Mise en place du référentiel COBIT

Jean Écard

CONSERVATOIRE NATIONAL DES ARTS ET METIERS

BORDEAUX

MEMOIRE

présenté en vue d'obtenir

le DIPLOME d'INGENIEUR CNAM

SPECIALITE : INFORMATIQUE

OPTION : ARCHITECTURE ET INGENIERIE DES SYSTEMES ET DES LOGICIELS

Par

Jean ECARD

Mise en place du Référentiel COBIT

Soutenu le 3 juillet 2012

JURY

PRESIDENT :

Monsieur le Professeur du Cnam, Pierre Paradinas,

MEMBRES :

Monsieur Richard Castanet, Professeur émérite, Institut Polytechnique de Bordeaux,

Monsieur Mohamed Mosbah, Professeur Institut Polytechnique de Bordeaux,

Monsieur Laurent Fallot, Maître de Conférences, Institut Polytechnique de Bordeaux,

Madame Florence Fourteau, Directeur Administratif et Financier de l'Association, Rénovation.

Remerciements

Pour leurs disponibilités et les conseils qu'ils m'ont prodigués tout au long de mon cursus et pour le présent mémoire, je tiens à remercier chaleureusement M. Richard CASTANET, Professeur émérite de l'Institut Polytechnique de Bordeaux et M. Mohamed MOSBAH, Professeur à l'Institut Polytechnique de Bordeaux.

Je tiens aussi à adresser de vifs remerciements aux enseignants du CNAM. Leurs précieux enseignements sont pour moi la base d'une réussite professionnelle.

Un grand merci au personnel du CNAM Aquitaine et plus précisément à Mme Dominique NEVEU et Nathalie GOURDIN. Leur travail d'accompagnement est vraiment formidable.

Il est également impensable d'oublier Madame Florence FOUTEAU et la toute la Direction de l'Association Rénovation sans qui ce projet n'aurait jamais pu voir le jour.

Enfin, un merci du fond du cœur à tous mes proches pour leur encouragement au quotidien.

Merci à tous.

GLOSSAIRE

ADU : A Définir Ultérieurement.

ACTIVITE (COBIT) : Il s'agit d'actions nécessaires pour réaliser tout ou partie d'un processus.

AG : Assemblée générale

AGEFIPH : Association pour la Gestion, la Formation et l'Insertion des Personnes Handicapées.

ARS : Agence Régionale de Santé rattachée au ministère de la santé.

CATEGORIE (COBIT) : COBIT compte 4 catégories qui contiennent les 34 processus. Il s'agit de Planification et Organisation notée PO, Distribution et Support notée DS, Acquérir et Implémenter notée AI et enfin Surveillance notée ME pour Mesure and Evaluate en anglais.

COBIT: Control Objectives for Information and related Technology

CMMI: Capability Maturity Model Integration

CNIL : Commission Nationale Informatique et Liberté

C.S.M.I : Centre de Soins des Maladies Infantiles

DPI : Dossier Patient Informatisé

DMP : Dossier Médical Partagé

DSL : Digital Suscriber Line. Ce type de ligne peut être asymétrique lorsque le débit montant et le débit descendant sont différents. On parle alors de ligne ADSL. Il peut également être symétrique. On parle alors de ligne SDSL.

ETAP : Etablissement Thérapeutique pour Adolescent à Pons

HAS : Haute Autorité de Santé.

ISACA: Information Systems Audit and Control Association, est une association professionnelle internationale dont l'objectif est d'améliorer la gouvernance des

systèmes d'information, notamment par l'amélioration des méthodes d'audit informatique.

IT : Technologie de l'information ou Information Technology en anglais. Dans le présent document ce terme est utilisé en remplacement de Système d'information.

ITIL: Information Technology Infrastructure Library.

ITEP : Institut Thérapeutique Educatif et Pédagogique

OBJECTIF IT ou SI (COBIT) : C'est un objectif déclaré par le RSI et en lien direct avec un ou des objectifs métiers.

OBJECTIF METIER (COBIT) : C'est un objectif déclaré par les responsables métiers. Il n'a pas de lien direct avec le SI mais uniquement avec les activités du métier.

OGC: Office of Government Commerce.

OS : Système d'exploitation (Operating System).

PROCESSUS: Un processus est un ensemble structuré d'activités déclenché par un ou plusieurs événements spécifiques, générant des résultats spécifiques pour des clients ou des parties prenantes et pouvant être mesuré.

RSI : Responsable du Système d'Information.

SEI : Software Engineering Institute, éditeur du CMMI.

SERVICE DESK : Service chargé de la gestion des demandes de corrections et d'évolutions du SI en place. C'est le point de contact entre l'utilisateur des ressources SI et le département SI.

SLA : Service Level Agreement ou contrat de niveau de service. Il s'agit de définir une qualité de service entre le fournisseur et le consommateur. Le fournisseur a l'obligation contractuelle de l''atteindre. Dans le cas contraire, des pénalités contractuelles peuvent lui être appliquées.

SLO : Service Level Objective ou objectif de niveau de service. Il s'agit de définir une qualité de service entre le fournisseur et le consommateur. Le fournisseur doit mettre en œuvre toutes les ressources nécessaires pour atteindre cet objectif mais n'y est pas tenu contractuellement.

SESSAD : Service d'Education Spécialisée et de Soins à Domicile. Il s'agit d'une structure d'aide à l'intégration scolaire qui agit majoritairement au domicile des usagers.

TI : Voir **IT**.

VPN : Virtual Private Network réseau informatique permettant de relier des machines de différents sites en se basant sur le réseau Internet sans mettre en danger la confidentialité des données transmises.

Sommaire

Introduction

Un changement de Direction en juillet 2010 a révélé de nouveaux besoins.

Le premier est la nécessité de réévaluer et de contrôler les risques liés à l'utilisation du SI dans un contexte sanitaire, médico-social et social tourné principalement vers l'enfance et l'adolescence.

Le deuxième est la nécessité de rapprocher la gestion du Système d'Information (SI) des standards actuels pour permettre de faciliter l'audit des organismes externes et pour éviter une trop forte dépendance par rapport à un individu.

Dans un même temps, le technicien informatique de l'Association à rejoint une nouvelle société. Le renouvellement de ce poste doit être l'occasion d'évaluer la charge de travail de ce poste en constante augmentation depuis 5 ans. Pour ne pas perdre la qualité des services fournis par ce service, la Direction souhaite recruter un profil aux responsabilités élargies.

Le poste de Responsable du Système d'Information est alors crée.

Des objectifs métiers parfaitement définis, un référentiel de SI à mettre en place, voici une parfaite opportunité pour étudier les référentiels actuels et leur pertinence dans le contexte de l'Association.

1 L'existant et le choix COBIT

En premier lieu, est présenté l'Association, pour qu'une fois le contexte connu, l'adéquation du SI en place avec les objectifs métiers puisse être étudiée.

Ensuite, l'étude des référentiels à disposition et leurs capacités à se conformer aux exigences de l'Association va permettre de conclure sur le choix du COBIT.

1.1 L'Association Rénovation

Pour présenter l'Association Rénovation, ses métiers et son organisation, ce chapitre s'appuie principalement sur les travaux réalisés et validés par les membres du Conseil d'Administration, disponibles sur le site officiel www.renovation.asso.fr . Des détails permettant d'appréhender la complexité du SI ont été ajoutés comme, par exemple, la couverture géographique et les exigences des financeurs.

1.1.1 Présentation générale

L'Association Rénovation est spécialisée dans la prise en charge d'adolescents et d'adultes affectés par des troubles du comportement et des maladies psychiques. Sa mission se situe dans le mouvement associatif laïc.

Depuis sa création, il y a un demi-siècle, Rénovation a beaucoup grandi : l'Association compte aujourd'hui plus de 600 salariés, répartis entre 14 établissements de divers types (instituts spécialisés pour enfants et adolescents, foyers pour adultes souffrant de troubles psychiques, services de placement familial, accueil en milieu ouvert, consultation, insertion en milieu ordinaire du travail, etc.).

La mission de Rénovation s'adresse à des publics de tranches d'âge variées (adolescents, enfants, adultes), et présentant différents types de problèmes (troubles du comportement, maladies mentales, addictions).

Pour chacun de ces types d'usagers, son action a pour but de reconstruire une personnalité abîmée par la maladie, les accidents de la vie, ou un contexte familial difficile. Chaque année, l'action entreprise par Rénovation permet à de nombreux adolescents de se réinsérer dans une trajectoire scolaire et professionnelle. Des adultes en proie à des maladies mentales y trouvent un complément ou une alternative à l'hospitalisation, voire, dans certain cas, une transition vers une vie plus ou moins

autonome. Des personnes handicapées retrouvent une place en entreprise, confirmée souvent par un contrat à durée indéterminée.

Dans une société où les problèmes de délinquance, de conduites à risque de l'adolescence et de prise en charge des malades mentaux prennent une importance croissante, Rénovation occupe dans le grand sud-ouest une place importante dans le dispositif médical, médico-social et social.

L'Association Rénovation, reconnue d'utilité publique, est de type loi 1901. Son fonctionnement est réglé par ses statuts. Avant d'aborder ce dernier en détail dans le paragraphe 1.2.3, il est important de se pencher sur ses principes moraux. Les lignes de conduites de l'Association sont en effet formalisées dans sa charte, qui influence les plus grandes décisions jusqu'aux gestes les plus courants.

1.1.2 La Charte

Ce texte recense les principes fondamentaux qui guident les actions des professionnels de l'Association. Il est issu des réflexions du Bureau de l'Association et des Directeurs d'Etablissements. Il comporte sept articles, dont le septième retranscrit ci-dessous, s'avère le plus directement applicable :

Art 7. : Nous cherchons dans notre pratique la participation des usagers et de leurs familles pour une meilleure qualité de la communication, du dialogue, et donc du service dans un climat participatif. Nous nous engageons à situer notre action et notre réflexion dans le sillage de ces règles fondamentales, garantissant le respect des usagers, de nos collègues et de nos partenaires.

1.1.3 Organisation Hiérarchique

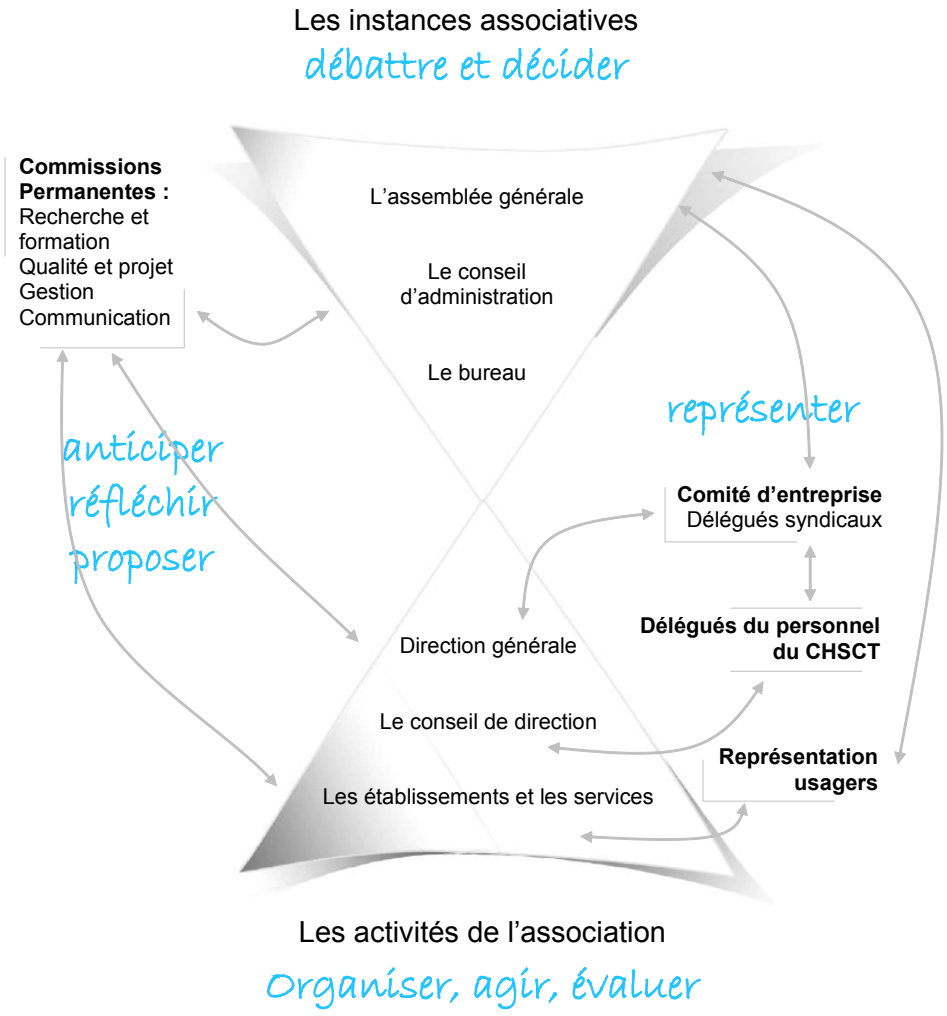


Figure 1 - Organisation de l'Association

1.1.3.1 Les Instances Dirigeantes

1.1.3.1.1 L'Assemblée générale (AG)

C'est la plus haute instance de l'Association, elle est souveraine : ses décisions s'imposent aux autres instances dirigeantes. En particulier, elle désigne les membres du Conseil d'Administration (CA), du Bureau et le Président.

Elle est composée des membres de l'Association. Les salariés membres n'ont néanmoins qu'une voix consultative.

Elle se réunit au moins une fois par an pour approuver ou désapprouver la gestion de l'Association sur les bases du rapport d'activité et du rapport financier.

1.1.3.1.2 Le Conseil d'Administration

Le Conseil d'Administration (CA) a la charge de déterminer la stratégie à appliquer pour mettre en œuvre la politique choisie par l'AG et de s'assurer de sa mise en œuvre.

Il est composé de 24 administrateurs élus par l'AG parmi ses membres pour une durée de 4 ans.

Il se réunit au moins 2 fois par an.

1.1.3.1.3 Le Bureau

Le CA délègue une partie de ses pouvoirs au Bureau, qui a donc la charge de veiller à l'exécution des décisions du CA.

Il est composé de 7 membres élus par le CA parmi ses membres pour une durée de 2 ans. Les fonctions de ses membres sont réparties comme suit :

- Un Président,
- Un ou deux Vice-Présidents,
- Un Secrétaire et un Secrétaire-Adjoint,
- Un Trésorier et un Trésorier-Adjoint.

1.1.3.1.4 Le Président

Il représente l'Association dans tous les actes de la vie civile.

1.1.3.2 Les instances Exclusives

1.1.3.2.1 La Direction Générale

La création de la Direction Générale en 1974, s'est justifiée par la multiplication et la diversification des équipements créés par l'Association, créant un besoin de mutualisation de services dans le souci de garantir la qualité des actions et la bonne gestion des moyens.

1.1.3.2.2 Le Directeur Général

Le Directeur Général, professionnel de l'action sanitaire et sociale, a pour mission d'animer et de mettre en œuvre la politique de l'Association dans l'ensemble de ses

activités. A cette fin il est soutenu par les services de la Direction Générale et du siège social, ainsi que par les Directeurs de chaque établissement ou service.

1.1.3.2.3 Le Directeur Des Ressources Humaines

La Directrice des Ressources Humaines a pour mission de soutenir le recrutement et la mobilisation des professionnels. Elle soutient et contrôle la gestion du personnel, développe une politique de gestion prévisionnelle des emplois et compétences, en insistant notamment sur la formation.

1.1.3.2.4 Le Directeur Administratif Et Financier

La Direction Administrative et Financière assure la gestion administrative et économique de l'ensemble des projets : liaison avec les partenaires administratifs, évaluation des équilibres économiques, contrôle de gestion, réalisation d'audits internes, suivi et contrôle de la comptabilité et de la paie, suivi et gestion du patrimoine, dossiers budgétaires, établissement des comptes annuels.

1.1.3.2.5 Le Responsable Du Système D'information

Voir Paragraphe 1.2.3.

1.1.4 Les Secteurs

Chaque établissement de l'Association est spécialisé dans un des trois domaines suivants : Le domaine médico-social, le domaine sanitaire ou le domaine social. Pour chacune de ces spécialités, il existe un financeur public principal qui affecte les missions et contrôle leurs bonnes réalisations. Ces moyens alloués permettent d'engager du personnel aux compétences spécifiques par secteurs et de mettre à leurs dispositions les moyens nécessaires à leurs activités.

1.1.4.1 Secteur Médico-social

Dans le secteur médico-social, les 5 établissements de l'Association accueillent des enfants et adolescents présentant des difficultés psychologiques s'exprimant par des troubles du comportement.

Les principaux financeurs sont l'Agence Régionale de Santé (ARS) et le Conseil Général.

Les compétences nécessaires pour réaliser les missions confiées sont les suivantes :

- Médical et paramédical : *Médecins thérapeutes, Orthophonistes, Psychologues, Psychomotriciens, Infirmiers.*
- Educatif, pédagogique et social : *Animateurs, Assistantes familiales, Assistantes sociales spécialisées, Educateurs spécialisés, Educateurs sportifs, Educateurs techniques, Professeur d'EPS, Professeurs des écoles.*
- Logistique *: Agents de service intérieur, Maîtresses de maison, Cuisiniers, Surveillants de nuit, Comptables.*

1.1.4.1.1 ITEP Rive Gauche

L'ITEP (Institut Thérapeutique Educatif et Pédagogique) Rive Gauche accueille 71 adolescents et adolescentes de 11 à 20 ans, d'intelligence normale, qui présentent des troubles du comportement et de la conduite. Il leur offre un parcours et un projet personnalisé souple et adapté à partir d'une palette de services diversifiés : unités de jour, Service d'Éducation Spéciale et d'Aide à Domicile (SESSAD), hébergement en petites unités de vie dans des quartiers résidentiels, appartement.

1.1.4.1.2 ITEP Rive Droite

L'ITEP Rive Droite accueille des enfants ou adolescent(e)s de 3 à 18 ans, qui présentent des difficultés psychologiques dont l'expression, notamment l'intensité des troubles du comportement, perturbent gravement la socialisation et l'accès aux apprentissages. Ces jeunes se trouvent, malgré des potentialités intellectuelles et cognitives préservées, engagés dans un processus handicapant qui nécessite le recours à des actions conjuguées et à un accompagnement personnalisé adapté.

1.1.4.1.3 ITEP Chalossais

L'ITEP Chalossais, implanté dans le département des Landes à Hagetmau, accueille 51 garçons et filles, âgés de 8 à 18 ans (pour l'ITEP) ou de 6 à 18 ans (pour le SESSAD), qui présentent des difficultés psychologiques dont l'expression, notamment l'intensité des troubles du comportement, perturbent gravement la socialisation et l'accès aux apprentissages. Il leur offre un parcours et un projet personnalisé souple et adapté à partir d'une palette de services diversifiés : Unité de jour, hébergement en petites unités, Service d'Éducation Spéciale et d'Aide à Domicile (SESSAD).

1.1.4.1.4 FAM Triade

Le FAM (Foyer d'Accueil Médicalisé) Triade, structure de réinsertion sociale et de soins reçoit 36 personnes handicapées psychiques en accueil permanent. L'établissement propose un hébergement diversifié (foyer, appartements collectifs, studios individuels) afin de répondre aux besoins des résidents dans leur parcours d'autonomisation et d'intégration sociale. Les personnes accueillies, âgées de 20 à 60 ans, bénéficient d'un accompagnement médico-social pour assurer la continuité des soins et remobiliser la dynamique nécessaire à la construction progressive d'un projet de vie, si possible, en milieu ordinaire.

L'établissement est financé par le Conseil Général de la Gironde pour la partie hébergement. Les prestations de soins relèvent d'une dotation globale de l'Assurance Maladie allouée par l'ARS d'Aquitaine.

1.1.4.1.5 ESTANCADE

L'Estancade, situé à Saint-Sever dans les Landes, accueille 12 jeunes, filles et garçons, de 11 à 18 ans, résidant dans les Landes, présentant des troubles du caractère et du comportement, en rupture familiale, scolaire et sociale.

1.1.4.2 Secteur Sanitaire

Dans le secteur sanitaire, 4 établissements accompagnent des enfants, des adolescents et des adultes présentant des troubles psychiques relevant d'une maladie mentale, en dehors de la phase aigue, en amont ou en aval de l'hospitalisation.

