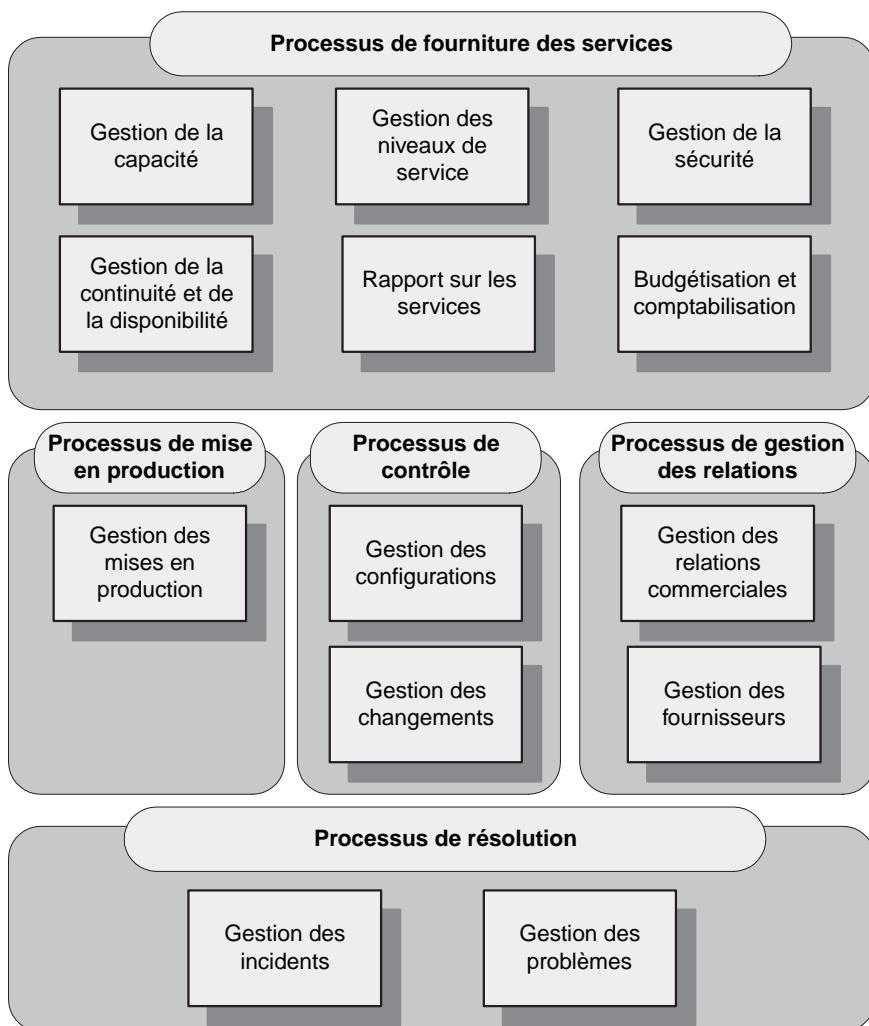


Figure -D1 : Les processus de la norme ISO 20000:2005

- gestion de la continuité et de la disponibilité du service ;
- gestion de la sécurité de l'information ;
- budgétisation et comptabilisation des services informatiques ;
- les processus de contrôle :
 - gestion des configurations ;
 - gestion des changements ;
- les processus de résolution :
 - gestion des incidents ;
 - gestion des problèmes ;
- les processus de mise en production :
 - gestion des mises en production ;
- les processus de gestion des relations :
 - gestion des relations commerciales ;
 - gestion des fournisseurs.

Exigence d'un système de gestion

La norme ISO 20000 demande la mise en place d'un système de gestion des services. Ce système n'est pas obligatoirement informatisé, même si cela aide lors de son utilisation. Ceci doit s'accompagner de la mise en place des différentes politiques et d'une structure permettant de gérer et mettre en œuvre efficacement tous les services informatiques.

Responsabilité de la direction

La direction de l'entreprise doit démontrer son engagement dans la démarche de gestion des services informatiques. Elle doit en particulier en établir la politique générale, les objectifs et la planification de la gestion des services. Une communication effective sur l'importance d'atteindre des objectifs est également nécessaire afin que les différents intervenants se trouvent au même niveau d'information. La direction doit en outre s'assurer que les exigences des clients sont définies et respectées. L'atteinte de ces objectifs ne peut se faire qu'en nommant un responsable de la gestion et coordination de tous les services et en déterminant et fournissant les ressources. Enfin, il est de la responsabilité de la direction de gérer les risques inhérents à la gestion des services et en particulier de planifier et d'effectuer des revues régulières des processus afin d'éviter les dérives.

Exigences relatives à la documentation

Au-delà de ces engagements formels, l'entreprise doit fournir la documentation et les informations nécessaires pour assurer la planification, l'exploitation et le contrôle efficace de la gestion des services. Ces documents comprennent en particulier :

- les plans de gestion ;
- les engagements de niveaux de services (SLA) ;

- les processus et procédures de la gestion des services ;
- les différents enregistrements associés.

Compétence, sensibilisation et formation

L'ensemble des rôles et des responsabilités des membres de l'équipe de gestion des services doit être défini. Un plan de formation et de sensibilisation permet de s'assurer que les employés ont conscience de la pertinence et de l'importance de leurs activités.

Planification et mise en œuvre de la gestion de service

La norme ISO 20000 met en avant l'utilisation du cycle de Deming dans le processus d'amélioration continue de la qualité des services. Comme on peut le voir sur la figure D-2, les quatre étapes du cycle prennent en compte la planification, la mise en œuvre, la vérification puis la phase d'amélioration des services.

Planification de la gestion des services

La phase de planification est l'occasion de définir :

- le domaine d'application de la gestion des services ;
- les exigences et les objectifs à atteindre ;
- les processus à mettre en œuvre ;

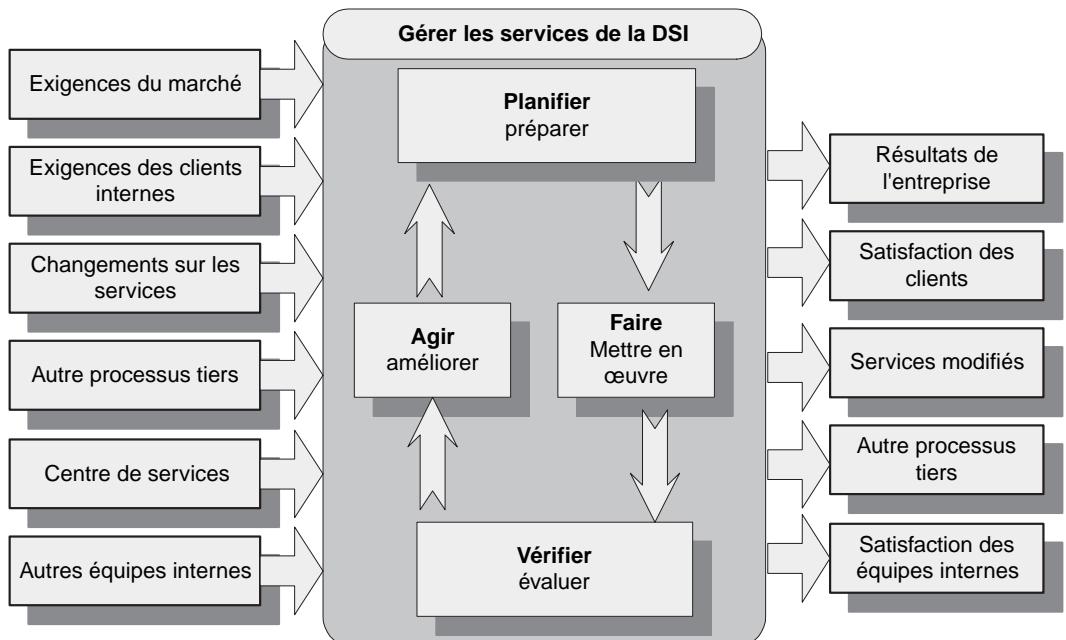


Figure D-2 : Le PDCA dans la gestion des services

- les rôles et responsabilités de la direction et des différents propriétaires de processus ;
- les interfaces entre les différents processus de la gestion des services et la coordination des activités ;
- comment identifier, évaluer et gérer les problèmes et les risques pour atteindre les objectifs définis ;
- les relations avec des projets qui créent ou modifient des services ;
- les ressources nécessaires à l'atteinte des objectifs ;
- les outils utilisés lors de la mise en œuvre des processus ;
- le mode de gestion, les méthodes d'audit et d'amélioration de la qualité du service.

Mise en œuvre de la gestion des services

Après la planification, la mise en œuvre des objectifs et du plan de gestion des services passe par l'étape du « faire » de Deming.

Les activités à mettre en place dans le but de fournir les services concernent :

- l'attribution des budgets et des ressources ;
- l'attribution des rôles et des responsabilités aux différents membres de la gestion des services ;
- la mise en place de la documentation et le maintien des politiques, plans, procédures et définitions propres à chacun des processus ou ensemble de processus de la gestion des services ;
- l'identification des risques encourus par le service et leur gestion durant le cycle de vie du service ;
- la gestion des équipes et de leurs connaissances ;
- la gestion des installations et du budget ;
- la gestion des équipes d'assistance des services ;
- les rapports d'avancement ;
- la coordination des différents processus.

Surveillance, mesure et revue

Cette troisième étape du cycle a pour but de garantir qu'un contrôle réaliste est opéré sur la gestion des services. Les activités de surveillance et de mesure collectent des informations. Par la suite, des passages en revue sur les objectifs et la planification de la gestion des services permet de s'assurer qu'ils sont réalisés.

Les méthodes appliquées doivent démontrer la capacité des processus à atteindre les engagements pris avec les clients.