Les principaux financeurs sont les ARS d'Aquitaine et de Poitou-Charentes.

Les compétences nécessaires pour réaliser les missions confiées touchent 3 secteurs. Le premier est le domaine médical et paramédical et demande des médecins thérapeutes, des orthophonistes, des psychologues, des psychomotriciens et bien sûr, des infirmiers. Le second est le domaine éducatif et réclame des éducateurs spécialisés et des animateurs. Enfin, le dernier concerne la logistique avec des agents de service intérieur, des cuisiniers, des surveillants de nuit, des comptables et du personnel administratif.

1.1.4.2.1 HOPITAL DE JOUR DU PARC

L'hôpital de jour du Parc est un externat installé à Bordeaux. Il accueille 35 adolescents, garçons et filles, âgés de 12 à 18 ans (dérogations possibles jusqu'à 21

ans) présentant des troubles graves de la personnalité : psychoses et névroses graves.

En tant qu'établissement sanitaire, le Parc est agréé par la Sécurité Sociale et l'Aide Sociale. (Date de l'habilitation à recevoir des bénéficiaires de l'aide sociale : 23 juillet 1975). Participation au Service Public Hospitalier depuis 2001. Le Centre d'Accueil Thérapeutique à Temps Partiel (CATTP) "Escapa" a été ouvert le 01 juillet 2003.

1.1.4.2.2 CENTRE de Réadaptation

Le Centre de Réadaptation est un établissement de postcure psychiatrique. Il s'adresse à de jeunes adultes (18-30 ans) atteints de troubles psychiques graves auxquels il propose, en deuxième intention, une prise en charge globale dans une perspective de réadaptation psychosociale.

Il est composé de trois foyers (internat) de petites dimensions, situés en centre ville. Sa capacité d'accueil est de 44 personnes.

1.1.4.2.3 ETAP

« L'ETAP » (Etablissement Thérapeutique pour Adolescent à Pons) est un établissement de santé pour adolescents. Il participe à l'intervention en psychiatrie infanto-juvénile dans la prise en charge de soins de longue durée. Sa capacité d'accueil est de 15 personnes.

1.1.4.2.4 CSMI

Le C.S.M.I, (Centre de Soins des Maladies Infantiles) réalise ses activités sur quatre pôles répartis sur les cantons de Bordeaux Nord, du Nord-Ouest de la CUB et du Médoc. Il assure une activité de consultation, de soin et de prévention pour les enfants et adolescents de 0 à 18 ans.

1.1.4.3 Secteur social

Dans ce secteur, 3 types de missions sont confiés à l'Association.

Les établissements et services de protection de l'enfance sont confrontés depuis toujours à des situations de difficultés sociales et familiales, de carences éducatives et de maltraitances. Les prises en charge demandées par ces services peuvent se situer

dans un accompagnement, une restauration des compétences familiales, la participation à des actions collectives. Deux établissements de l'Association sont chargés de ces missions : le SAF et l'AED.

L'accompagnement des personnes handicapées psychiques dans la cité est une exigence croissante qui suppose de réduire les temps en institution avec les risques de chronicisation qu'ils entraînent, et de développer les services en milieu naturel en articulation avec le soin : appartements, accompagnement à la vie sociale. Le SAVS est chargé de ces missions.

Enfin, l'insertion professionnelle des personnes handicapées est un droit, confirmé par la loi du 11 février 2005. L'établissement MEDIA s'inscrit dans ce cadre en privilégiant des actions spécifiques en faveur des personnes handicapées psychiques pour leur insertion en entreprise ou en situation de travail protégé.

Les principaux financeurs sont le Conseil Général et l'AGEFIPH.

Les compétences nécessaires pour réaliser les missions confiées touchent 3 secteurs. Le premier est le domaine médical et paramédical et demande des médecins psychiatres et des psychologues. Le second est le domaine éducatif et réclame des éducateurs spécialisés, des sociologues et des assistants familiaux. Enfin, le dernier concerne la logistique et s'appuie sur des comptables et du personnel administratif.

1.1.4.3.1 MEDIA

Média Hand'treprise est un établissement mobilisé sur l'insertion professionnelle des travailleurs handicapés. Il gère un Cap Emploi conventionné avec l'AGEFIPH, le POLE EMPLOI, et le FIPHFP, chargé de développer l'accès à l'emploi.

Cet établissement dispose également d'un service de maintien dans l'emploi des travailleurs handicapés financé par l'AGEFIPH.

1.1.4.3.2 AED

Le service d'action éducative à domicile intervient à titre préventif dans les familles lorsque la santé de l'enfant, sa sécurité, son entretien ou son éducation l'exige.

Ce service est lié par convention au Conseil Général de la Gironde. Il travaille en articulation étroite avec la Direction Enfance-Famille et accomplit une mission fondamentale de prévention.

1.1.4.3.3 SAVS

Le Service d'Accompagnement à la Vie Sociale est ouvert à 39 personnes reconnues handicapées mais bénéficiant d'une autonomie suffisante pour vivre à leur domicile ou se préparant à le faire.

Ces personnes souffrent de troubles psychiques stabilisés qui ont fragilisé leurs capacités d'autonomie et peuvent les mettre en situation de difficultés sociales.

1.1.4.3.4 SAF

Le service d'accueil familial de Saint-Sever, dans les Landes, accueille des enfants et adolescents, garçons et filles, de 0 à 21 ans, dans une famille d'accueil, avec le soutien d'une équipe psycho-éducative. Il leur apporte un soutien matériel, éducatif et psychologique, ainsi qu'à leur famille, lorsqu'ils sont confrontés à des difficultés sociales susceptibles de compromettre gravement leur équilibre.

Sa capacité d'accueil est de 141 jeunes de 0 à 21 ans.

1.1.4.4 Synthèse

Etablissement	Secteur	Departement couvert	Nombre de sites
ITEP RIVE DROITE	Médico-social	33	5
ITEP RIVE GAUCHE	Médico-social	33	5
ITEP CHALOSSAIS	Médico-social	40	2
FAM TRIADE	Médico-social	33	2
HOPITAL DE JOUR DU PARC	Sanitaire	33	1
ETAP	Sanitaire	17	1
CENTRE DE READAPTATION	Sanitaire	33	4
CSMI	Sanitaire	33	5
DG	Siège social	33	1
MEDIA	Social	33	3
SAVS	Social	40	1
AED	Social	33	1
SAF	Social	40/64	2
ESTANCADE	Social	40	1
Totaux		4	34

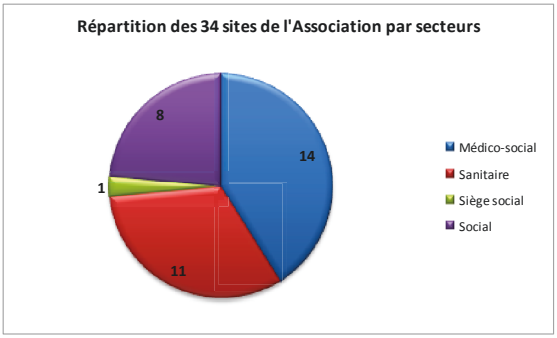


Figure 2 - Répartition sectorielle et géographique des établissements et de leurs sites.

L'Association répartie donc harmonieusement ses établissements sur les 3 secteurs. Géographiquement, elle couvre 4 départements.

Le secteur médico-social, du fait de ses différentes sous-activités et des exigences de répartitions des financeurs, déploie 14 sites. Ce chiffre le place en tête du nombre de sites par secteurs.

Le sanitaire, pour répondre aux exigences de répartition de l'ARS situe ses antennes de Bordeaux jusqu'à Lesparre dans le Médoc. Le centre de Réadaptation concentre ses 3 foyers et son administration sur Bordeaux.

Le secteur social, contrairement aux 2 précédents, déploie ses équipes vers ses usagers. C'est pourquoi il nécessite moins de site de consultation.

Le système d'information doit alors prendre en compte d'une part, cette couverture géographique importante et, d'autre part, les exigences métiers propres à chaque domaine. De ce dernier point de vue, le secteur sanitaire à travers une politique d'identification, de sécurité des données et de recueil d'activité médicale psychiatrique (RIM-PSY), est le plus contraignant. Le profil des utilisateurs est également très varié avec des éducateurs spécialisés, des comptables, des psychiatres, des infirmiers, des sociologues, etc.

1.2 Le SI

Le paragraphe précédent a permis de mettre en évidence une grande variété de métiers, de profils d'utilisateurs et une couverture géographique très large. Pour terminer de cerner les contraintes auxquelles doit répondre le SI, il convient maintenant de connaître le nombre d'utilisateurs, de machines et de logiciels en place.

Une fois ces paramètres quantitatifs connus, l'architecture physique et organisationnelle retenue pour répondre à ces besoins, ainsi que les coûts de fonctionnement associés, vont être présentés.

1.2.1 Utilisateurs et Ressources : Les Chiffres

Etablissement	Nombre d'utilisateurs	Nombre postes Informatique	Nombre mobiles
ITEP RIVE DROITE	43	21	13
ITEP RIVE GAUCHE	20	11	14
ITEP CHALOSSAIS	10	6	11
FAM TRIADE	27	9	4
HOPITAL DE JOUR DU PARC	34	14	4
ETAP	39	14	6
CENTRE DE READAPTATION	40	8	6
CSMI	55	11	2
DG	22	20	4
MEDIA	40	31	9
SAVS	4	3	3
AED	44	12	25
SAF	20	19	11
ESTANCADE	5	4	5
Totaux	**403**	**183**	**117**

Figure 3 – Répartition des ressources physiques et des utilisateurs

Avec un total de quelques 400 utilisateurs pour environ 200 postes informatiques disponibles, il apparaît que le parc informatique doit pouvoir être partagé facilement par ses utilisateurs. C'est pour l'instant une réalité puisque des profils comme les éducateurs, les infirmières, ne sont amenés à saisir leurs activités que de manière ponctuelle. En conséquence, ils ne mobilisent pas, un poste à temps plein contrairement aux profils administratifs.

La répartition des téléphones mobiles ne suit pas cette logique. Les personnels amenés à se déplacer ou devant être joint rapidement sont ici privilégiés. Ainsi les profils retenus sont éducateurs, les animateurs et les directeurs. C'est pourquoi les établissements sociaux et médico-sociaux sont les principaux consommateurs de cette ressource.

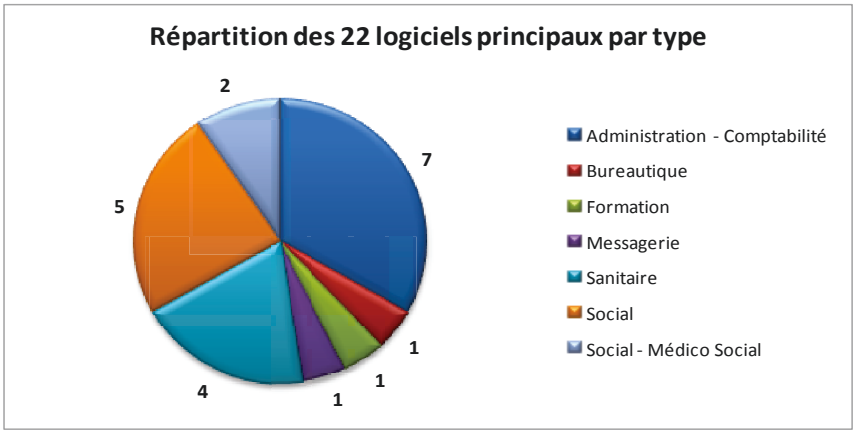


Figure 4 - Répartition des logiciels par catégories et fonctionnalités

Il est possible de classer les logiciels en catégories suivant qu'ils servent directement une fonctionnalité métier, comme la transmission d'informations médicales pour le secteur sanitaire ou une fonctionnalité technique plus transversale, comme la bureautique ou la messagerie.

Les catégories d'activités nécessitant le plus de variétés de logiciels sont sans conteste, l'administration, le secteur social et le secteur sanitaire.

Pour l'administration, la variété des exigences des acteurs externes impose de nombreux produits : Comptabilité, indicateurs standardisés, gestion des paies et du temps de travail.

Pour le secteur social, les mêmes causes produisent le même effet : suivi standardisé des usagers, des offres de services, des entreprises, (en particulier pour MEDIA Hand'treprise qui s'insère directement dans le SI de Pôle Emploi et de l'AGEFIPH).

Pour le secteur sanitaire, le Dossier Patient Informatisé (DPI) et sa liaison avec les logiciels d'administration (admissions, sorties et facturations) impose 2 logiciels, de même que le RIM-P (Relevé d'Information Médicale Psychiatrique).

Les catégories métiers comme le médico-social et la formation se contentent pour l'instant d'un existant réduit.

Les catégories techniques, très homogénéisées, n'utilisent que la suite Office.

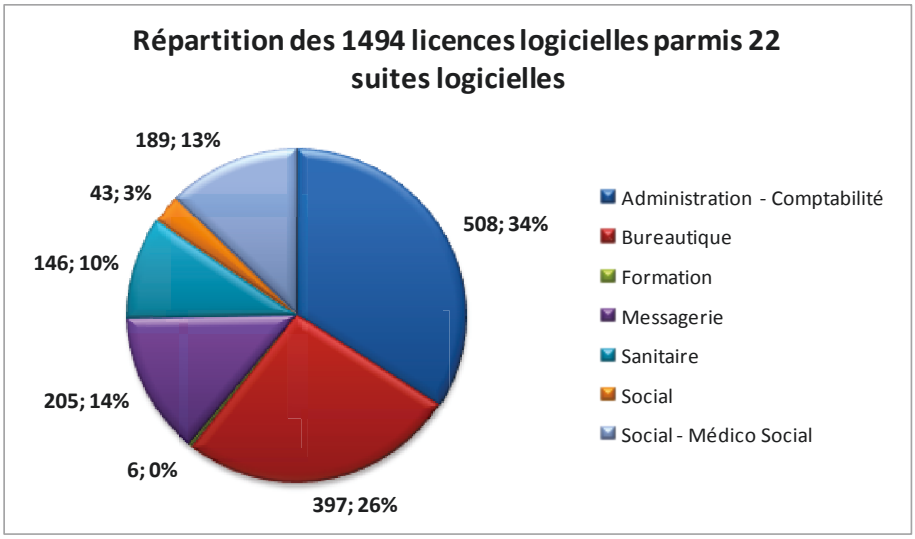


Figure 5 - Répartition des licences logicielles

Concernant le nombre d'utilisateurs de logiciel, le domaine administratif s'avère le plus sollicité. C'est en effet cette catégorie qui couvre le plus grand nombres de fonctionnalités (la gestion des ressources humaines, gestions de la paie, le suivi des plannings et horaires, la comptabilité générale, analytique, etc.).

Les logiciels métiers propres aux domaines sanitaires et sociaux sont, quant à eux, moins utilisés que la suite bureautique (Office 2007). Ceci s'explique en grande partie par le fait que ces logiciels métiers, sont, soit partiellement utilisés, soit insuffisants pour répondre à tous les besoins. Ils sont alors suppléés par des documents génériques de type texte ou tableur.

La messagerie est volontairement limitée à quelques acteurs clés par l'application d'une politique de l'Association.

L'utilisation d'un logiciel de formation est très limitée car le service formation est centralisé et ne mobilise que 2 ressources.

1.2.2 Architecte Réseau

1.2.2.1 Serveurs d'applications

L'ensemble des applications évoqué dans les paragraphes précédents est hébergé sur des serveurs gérés entièrement par un prestataire de service : ALFA, ce même prestataire, spécialisé dans le médico-social, édite la majorité des applications métiers.

L'architecture retenue, décrite dans le schéma ci-après, a permis de supprimer tous les serveurs maintenus sur les sites de l'Association. Elle est accompagnée d'un contrat de service garantissant une disponibilité de 99.5% pendant les heures ouvrées.

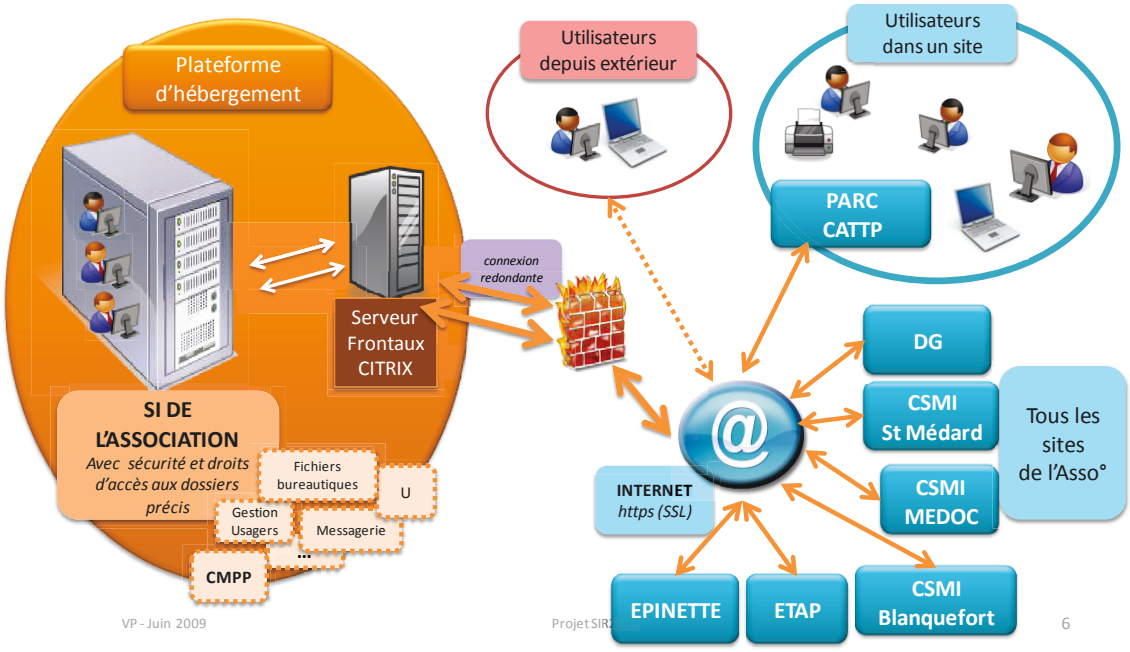


Figure 6 - Architecture réseau

Le système Citrix a été choisi pour sa consommation en bande passante Internet à la fois, parfaitement déterminée et faible. En effet, pour manipuler les applications, le client final consomme 50 Kbits en débit montant et descendant. En revanche, les consommations générées par les impressions (des serveurs Citrix vers les sites) et par les scans (des sites vers les serveurs Citrix), heureusement ponctuelles, peuvent imposer des débits supérieurs.

Ce système permet de déléguer la complexité de gestion des serveurs et du réseau privé, vers les terminaux à un prestataire. Les réseaux locaux, dont l'architecture a pu être considérablement allégée, restent sous la responsabilité du RSI.

1.2.2.2 Réseaux Locaux

Chaque site dispose de l'architecture réseau suivante :

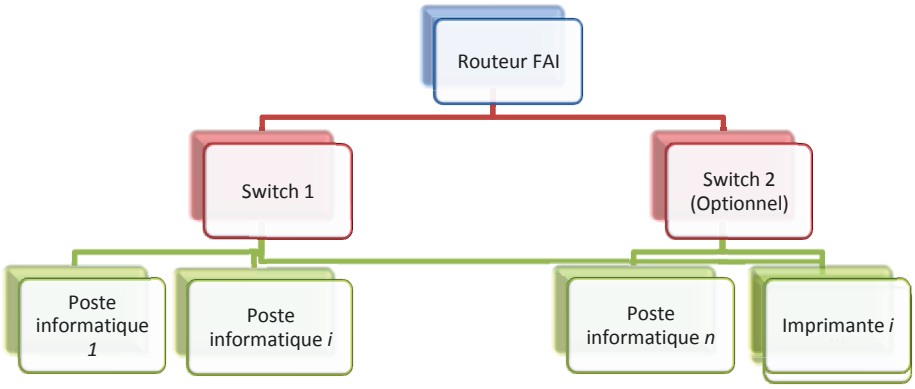


Figure 7 - Architecture du réseau local

Le Routeur FAI est l'interface entre les serveurs d'applications et le réseau local Il assure la connexion au réseau Internet et indirectement aux serveurs applicatifs hébergés. Il s'appuie sur des technologies Digital Suscriber Line (DSL) avec débit garanti ou non. Un service de Garantie de Temps de Rétablissements de 4 heures permet une reprise d'activité fiable sur cette ressource critique.

La technologie DSL montre cependant des limites sur des zones géographiques peu denses (Département 40, Landes). Il apparait des temps de latence importants qui perturbent les transmissions, que le débit soit garanti ou non. La technologie fibre optique, qui permettrait de garantir des temps de latence faibles, est actuellement indisponible ou financièrement démesurée.

Les Switchs assurent à tous les postes du réseau, un accès aux applications hébergées. Là encore, ces appareils sont accompagnés d'un service d'échange standard soit, le lendemain de la déclaration de panne. Durant cette période, un second Switch assure l'activité sur site. Cette redondance est en cours de généralisation.

Les Postes Informatique sont décrits dans le paragraphe suivant (1.2.2.3).

Les imprimantes et scanners sont les moyens de dématérialisation et de matérialisation. Le parc d'imprimante individuelle par poste bascule vers des systèmes d'impressions réseau tout en un (Impression, Fax, Scanner, Copie). Ce dernier est accompagné d'un service de maintenance, garantissant des faibles durées d'indisponibilité. Lorsque ces systèmes sont critiques, ils sont redondés. Tel le cas de la Direction Générale pour qui, l'édition des fiches de paies ne peut supporter une interruption supérieure à une demi-journée.

1.2.2.3 Postes Informatiques

Les postes informatiques sont de 3 types. Le plus répandu, environ 60% du parc est le poste lourd avec son disque dur, son lecteur DVD et son système d'exploitation le rendant, si besoin, indépendant des serveurs applicatifs.

Les ordinateurs portables représentent l'autre grande partie du parc avec environ 30% des machines. Ils ont les mêmes fonctionnalités que les postes lourds et présentent l'avantage d'être mobiles.

Enfin, le dernier type de terminal est le client léger. Contrairement aux postes lourds ils ne disposent pas de disque dur et leur système d'exploitation est limité puisque il ne permet que la navigation Internet et la connexion aux serveurs applicatifs via Citrix. Les principaux avantages de ces postes sont le prix et la conservation des performances initiales au fil du temps.

Majoritairement de la marque HP, ces terminaux fonctionnent sous le système d'exploitation (OS) Windows et sont accompagnés d'un service de maintenance garantissant un échange standard, le lendemain de la déclaration d'incident. La sécurité du réseau local est assurée sur ces terminaux via une application Antivirus, Firewall éditée par F-Secure.

1.2.3 Organisation du Département Informatique

Pour assurer la maintenance et les évolutions des services informatiques, l'Association s'est dotée d'un service informatique central confié à un cadre, le Responsable du Système d'Information (RSI). Ses relations avec les instances dirigeantes, les établissements et ses missions sont détaillées dans les paragraphes ci-dessous.

1.2.3.1 Organisation interne

1.2.3.1.1 RELATIONS

Le responsable hiérarchique du RSI est le Directeur Général.

Fonctionnellement les interlocuteurs privilégiés sont, le Directeur Administratif et Financier (DAF), la Directrice des Ressources Humaines, les Directeurs et Directeurs Adjoints d'établissements et enfin, les secrétaires d'établissements.

1.2.3.1.2 Missions

Les principales activités du RSI sont réparties en 5 sous-activités.

La première est la **gestion des projets** associatifs.

La seconde concerne la **gestion des achats.** En lien avec le Directeur Administratif et Financier il supervise la mise en concurrence des prestataires et suit l'exécution conforme des contrats. La téléphonie, mobile ou fixe, entre dans cette catégorie.

La troisième, plus technique que les précédentes, touche l'**administration du réseau.** Le RSI supervise la création des droits d'accès et des mots de passe, assure le reporting des dysfonctionnements et évalue les risques actuels ou potentiels,

La quatrième concerne la maintenance **des matériels et des logiciels**. Il supervise l'utilisation du réseau en accord avec les contrats négociés avec les prestataires (Coupure de service etc.). Il est le relais lors des incidents récurrents entre les utilisateurs et les prestataires.

Enfin, la dernière activité traite de la **formation** des utilisateurs. En lien avec la DRH et le service formation, le RSI identifie leurs besoins et anime des sessions.

1.2.3.2 Organisation externe

Les paragraphes précédents ont mis en évidence une architecture en 3 parties. La première concerne l'hébergement des applications et des données chez un prestataire. La seconde concerne le réseau utilisé pour se connecter aux sites de l'Association sur ces serveurs hébergés. La dernière concerne le parc des terminaux sur chaque site. Il est le lieu d'accès de tous les utilisateurs.

Figure 8 - Architecture en 3 parties

La fourniture des services de chacune de ces parties est confiée à un ou plusieurs prestataires. La flotte mobile est déléguée à un fournisseur unique.

1.2.3.2.1 Prestataires d'hébergement

Cette branche est confiée en quasi totalité, à une seule société : *ALFA*. Celle-ci héberge d'une part, toutes les applications et les données de l'Association, et d'autre part, en édite une grande partie. Le contrat qui défini le périmètre de ces prestations est valable jusqu'en juin 2014.

1.2.3.2.2 FAI

Ce domaine est entièrement confié à une seule société : *ORANGE*. Les accès Internet sont principalement de type DSL mais certains Directeurs disposent également d'une connexion 3G. ORANGE héberge aussi le serveur de mail de l'Association. Le contrat qui défini le périmètre de ces prestations est valable jusqu'en juin 2012.

1.2.3.2.3 Fournisseur du Parc

Les terminaux informatiques sont fournis par le prestataire d'hébergement, ALFA, partenaire du constructeur Hewlett Packard. Les solutions d'impressions sont, depuis 2011, confiées à 3 partenaires : La société EUROPA pour les systèmes inférieurs à 150 euros, la société ALFA pour des budgets situés entre 150 et 500 euros et, la société R2S pour les budgets supérieurs à 500 euros. Les contrats de maintenance de 3 ou 5 ans sont valables dès la mise en service de chaque machine.

1.2.3.2.4 Fournisseur Téléphonie

La flotte mobile, avec ces quelques 120 terminaux, est entièrement confiée à la société BOUYGUES Telecom. Le contrat qui défini le périmètre de ces prestations est valable jusqu'en novembre 2012.

1.2.4 Budget

1.2.4.1 Coût de fonctionnement

L'étude suivante montre le coût de fonctionnement d'un poste informatique pour une année (référence Janvier 2011). Les éléments pris en compte sont les suivants :

1. La maintenance matérielle et logicielle,
2. L'hébergement des logiciels et des données,
3. Les accès Internet,
4. La messagerie mails,
5. Le site Internet www.renovation.asso.fr.

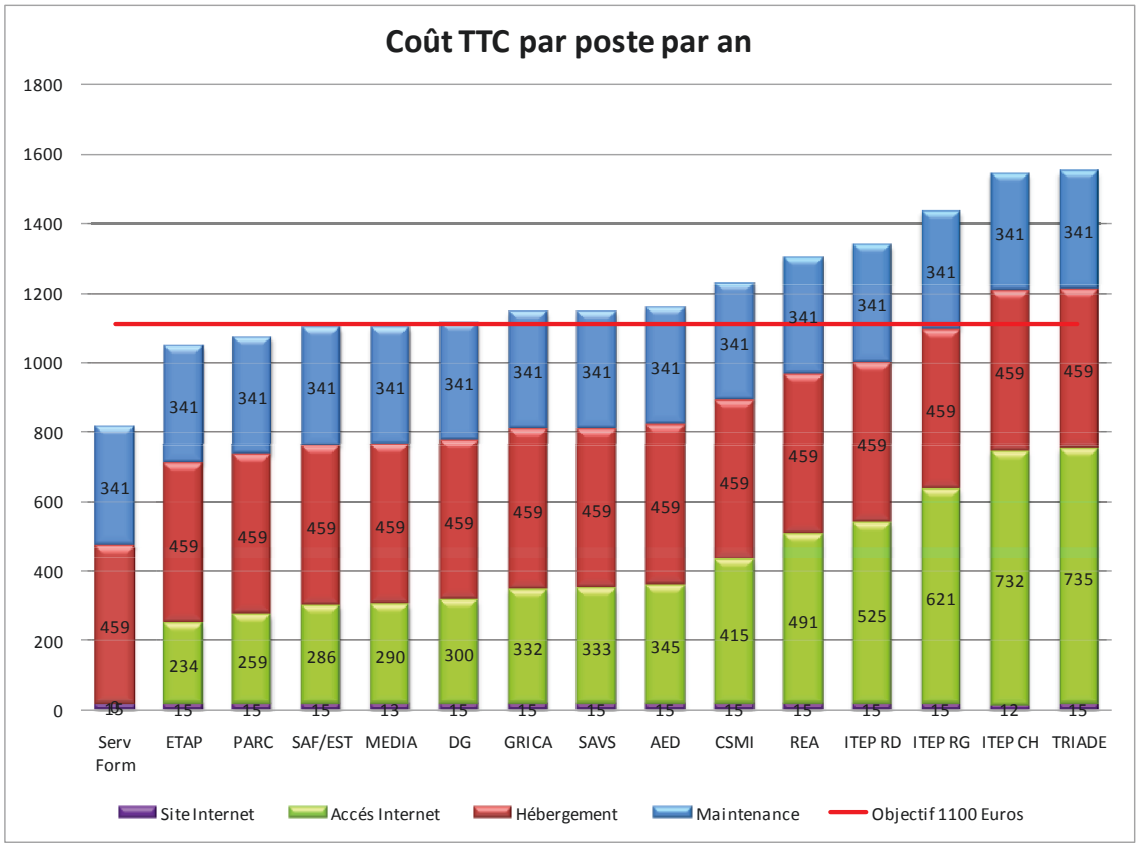


Figure 9 - Budget de fonctionnement du SI

Les contrats d'hébergement et de maintenance sont exclusivement gérés avec la société ALFA. L'Association étant un de ses plus grands comptes, il existe ainsi une très forte relation d'interdépendance entre ces deux sociétés.

Les accès Internet sont des de type nu (par opposition aux services VPN) et fournis par la société Orange. Le coût varie en fonction de la situation géographique des sites qui peut imposer l'utilisation de technologie SDSL dans des lieux ou l'ADSL est peu performante.

1.2.4.2 Investissements

Les investissements informatiques (postes, imprimantes et matériels réseau) sont gérés indépendamment pour chaque site en fonction de leur budget. La présentation de ce budget ne rentre pas dans le cadre de la présente étude, néanmoins, voici un modèle permettant d'évaluer le montant des investissements renouvelables tous les 5 ans, au 30 juin 2011. Une enveloppe de 800 euros TTC est en moyenne nécessaire pour acquérir un poste informatique. Pour un système d'impression/scan destiné à une dizaine d'utilisateurs, 2500 euros sont investis. L'installation d'un réseau informatique (hors câblage) demande 400 euros pour une dizaine de postes.

1.2.5 Synthèse

L'organisation des ressources du SI retenue par l'Association permet de :

1. donner un accès sécurisé à des applications spécifiques pour chaque site quelque soit son secteur d'activité,
2. d'organiser le département informatique avec 1 ETP en déléguant à des prestataires choisis, les services de maintenances et d'hébergement,
3. de définir et de contrôler le budget de fonctionnement et d'investissement,
4. d'identifier et de maintenir les besoins en compétences nécessaires au fonctionnement et à l'utilisation du SI.

Les ressources du SI étant définies, il est nécessaire de caractériser les besoins métiers de l'Association, pour ensuite déterminer si elles sont en adéquation (objet du paragraphe suivant). Cette adéquation sera mesurée avec un standard dont le choix sera abordé dans les paragraphes suivants.

1.3 Les Objectifs Métiers

1.3.1 Contrôle des risques

Comme présenté en introduction, l'objectif principal de la nouvelle direction est de contrôler les risques liés à l'utilisation du SI, dans le contexte sensible de l'Association.

En effet, les « clients » de l'Association Rénovation sont des adolescents et des adultes affectés par des troubles du comportement et des maladies psychiques. Ainsi, la simple information formée par le couple (nom du patient ; Association Rénovation),

rendue publique, peut être extrêmement préjudiciable pour le patient, soit, dans recherche d'un emploi, la contraction d'une assurance, d'un crédit, etc.

De la même manière qu'une information non rendue publique, l'identification d'une pathologie ne doit pas être accessible aux personnels non habilités, ni bien sûr, aux autres patients.

Dans la suite du document, cet objectif sera identifié comme OBJ1.

Objectif métier, OBJ1 : Contrôler les risques liés à l'utilisation du SI dans le contexte sensible de l'Association.

La responsabilité du contrôle et du reporting vers la direction de la satisfaction de ce besoin, compte tenu de l'organisation précédemment décrite, est naturellement confiée au RSI. Cette responsabilité vient s'ajouter aux missions décrites dans le paragraphe 1.2.3.1.2.

1.3.2 Maintien des performances des ressources

Pour atteindre OBJ1, sans altérer les performances actuelles du département informatique, il convient en premier lieu, de fournir les moyens d'actions nécessaires au RSI.

Ainsi, pour la Direction, les objectifs métiers à atteindre en priorité sont de maîtriser la charge de travail du RSI pour, garantir que les moyens d'actions et les performances sont en phases avec les missions confiées, et, assurer qu'OBJ1 peut être atteint.

Dans la suite du document, ces objectifs seront identifiés comme OBJ2 et OBJ3.

Objectif métier, OBJ2 : Garantir l'adéquation entre la charge de travail et les missions confiées.

Objectif métier, OBJ3 : Maintenir la performance du service informatique de l'Association.

Dans le cadre de la présente étude, seuls ces objectifs prioritaires seront pris en compte.

1.3.3 Etat des lieux du respect des objectifs

Avant la mise en place du référentiel d'évaluation, force est de constater qu'il est difficile de mesurer la satisfaction des 3 objectifs précités.

Concernant OBJ1, il n'existe pas d'inventaire des risques liés à la diffusion d'informations sensibles via le SI.

Outre la confidentialité de ces données, d'autres paramètres sont à prendre en compte pour évaluer les risques liés à leurs utilisations :

- *L'intégrité* : ce paramètre concerne l'exactitude et l'exhaustivité de l'information,
- *La disponibilité*: ce paramètre concerne la disponibilité de l'information au moment opportun,
- *La conformité* : ce paramètre concerne l'adéquation aux lois en vigueur, mais aussi, le respect des contrats auxquels est soumis le processus fonctionnel par les partenaires externes de l'Association (Exemple Transmission du Recueil d'Information Médicale Psychiatrique RIMP-P à l'ARS (via l'Agence Technique de l'Information Hospitalière) pour les établissements sanitaires).

Ce manque de formalisme ne signifie pas que des mesures préventives sont absentes pour minimiser l'apparition des risques. Elle dénote au minimum un manque de contrôle.

Concernant l'OBJ2, Il n'existe pas d'outil de mesure de la répartition de la charge de travail du RSI. Néanmoins, les hypothèses suivantes ont été retenues lors de sa prise de fonction :

- 30 % du temps est alloué au service desk,
- Les 70 % restants sont alloués à la gestion des projets de l'Association.

Cette répartition devrait permettre de répondre de manière satisfaisante aux demandes de supports des utilisateurs du SI, et également, de mettre en place dans les délais et les budgets alloués, les projets en SI de chaque établissement.

Il convient de préciser ici que l'importante charge de travail et l'organisation du département informatique ont été une des raisons du départ du précédent Responsable Informatique, peu de temps avant l'arrivée du nouveau Directeur Général. La mise en place d'un référentiel doit aboutir à mesurer et optimiser la charge du département.

Concernant OBJ3, il n'existe pas d'étude ou d'indicateur de performance et de satisfaction du département informatique par les usagers du SI. Là encore, cela ne signifie pas que le service précédent n'était pas performant mais simplement que cette satisfaction n'était pas mesurée et formalisée. Il n'existe par exemple pas d'exigences de délai formalisé pour résoudre les incidents déclarés.

1.3.4 Conclusion

Afin de contrôler les risques liés à l'utilisation de son SI, l'Association doit avant toute chose, s'assurer de disposer des moyens nécessaires au maintien et à l'évolution de l'organisation en place. A l'heure actuelle, il n'existe aucune donnée permettant de contrôler cette adéquation.

La Direction Générale a alors choisi de mettre en place, un référentiel d'évaluation pour mesurer et améliorer l'adéquation entre le SI en place et les objectifs métiers qu'elle s'est fixée. Le choix et la justification de ce référentiel sont traités dans les paragraphes suivants.

1.4 Choix du Référentiel d'évaluation

1.4.1 La stratégie

La Direction Générale souhaite s'appuyer sur un référentiel pour mesurer et améliorer l'adéquation entre le SI en place et les objectifs métiers qu'elle s'est fixée.

Pour déterminer quel référentiel utiliser, elle doit réaliser avec le RSI, une base d'exigences. Ces spécifications établies il sera alors possible de comparer puis de choisir l'un des 3 candidats suivants :

- « Information Technology Infrastructure Library » (**ITIL**),
- « Capability Maturity Model Integration » (**CMMI**),
- « Control Objectives for Information and related Technology » (**COBIT**).

La Direction n'étant pas familiarisée avec les standards SI, ne peut pas fixer efficacement des exigences à un référentiel. Quant au nouveau RSI, n'étant pas familiarisé avec la gestion d'un système d'information, il ne peut définir les processus devant être abordés en priorité par un système d'évaluation. Dans ce contexte, il n'est pas possible d'établir une base d'exigences.

Pour sortir de cette impasse, le RSI propose d'étudier un référentiel et de le présenter à la Direction Générale. Fort de ces connaissances il sera alors possible pour les 2 parties d'établir une base de spécifications pertinentes. Cette proposition est retenue.

Cette base de spécifications réalisée, il devient alors possible de mesurer les performances des 3 candidats.

Pour sa capacité à intégrer les référentiels ITIL et CMMI, COBIT a été retenu comme référentiel à étudier pour générer la base d'exigences. Ce choix est conforté également par le fait que l'ISACA, l'organisme qui publie COBIT, édite des ouvrages mesurant son référentiel à CMMI et ITIL (Documents [1] et [2]). Cette publication viendra en complément des connaissances pratiques de CMMI et théoriques d'ITIL du RSI.

1.4.2 Etude des capacités du référentiel COBIT

COBIT est un référentiel développé par l'ISACA (Information Audit and Control Association) en 1994 (35000 membres, 100 pays représentés), et repris maintenant par l'IT Governance depuis 1998. Le rôle de COBIT est d'améliorer la gouvernance des SI par une compréhension et une gestion des risques.

La **gouvernance**, selon l'IT Governance Institute, "a pour but de fournir l'orientation stratégique, de s'assurer que les objectifs sont atteints, que les risques sont gérés comme il faut et que les ressources sont utilisées dans un esprit responsable".

COBIT en reliant les objectifs du SI avec les objectifs de l'entreprise, permet d'en contrôler l'adéquation.

Il établit 7 objectifs qualitatifs que doivent atteindre les informations fournies par le SI pour répondre aux besoins métiers.

Le premier est l'**efficacité** qui qualifie toute information pertinente utile aux processus métiers, livrée au moment opportun, sous une forme correcte, cohérente et utilisable.

Le second est l'**efficience** qui qualifie la mise à disposition de l'information grâce à l'utilisation optimale (la plus productive et la plus économique) des ressources.

Le troisième est la **confidentialité** qui concerne la protection de l'information sensible contre toute divulgation non autorisée.

Le quatrième est l'**intégrité** qui touche à l'exactitude et à l'exhaustivité de l'information ainsi qu'à sa validité au regard des valeurs de l'entreprise et de ses attentes.

Vient ensuite la **disponibilité** qui qualifie l'information dont peut disposer un processus métier tant dans l'immédiat qu'à l'avenir. Elle concerne aussi la sauvegarde des ressources nécessaires et les moyens associés.

La **conformité** quant à elle consiste à se conformer aux lois, aux réglementations et aux clauses contractuelles auxquelles le processus métier est soumis, c'est-à-dire aux critères professionnels imposés par l'extérieur comme par les politiques internes.

Enfin, la **fiabilité** concerne la fourniture d'informations appropriées qui permettent au management de piloter l'entreprise et d'exercer ses responsabilités fiduciaires et de gouvernance.

Pour tendre vers ces objectifs, le SI utilise des **ressources**.