Les revues pratiquées à intervalles réguliers déterminent si les exigences de gestion de service sont :

- conformes au plan de gestion des services et aux exigences de la présente norme ;
- mises en œuvre et maintenues de manière efficace.

Amélioration continue

Cette quatrième et dernière étape du cycle permet de capitaliser sur l'expérience acquise durant l'itération. À la lumière de ces informations, il est possible d'entreprendre des changements pour améliorer l'efficacité de la gestion des services. L'entreprise doit prendre en compte trois éléments distincts pendant cette phase d'amélioration. Il convient en premier lieu de mettre en place et de publier une politique d'amélioration des services dans laquelle seront définis les rôles et les responsabilités. Concernant la gestion des améliorations, toute suggestion doit être évaluée et autorisée, puis planifiée.

Pour parvenir à cette étape du cycle, l'organisation doit réaliser les activités suivantes :

- recueil et analyse de données de référence pour l'évaluation de la capacité à gérer et à fournir les services et les processus de gestion des services ;
- identifier, évaluer, planifier et mettre en œuvre les améliorations ;
- consulter les parties concernées ;
- fixer des objectifs d'amélioration en matière de qualité, de coûts et d'utilisation des ressources ;
- prendre en considération les éléments provenant des autres processus de gestion des services permettant des améliorations ;
- mesurer, rapporter et communiquer les améliorations des services ;
- réviser les politiques, les processus, les procédures et les plans de gestion des services ;
- valider que les actions approuvées ont été mises en œuvre et qu'elles ont atteint les objectifs prévus.

Planification et mise en œuvre des services nouveaux ou modifiés

Cette partie de la norme concerne les évolutions de services ou les nouveaux services à mettre en œuvre. L'objectif de cette étape est de s'assurer que le démarrage de nouveaux services ou les modifications apportées aux services existants seront fournis et gérés conformément aux coûts et la qualité qui a été validée.

Le cycle de vie des services, y compris leur retrait, doit être planifié et approuvé par le biais d'une gestion des changements formelle et doivent comprendre :

- les rôles et les responsabilités des membres de la gestion des services impliqués dans la mise en œuvre, l'exploitation et la maintenance des services ;

- la liste des changements apportés aux services et à la structure de gestion des services en place ;
- les communications d'informations aux parties concernées ;
- les modifications à apporter aux contrats et accords signés en fonction de l'évolution survenue dans les besoins de l'entreprise ;
- les besoins en termes de ressources humaines ;
- les besoins en termes de formation ;
- les méthodes et outils à utiliser avec le nouveau service ;
- les budgets et les calendriers de mise en œuvre ;
- les critères d'acceptation des services ;
- les résultats attendus de l'exploitation de ce nouveau service, exprimés en termes mesurables.

Les nouveaux services seront testés et validés avant d'être appliqués dans l'environnement de production. Le fournisseur de services doit rendre compte des résultats obtenus. Il faut également effectuer une revue post-implémentation, comparant les résultats réels aux résultats attendus.

Processus de fourniture des services

Gestion des niveaux de service

L'objectif de ce processus est de définir, d'accepter, d'enregistrer et de gérer les niveaux de service proposés aux clients.

Chaque service fourni doit être défini, validé et documenté dans un ou plusieurs contrat(s) de service (SLA).

Pour chaque service, la norme ISO 20000 précise que l'on doit être en mesure de fixer des objectifs sur les niveaux de service à atteindre. La conformité à la norme ISO 20000 peut être démontrée par la création de rapports sur les conditions documentées du niveau de service.

Parce que le contrat de services est considéré comme un élément de configuration, il tombe du même coup sous le contrôle de la gestion des changements et satisfait l'exigence de la norme ISO 20000 à cet égard.

Il faut mesurer les niveaux de service et les comparer aux objectifs, dans le but d'identifier les axes d'amélioration.

Rapport sur le service

Cette activité produit des rapports validés, fiables et précis pour une prise de décision éclairée et une communication efficace. Les différents rapports de service doivent être clairement décrits en indiquant les objectifs, les destinataires ainsi que les éléments descriptifs des sources de données utilisées. On y retrouvera en particulier les performances réalisées au vu des objectifs de niveaux de service, les problèmes de non-conformité, les failles de sécurité, la charge de travail et l'utilisation de ressources. On y

trouvera également les rapports de performance, les informations relatives aux tendances et les analyses de satisfaction.

Gestion de la continuité et de la disponibilité des services

Ce processus unique dans l'ISO 20000 se trouve documenté comme deux processus distincts dans ITIL. L'approche qui tend à réunir les deux dans un seul grand processus unifié semble tout de même un peu risquée. En conséquence, l'ISO 20000 doit prendre en compte la dimension tactique (disponibilité) et stratégique (continuité de service) lors des recherches de preuves au cours de l'audit. Le public prescripteur n'étant pas le même, cette recherche de documentation pourrait s'avérer difficile. Ceci dit, le but de ce processus est de s'assurer que les engagements pris avec les clients en termes de continuité et de disponibilité des services seront réalisés en toutes circonstances. Les besoins de disponibilité et de continuité de service sont identifiés par des plans d'activité, des contrats de service et l'évaluation des risques métier. La disponibilité doit être mesurée et enregistrée. Toute indisponibilité non planifiée fera l'objet d'une investigation et des mesures correctives seront prises.

Ce processus doit également fournir un ensemble de statistiques sur les disponibilités des services. Il est facile de déterminer le temps d'immobilisation d'un service ou d'un actif si vous enregistrez tous les incidents et si vous savez quel service/actif est affecté et si le système est hors service (indicateur H.S). Cela signifie que, conformément à l'exigence de la norme ISO 20000, les périodes de non-disponibilité imprévues sont détectées et examinées.

Budgétisation et comptabilisation des services IT

Ce processus est orienté vers les fonctions financières de la gestion des services. Son but est de budgétiser et de comptabiliser le coût de la fourniture de services. Des politiques et des procédures claires doivent être établies pour identifier, budgétiser et comptabiliser les éléments entrant dans la production des services, y compris les biens liés aux technologies de l'information, les ressources partagées, les frais généraux, les services assurés par des fournisseurs externes, le personnel, les assurances et les licences. Cette activité rend efficaces le contrôle financier et la prise de décisions.

Gestion de la capacité

Cette activité assure que le fournisseur de services dispose à tout moment d'une capacité suffisante pour répondre aux demandes validées, actuelles et futures, de l'entreprise. Le processus produit et maintient un plan de capacité. Certaines méthodes et techniques seront utilisées pour surveiller les services, affiner leurs performances et fournir une capacité appropriée en fonction de leur cycle de vie.

Gestion de la sécurité de l'information

L'objectif de ce processus est de gérer de manière efficace la sécurité de l'information au sein de toutes les activités de service. Pour définir précisément les activités de ce processus, il est recommandé de mettre en œuvre les principes décrits dans la norme ISO 17799-1.

La norme ISO 20000 exige que les incidents relatifs à la sécurité soient isolés, identifiés et signalés de manière appropriée.

Des mécanismes spécifiques de détection et de surveillance des incidents et dysfonctionnements liés à la sécurité en fonction de leur type, de leur fréquence et de leur impact doivent être mis en place. Ces contrôles sont destinés à valider que les exigences définies dans la politique de sécurité de l'information permettent de gérer efficacement les risques liés aux accès au service ou aux systèmes. Les actions d'amélioration identifiées au cours de ce processus sont enregistrées et alimentent le plan d'amélioration des services.

Processus de gestion des relations

Gestion des relations commerciales

L'objectif de ce processus est d'établir et de maintenir de bonnes relations entre le fournisseur de services, qu'il s'agisse de la DSU interne ou d'un service externalisé, et le client, fondées sur la compréhension du métier du client et de ses facteurs opérationnels.

La norme ISO 20000 exige que des réunions soient organisées afin de discuter des performances, des succès, des problèmes et des plans d'action. En ce qui concerne la procédure de plainte, elle est traitée comme un type d'incident et les appels sont reçus via le Service Desk.

Gestion des fournisseurs

Ce processus gère les fournisseurs de manière à assurer une continuité de service et une qualité convenue.

Le fournisseur de services doit s'appuyer sur des processus documentés et désigner un gestionnaire des contrats responsable de chaque fournisseur. Un processus de traitement des litiges contractuels doit exister.

Processus de résolution

Gestion des incidents

L'objectif principal de la gestion des incidents est de rétablir dès que possible le service convenu. La gestion des incidents est au cœur de la gestion des services informatiques. Il n'est donc pas surprenant de constater que la norme ISO 20000 lui accorde une place si importante. La norme exige en particulier que tous les incidents, y compris les incidents majeurs, soient enregistrés et puissent être classifiés.

Le suivi des incidents collecte des informations sur chaque incident ou incident majeur dans les aspects requis par la norme, c'est-à-dire l'enregistrement, la définition de priorités, le niveau d'impact sur l'entreprise, la classification, le suivi, la mise à jour, l'escalade, la résolution et la clôture formelle.

La norme ISO 20000 exige en outre que les incidents affectant le service soient gérés de manière efficace et que les clients soient tenus informés de leur progression.

L'utilisation d'une base de connaissances globale à laquelle s'ajoute la possibilité de détecter des similitudes parmi les incidents, les problèmes et les erreurs connues est un outil très pertinent avec la mise en place d'une CMDB.

Gestion des problèmes

Le processus de gestion des problèmes doit limiter au maximum les interruptions de service causées à l'entreprise lors des dysfonctionnements, par l'identification et l'analyse proactives de la cause des incidents et par la gestion des problèmes tout au long de leur cycle de vie.

La norme ISO 20000 stipule que l'on doit superviser, revoir et créer des rapports sur l'efficacité de la gestion des problèmes.

Les informations recueillies servent ensuite non seulement à éliminer la cause première des incidents, mais également à faciliter la création de bases de connaissances afin d'aider les personnes de l'assistance technique à mieux identifier les récurrences futures d'un problème et, ce faisant, à augmenter le taux de résolution au premier appel.