D'une part, des **applications** qui traitent l'information en s'appuyant sur une **infrastructure** constituée de technologies et d'équipements (machines, OS, SGBD, réseaux, multimédia ainsi que l'environnement qui les héberge et en permet le fonctionnement).

D'autre part, des **personnes** pour planifier, organiser, acheter, mettre en place, livrer, assister, surveiller et évaluer les systèmes et les services informatiques. Ces personnes peuvent être internes, externes ou contractuelles selon les besoins.

Bien sûr, l'**information,** constituée des données sous toutes leurs formes, saisies, traitées et restituées par le système informatique sous diverses présentations, et utilisées par les métiers est la ressource principale de la structure.

Enfin, pour gérer ces ressources produisant ces données, le COBIT a défini 34 **processus** répartis en 4 domaines.

Le premier est l**a planification et l'organisation** et consiste à définir les besoins fonctionnels, financiers, les priorités de l'organisation et ses projets.

Le second est **l'acquisition et la mise en place** et consiste à identifier les solutions, puis à les faire développer en interne ou à les acquérir, et à les intégrer dans les processus métiers. La maintenance de systèmes existants à travers la conformité aux besoins métiers, fait également partie de ce domaine.

Le troisième concerne **la distribution et le support** et permet de garantir l'efficacité et l'efficience du système en place. Les processus de continuité d'activité et de sécurité font partie de cette catégorie.

Pour finir, **la surveillance** consiste quant à elle à évaluer de façon périodique tous les processus, et à vérifier leur conformité par rapports aux exigences de l'entreprise.

Pour chacun de ces processus, COBIT définit des objectifs de contrôles qui fournissent l'assurance que les procédures, les pratiques et les organisations en place, sont bien conçues pour répondre aux objectifs métiers et que les événements indésirables sont prévenus, détectés et corrigés.

En synthèse, comme le montre le schéma suivant, les ressources informatiques sont gérées par des processus informatiques pour atteindre des objectifs informatiques qui répondent aux exigences métiers.

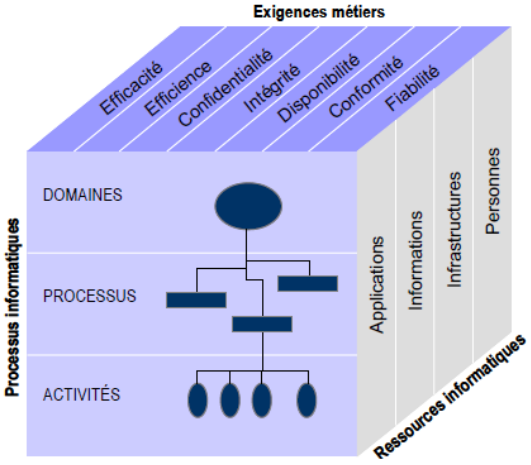


Figure 10 - Le cube COBIT

1.4.3 Les exigences pour la mise en place d'un référentiel d'évaluation

En poursuivant la stratégie de choix d'un référentiel d'évaluation précitée, il convient maintenant d'établir une base d'exigences.

Il a été décidé que le référentiel choisi doit être **compréhensible**, **adapté**, **couvrant** et enfin, **compatible** avec les principes du **Plan Do Check Act** (Planifier, Exécuter, Contrôler, Corriger et Améliorer). Voici une description détaillée de ces spécifications :

1.4.3.1 Compréhensible

Pour être présenté, adopté, mis en application et maintenu, le référentiel doit pouvoir être pris en main par toutes les parties prenantes du SI et pas seulement par le RSI. Ainsi, compte tenu du contexte de l'Association, une édition en **français** doit être disponible et maintenue et son contenu doit être **destiné** aux Directions Générales, Financières et Administratives.

1.4.3.2 Adapté

Pour être applicable, le référentiel doit être adapté à une organisation de taille moyenne bien sûr être compatible avec les objectifs métiers OB1, OBJ2 et OBJ3.

Il doit également permettre de traiter les caractères de données spécifiques à chacun des 3 secteurs de l'Association. Pour le sanitaire, la **confidentialité**, **l'intégrité** la **disponibilité** et la **conformité** sont une priorité. Pour le médico-social/social la plus forte contrainte concerne la confidentialité et enfin pour la Direction générale et Financière c'est la **fiabilité** qui est prioritaire.

1.4.3.3 Couvrant

Spécifiquement, le référentiel doit permettre de couvrir au moins les domaines suivants, même s'ils ne seront adressés qu'après cette étude :

- Gestion de projet (PO10),
- Les orientations technologiques (PO3),
- La formation des utilisateurs (DS07),
- La gestion de la performance et des capacités du Service Desk (DS03, DS04, et DS08),
- La résilience et la sécurité du SI(DS5),
- La gestion des investissements IT(PO5).

1.4.3.4 Compatible PDAC

Le référentiel doit dans un premier temps, permettre d'évaluer le SI en place puis, dans un second temps guider la mise en place et l'amélioration des processus nécessaires à son adéquation avec les objectifs métiers.

1.4.4 Les solutions envisagées

1.4.4.1 COBIT pour la gouvernance

La stratégie retenue implique que COBIT répond à toutes les exigences. La suite de l'étude va permettre d'établir s'il s'agit du référentiel le plus satisfaisant.

1.4.4.2 ITIL pour la gestion de production

1.4.4.2.1 Présentation Générale

ITIL a été mis en place en 1998 par l'organisation du commerce britannique (OGC). Dans sa version 3, c'est un référentiel désormais utilisé en Europe et aux Etats-Unis.

Les bonnes pratiques de ce référentiel sont organisées autour de la notion de services gérés sous formes de processus. Ces derniers permettent de favoriser l'utilisation et la gestion de l'infrastructure du SI, pour promouvoir un service optimal aux utilisateurs à des coûts justifiables.

ITIL s'articule autour de la notion de catalogue de service et met l'accent sur le cycle de vie de service suivant :

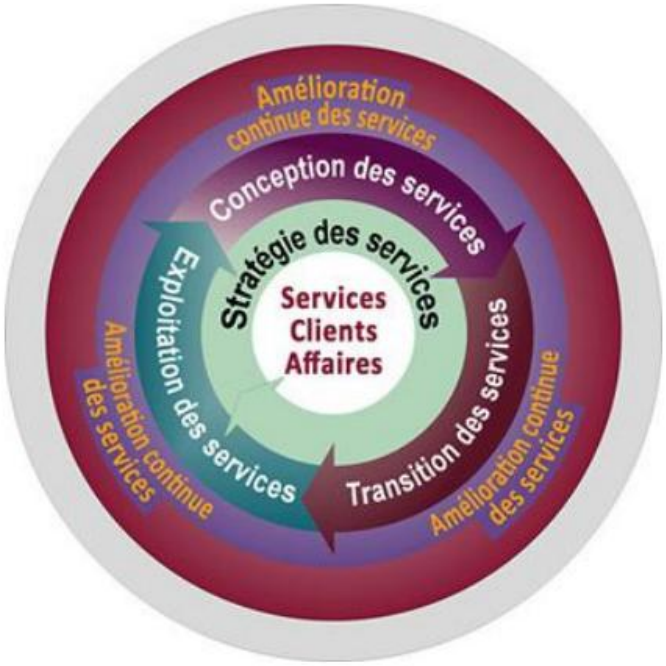


Figure 11 - Catalogue des services COBIT

En synthèse, la **stratégie de services** permet d'aligner l'organisation informatique sur les besoins d'affaires et la **conception**, la **transition** et **l'exploitation** des services

sont la matérialisation de la stratégie. **L'amélioration continue** des services permet de rester aligné et d'améliorer le système en place.

En détail, la **stratégie des services (SS)** a pour but de définir les objectifs à atteindre, les politiques à mettre en place, les ressources à mobiliser et la planification à mettre en place pour aligner la stratégie de l'entreprise avec celle du SI. Cette partie du cycle s'apparente à la catégorie Planifier et Organiser (PO) de COBIT.

La **conception des services (SD)** permet de concevoir les architectures, les processus informatiques, les outils internes de gestion pour répondre efficacement à la demande et fournir les niveaux de services convenus contractuellement (SLA) et suivant la stratégie définie précédemment. Cette partie utilise majoritairement les processus de la catégorie Distribution et Support (DS) de COBIT.

La **transition des services (ST)** permet d'élaborer et de gérer les plans de transition, l'accompagnement au changement, les risques et les critères d'acceptation, tester et valider les solutions, déployer et enfin de capitaliser les connaissances. Cette partie du cycle est abordée dans les processus de la catégorie Acquérir et Implémenter (AI) de COBIT.

L'**exploitation des services (SO)** prend en charge l'application des plans opérationnels, les procédures pour fournir la qualité de service convenue contractuellement, la surveillance et le reporting. Cette partie du cycle s'apparente majoritairement à la catégorie Distribution et Support (DS) du COBIT.

L'**amélioration continue des services (CSI)** aborde la production des rapports et l'analyse du fonctionnement de ce qui a été mis en place (solutions, processus, organisation, etc.) et la définition, le lancement et le pilotage des plans d'amélioration. Elle s'apparente principalement à la catégorie Mesure et Evaluation (ME) et Planifier et Organiser (PO) du COBIT.

Le document [2], à travers la figure 13 détaille pour chaque service les processus COBIT couvrant le domaine étudié.

1.4.4.2.2 Compréhensible

L'auditoire prévu par les exigences est bien pris en compte par ce référentiel (Figure 12 - Audience ITIL) et une version française est disponible.

Catégorie COBIT - Service ITIL / Rôle	Direction (Générale, Administrative et Financière)	Directionsmétiers	RSI	
Planifier et Organiser	S	S	A	COBIT
Acquérir et mettre en place	S	S	A	
Distribution et support	S		A	
Surveillance	S	S	A	
Stratégie de service	S	S	A	ITIL
Conception des services		S	A	
Transition des services	S	S	A	
Exploitation des services	S		A	
Amélioration continue des services	S	S	A	

***S** : Connaissance en synthèse - **A** : Connaissance Approfondie*

Figure 12 - Audience ITIL

Conclusion : ITIL, comme le COBIT, a été conçu pour être compréhensible par les Directions. La maitrise des complexités du référentiel est confiée au seul RSI.

1.4.4.2.3 ADAPTE

ITIL V3 et largement répandue dans les grandes structures. Il est également présent dans les organisations de taille moyenne comme l'Association.

Concernant la qualité des données adressées, la **confidentialité** (confidentiality) et **l'intégrité** (integrity) ne sont pas priorisés. De plus, la **conformité** (compliance) n'est pas abordée ce qui pénalise les établissements sanitaires (Figure 13 - Couverture des objectifs de données par ITIL).

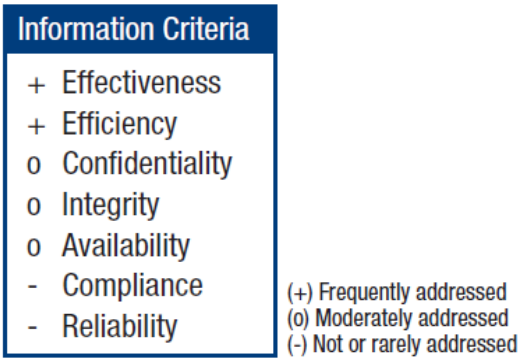


Figure 13 - Couverture des objectifs de données par ITIL

Enfin, la capacité d'ITIL à répondre aux OBJ, OBJ2 et OBJ3 est satisfaisante voir même excessive, pour la fonction Service de support niveau 2 du RSI de Rénovation estimée à 0.3 ETP. Le niveau 1, le plus sollicité, est en effet assuré par le fournisseur ALFA.

1.4.4.2.4 Couvrant

Le Document [1] à travers la Figure 14 - Couverture des processus COBIT par ITIL, permet d'évaluer les capacités d'ITIL à répondre au moins aussi bien aux objectifs des processus COBIT (en bleue foncé) ou au contraire son incapacité à les satisfaire (en blanc).

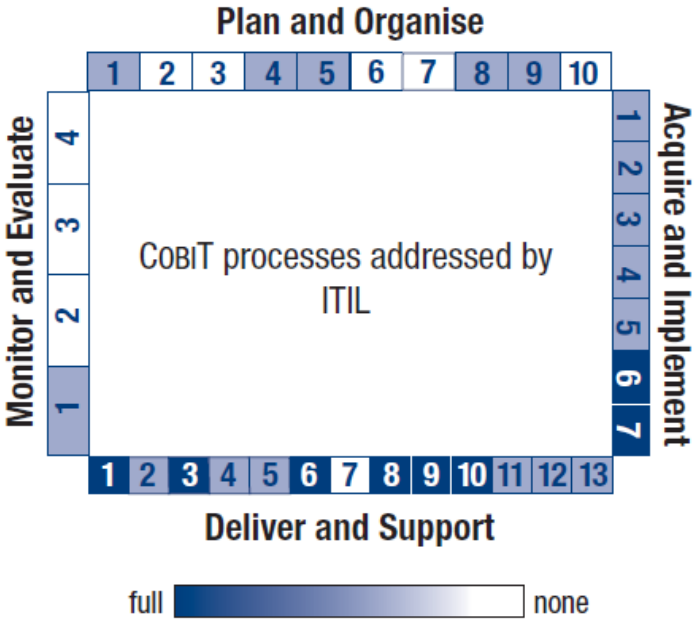


Figure 14 - Couverture des processus COBIT par ITIL

Ainsi, il est possible de constater que les processus retenus initialement ne sont pas tous couverts :

- Gestion de projet (PO10) : Meilleure capacité d'ITIL,
- Les orientations technologiques (PO3) : Non adressé par ITIL,
- La formation des utilisateurs (DS07) : Non adressé par ITIL,
- La gestion de la performance et des capacités du Service Desk (DS03, DS04, et DS08) : Meilleure performance d'ITIL à l'exception de la continuité de service.
- La résilience et la sécurité du SI(DS5) : Meilleure capacité de COBIT,
- La gestion des investissements IT(PO5) : Meilleure capacité de COBIT.

Conclusion : Bien qu'ITIL adresse mieux les fonctionnalités du Service Desk, les manquements sur la formation et les orientations technologiques le pénalise.

1.4.4.2.5 Compatible

Comme pour le COBIT, l'amélioration continue fait également partie d'ITIL à travers l'amélioration continue des services.

Conclusion : Les 2 référentiels offrent des garanties satisfaisantes pour permettre de maintenir une amélioration permanente des services.

1.4.4.2.6 Conclusion

Le référentiel ITIL principalement orienté vers les services informatiques aux utilisateurs, semble posséder une couverture des domaines du SI moins large que celle de COBIT. Néanmoins, la partie Distribution et Support (DS) du COBIT parait moins détaillée que celle d'ITIL.

Sachant que l'ITIL peut être parfaitement intégré dans le référentiel COBIT, ce dernier est retenu (voir Document [5]).

1.4.4.3 CMMI pour la gestion du développement

1.4.4.3.1 Présentation Générale

Ce référentiel a été conçu par le SEI (Software Engineering Institute) de l'université américaine de Carnegie-Mellon.

La première version est sortie en 2001 et était basée sur le précédent référentiel CMM. La version 1.2 retenue dans la présente étude date de 2006. La version 1.3 du référentiel a été éditée en 2011.

Les bonnes pratiques de ce référentiel sont organisées autour de 22 processus relatifs aux activités de développement et de maintenance associées.

La mise en place de CMMI peut se faire en considérant deux types de représentation.

La première, la plus répandue, est la représentation étagée (80 % des utilisateurs). Il s'agit d'une évaluation globale de l'entreprise en 5 niveaux. Le référentiel propose d'évaluer 7 processus au niveau 2, puis 11 au niveau 3, jusqu'à obtenir les 22 processus au niveau 5. Il n'y a que peu de place au choix des processus dans cette représentation.

La seconde, est la représentation dite Continue. Avec cette méthodologie, chaque processus est évalué indépendamment des autres pour déterminer son niveau d'aptitude dans l'entreprise.

La mise en place de ce référentiel devrait se faire en considérant la méthode la plus répandue, à savoir, la représentation étagée. Elle garantie en plus des choix de processus cohérents puisque ils sont réalisés par le SEI. La Figure 15 - Structure d'un niveau CMMI en représentation étagée apporte un premier aperçu de cette modélisation.

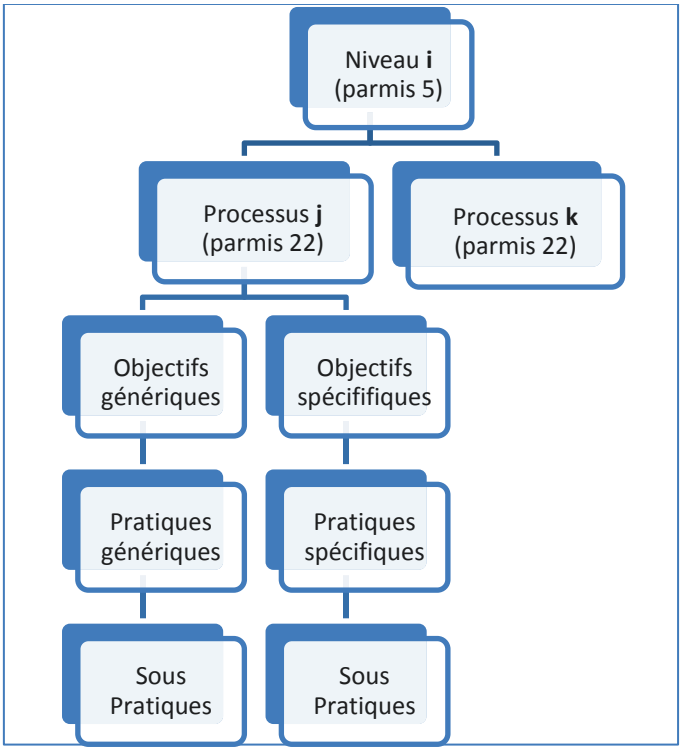


Figure 15 - Structure d'un niveau CMMI en représentation étagée

- *Niveau* : De 1 à 5,
- *Processus* : un processus parmi les 22 disponibles,

- *Objectifs génériques* : Les objectifs généraux communs à tous les processus ; le nombre d'objectifs retenus dépend du niveau,
- *Objectifs spécifiques* : Propres à chaque processus ; le nombre d'objectifs dépend du niveau,
- *Pratiques* : Elles comportent une définition, des commentaires,
- *Sous-pratiques* : Elles comportent des informations complémentaires aux pratiques.

Les 5 niveaux de maturités allant du plus faible (le niveau 1), au plus élevé (le niveau 5) sont détaillés ci-dessous :

Le **niveau 1**, dit niveau **initial** se caractérise par l'absence de processus. C'est le niveau de départ caractérisé par un mode « urgence permanente » sans planification.

Le **niveau 2**, dit **discipliné**, se consacre à la bonne réalisation d'un projet en considérant que les exigences initiales sont parfaitement définies. Les pratiques ne sont pas homogènes d'un projet à l'autre mais sont efficaces. 7 processus et leurs objectifs de niveau 2 sont retenus par CMMI : La gestion des exigences, la planification du projet, la conduite et la maîtrise du projet, la gestion des achats, la production et l'analyse des indicateurs, l'assurance qualité des processus et des produits et enfin la gestion de la configuration.

Le **niveau 3**, dit **standardisé**, améliore le niveau précédent en fournissant un environnement homogène de gestion de projet (Framework). 11 nouveaux processus et leurs objectifs de niveaux 3 en plus des 7 processus précédents doivent être maitrisés. Il s'agit d'analyse et prise de décision, du développement des exigences, de la gestion de projet intégrée, de la définition du processus organisationnel, de la focalisation sur les processus organisationnels, des solutions techniques, de l'intégration du produit, des recettes techniques, des recettes fonctionnelles, de la formation à l'organisation et enfin de la gestion des risques.

Le **niveau 4**, dit **quantifié**, permet d'alimenter un référentiel statistique mesurant l'efficacité des pratiques sur les projets de l'entreprise. 2 nouveaux processus et leurs objectifs de niveaux 4 et plus des 18 processus précédents doivent être maitrisés : La performance des processus et la gestion quantitative du projet.

Le **niveau 5**, dit **optimisé**, s'appuie sur les données statistiques précédemment acquises pour améliorer le référentiel en place. A ce niveau tous les objectifs de tous

les processus doivent être maitrisés. Viennent s'ajouter les 2 derniers processus concernant l'innovation organisationnelle et l,'analyse causale et solution des problèmes.

En 2009, les SSII françaises évaluées avec succès à ce dernier niveau, se comptent sur les doigts d'une main.