Processus de contrôle

La norme ISO 20000 préconise l'adoption d'une approche intégrée entre la gestion des changements et la gestion des configurations.

Gestion des configurations

La gestion des configurations définit et contrôle les éléments de configuration qui composent le service et l'infrastructure ; de plus, elle conserve des informations de configuration exactes.

L'apport de la gestion des configurations dans le processus de changement est d'envisager l'impact potentiel des changements sur le système d'information. La norme ISO 20000 exige en outre que la mise à jour des enregistrements dans la CMDB soit soumise à un contrôle strict.

Gestion des changements

La gestion des changements a pour objectif de s'assurer que tous les changements sont maîtrisés. Le processus doit prendre en compte l'évaluation, l'approbation, l'implantation, la revue finale et la documentation. S'il s'avère que le changement entrepris est un échec, le processus doit être

capable de le gommer ou d'y remédier. Selon la norme ISO 20000, une organisation doit disposer d'une planification des changements à venir ainsi que d'une procédure de changement d'urgence.

Processus de mise en production

Gestion des mises en production

Ce processus fournit, diffuse et surveille les différents changements qui se produisent sur le système lors d'une mise en production.

Il existe des liens forts entre le processus de gestion des mises en production et les processus de gestion des configurations et des changements.

La mise en production des services, des systèmes, du logiciel et du matériel est planifiée. Les plans de déploiement de la mise en production sont validés et autorisés par l'ensemble des parties concernées. Le processus de mise en production permet la traçabilité des dates, des livrables et faire référence aux demandes de changement associées, aux erreurs et aux problèmes connus. L'impact des demandes de changement est évalué. Les procédures de gestion des mises en production prévoient la mise à jour et le changement des données de configuration, ainsi que les enregistrements de changements. Un processus de gestion des mises en production urgentes doit également être mis en place.

Un environnement de pré-production est mis à disposition pour les tests afin de préparer les mises en production avant leurs distributions. En cas d'échec d'une mise en production, le processus propose un retour en arrière.

Comment obtenir la certification ISO 20000 ?

Un projet de certification ISO 20000 commence graduellement et est la plupart du temps l'aboutissement d'un projet plus long d'amélioration de la gestion de services informatiques. Pour obtenir la certification, un fournisseur de services informatiques doit satisfaire aux exigences stipulées dans la première partie de la norme ISO 20000. En clair, l'essentiel est de pouvoir démontrer qu'il met en œuvre un certain nombre de processus précis censés garantir un contrôle de ces activités, et une volonté d'amélioration continue de ces services.

Qu'est-ce que cela implique ?

Lorsqu'elle recherche la certification, une organisation démontre qu'elle prend au sérieux la gestion de services informatiques. Dans ce cas, la première étape consiste à s'adjointre les services d'une organisation d'audit accréditée, puis d'organiser la prestation d'audit. En réalité, cette étape est une des dernières à déclencher au sein d'un projet de grande ampleur.

Durant cette étape, une organisation doit :

- s'assurer qu'elle dispose bien des preuves de sa conformité à la norme que l'auditeur ne manquera pas de lui demander ;
- obtenir un avis extérieur de la part d'un consultant externe ou d'une équipe interne sous forme d'un audit « à blanc » avant de réaliser le véritable audit ;
- préparer, organiser et participer à la revue formelle des systèmes réalisée par l'organisme de certification ;
- préparer, organiser et participer à l'audit formel des systèmes dirigé par l'organisme de certification.

Cette approche laisse envisager l'audit sans surprise. Elle permet à l'organisation d'anticiper les problèmes importants afin de les traiter au préalable. Dans d'autres situations, l'audit mettra le doigt sur les faiblesses des processus et identifiera les points où la démonstration de conformité nécessite des explications plus spécifiques.

Comment démontrer sa conformité à la norme ISO 20000 ?

La partie de la démonstration de conformité repose généralement sur la production de « preuves ». Celles-ci correspondent globalement à un ensemble de documents et sur les diverses données produites par le système d'information.

L'auditeur s'assurera également que les procédures correspondent effectivement à des pratiques de travail courantes. Pour cela, il réalisera des entretiens avec les membres du personnel impliqués dans ces processus. Le but recherché est évidemment de savoir comment les choses se passent réellement.

En conséquence, l'auditeur essaiera d'établir si :

- l'organisation dispose de processus adéquats,
- les processus sont suffisamment documentés,
- les personnes impliquées comprennent et respectent les processus mis en place.

Les éléments « certifiables »

Dans le domaine de la gestion des services, les éléments susceptibles d'être certifiés, c'est-à-dire qu'il est possible de leur reconnaître un respect de la norme, sont les personnes et les entreprises.

Les certifications individuelles sont de deux types :

- ITIL (certifications *foundation, practitioner* et *manager*) ;
- Auditeurs ISO 20000 (ICA).

La certification des organisations n'est possible que par l'ISO :

- ISO/IEC 20000.

Concernant la certification de produit permettant d'automatiser et de faciliter la gestion des services, aucune disposition n'est prise dans ce sens pour l'instant. Cela implique qu'un logiciel qui ne pouvait évidemment pas être certifié ITIL auparavant, ne pourra pas non plus être certifié ISO 20000. Donc, messieurs et mess-dames du marketing, vous voici prévenus ! Inutile de chercher à nous abuser...

Comment devenir auditeur ISO 20000 ?

La certification ISO 20000 pour les individus ne s'applique qu'aux personnes qui désirent devenir « auditeurs ISO 20000 ».

Pour obtenir ce statut, la première étape consiste en une formation d'auditeur ISO 20000 de cinq jours auprès de l'ICA (Institut de certification des auditeurs) de l'AFNOR. Pour suivre cette formation, certains critères pré-requis sont nécessaires. Il faut :

- avoir suivi un cursus scolaire et universitaire (minimum bac+2) ;
- disposer d'une expérience professionnelle d'au moins cinq ans en informatique avec deux ans dans la gestion des services ;
- être au minimum diplômé « ITIL fondation » ;
- avoir déjà réalisé des audits (au moins 20 jours ou 6 audits).

À l'issue de la formation, chaque candidat subit un examen écrit sous forme d'un QCM portant sur la première et la seconde partie de l'ISO 20000, mais également sur la norme ISO 19011 et sur toute une partie de culture générale de la gestion de service, c'est-à-dire ITIL !

Après cet examen, le candidat passe un entretien oral devant un jury composé de deux personnes (membres de l'AFNOR et professionnels de l'informatique).

À partir de ce moment, le candidat devient auditeur stagiaire. Il ne sera validé en tant qu'auditeur certifié qu'après son premier audit ISO 20000.

Le principe de l'audit ISO 20000

L'objectif de l'audit ISO 20000 est d'établir pour une entreprise, à un instant donné, un constat de conformité entre les pratiques et le référentiel utilisé par l'entreprise. Ce pré-diagnostic qui peut également faire office d'audit à blanc est utilisé dans l'évaluation des écarts à la norme.

Par la suite, les conclusions de cet audit pourront être utilisées dans un objectif d'amélioration continue de la qualité (gain en maturité) ou dans la préparation à la certification ISO 20000.

Le constat des écarts par rapport à ce référentiel fait état de remarques sur :

- les écarts de conformité du système audité par rapport à la norme ISO 20000 ;
- l'insuffisance de formalisation de ce qui est effectivement réalisé ;
- le manque d'efficacité de la mise en œuvre du système audité.

Le constat de ces écarts est suivi de la mise en place d'actions correctives ou préventives lors de l'identification des risques potentiels.

On comprend aisément que l'audit des services d'une DSI est un des éléments clés de l'amélioration continue des processus. En effet, il analyse les écarts (outil de mesure et/ou de surveillance), et aide à déterminer les objectifs d'amélioration au travers du plan de progrès. L'audit propose une

ISO 19011

La norme

ISO 19011:2002

définit les lignes directrices et les principes de l'audit, la gestion des programmes d'audit, la réalisation d'audits de systèmes de gestion de la qualité et/ou de management environnemental ainsi que sur la compétence des auditeurs de ces systèmes.

C'est le « guide » des bonnes pratiques de l'auditeur !

évaluation de l'état du système et de ses évolutions et, par extension, de sa maturité.

La démarche de l'audit

Les principales étapes successives de l'audit sont les suivantes :

- Initialisation
 - prise de connaissance de l'entreprise ;
 - réunion de lancement ;
 - fixation des objectifs ;
 - détermination du périmètre d'audit.
- Préparation
 - planification de la mission ;
 - identification des différents acteurs ;
 - planification des entretiens individuels.
- Revue documentaire du système existant
 - analyse et évaluation des modes opératoires, des processus et procédures, des enregistrements de suivi et du système d'information.
- Entretiens
 - déroulement des entretiens ;
 - vérification des tâches de chaque processus ;
 - contrôle des livrables ;
 - identification des écarts à la norme ;
 - analyse des outils du système qualité ;
 - rédaction des comptes rendus d'entretiens.
- Rapport
 - comparaison des constats avec la norme ;
 - synthèse des informations recueillies ;
 - rédaction du rapport.
- Présentation des résultats
 - préparation d'une synthèse du rapport ;
 - présentation de la synthèse en réunion de Direction.

Bibliographie

Livres

Ouvrages français

itSMF France

Gestion des services liés aux technologies de l'information – Juin 2004.

Synthèse des processus de soutien et de fourniture des services.

ITPMs

Introduction à ITIL de Christian Nawrocki – Août 2005.

Présentation des processus de soutien et de fourniture des services.

DUNOD

ITIL et la gestion des services de Thierry Chamfrault et Claude Durand – Octobre 2006.

Présentation des processus de soutien des services.

HERMES

Management des opérations informatiques et ITIL de J. Moulinec, L. Loyer et H.Guyader – Février 2006.