CMMI étant présenté, il est possible d'étudier sa capacité à répondre aux exigences de la Direction.

1.4.4.3.2 Compréhensible

Le CMMI, compte-tenu de sa portée internationale, est traduit en français, l'instar de ses 2 concurrents. Les concepts introduits par CMMI, particulièrement pour le développement logiciel, étant relativement éloignés des considérations métiers de l'Association, il est moins compréhensible que les référentiels COBIT et ITIL.

Conclusion : COBIT et ITIL abordant plus directement les objectifs métiers ou les services aux utilisateurs sont moins abstraits pour la Direction.

1.4.4.3.3 Adapté

Les sociétés utilisant CMMI sont, en France, principalement des SSII et des industriels de grandes tailles (Thalès, Airbus, etc.). Un niveau CMMI 3 ou supérieur a été dans le domaine aéronautique, un élément nécessaire pour pouvoir répondre à certaines offres de marché (en particulier aux USA).

Concernant la qualité des données, la confidentialité (Confidentiality), l'intégrité (integrity) et surtout la conformité (compliance) ne sont pas abordées dans CMMI comme le montre la Figure 16 - Couverture des objectifs de données par CMMI.

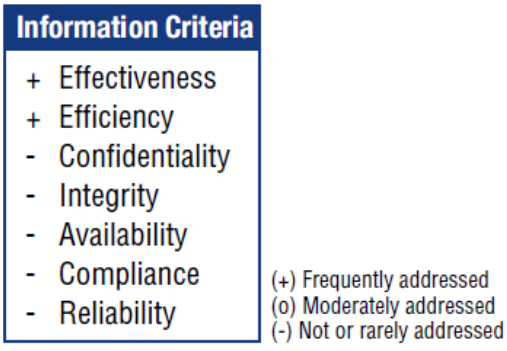


Figure 16 - Couverture des objectifs de données par CMMI

Sa capacité à répondre aux OBJ1 est satisfaisante grâce à un processus dédié.

Sa capacité à atteindre OBJ2 est nulle, puisque la gestion des ressources en dehors des projets n'est pas abordée.

Enfin, les possibilités de gérer les performances du Service informatique (OBJ3) vont se limiter, pour les mêmes raisons, à la gestion des projets SI en excluant le Service Desk.

Conclusion : Même si le CMMI déploie une batterie de processus pour maîtriser la gestion de projets, le COBIT, en ajoutant la gestion du Service Desk, reste le référentiel le plus adapté aux objectifs de la Direction.

1.4.4.3.4 Couvrant

Le Document [1] à travers la Figure 17 - Couverture des processus COBIT pour CMMI, permet d'évaluer les capacités d'du CMMIITIL à répondre au moins aussi bien aux objectifs des processus COBIT (en bleue foncé) ou au contraire son incapacité à les satisfaire (en blanc).

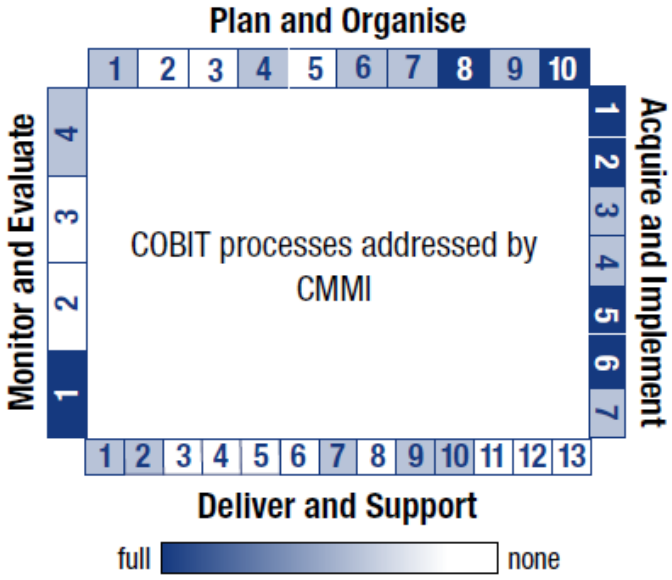


Figure 17 - Couverture des processus COBIT pour CMMI

Ainsi, il est possible de constater que les processus retenus initialement ne sont pas tous couverts :

- Gestion de projet (PO10) : Meilleure capacité de COBIT.
- Les orientations technologiques (PO3) : Non adressé par CMMI,
- La formation des utilisateurs (DS07) : Meilleure capacité de COBIT.

- La gestion de la performance et des capacités du Service Desk (DS03, DS04, et DS08) : Non adressé par CMMI,
- La résilience et la sécurité du SI(DS5) : Non adressé par CMMI,
- La gestion des investissements IT(PO5) : Non adressé par CMMI.

Conclusion : COBIT a systématiquement de meilleures capacités de couverture pour les processus retenus. En effet, principalement destiné à la gestion des projets informatiques, CMMI ne couvre que peu les exigences de l'Association.

1.4.4.3.5 Compatible

A l'instar des 2 autres référentiels, l'amélioration continue fait également partie de CMMI. Les principes de niveaux de maturités sont d'ailleurs repris dans COBIT pour évaluer les processus.

Conclusion : L'amélioration continue est intrinsèquement liée à CMMI qui en fait même un niveau de maturité (5).

1.4.4.3.6 Conclusion

Principalement orienté vers la production logicielle, CMMI n'est pas adapté à l'Association qui n'envisage aucun projet de développement. La gestion de projets CMMI, plus détaillée que celle de COBIT, pourrait toutefois être inclue dans le référentiel de l'Association grâce à la capacité d'intégration de COBIT.

De plus, la représentation étagée communément utilisée, impose l'évaluation de processus non prioritaires pour la Direction.

Le référentiel COBIT est donc toujours retenu.

1.4.5 La solution retenue

Comme le montre la Figure 18 - Résultat de comparaison des référentiels, l'approche précédente a permis de sélectionner le référentiel s'approchant le plus des besoins de l'Association.

	COBIT	ITIL	CMMI
Compréhensible	1	1	0
Adapté	2	1	0
Couvrant	2	1	0
Compatible PDCA	1	1	2
Total	6	4	2

Figure 18 - Résultat de comparaison des référentiels

1.4.5.1 Présentation détaillée de COBIT

Le paragraphe 1.4.2 a permis de montrer comment COBIT met en relation la production d'information de qualité par des ressources déterminées à travers des processus pour soutenir les objectifs métiers.

1.4.5.1.1 Des Objectifs métiers aux objectifs de contrôles des processus

L'annexe 1 du document [5] présentée dans les Figure 61 - Lien entre objectifs métiers et objectifs IT et Figure 62 - Lien entre objectifs IT et Processus, fournit une traçabilité d'un ensemble d'**objectifs métiers** génériques vers leurs traductions en **objectifs informatiques,** jusqu'aux **processus** les soutenant. La Figure 19 - Lien entre objectifs métiers et objectifs de contrôles de processus schématise cette traçabilité en s'appuyant sur l'objectif métier « Etablir une continuité de service ». Elle introduit également la notion d'**activité** vue dans le cube COBIT.

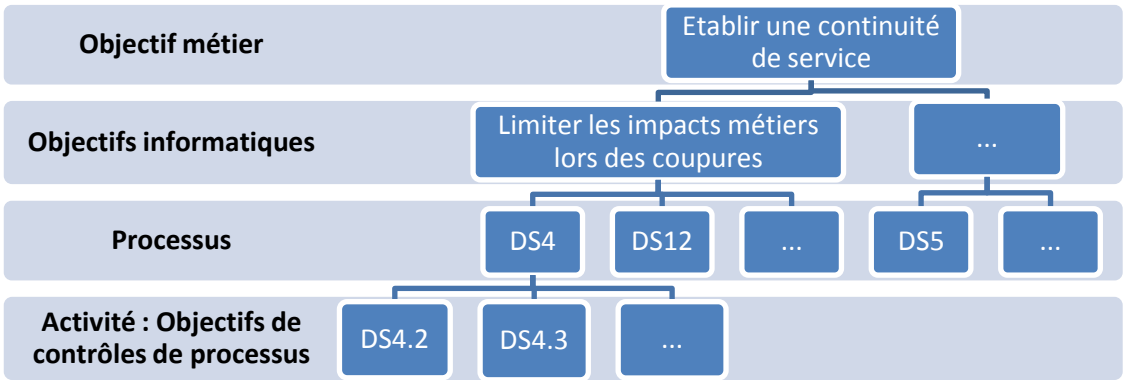


Figure 19 - Lien entre objectifs métiers et objectifs de contrôles de processus

1.4.5.1.2 Qualité des données

L'importance des 7 critères de qualité (voir paragraphe 1.4.2) des données produites par un processus, est bien sûr indiquée au niveau de chacun d'eux. Cette importance peut prendre trois valeurs :

- P : Principal, indique que ce critère est prépondérant dans les activités du processus,
- S : Secondaire, indique que ce critère est traité sans être prépondérant dans les activités du processus,
- Aucune valeur : indique que ce critère n'est pas traité dans les activités du processus.

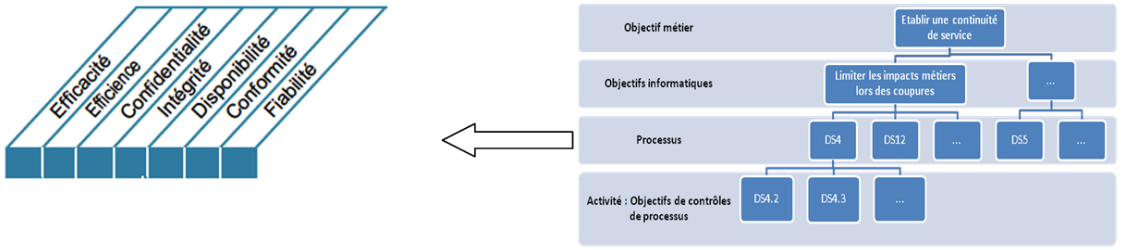


Figure 20 - Lien entre qualité de données et processus

1.4.5.1.3 Utilisation des ressources

Les ressources utilisées (voir paragraphe 1.4.2) dans la production des données produites par un processus sont naturellement indiquées au niveau de chacun d'eux.

La Figure suivante indique le formalisme retenu dans le document [5] pour qualifier les données.

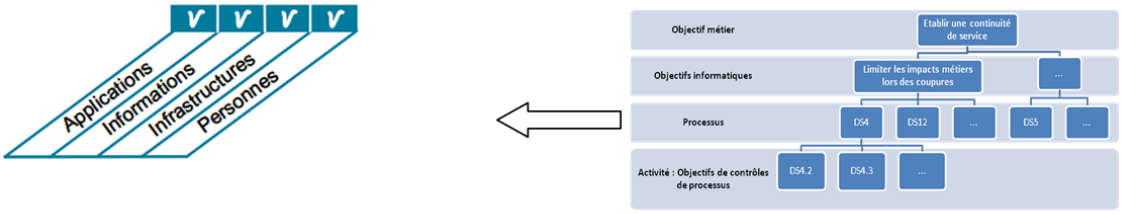


Figure 21 - Lien entre ressources et processus

1.4.5.1.4 Les Responsables des données

COBIT identifie des rôles génériques impliqués dans le fonctionnement de tout le processus. Etant trop générique, ces rôles ont été adaptés à l'Association comme le montre la Figure suivante.

Rôles COBIT	Responsables correspondants dans l'Association
Directeur Général (DG)	**Directeur Général (DG)**
Directeur Financier	Directeur Financier
Direction métier	**DG et groupes de Directeurs d'établissements**
Directeur Informatique DSI	RSI
Propriétaire de processus métier	**Groupe de Directeurs d'établissements**
Responsable de l'exploitation	Directeur d'établissements
Responsable de l'architecture	**RSI**
Responsable des développements	RSI
Responsable adminstratif de l'informatique	**RSI**
Responsable de la gestion des projets	RSI
Conformité, audit, rsique et sécurité	**Qualiticien & RSI**

Figure 22 - Lien entre Responsables COBIT et Responsables Association

Le terme « DG » regroupe ici le Directeur Général, Le Directeur Administratif et Financier et le Directeur des Ressources Humaines.

A chacun de ces rôles, en fonction du processus, est assignée une des 4 fonctions suivantes :

- **R**esponsable : celui qui exécute ou fait exécuter l'activité,
- **A**pprouver : celui qui donne les orientations et qui autorise une activité,
- **C**onsulté : Celui qui doit être informé et soutenir l'activité,
- **I**nformé : Identique au consulté mais avec un soutien de l'activité moins fréquent.

Dans le document [5] les relations Rôle/Fonction sont synthétisées, pour chaque processus, dans un tableau dit tableau « **RACI** ».

1.4.5.1.5 Mesure de la performance des processus

Une fois les ressources affectées aux processus il devient possible de produire des informations de qualité en vue de répondre à des objectifs métiers. Il est nécessaire d'établir des mesures pour constater ou non la réussite du processus, et de mettre en place des indicateurs pour évaluer les tendances de succès ou d'échec.

Dans COBIT, ces deux notions sont appelées **mesures de résultats** (ou *outcome measures* en anglais) pour indiquer si les objectifs ont été atteints, et **indicateurs de performance** (*performance indicator* en anglais) pour indiquer si les objectifs pourront être atteints.

Des mesures de résultats sont disponibles, des objectifs métiers jusqu'aux activités de processus comme le montre la Figure 23 - Lien entre Mesures de résultat et Objectifs.

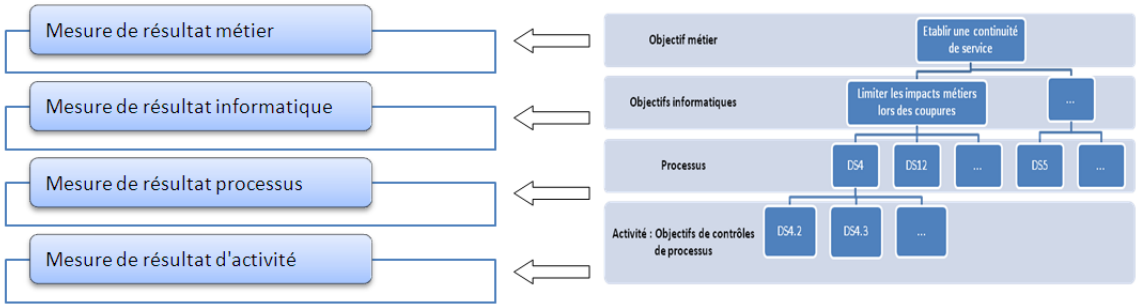


Figure 23 - Lien entre Mesures de résultat et Objectifs

Les indicateurs de performances correspondent au résultat de mesures du niveau immédiatement inférieur, comme le montre la Figure 24 - Lien entre Indicateur de performances et Objectifs.

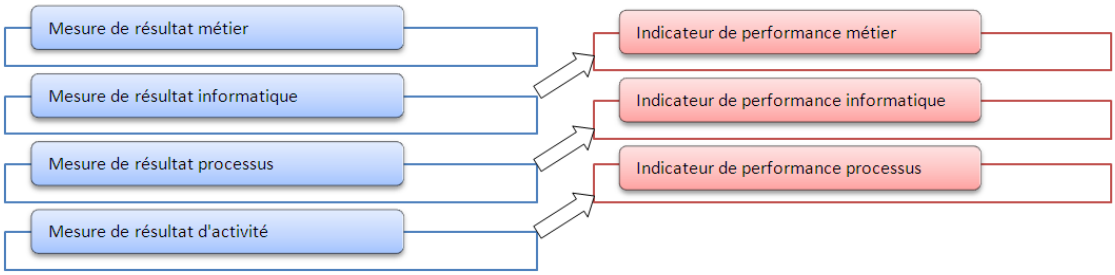


Figure 24 - Lien entre Indicateur de performances et Objectifs

1.4.5.2 Conclusion

Le référentiel COBIT semble donc le mieux placé pour répondre aux objectifs métiers OBJ1, OBJ2 et OBJ3. Il propose de les atteindre en mettant en place un ensemble de processus composés d'activités. Chacun de ces processus est capable de fournir une information de qualité en s'appuyant sur des ressources et des responsabilités clairement établies. Ces informations permettent de mesurer le respect de ces objectifs et les tendances actuelles.

Il reste dans un premier temps, à sélectionner les processus les plus pertinents parmi les 34 existants, et choisir une stratégie de mise en place adaptée à l'Association. Ces points sont traités dans les chapitres suivants.

2 Mise en place du référentiel COBIT

Avant de déterminer quelle est la stratégie à adopter pour mettre en place COBIT pour l'évaluation et l'amélioration du SI en place, il convient de se poser une question essentielle : Quels sont les moyens mis à disposition pour réaliser cette étude ?

2.1 Les moyens disponibles

Au lancement du projet, l'Association ne dispose d'aucune base permettant d'estimer le temps nécessaire à l'évaluation et la mise en place d'un processus COBIT. Considérant qu'il existe plus de 30 processus et ne disposant que d'une ressource (RSI) pour effectuer ces opérations dans des délais raisonnables, il a été décidé arbitrairement de n'auditer que 4 processus et d'en implémenter 2. Cet objectif pourra être revu à la baisse ou à la hausse en fonction de l'avancement constaté.

En s'appuyant sur une première phase de choix des processus il est alors envisagé de commencer l'implémentation du référentiel en s'appuyant sur le plan de développement présenté à la Figure 22.

Figure 25 - Implémentation du référentiel en 5 étapes

2.1.1 Budget

Financièrement, dans sa première itération, le projet possède une enveloppe de1700 euros, correspondant au coût de présentation du présent mémoire et à l'acquisition des ouvrages de référence.

D'un point de vue de la mobilisation des ressources, sont impliquées par ordre de charge de travail décroissante :

- Le RSI,
- Le Directeur Général,
- Le Directeur Administratif et Financier.
- Les Directeurs d'établissements.

La charge de travail allouée au RSI est de :

- **Phase 0** : 10 jours
- **Phase 1** : 30 jours.
- **Phase 2** : 20 jours.
- **Phase 3** : 40 jours
- **Phase 3** : A évaluer et à intégrer dans les charges courantes.

Les charges de travail des autres ressources ne sont pas évaluées.

2.1.2 Délai

D'un commun accord avec le Directeur Général et les Directeurs d'établissements, les délais pour réaliser l'implémentation sont les suivants :

- **Phase 0 et phase 1** : Du 01 janvier au 01 avril 2011.
- **Phase 2 et phase 3**: Du 15 mars au 31 décembre 2011.
- **Phase 4** : dès la phase 3 périodiquement.

2.2 Le plan d'implémentation

Les moyens disponibles pour l'implémentation étant connus, il convient maintenant de planifier leurs utilisations.

COBIT à travers les documents [3] et [4] propose deux approches de mise en œuvre.

La première, issue du document [3], s'adresse à des sociétés disposant de nombreuses ressources humaines et d'un budget conséquent. Aussi, c'est la deuxième approche, via le document [4], plus adaptée aux petites entreprises qui est préférée.

COBIT, à travers le document [4] (*figure 8 –Implementation Process*) propose une stratégie d'implémentation qui peut être rattachée aux phases précitées. C'est un plan en 7 étapes, insérant cette stratégie, qui est intégré et présenté dans la figure suivante.

	TITRE	DESCRIPTION	LIVRABLES	PHASE
ETAPE 0	Sélection des processus	Elaboration et mise en application des stratégies de sélection de 4 processus parmi le 34 disponibles.	4 processus sélectionnés	Phase 0
ETAPE 1	Compatibilité avec COBIT QuickStart	Réalisation des 2 tests de compatibilité de COBIT QuickStart avec le contexte de l'Association.	Utilisation de COBIT QuickStart validée	Phase 1
ETAPE 2	Evaluation de l'état courant	Audit des pratiques actuelles de l'Association en regard des processus COBIT retenus.	Performance actuelle des 4 processus sélectionnés	Phase 1
ETAPE 3	Détermination des objectifs	Détermination des nouveaux objectifs à atteindre avec la Direction.	Performance visée des 4 processus sélectionnés	Phase 1
ETAPE 4	Analyse des écarts	Détermination des pratiques manquantes attendues par COBIT et permettant l'atteinte des objectifs	Pratiques à mettre en place	Phase 1
ETAPE 5	Projets d'amélioration	Définition et ordonnencement des projets permettant de mettre en place les pratiques manquantes. Ils peuvent ou non être rattachés à différents processus.	Projets d'amélioration définis (charges, délais, conception technique et organisationnelle)	Phase 2
ETAPE 6	Réalisation des améliorations	Mise en œuvre des projets conformément aux priorités retenues.	Les projets	Phase 3
ETAPE 7	Contrôle et actions	Contrôle de l'atteinte des objectifs et mise en place des plans d'actions correctifs et d'améliorations.	Les plans d'actions	Phase 4

Figure 26 - Plan d'implémentation de COBIT

2.3 ETAPE 0 : Sélection des processus

Pour déterminer les processus les plus pertinents à évaluer, 2 stratégies ont été retenues.

La première consiste à prendre connaissance de tous les processus COBIT et de retenir et prioriser les plus intéressants pour la Direction. Cette approche pourrait être qualifiée d'ascendante puisque le point de départ de l'analyse est l'ensemble des 34 processus, et le point d'arrivée est un filtrage et une priorisation de ces processus par la Direction. Cette stratégie a l'avantage de présenter le référentiel COBIT dans son intégralité.

Dans la suite du document, cette stratégie sera référencée par STRAT1.

Stratégie d'évaluation STRAT1 : Approche Ascendante.

La deuxième consiste à utiliser le référentiel COBIT pour déterminer quels sont les processus les plus révélateurs pour répondre aux objectifs métiers OBJ1, OBJ2 et OBJ3. On pourrait qualifier cette approche de descendante puisque le point de départ de l'analyse est une sélection d'objectifs métiers, et le point d'arrivée, un sous-ensemble de processus couvrant au mieux les objectifs initiaux. Cette stratégie a l'avantage d'assurer un maximum de cohérence entre objectifs métiers et processus COBIT.

Dans la suite du document, cette stratégie sera référencée par STRAT2.

Stratégie d'évaluation STRAT2 : Approche Descendante.

Les résultats de ces 2 stratégies vont être confrontés pour en déduire les processus effectivement retenus pour l'audit.

2.3.1 Priorisation des catégories à évoluer

2.3.1.1 Stratégie 1

Toutes les (4) catégories sont retenues par la Direction. L'objectif fixé est de retenir au moins un processus de chaque catégorie pour avoir une vision étendue de COBIT. A ce moment là, ne sachant pas si la charge allouée est suffisante pour réaliser cet objectif, une priorisation doit être opérée. Voici donc l'ordre retenu (du plus important au moins important) :

2.3.1.1.1 Distribution et Support (DS)

Ce domaine concerne principalement les capacités actuelles du SI, à fournir les services demandés en conformité avec les besoins métiers et avec les règles de sécurité. Principalement adressé au RSI, ce domaine est privilégié puisque ce dernier vient de prendre ces fonctions, et qu'il mettra tout d'abord en œuvre l'implémentation de COBIT.

2.3.1.1.2 Acquisition et Implémentation (AI)

Ce domaine concerne l'identification des besoins et des solutions puis le développement ou l'acquisition de produits sur étagères, et enfin, leurs intégrations dans les processus d'affaires. La maintenance des systèmes existants et également pris en compte lors des acquisitions. Avec un projet à moyen terme, d'acquisition d'un logiciel de gestion de l'usager pour le secteur médico-social, cette catégorie est également privilégiée.

2.3.1.1.3 Planification et Organisation (PO)

Ce domaine consiste à définir la stratégie du SI pour faire contribuer au mieux le SI, et les objectifs de l'Association. La mise en œuvre de cette stratégie commence par une planification, puis est communiquée à la Direction. Il est alors possible de mettre en

place une organisation et une infrastructure technologique adéquate. Dans un premier temps, l'organisation et les performances de l'infrastructure technologiques en place vont être étudiées à travers la catégorie « Distribution et Support ». Une fois un premier bilan réalisé, les améliorations à mettre en place seront supportées par les processus de la présente catégorie.

2.3.1.1.4 Surveillance (ME)

Ce domaine consiste à évaluer régulièrement tous les processus en place et à vérifier leur conformité par rapport aux exigences de l'entreprise. La communication de ces résultats aux parties concernées fait également partie de ce domaine. Ce domaine est considéré comme le moins prioritaire, car des comptes-rendus réguliers de l'avancement de l'implémentation du référentiel, sont déjà planifiés avec le Direction et les Directeurs d'établissements.

2.3.1.2 Stratégie 2

Cette stratégie ne laisse pas la possibilité de prioriser les catégories à auditer puisque tous les processus sont étudiés, quelque soit leur catégorie.

2.3.2 Priorisation des processus à évaluer

2.3.2.1 Stratégie 1

L'ensemble des processus et de leurs objectifs a été parcouru avec la Direction Générale et sont présentés, ceux qui ont été retenus accompagnés d'une justification.

2.3.2.1.1 Assurer une continuité de service (DS04)

Le but de ce processus est de minimiser l'impact d'une interruption du SI, sur les utilisateurs de services sensibles, et de garantir un rétablissement rapide, sans perte majeure de données. Ce processus a été retenu car la mise en place de la nouvelle architecture a, au minimum, impliqué une très forte dépendance à une connexion Internet.

Ce processus est en lien direct avec OBJ1 et OBJ3.

2.3.2.1.2 Gestion du Service Desk et des incidents (DS08)

Le but de ce processus est de fournir aux utilisateurs du SI, des réponses de qualité et dans des délais raisonnables à toutes questions ou problèmes rencontrés. Avec la pertinence des solutions logicielles en place, c'est un des axes principaux de mesure de la satisfaction des utilisateurs.

Ce processus est en lien direct avec OBJ2 et OBJ3.

2.3.2.1.3 Garantir la sécurité du Si (DS05)

Ce processus permet d'évaluer et d'améliorer la pertinence et l'application des politiques de sécurité techniques et organisationnelles, pour minimiser les impacts résultants de l'utilisation d'une faille de sécurité. Les données sensibles relatives aux usagers, manipulées par l'Association sont particulièrement concernées par ce processus.

Ce processus est en lien direct avec OBJ1.

2.3.2.1.4 Gestion de l'environnement physique (DS12)

Ce processus permet d'évaluer et d'améliorer les exigences d'environnement du matériel professionnel. Il a été retenu car de nombreux sites professionnels sont directement implantés dans les bâtiments des usagers. Des accès à des données sensibles, à des personnes non autorisées, sont donc tout à fait envisageables et envisagés.

Ce processus est en lien direct avec OBJ1.

2.3.2.1.5 Acquisition et maintenance des infrastructures technologiques (AI03)

Ce processus permet d'évaluer et d'améliorer les processus d'acquisition, d'intégration et de maintenances des éléments d'architectures du SI.

Ce processus a été retenu car en 2009, un changement stratégique important à été effectué : Disparition des serveurs d'applications sur site, au profit d'un hébergement mutualisé. Les stratégies de choix des terminaux ont donc été considérablement revues et leurs efficacités doivent, au terme des 2 ans écoulés, être évaluées.

Ce processus est en lien direct avec OBJ3.

2.3.2.1.6 Gestion des investissements du SI (PO05)

Ce processus permet d'établir et de maintenir un cadre de gestion des investissements financiers du SI. Il prend en compte : Les coûts de fonctionnements, les investissements, les objectifs budgétaires et leurs satisfactions. Ce processus a été retenu pour évaluer et améliorer les procédures en place entre la Direction financière et le RSI.

Ce processus est lié à OBJ3.

2.3.2.1.7 Evaluation et gestion des risques (PO09)

Ce processus permet d'analyser et de communiquer les risques en lien avec l'utilisation du SI et leurs impacts avec les processus et les objectifs métiers. Il est l'expression directe de l'objectif métier OBJ1.

2.3.2.1.8 Gestion de projets (PO10)

Ce processus permet d'évaluer et d'améliorer le cadre de gestion des projets en cours et à venir dans le SI. Il a été retenu dans le cadre des nouvelles responsabilités du RSI : Assurer la gestion des projets SI en respectant les objectifs de qualité, les coûts et les délais alloués.

Ce processus est en lien direct avec OBJ2.

2.3.2.1.9 ME03

Ce processus permet d'assurer la conformité de l'utilisation du SI avec les lois et les obligations contractuelles. Il a été retenu dans le cadre de la manipulation d'informations médicales des usagers, pour les établissements sanitaires et médico-sociaux. Il est bien entendu directement lié à l'objectif métier OBJ1.

2.3.2.2 Stratégie 2

Pour aider une organisation à définir les objectifs métiers, COBIT propose 17 objectifs métiers génériques organisés selon les 4 perspectives suivantes :

- Financières,
- Client,
- Interne,
- Apprentissage et croissance.

Ils sont reliés aux critères d'information les plus significatifs (voir Appendice 1 du document [5]). A chacun d'eux est associée une liste d'objectifs SI génériques.

Une fois les objectifs métiers les plus significatifs choisis, il convient d'utiliser une matrice intitulée « Lier les objectifs SI aux processus COBIT » (voir Appendice 1 du document [5]). Elle propose de lier les 28 objectifs SI génériques aux processus COBIT les plus pertinents pour y répondre, et également de les relier aux critères d'information mais de manière plus fine.

Les paragraphes suivants dévoilent la mise en œuvre de cette stratégie.

2.3.2.2.1 Les objectifs métiers retenus

La Figure 27 - Traçabilité entre les objectifs métiers génériques de COBIT et ceux de l'Association présente la matrice de traçabilité retenue entre les 3 objectifs OBJ1, OBJ2 et OBJ3 et les objectifs métiers génériques proposés par COBIT.

Dans le contexte de l'Association, la différenciation entre la catégorie « Client » et « Interne » a peu de sens. En effet, si l'on considère que les clients sont les usagers, ces derniers n'ont pas accès au SI. Si l'on considère que les clients sont les financeurs, ce sont eux qui donnent accès à leur SI et non le contraire. Ainsi, dans la suite, les catégories « Client » et « Interne » ne seront pas différenciées et concerneront les utilisateurs du SI de l'Association.

		Business Goal	OBJ1	OBJ2	OBJ3
Financière	Retour sur investissement	BG01			
	Gérer les risques métier	BG02	X		
	Améliorer la gouvernance	BG03			
Client	Améliorer l'orientation client et le service client	BG04			X
	Offrir des produits et des services compétitifs	BG05			
	Etablir la continuité et la disponibilitré des services SI	BG06			X
	Rapidité à s'adapter aux modifications des exigences	BG07			
	Optimisation des coûts de la fourniture de services	BG08			
	Informations fiables et utiles à la prise de décision stratégique	BG09			
Interne	Améliorer et maintenir à niveau le fonctionnement des processus métier	BG10			
	Coûts des processus plus bas	BG11		X	
	Conformité aux lois et règlements externes	BG12			
	Conformité aux politiques internes	BG13			
	Innovation produits/métier	BG14			
	Améliorer et maintenir la productivité opérationnelle et celle du personnel	BG15		X	
Apprentissage & croissance	Gérer les innovations métiers et technologiques	BG16			
	Se procurer et conserver un personnel compétent et motivé	BG17		X	

Figure 27 - Traçabilité entre les objectifs métiers génériques de COBIT et ceux de l'Association

2.3.2.2.2 Les objectifs Si liés aux objectifs métiers retenus

Fort de ce choix d'objectifs métiers, il est désormais possible de sélectionner les objectifs IT les plus pertinents :

ID	Objectif IT	Retenu
IT2	Réagir aux exigences de la gouvernance en accord avec les orientations de la direction générale	
IT3	S'assurer de la satisfaction des utilisateurs finaux à l'égard des offres et des niveaux de services	X
IT7	Acquérir et maintenir fonctionnels des systèmes applicatifs intégrés et standardisés	
IT8	Acquérir et maintenir opérationnelle une infrastructure TI intégrée et standardisée	X
IT9	Se procurer et conserver les compétences nécessaires à la stratégie TI	X
IT10	S'assurer de la satisfaction réciproque dans les relations avec les fournisseurs tiers	
IT11	Intégrer progressivement des solutions informatiques aux processus métier	
IT13	S'assurer d'une bonne utilisation et des bonnes performances des applications et des solutions	X
IT14	Protéger tous les actifs TI et en être comptable	X
IT15	Optimiser l'infrastructure, les ressources et les capacités TI	X
IT16	Réduire le nombre de défauts et de tâches à refaire touchant la fourniture de solutions et de services	X
IT17	Protéger les objectifs TI	
IT18	Montrer clairement les conséquences pour l'entreprise des risques liés aux objectifs et aux ressources IT	X
IT19	S'assurer que l'information critique et confidentielle n'est pas accessible à ceux qui ne doivent pas y accéder.	X
IT20	S'assurer que les transactions métier automatisées et les échanges d'informations sont fiables	X
IT21	S'assurer que les services et l'infrastructure TI peuvent résister/récupérer convenablement en cas de panne due à une erreur, à une attaque délibérée ou à un sinistre	X
IT22	S'assurer qu'un incident ou une modification dans la fourniture d'un service TI n'ait qu'un impact minimum sur l'activité	X
IT23	S'assurer que les services TI sont disponibles dans les conditions requises	X
IT24	Améliorer la rentabilité des TI et leur contribution à la profitabilité de l'entreprise	X

Figure 28 - Les objectifs SI retenus

Justifications :

IT2 : Cet objectif n'a pas été retenu car la Direction n'a pas encore spécifié d'exigences de gouvernance. La définition des 3 objectifs métiers OBJ1, OBJ2 et OBJ3 est déjà une première étape dans ce sens.

IT7 : Au lancement de l'audit COBIT, cet objectif n'a pas été retenu, car aucun projet d'acquisition d'application n'a été lancé. La maintenance des applications existantes est, quant à elle, contractuellement déléguée aux 2 fournisseurs principaux ALFA et CORWIN. Dans le courant de l'année 2011 un projet d'acquisition d'un logiciel de gestion du dossier de l'usager a vu le jour pour l'ensemble des établissements médico-sociaux.

IT10 : Cet objectif n'a pas été priorisé car la gestion de relations fournisseurs est initialement réalisée en tandem avec le Directeur Administratif et Financier. La pertinence de l'utilisation de COBIT pour gérer cette mission sera évaluée ultérieurement.

IT11 : Cet objectif n'a pas été retenu pour les mêmes raisons que pour l'objectif IT7.

IT17 : Cet objectif n'a pas été retenu car, dans le contexte de l'Association, il concerne principalement l'identification et la gestion des risques liés à l'utilisation du SI. Ce point est couvert par l'objectif IT18 qui lui, a été retenu.

2.3.2.2.3 Les processus retenus

Fort des 14 objectifs métiers précédemment retenus, il est possible, grâce à la matrice « Lien entre Objectifs TI et Process TI » (voir Figure 62), de dresser une liste des processus COBIT répondant à ces derniers. Chaque processus pouvant couvrant plusieurs objectifs, il devient nécessaire de compter le nombre de fois où ils sont référencés. La figure suivante synthétise le nombre de référencement par processus pour les 14 objectifs métiers retenus :

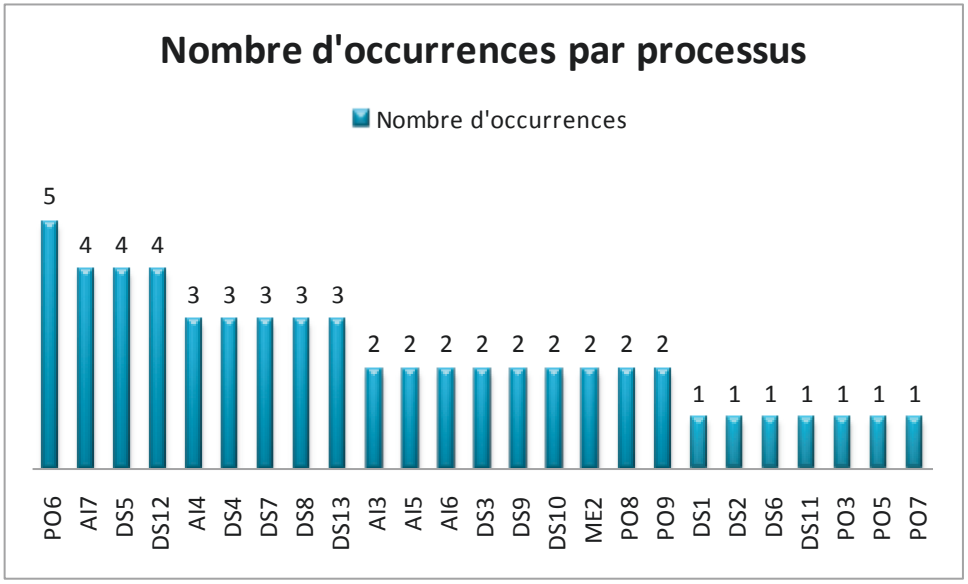


Figure 29 - Sélection de Processus par la stratégie 2

Il est encore possible de réduire cette liste de 25 processus à 18 en excluant ceux n'apparaissant que pour un seul objectif IT.

2.3.3 Les processus retenus

Les 2 stratégies donnent des résultats qui sont synthétisés dans la Figure 30 - Synthèse des stratégies STRAT1 et STRAT 2

	STRAT 1	STRAT 2	RETENU
AI3	X	X	
AI4		X	
AI5		X	
AI6		X	
AI7		X	
DS3		X	X
DS4	X	X	X
DS5	X	X	X
DS7		X	
DS8	X	X	X
DS9		X	
DS10		X	
DS12	X	X	
DS13		X	
PO5	X		
PO6		X	
PO8		X	
PO9	X	X	
P10	X		
ME2		X	
ME3	X		
Total	9	18	4

Figure 30 - Synthèse des stratégies STRAT1 et STRAT 2

Comme cela a été précisé en début de chapitre, seulement 4 processus seront audités lors de la première itération.

Entièrement sous la responsabilité du RSI, la catégorie Distribution et Support est privilégiée. Un processus est retenu s'il est sélectionné dans les deux stratégies. Ainsi, les processus DS4, DS5, DS8sont choisis.

Le processus DS3 est retenu au dépend du processus DS12 pour sa capacité à optimiser l'utilisation des ressources, pour répondre aux besoins métiers et ainsi satisfaire l'objectif OBJ2.Il est en effet inutile de lancer des projets d'améliorations de la sécurité physique si aucune ressource n'est disponible.

Le processus DS12 sans être remplacé, est partiellement couvert par le processus DS5 pour l'aspect sécurisation des accès aux terminaux. L'aspect redondance des données est déjà largement assuré par l'hébergement chez le fournisseur ALFA.

Justifications :

AI3 : Cette activité et les processus associés, en particulier le AI3 (Acquisition et maintenance des infrastructures technologiques), n'ont pas été retenus pour la première évaluation pour deux raisons : La première, est que, la maintenance des infrastructures et des applications est confiée en premier niveau au fournisseur ALFA. La seconde, est qu'à court terme, aucun projet d'acquisition d'applications ou de terminaux n'est envisagé.

PO9 : Ce processus (évaluer et gérer les risques IT), n'a pas été retenu pour la première évaluation car il nécessite en entrée deux processus déjà retenus : DS4 pour la continuité de service et DS5 pour la sécurité du SI. Il sera évalué en priorité lors de la prochaine itération.

2.4 ETAPE 1 : Compatibilité COBIT QUICKSTART

Le document [4] propose une méthode d'implémentation du référentiel COBIT adaptée aux PME. En synthèse, cette méthode s'appuie sur :

- Un plan d'implémentation simplifié (le présent plan),
- Sur une liste réduite d'objectifs de contrôles.

Afin de garantir de bonnes chances de réussite, sont proposés 2 tests (voir figure 5 et figure 6 du document [4]). Ainsi, originellement, la présente étape consiste à passer et valider ces tests.

Dans le cadre de la mise en place du référentiel pour l'Association, ces tests ne seront pas réalisés. Seul le plan d'implémentation est retenu.

Ce choix n'engendre aucun risque puisque les objectifs de contrôles qui vont être retenus correspondent à la version complète de COBIT et ne sont pas limités comme le préconise le document [4].

2.5 ETAPE 2 : Evaluation de l'état courant

2.5.1 Choix des sources de données

On peut identifier 3 sources de données pour l'évaluation. La première est basée sur l'évaluation in situ avec les Directeurs d'établissements. La seconde est basée sur les documents de gestion du parc Informatique existants : Inventaire, bilans financiers validés, base de suivi des incidents, etc. La dernière consiste à étudier les comptes-rendus d'activités et les bilans validés avec les représentants des sous-traitants.