Retour d'expériences autour des processus ITIL.

OGC/TSO (traduction itSMF)

Soutien des services

Gestion opérationnelle des services – Juin 2005.

Prise d'appels, résolution des dysfonctionnements, gestion des évolutions, application des contrats de service.

Fourniture des services

Gestion stratégique des services – Avril 2006.

Gestion des contrats de service, gestion transversale des problématiques communes à tous les contrats de service, gestion financière.

Ouvrages anglais

OGC/TSO

Service Support

Gestion opérationnelle des services – Juin 2000.

Prise d'appels, résolution des dysfonctionnements, gestion des évolutions, application des contrats de service.

Service Delivery

Gestion stratégique des services – Avril 2001.

Gestion des contrats de service, gestion transversale des problématiques communes à tous les contrats de service, gestion financière.

Planning to implement Service Management

Planification de l'implémentation de la gestion des services – Avril 2002.

Aide à la planification de la mise en place de ITIL dans l'entreprise.

Security Management

Gestion de la sécurité – Avril 1999.

Aspects sécurité sur tous les processus ITIL.

ICT Infrastructure Management

Gestion de l'infrastructure TIC – Octobre 2002.

Gestion de l'installation de l'infrastructure, gestion des composants techniques de l'infrastructure, gestion des services réseau, gestion de la production.

Application Management

Cycle de développement des applications – Septembre 2002.

Expressions des besoins et implémentation pour répondre aux besoins des utilisateurs.

The Business Perspective

La perspective métier – Octobre 2004.

Principes et besoins de l'organisation Business et communications avec le service informatique et plus particulièrement la direction informatique.

Liens Internet

Sites en français

<http://www.itsmf.fr/index.asp>

Le site de l'association itSMF en France.

<http://paul.vincent2.free.fr/livriel.php?livriel=itil>

Site personnel présentant une synthèse comparable au livre de l'itSMF France sur les processus de soutien et de support.

<http://www.eurotil.com/index.php?lNg=fr>

Site personnel offrant un ensemble de documents, synthèses et graphiques sur les processus de soutien et de support.

Sites en anglais

<http://www.itil.co.uk>

Le site officiel ITIL présenté par l'OGC.

<http://www.ogc.gov.uk/prince/>

Le site officiel Prince2, présentant la méthodologie de gestion de projet associée à ITIL.

http://www.itil.org/itil_e/index_e.html

Un portail sur les meilleures pratiques.

Site web en anglais et allemand qui présente les différents processus ITIL (v2 & v3), ISO 20000, Cobit...

<http://www.itservicecmm.org>

Site officiel de IT Service Capability Maturity Model.

<http://www.itlibrary.org/index.php?page=ITIL>

Site de documentation ITIL.

<http://www.toolselector.com/index.php>

Site web en anglais proposant des fiches comparatives entre différents outils de gestion des services informatiques.