2.5.2 Adaptation des CHECK-LISTS

Le référentiel d'évaluation des processus proposé dans le document [4] est considérablement allégé par rapport à la version complète décrite dans le document [5]. Les principaux allégements concernent :

- La grille des responsabilités est réduite à 5 rôles : Le comité exécutif (ici la Direction Générale), le responsable du SI (ici le RSI), le responsable des développements du SI (ici à nouveau le RSI, le responsable des services du SI (ici à nouveau le RSI) et les responsables métiers (ici, suivant le contexte, des groupes de Directeurs d'établissements, le Directeur Administratif et Financier, la Directrice de Ressources Humaines).
- Le nombre d'objectifs de contrôles.
  Dès la première évaluation ce sera bien la totalité des objectifs présentés dans le document [5] qui sera évaluée.
- Les mesures de résultats et les indicateurs de performances sont maintenus.
- Le modèle de maturité est simplifié. Cependant, c'est le modèle de maturité du processus complet qui est retenu dès la première évaluation.

2.5.3 Choix des mesures de résultats

2.5.3.1 DS08

2.5.3.1.1 Métier

Dans l'optique de fournir des services de qualité à ces utilisateurs, en relation directe avec OBJ3, le taux de satisfaction des utilisateurs des services est retenu. Soit **DS08-MR-MET01** cette mesure de résultat.

OBJ1 et OBJ3 ne sont pas directement impactés par ce processus DS08.

2.5.3.1.2 Informatique

Pour la première mise en application de COBIT, ce sont les performances du service informatique interne à l'Association, à travers son RSI, qui vont être suivies. Les performances des services des sous-traitants seront observées ultérieurement.

Ne disposant que d'une ressource, il est impossible de garantir un délai de résolution constant (SLA pour Service Level Agreement en anglais). En effet, pendant les absences du RSI, n'étant pas remplacé, les délais ne pourraient être tenus. Néanmoins, il est possible de mettre en place un objectif de délai de service (SLO pour Service Level Objective en anglais).

Ainsi, c'est le pourcentage d'incidents résolus dans les délais fixés par les contrats d'objectifs (SLO) qui est retenu comme mesure de résultat. Soit **DS08-MR-INFO01** cette mesure.

2.5.3.1.3 Processus

Afin de pouvoir fixer des objectifs de délais de service interne, il est nécessaire de suivre les capacités de résolutions par type de demandes.

C'est pourquoi la durée de vie moyenne des incidents par type est retenue comme mesure de résultat. Soit **DS08-MR-PRO01** cette mesure.

2.5.3.1.4 Activité

En lien direct avec les objectifs de délais de services, les incidents ouverts et fermés doivent être suivis périodiquement. Cela permet de déterminer les capacités de traitement du service interne et de planifier les résolutions des incidents en fonction des disponibilités du RSI. Parmi ces incidents, les plus chronophages, pour le service interne, sont ceux qui réclament une intervention sur site ou qui ne peuvent être délégués à des services extérieurs. Aussi, 2 mesures de résultat ont été retenues :

- Nombre d'incidents enregistrés par mois. **DS08-MR-ACT01** cette mesure de résultat,
- Nombre d'incidents résolus par mois. **DS08-MR-ACT02** cette mesure de résultat.

2.5.3.2 DS03

2.5.3.2.1 Métier

Dans l'optique de garantir une adéquation convenable entre la charge de travail et les missions confiées à ses services, en relation directe avec OBJ2, le nombre de ressources humaines en surcharge est retenu par la Direction Générale. Soit **DS03-MR-MET01** cette mesure de résultat.

OBJ1 et OBJ3 ne sont pas impliqués directement dans ce processus.

2.5.3.2.2 Informatique

Pour la première mise en application de COBIT, la charge de travail du service informatique interne à l'Association, à travers son RSI, va être suivie. Alors que le processus DS08 contrôle la performance du service informatique interne, le présent processus est l'occasion de suivre la charge allouée aux projets SI et au service desk. L'objectif est de pouvoir détecter la sur-utilisation chronique du RSI par le Service Desk au dépend des projets SI.

Aussi, la répartition de charge entre les projets SI et le service Desk est retenue comme mesure de résultat. Soit **DS03-MR-INFO01** cette mesure.

2.5.3.2.3 Processus

Le suivi du respect des objectifs de délais pour le service Desk étant assuré via le processus DS08, le processus DS03 s'attache à la gestion des projets SI. Ainsi les 2 mesures de résultats suivantes sont retenues :

- Nombre de projets SI en cours. Soit **DS03-MR-PRO01** cette mesure de résultat.
- Nombre de projet dans les délais. Soit **DS03-MR-PRO02** cette mesure de résultat.

2.5.3.2.4 Activité

Pour s'assurer que les délais alloués aux projets SI sont respectés, il est nécessaire de revoir régulièrement les plannings et de s'assurer que les décalages éventuels sont bien transmis aux parties prenantes.

C'est pourquoi la fréquence des mises à jour et des validations du planning est retenue comme principale mesure de résultat. Soit **DS03-MR-ACT01** cette mesure de résultat.

2.5.3.3 DS04

2.5.3.3.1 Métier

Pour la Direction, à travers les objectifs OBJ1 et OBJ3, le nombre d'heures perdues dû à une indisponibilité des ressources matérielles est retenu comme mesure de résultat. Soit **DS04-MR-MET01** cette mesure.

OBJ2 n'est pas impliqué dans ce processus.

2.5.3.3.2 Informatique

Pour le département informatique, les indisponibilités du SI peuvent impacter 3 types d'usagers : L'Association dans son ensemble, en cas de rupture des services d'hébergement, un site, en cas de rupture d'une connexion Internet ou, un utilisateur, en cas de panne de terminal.

Ainsi, le nombre d'heures d'indisponibilité du SI par type et pendant les horaires de travail est retenu comme mesure de résultat. Soit **DS04-MR-INFO01** cette mesure.

2.5.3.3.3 Processus

Le principal moyen de rétablir des ressources matérielles dans un délai donné est une organisation spécifique du fournisseur qui peut alors, garantir contractuellement un temps de rétablissement maximal (Cette garantie est connue sous le nom de GTR pour Garantie de Temps de Rétablissement).

Aussi, le nombre de postes non maintenus via une GTR est retenu comme mesure de résultat. Soit **DS04-MR-PRO01** cette mesure de résultat.

2.5.3.3.4 Activité

Pour s'assurer que les garanties de temps de rétablissements sont correctement réparties, il convient de tester les plans de continuité d'activité pour s'assurer d'une part, de leur efficacité, et d'autre part, de leurs mises à jour.

Ainsi, la fréquence des tests et des revues des plans de continuité d'activité est retenue comme mesure de résultat. Soit **DS04-MR-ACT01** cette mesure.

2.5.3.4 DS05

L'implémentation retenue pour les mesures de résultats de ce processus est directement issue du document [5] figure 27 et 28 référencés en annexe.

2.5.3.4.1 Métier

La mesure de résultat retenue pour ce processus, en lien direct avec OBJ1 est le nombre d'incidents qui ont permis à des tiers d'accéder à des infirmations sensibles des usagers. La présence d'un usager au sein de l'Association est déjà une donnée sensible. Soit **DS05-MR-MET01** cette mesure.

OBJ2 et OBJ3 ne sont pas directement impactés par ce processus.

2.5.3.4.2 Informatique

Compte tenu des possibilités d'accès par les usagers aux outils professionnels, 2 mesures de résultats ont été retenues à ce niveau :

- Nombre d'incidents avec impact potentiel sur des tiers. Soit **DS05-MR-INFO01** cette mesure. Ce résultat sera issu de la base d'incidents des services Desk internes et externes.
- Délai de changement des droits d'accès au système. Soit **DS05-MR-INFO02** cette mesure. Ce résultat sera issu du service Desk interne.

2.5.3.4.3 Processus

Au niveau du processus, le nombre d'utilisateurs ayant un mot de passe ne répondant pas aux règles de sécurité a été retenu comme mesure de résultat. Soit **DS05-MR-PRO01** cette mesure.

2.5.3.4.4 Activité

En lien avec la mesure de résultat précédente, 2 mesures de résultats pour les activités de ce processus sont retenues :

- Nombre de comptes obsolètes, c'est-à-dire un compte utilisateur actif alors que ce dernier n'a plus de fonction dans l'Association (retraite, démission, exclusion, etc.). Soit **DS05-MR-ACT01** cette mesure.
- Nombre de comptes créés et révoqués par mois. Soit **DS05-MR-ACT02** cette mesure.

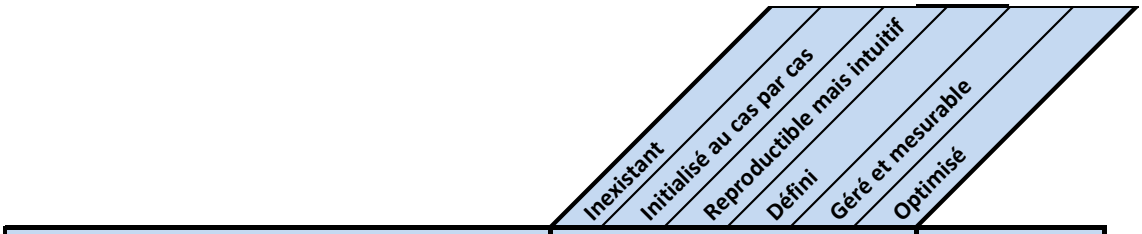
2.5.4 Résultat d'Audit

L'évaluation des 5 processus dans l'ensemble des sites de l'Association, s'est déroulée du mois de décembre 2010 au mois de mars 2011. La situation rencontrée

correspondait à celle laissée par le précédent responsable informatique. Les impacts dus à l'arrivée du nouvel RSI n'étaient pas encore mesurables.

2.5.4.1 DS8

L'évaluation de ce processus concerne uniquement la gestion interne des incidents. Les services de supports des fournisseurs logiciels, matériels et accès Internet seront évalués ultérieurement, dans le cadre de la gestion de la sous-traitance.



Processus		Evaluation						Rôles		
ID	Objectif de contrôle	0	1	2	3	4	5	DG	RSI	Resp. Métier
DS8.1	Service Desk		X						G/R	
DS8.2	Enregistrement des demandes		X						G/R	
DS8.3	Procèdure d'escalade		X						G/R	
DS8.4	Cloture des demandes		X						G/R	
DS8.5	Reporting et analyse des tendances		X					I	G/R	

***R** : Responsable, **G** : Garant, **I** : Informé, **C** : Consulté*

Figure 31 - Evaluation DS8

ID	Libellé	Mesure
DS08-MR-MET01	Taux de satisfaction des utilisateurs	NC
DS08-MR-INFO01	pourcentage d'incidents résolus dans les délais (SLO)	NC
DS08-MR-PRO01	Durée moyenne d'ouverture des incidents par type	NC
DS08-MR-ACT01	Nombre d'incidents enregistrés par mois	NC
DS08-MR-ACT02	Nombre d'incidents résolus par mois	NC
DS08-MR-ACT03	Nombre d'incidents nécessitant une intervention RSI	NC

***NC** : Non connu*

Figure 32 - Mesures de résultats DS8

Interprétation :

La maturité :

Aucun processus ne décrit les activités de support du service informatique de l'Association. En cas de problème, son responsable est directement sollicité par téléphone ou par mail. Il n'existe pratiquement aucun suivi des incidents permettant à une personne externe de savoir s'ils sont résolus ou en attente d'actions spécifiques. La seule exception concerne les incidents déclarés au fournisseur ALFA, dans

certaines conditions. La Direction est consciente de ce besoin de support interne, et l'a formalisé à travers la fiche de poste du nouveau RSI.

Le processus est donc évalué au niveau de maturité 1.

Les rôles:

Le responsable informatique précédent réalisait avec le Directeur Administratif et Financier, des réunions à sa demande pour faire un point sur l'état des travaux en cours. Ces réunions ne donnaient pas systématiquement lieu à des comptes-rendus.

Les mesures de résultats disponibles :

Il n'existe aucun enregistrement permettant de fournir les mesures de résultats attendues. Néanmoins, la satisfaction des services rendus par le précédent responsable informatique, a été fréquemment évoquée par les utilisateurs.

2.5.4.2 DS3

Ce processus est uniquement évalué pour la ressource informatique RSI. La gestion de ses capacités et de ses performances est directement liée aux objectifs métiers OBJ2 et OBJ3. Les capacités et les performances des infrastructures et des applications informatiques seront évaluées ultérieurement.

Processus		Evaluation						Rôles		
			Inexistant	Initialisé au cas par cas	Reproductible mais intuitif	Défini	Géré et mesurable	Optimisé			
ID	Objectif de contrôle	0	1	2	3	4	5	DG	RSI	Resp. Métier
DS3.1	Planning de performance et de capacité		X						R	
DS3.2	Performance et capacité actuelles		X						R	
DS3.3	Performance et capacité prévisionnelles		X						R	
DS3.4	Disponibilité des ressources IT		X					G		
DS3.5	Suivi et comtpe-rendu		X						R	

***R** : Responsable, **G** : Garant, **I** : Informé, **C** : Consulté*

Figure 33 - Evaluation DS3

ID	Libellé	Mesure
DS03-MR-MET01	Nombre de ressources humaines en surcharge	NC
DS03-MR-INFO01	Répartition de charge entre les projets SI et le service Desk	70%/30%
DS03-MR-PRO01	Nombre de projets SI en cours	NC
DS03-MR-PRO02	Nombre de projet dans les délais	NC
DS03-MR-ACT01	Fréquence des mises à jour et des validations du planning	NC

NC *: Non connu*

Figure 34 - Mesures de résultat DS3

Interprétation :

La maturité :

Il n'existe aucune planification formalisée des deux missions principales du département informatique :

- Service Desk,
- Gestion des projets SI.

La performance du Service Desk, comme cela a été présenté dans le processus DS8, n'est pas non plus évaluée.

Le processus est donc valorisé au niveau de maturité 0.

Les rôles :

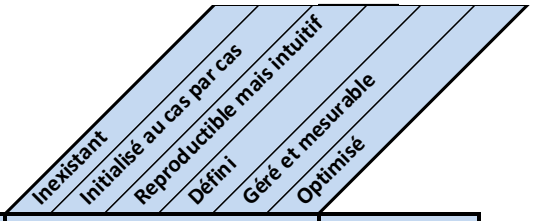
Sans mesure des capacités et des performances, aucun rôle n'a pu être attribué aux intervenants.

Les mesures de résultats disponibles :

Aucune mesure de résultat n'a pu être réalisée compte tenu du niveau de maturité du processus. Une estimation réalisée par la Direction donne une charge de travail répartie à 70 % sur la gestion de projets, et donc à 30 % sur la gestion du Service Desk interne.

2.5.4.3 DS4

Ce processus est évalué du point de vue de la continuité de service et inclut la reprise d'activité et les plans de communications associés.



Processus		Evaluation						Rôles		
ID	Objectif de contrôle	0	1	2	3	4	5	DG	RSI	Resp. Métier
DS4.1	Référentiel de continuité informatique	X								
DS4.2	Plans de continuité informatique		X						R	
DS4.3	Ressources informatiques critiques			X				I	G	
DS4.4	Maintenance du plan de continuité des SI	X								
DS4.5	Tests du plan de continuité des SI	X								
DS4.6	Formation au plan de continuité des SI	X								
DS4.7	Diffusion du plan de continuité des SI		X						G/R	
DS4.8	Restauration et redémarrage des services			X					G	
DS4.9	Stockage de sauvegardes hors site				X				G	
DS4.10	Revue après redémarrage		X							

***R** : Responsable, **G** : Garant, **I** : Informé, **C** : Consulté*

Figure 35 - Evaluation DS4

ID	Libellé	Mesure
DS04-MR-MET01	Nombre d'heures perdues dues à une indisponibilité des ressources matérielles (2010)	16
DS04-MR-INFO01	Nombre d'heures d'indisponibilité du SI par type (2010)	**Hebgt** : 16 **FAI** : NC **Poste** : NC
DS04-MR-PRO01	Nombre de postes non couverts par une GTR (2010)	NC
DS04-MR-ACT01	Fréquence des tests des plans de continuité d'activité	0

***NC** : Non connu*

Figure 36 - Mesure de résultat DS4

Interprétation :

La maturité :

Il n'existe aucun référentiel spécifiant les attentes en matière de continuité d'activité. De même, le service informatique interne n'est pas organisé pour planifier cette activité et est essentiellement réactif. Néanmoins les ressources critiques comme les serveurs d'hébergement, les accès Internet ou encore les terminaux informatiques, bénéficient de contrats offrant des garanties de temps de rétablissements. Enfin, les interruptions

programmées ou les reprises d'activité, le sont en fonction des besoins de l'informatique et non des responsables métiers.

Le processus est donc globalement évalué au niveau de maturité 1.

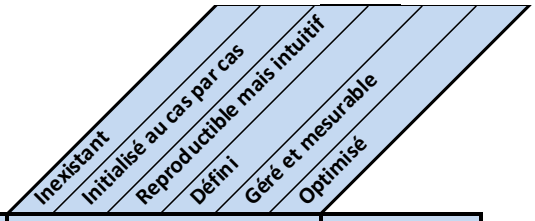
Les rôles :

Le RSI est garant de la continuité des services. La responsabilité est déléguée aux fournisseurs d'hébergement ALFA, au FAI ORANGE, et au fournisseur de matériel ALFA. Le Directeur Administratif et Financier est tenu informé des interruptions de service d'hébergement.

Les mesures de résultats disponibles :

Seul le suivi des heures d'indisponibilité du prestataire d'hébergement est disponible.

2.5.4.4 DS5



Processus		Evaluation						Rôles		
ID	Objectif de contrôle	0	1	2	3	4	5	DG	RSI	Resp. Métier
DS5.1	Gestion de la sécurité IT		X					G	R	
DS5.2	Plan de sécurité IT	X								
DS5.3	Gestion de l'identification		X						G/R	
DS5.4	Gestion des comptes utilisateurs		X						G/R	
DS5.5	Test et suivi de la sécurité	X								
DS5.6	Définition des incidents de sécurité	X								
DS5.7	Gestion des technologies de la sécurité	X								
DS5.8	Gestion des clés de cryptographies	X								
DS5.9	Prévention, détection et correction des logiciels malveillants		X						G/R	
DS5.10	Sécurité du réseau		X						G/R	
DS5.11	Transmission des données sensibles	X								

***R** : Responsable, **G** : Garant, **I** : Informé, **C** : Consulté. **NE** : Non évalué*

Figure 37 - Evaluation DS5

ID	Libellé	Mesure
DS05-MR-MET01	Nombre d'incidents qui ont mis l'Association en difficulté par rapport à ses usagers	0
DS05-MR-INFO01	Nombre d'incidents avec impact potentiel sur des tiers	NC
DS05-MR-INFO02	Délai de changement des droits d'accès au système	NC
DS05-MR-PRO01	Nombre de compte ayant un mot de passe ne répondant pas aux règles de sécurité	NC
DS05-MR-ACT01	Nombre de comptes obsolètes	NC
DS05-MR-ACT02	Nombre de comptes crées et révoqués par mois	NC

***NC** : Non connu*

Figure 38 - Mesure de résultat DS5

Interprétation :

La maturité :

Le Direction reconnait le besoin de gérer la sécurité du SI et l'affiche clairement à travers l'objectif métier OBJ1. Aucune politique de sécurité n'est formalisée et les responsabilités de la sécurité du SI ne sont pas nettement définies. Concrètement, elles oscillent entre les RSI et les utilisateurs. Aucun enregistrement des failles de sécurité existantes ou des incidents relatifs à la sécurité n'est disponible. Le précédent RSI et l'hébergeur ALFA géraient la sécurité de manière réactive mais néanmoins, de manière satisfaisante d'après les utilisateurs.

La valeur de la maturité est située entre 0 et 1 car certains objectifs de contrôles ne semblent pas abordés, en particulier l'échange de données sensibles entre confrères dans le secteur sanitaire.

Les rôles :

La Direction Générale et les Directeurs d'établissements définissent et accordent les droits d'accès au réseau.

Les mesures de résultats disponibles :

Compte tenu des outils à disposition, aucune des mesures de résultats prévues ne peut être relevé.