Index

A

ACD (Automatic Call Distribution) 77

amortissement 233

analyse

de l'impact 212, 215

de la satisfaction client 78

de tendance 184

des problèmes (méthodes) 105

des risques 212

attentes de l'entreprise 14

B

base de données de gestion de la capacité 176

BCM (Business Capacity Management) 32, 175, 177, 210, 211

besoins de l'entreprise 23, 26

BIA (Business Impact Analysis) 212, 215, 221

bibliothèque logicielle des versions définitives 146

BLM (Business Level Management) 176

BRM (Business Relationship Management) 25

BS 15000 (norme) 10

budget 225, 229

budgétisation 227, 228

C

CAB (Change Advisory Board) 53, 56, 131, 132, 134, 136, 185

calcul de la disponibilité 198

call center 72

capacité

de maintenance 189

des ressources 176, 177

des services 176, 177, 191

métier 175, 176

catalogue de services 159, 162

CCTA 311

CCTA (Central Computer & Telecommunication Agency) 4

CDB (Capacity DataBase) 176

centre de services 28, 52, 56, 64, 69

local 76

mutualisé 76

virtuel 76

certification 14, 40, 49, 63, 260, 311

ITIL Foundation 14

ITIL Practitioner 14

ITIL Service Manager 14

- CFIA** 195
changement 132
CI (Component Item) 28, 114
client 22
CMDB (Configuration Management Database) 28, 51, 89, 105, 107, 115, 116, 117, 122, 131, 144, 145, 152
cold stand by 217
comité de crise 219
communication 16, 21
composant
 de l'infrastructure 114, 115
 logiciel 146
comptabilisation 227, 228, 232
concepts 260
 fondateurs 15
contrats
 de service 21
 de sous-traitance 160
contrôle des dépenses 225
convention de nommage 120
couplage téléphonie/informatique 77
coût total de possession 234
CRAMM (Computer Risk Analysis Management Method) 195, 212, 215, 221
critères de disponibilité 194
CS (Catalog Services) 159
CSIP (Continuous Services Improvement Program) 28, 32
CTI (Couplage Téléphonie Informatique) 77
Customer Focus 15
cycle de vie 16, 17, 33, 36, 121
-
- D**
-
- delta release** 145
demande de changement 91, 101
- démarche qualité** 16, 19
déploiement différentiel 145
DHS (Definitive Hardware Store) 30, 117, 147, 151
disponibilité 189
DownTime 192
DSL (Definitive Software Library) 30, 117, 144, 146, 151
durée d'un incident 78
-
- E**
-
- élément de configuration** 28, 101, 103, 107, 114, 121
erreur connue 91
escalade 56, 91
et 49
EXIN 13, 49, 312
-
- F**
-
- facturation** 79, 226, 227, 228, 236
fiabilité 189
fonction métier critique 196
formation 14, 260, 311
fournisseur
 externe 22
 interne 22
fourniture des services 11, 30
FSC (Forwarded Schedule of Changes) 132, 136
FTA (Fault Tree analysis) 195
full release 145

G

gestion

- de l'infrastructure TIC 11, 55, 57
- de la capacité 32, 54, 56, 65, 173
- de la continuité de service 32, 54, 56, 66, 209
- de la disponibilité 33, 54, 56, 65, 187
- de la sécurité 11, 37, 55
- des actifs logiciels 11, 35
- des applications 11, 34
- des changements 30, 53, 56, 65, 107, 129
- des configurations 28, 51, 57, 64, 113
- des files d'attente 77
- des incidents 30, 52, 56, 65, 87
- des infrastructures TIC 33
- des mises en production 30, 53, 57, 65, 143
- des niveaux de service 30, 53, 157
- des problèmes 30, 52, 56, 65
- des services 23
- financière 32, 54, 56, 66, 225

H

help desk 72**hot stand by** 217

I

IAS-IFRS 63

- impact**
- 90, 195, 201
- d'un incident 78
 - métier
 - majeur 136
 - mineur 136
 - significatif 136

ISEB 13, 312**Ishikawa** 106**ISO 20000 (norme)** 10**ITAMM (IT Availability Metrics Model)**
196**ITSCM (IT Service Continuity Management)**
209, 212**itSMF (IT Service Management Form)**
13, 311

K

Kepner-Tregoe 105

L

liens

- d'inclusion 121
- d'utilisation 121
- de connexion 121

logiciel de contrôle de version 152

M

matériel de rechange 195**mise en production**

- complète 145
- groupée 145

mode

- proactif 103
- réactif 103

modèle

- de coûts 233
- de maturité 247

modélisation

- analytique 184
- par simulation 184

N

niveaux d'escalade 89

O

objectifs stratégiques 27

OGC (Office of Government Commerce)
4, 13, 311

OLA (Operational Level Agreements)
32, 34, 53, 159, 160, 161

P

package release 145

PDCA (Plan, Do, Check, Act) 20, 161

perspective métier 11, 25

phase de validation 145

PIR 133

PIR (Post Implementation Review) 132
plan

- de configuration 119
- de continuité 219
- de disponibilité 192, 194
- de mise à jour 145
- de reprise 218
- d'activité 119

planification

- de la mise en œuvre 11, 27
- des changements 132

plannings des interruptions 192

point

- de contact unique 69
- unique de panne 194

préoccupation client 16

pré-production 145, 147, 150, 151

problème 90

procédure d'escalade 78

processus 16, 18, 51

PSA (Projected Service Availability)
132, 136

R

RCM (Ressources Capacity Management) 32, 176, 177

reprise

- graduelle 217
- immédiate 217
- intermédiaire 217

réserve de matériel de recharge 147

résilience 190

revue post-implémentation 132, 133

RfC (Request For Change) 56, 101, 132

ROI (Return On Investment) 1, 3

roue de Deming 20, 158, 159, 160, 179, 228, 249

routage automatique des appels 77

S

SCM (Service Capacity Management)
32, 176, 177

sécurité 191

service 15

SIP (Service Improvement Program)
159

SLA (Service Level Agreements) 21, 25, 32, 34, 53, 83, 87, 89, 95, 119, 129, 136, 151, 157, 159, 160, 161, 165, 166, 167, 176, 179, 187

SLM (Service Level Management)
30, 53, 157, 158

SLR (Service Level Requirement) 30, 157, 159, 161, 164

SOA 64, 196

solution de contournement (palliative) 90

soutien des services 11, 28

spare 195

SPOC (Single Point of Contact) 69, 71, 83

SPOF (Single Point of Failure) 194, 202, 216

SRM (Suppliers Relationship Management) 25

stratégie d'investissement 226

structure ITIL

 V2 11, 23

 V3 11, 39

suivi des performances 173

T

taux de disponibilité 199

taxinomie 120

TCO (Total Cost of Ownership) 1, 71, 234

télédistribution 151

tuning 179

U

UC (Underpinning Contract) 159, 160, 161

urgence 90

utilisateur 22

V

VBF (Vital Business Functions) 187, 196

vocabulaire 16, 21, 22, 260, 261

W

warm stand by 217

Z

zone de stockage 146, 151