2.6 ETAPE 3 : Détermination des nouveaux objectifs

2.6.1 DS08

Processus		Evaluation						Rôles		
		0 Inexistant	1 Initialisé au cas par cas	2 Reproductible mais intuitif	3 Défini	4 Géré et mesurable	5 Optimisé			
ID	Objectif de contrôle							DG	RSI	Resp. Métier
DS8.1	Service Desk				X				G/R	
DS8.2	Enregistrement des demandes				X				G/R	I
DS8.3	Procèdure d'escalade				X				G/R	I
DS8.4	*Cloture des demandes*				X				G/R	I
DS8.5	Reporting et analyse des tendances					X		C	G/R	I

***R** : Responsable, **G** : Garant, **I** : Informé, **C** : Consulté*

Figure 39 - Objectifs de maturité DS8

Interprétation :

La maturité :

La Direction confie au RSI la définition d'un service de support et la formalisation de procédures de gestions d'incidents. Les procédures d'escalade sont inclues dans cette demande. Elle lui assigne également la responsabilité de mettre en place un système d'enregistrement et de suivi des incidents. Il devra par la suite, être accessible aux utilisateurs pour leur permettre de suivre l'avancement de leur demande. Il devra également permettre de générer automatiquement des bilans de traitements des incidents. Le niveau de maturité attendu est donc situé entre 3 et 4.

Les rôles :

La Direction veut mettre en place des comptes-rendus périodiques pour suivre les performances du Service Desk. Elle veut également que les responsables métiers, en particulier tous les Directeurs d'établissements, puissent être informés du déclenchement des procédures d'escalade résultant du dépassement d'un objectif de résolution d'incident.

Les mesures de résultats :

Les objectifs de résultats seront définis une fois que les premières mesures auront pu être évaluées.

2.6.2 DS03

Processus		Evaluation						Rôles		
		Inexistant	Initialisé au cas par cas	Reproductible mais intuitif	Défini	Géré et mesurable	Optimisé			
ID	Objectif de contrôle	0	1	2	3	4	5	DG	RSI	Resp. Métier
DS3.1	Planning de performance et de capacité			X					G/R	
DS3.2	Performance et capacité actuelles				X				G/R	I
DS3.3	Performance et capacité prévisionnelles				X				G/R	I
DS3.4	Disponibilité des ressources IT		X					G	R	I
DS3.5	Suivi et comtpe-rendu				X			C	G/R	I

***R** : Responsable, **G** : Garant, **I** : Informé, **C** : Consulté*

Figure 40 - Objectifs de maturité DS3

ID	Libellé	Mesure
DS03-MR-MET01	Nombre de ressources humaines en surcharge	NC
DS03-MR-INFO01	Répartition de charge entre les projets SI et le service Desk	70%/30%
DS03-MR-PRO01	Nombre de projets SI en cours	NC
DS03-MR-PRO02	Nombre de projet dans les délais	NC
DS03-MR-ACT01	Fréquence des mises à jour et des validations du planning	mensuelle

***NC** : Non connu*

Figure 41 - Objectifs de résultats DS3

Interprétation :

La maturité :

La Direction confie au RSI la réalisation d'un système de planification des capacités du service informatique interne. Ce système doit intégrer le respect des objectifs de délais de résolution du Service Desk et les délais de livraison des projets SI en cours. Il doit également prendre en compte les disponibilités des ressources humaines du service et les priorités de chaque projets SI.

Le niveau de maturité visé se situe entre 2 et 3.

Les rôles :

Des comptes-rendus réguliers et fiables doivent être mis en place entre le RSI et la Direction, pour suivre les performances et les capacités actuelles et prévisionnelles du Service Desk et des projets SI.

Les mesures de résultats :

La Direction estime à 70% la charge de travail destinée à la gestion des projets SI et à 30 % pour le SI. Le compte-rendu du RSI doit être au minimum mensuel.

2.6.3 DS04

Processus		Evaluation						Rôles		
		0 Inexistant	1 Initialisé au cas par cas	2 Reproductible mais intuitif	3 Défini	4 Géré et mesurable	5 Optimisé			
ID	Objectif de contrôle							DG	RSI	Resp. Métier
DS4.1	Référentiel de continuité informatique		X							
DS4.2	Plans de continuité informatique				X				R	
DS4.3	Ressources informatiques critiques				X			I	G	I
DS4.4	Maintenance du plan de continuité des SI		X							
DS4.5	Tests du plan de continuité des SI		X							
DS4.6	Formation au plan de continuité des SI		X					I		I
DS4.7	Diffusion du plan de continuité des SI		X					I	G/R	I
DS4.8	Restauration et redémarrage des services				X					
DS4.9	Stockage de sauvegardes hors site				X				G	
DS4.10	Revue après redémarrage	X						I	G/R	I

***R** : Responsable, **G** : Garant, **I** : Informé, **C** : Consulté*

Figure 42 - Objectifs de maturité DS4

ID	Libellé	Mesure
DS04-MR-MET01	Nombre d'heures perdues dues à une indisponibilité des ressources matérielles	<= taux de disponilité négociés
DS04-MR-INFO01	Nombre d'heures d'indisponibilité du SI par type	**Hebgt** : <= taux de disponilité contractuel **FAI** : <= taux de disponilité contractuel **Poste** : <= taux de disponilité contractuel
DS04-MR-PRO01	Nombre de postes non couverts par une GTR (2010)	0
DS04-MR-ACT01	Fréquence des tests des plans de continuité d'activité	ADU

***NC** : Non connu, **ADU** : A Définir Ultérieurement*

Figure 43 - Objectifs de résultats DS4

Interprétation :

La maturité :

La Direction confie au RSI la réalisation des spécifications de continuité de services en phase avec les besoins métiers. Ces spécifications doivent permettre de réaliser un plan de continuité exhaustif, incluant la gestion des 3 ressources physiques critiques : Les serveurs d'hébergement, les accès Internet et les postes informatiques. Ce plan sera présenté aux responsables de chaque site. Enfin, une priorisation des redémarrages d'applications devra être définie par les responsables métiers et arbitrée par la Direction Générale.

La maturité devrait donc être proche de 2.

Les rôles :

La Direction et les responsables métiers seront tenus informés des coupures de services et des modifications des plans de continuité.

Les mesures de résultats :

Elles devront pour chaque type de ressources permettre de constater que les engagements de disponibilités spécifiés sont bien respectés.

2.6.4 DS05

Processus		Evaluation						Rôles		
		0	1	2	3	4	5			
ID	Objectif de contrôle	Inexistant	Initialisé au cas par cas	Reproductible mais intuitif	Défini	Géré et mesurable	Optimisé	DG	RSI	Resp. Métier
DS5.1	Gestion de la sécurité IT		X						G/R	
DS5.2	Plan de sécurité IT		X					C	G/R	C
DS5.3	Gestion de l'identification		X						G/R	
DS5.4	Gestion des comptes utilisateurs			X				I	G	R
DS5.5	Test et suivi de la sécurité	X								
DS5.6	Définition des incidents de sécurité		X						G/R	
DS5.7	Gestion des technologies de la sécurité	X								
DS5.8	Gestion des clés de cryptographies	X								
DS5.9	Prévention, détection et correction des logiciels malveillants		X						G/R	
DS5.10	Sécurité du réseau		X						G/R	
DS5.11	Transmission des données sensibles		X						G	R

***R** : Responsable, **G** : Garant, **I** : Informé, **C** : Consulté. **NE** : Non évalué*

Figure 44 - Objectifs de maturité DS5

Interprétation :

La maturité :

Devant l'ampleur de la tâche d'amélioration de ce processus, la Direction souhaite procéder par étape.

La réalisation d'un plan de sécurité permettant d'identifier les différentes responsabilités est la première urgence.

Ensuite, la priorité est portée sur l'identification et le suivi des incidents relatifs à la sécurité.

Vient ensuite, l'amélioration des processus de gestion des comptes actuels.

Enfin, une attention particulière doit être portée sur l'échange de données sensibles dans les établissements sanitaires. En effet, il a été constaté que des données nominatives ont circulé sur des mails à destination de professionnels de santé. Or, en l'état, ce moyen de transmission ne permet pas de garantir l'identité du destinataire.

La maturité visée devrait donc être légèrement supérieur à 1.

Les rôles :

Bien que toujours fortement laissées au RSI, les responsabilités de sécurités devraient progressivement être assignées vers d'autres rôles. Les responsables métiers devraient être responsables des demandes de création, modification et suppression des comptes utilisateurs. Le personnel sanitaire devrait être responsable de l'extraction des données sensibles à destination de l'extérieur.

Les mesures de résultats :

Les objectifs de résultats seront définis une fois que les premières mesures auront pu être évaluées.

2.7 ETAPE 4 : Analyse des écarts

L'audit a permis de révéler un grand nombre de manquements par rapport aux bonnes pratiques préconisées par COBIT. Dans ce paragraphe, ce sont les pratiques absentes empêchant l'atteinte des objectifs fixés précédemment qui vont être mises en évidence.

2.7.1 DS08

DS8.1 Service Desk : Objectif visé Niveau 3

Malgré de nombreuses présentations à tous les protagonistes, les responsabilités du Service Desk interne sont pour la plupart des utilisateurs très floues et cela pénalise l'efficacité des déclarations d'incidents. Ainsi, les services de supports des sous-traitants peuvent être sous ou sur-sollicités, augmentant de ce fait les délais de résolution.

Il n'existe aucune qualification des incidents permettant de prioriser leurs traitements et surtout de fixer des objectifs de délais de résolution. Les utilisateurs ne peuvent donc s'organiser et leur satisfaction ne peut être mesurée objectivement.

Les manquements expliquant l'écart actuel avec l'objectif concernent donc:

- Non respect des attributions et des responsabilités du Service Desk interne,
- Classification des incidents,
- Définition d'objectifs de délais de résolution.

DS8.2 Enregistrement des requêtes utilisateurs : Objectif visé Niveau 3

Les utilisateurs déclarant un incident ne savent pas quand il a été pris en compte ni même s'il a été pris en compte. Il n'existe pas d'outil centralisant les incidents déclarés et leur état. Ainsi, le RSI, également en charge de la gestion des projets SI, ne dispose pas de moyens lui permettant de garantir les délais de livraisons et de résolutions.

Les manquements expliquant l'écart actuel avec l'objectif concernent donc:

- La disponibilité d'une base de données de gestion des incidents,
- La disponibilité d'évaluations de la charge nécessaire aux traitements des incidents en cours et des livraisons de projets SI,
- L'accès aux utilisateurs des suivis de leurs incidents.

DS8.3 Procédure d'escalade: Objectif visé Niveau 3

Sans objectif de délai de résolution il n'existe bien sûr aucune procédure d'escalade.

Le manquement expliquant l'écart actuel avec l'objectif concerne donc :

- La définition d'une procédure d'escalade lorsque les objectifs de délais de résolution ne sont pas tenus.

DS8.4 Fermeture des incidents : Objectif visé Niveau 3

Les incidents non résolus, comme les autres, ne sont pas enregistrés. Il est donc impossible de proposer des solutions de contournement aux utilisateurs.

Le manquement expliquant l'écart actuel avec l'objectif concerne donc :

- Le suivi des incidents non résolus,
- Le suivi des problèmes connus sur le SI.

DS8.5 Compte-rendu et tendance : Objectif Niveau 4

Lors de l'audit, la Direction n'a pas obtenu de chiffres permettant d'évaluer la performance du Service informatique faute de suivi des incidents. Il n'a pas non plus était possible de déterminer la charge consommée pour résoudre les demandes utilisateurs. Sans connaitre la charge consommée dans le passé par le service desk, il n'est pas possible de prévoir la charge nécessaire à venir. Ce manque de donnée impacte directement la planification des projets SI.

Le manquement expliquant l'écart actuel avec l'objectif concerne donc :

- Les statistiques de capacité de traitement d'incidents,
- Les mesures de résultats sélectionnés,
- La projection des charges de résolutions et de suivi de projets SI,
- Le compte-rendu formalisé et périodique avec la Direction.

2.7.2 DS3

DS3.1 Planning de performance et de capacité : Objectif visé Niveau 2

Concernant la gestion des projets SI, il n'existe aucun outil de planification des projets SI en cours, ni aucun suivi des charges sur les projets réalisés. Les charges allouées à chaque projet ne sont pas connues.

Concernant le Service Desk, il n'existe pas non plus d'outil permettant de mesurer les capacités de traitement actuelles. Aucun objectif de délai de résolution n'étant établi, il n'est pas possible de mesurer les performances du Service.

Les manquements expliquant l'écart actuel avec l'objectif concernent donc:

- Les outils de planification des charges du Service Desk et des projets SI,
- La définition d'objectifs de délais de résolution pour mesurer les performances du Service Desk.

DS3.2 Performances et capacités actuelles : Objectif visé Niveau 3

N'ayant actuellement aucune base de suivi des incidents, il est impossible de déterminer le temps moyen de traitement d'une demande, ni le nombre de requêtes en

cours. Il est donc délicat d'évaluer les capacités à allouer au Service Desk. Dans un premier temps, l'hypothèse fournie par la direction retenue et donc, que 30 % du temps du RSI est consacré au Service Desk.

Ne disposant pas de suivi des projets SI réalisés ni d'inventaire formalisé des projets en cours, il est également délicat d'évaluer la charge nécessaire à chaque projet.

Les manquements expliquant l'écart actuel avec l'objectif concernent donc:

- La connaissance du nombre d'incidents en cours,
- La formalisation des projets SI en cours.

DS3.3 Performances et capacités prévisionnelles: Objectif visé Niveau 3

Il n'existe pas de base de suivi des incidents ouverts auprès du Service Desk et aucun état des lieux des projets SI à venir.

Les manquements expliquant l'écart actuel avec l'objectif concernent donc:

- Les statistiques sur les créations d'incidents au Service Desk,
- Les statistiques sur les capacités et les performances de traitement des incidents,
- Les statistiques sur la gestion des projets SI réalisés,
- La visibilité sur les projets SI à venir.

DS3.4 Disponibilité des ressources IT : Objectif visé Niveau 1

Cet objectif de contrôle repose sur la disponibilité unique du RSI.

Les manquements expliquant l'écart actuel avec l'objectif concernent donc:

- L'intégration des disponibilités du RSI dans les plans de charges.

DS3.5 Suivi et compte-rendu : Objectif visé Niveau 3

La Direction n'est pas informée du traitement actuel et prévisionnel des incidents gérés par le Service Desk.

Les manquements expliquant l'écart actuel avec l'objectif concernent donc:

- Compte-rendu de l'avancement des projets SI en cours,
- Compte-rendu des capacités actuelles et à venir du Service Desk.

2.7.3 DS4

Le plan de continuité référencé dans la suite de ce paragraphe comprend :

- Le plan de communication couvrant la rupture et la reprise des services,
- Le plan de reprise d'activité,
- Le plan des moyens alternatifs de continuité de service.

DS4.1 Référentiel de continuité informatique: Objectif visé Niveau 1

Les besoins métiers en continuité de service ne sont pas définis. Les garanties de services sur les éléments critiques de l'infrastructure du SI, ne sont peut-être pas en phase avec ces besoins.

Les manquements expliquant l'écart actuel avec l'objectif concernent donc:

- La spécification du besoin de continuité de service sur les éléments critiques de l'infrastructure SI.

DS4.2 Plans de continuité informatique : Objectif visé Niveau 3

Le plan de continuité actuel ne concerne que les accès Internet et n'aborde pas les tests.

Les manquements expliquant l'écart actuel avec l'objectif concernent donc:

- La prise en compte de certaines ressources critiques de l'infrastructure du SI,
- Les procédures de tests.

DS4.3 Ressources informatiques critiques : Objectif visé Niveau 3

Lors du redémarrage des serveurs d'hébergement à la suite d'un incident majeur, le fournisseur n'a pas été en mesure de relancer toutes les applications simultanément. Il

a ainsi procédé à un ordre de redémarrage en fonction de ses contraintes et de l'appréciation qu'il avait de nos priorités sans concertation préalable. De même, les coupures de service pour mise à jour peuvent être programmées sans prendre en compte les impératifs métiers comme : La réalisation des fiches de paies les 25 de chaque mois, la présence des médecins pour consultation sur les établissements sanitaires.

Les manquements expliquant l'écart actuel avec l'objectif concernent donc:

- Identification et priorisation des applications métiers.

DS4.4 Maintenance du plan de continuité des SI : Objectif visé Niveau 1

Le plan de continuité existant n'est pas systématiquement mis à jour lors des changements affectant les ressources critiques : Création/Fermeture/Déménagement d'un site physique.

Les manquements expliquant l'écart actuel avec l'objectif concernent donc:

- Procédure garantissant la mise à jour du plan de continuité lors de changement impactant les ressources critiques physiques et applicatives.

DS4.5 Tests du plan de continuité des SI : Objectif visé Niveau 1

Les tests du plan de continuité existant sur les sites n'ont pas été formalisés ni même peut-être réalisés. Ainsi, il a été constaté que les plans de communications ne sont accessibles que si l'on dispose d'une connexion Internet fonctionnelle.

Les manquements expliquant l'écart actuel avec l'objectif concernent donc:

- Réalisation de campagne de tests du plan de continuité par site.

DS4.6 Formation au plan de continuité des SI : Objectif visé Niveau 1

Il n'existe aucun référent du plan de continuité sur les sites de l'Association. Le plan de continuité actuel a été uniquement transmis par mail.

Les manquements expliquant l'écart actuel avec l'objectif concernent donc:

- Personnel référent sur chaque site pour la mise en action du plan de reprise,
- Formation à la mise en application du plan de reprise.

DS4.7 Diffusion du plan de continuité des SI : Objectif visé identique

Le plan actuel est disponible sur le réseau et a été diffusé par mail.

DS4.8 Restauration et redémarrage des services informatiques : Objectif visé Niveau 3

Les manquements expliquant l'écart actuel avec l'objectif est le même que pour l'activité DS4.3.

DS4.9 Stockage de sauvegardes hors site : Objectif visé Identique.

Toutes les données applicatives sont stockées sur des serveurs redondés par le fournisseur ALFA. Un contrat décrit les engagements de ce dernier sur les délais de restauration. Aucune amélioration n'est envisagée.

DS4.10 Revue après redémarrage : Objectif visé identique

Après un redémarrage des services, les utilisateurs informent systématiquement le RSI sur les éventuels manquements du plan.

2.7.4 DS5

DS5.1 Gestion de la sécurité IT : Objectif visé identique

Il n'y a pour le moment aucun objectif d'amélioration de cet objectif de contrôle.

DS5.2 Plan de sécurité IT: Objectif visé Niveau 1

Il n'existe aucun document décrivant les exigences de sécurité dans le SI. Les exigences de sécurité métiers ne sont pas formalisées. Les utilisateurs ne sont pas tous informés et formés aux pratiques de sécurités.

Les manquements expliquant l'écart actuel avec l'objectif concernent donc:

- Expression des exigences de sécurité métiers,
- Définition et formation aux pratiques de sécurité pour les utilisateurs du SI.

DS5.3 Gestion de l'identification : Objectif visé identique

Actuellement, les terminaux n'étant pas utilisés pour un stockage local de données professionnelles, tous les terminaux d'un même site disposent des mêmes clés d'accès. Les identifications personnelles sont demandées lors de la connexion au serveur d'hébergement.

DS5.4 Gestion des comptes utilisateurs : Objectif visé Niveau 2

Les demandes de création, modification ou suppression de compte sont réalisées par les responsables métiers au RSI. Les profils de droits disponibles par établissements ne sont pas connus, ni par le RSI, ni en général par le Directeur du site. Il n'existe aucune trace de la réalisation d'une revue des comptes actifs.

Les manquements expliquant l'écart actuel avec l'objectif concernent donc:

- Définition et diffusion des profils disponibles par site,
- Revue de conformité des comptes utilisateurs.

DS5.5 Test et suivi de la sécurité: Objectif visé identique

Les spécifications des comptes-utilisateurs n'étant pas encore réalisées, cette étape est reportée.

DS5.6 Définition des incidents de sécurité: Objectif visé Niveau 1

Comme tous les incidents déclarés au Service Desk interne et externe, il n'existe aucune classification de sécurité. Cette identification est nécessaire avant de mettre en place un traitement spécifique.

Les manquements expliquant l'écart actuel avec l'objectif concernent donc:

- Classification des incidents relatifs à la sécurité.

DS5.7 Gestion des technologies de la sécurité : Objectif visé identique

Cet objectif sera abordé dans une prochaine itération.

DS5.8 Gestion des clés de cryptographies : Objectif visé identique

Cet objectif sera abordé dans une prochaine itération.

DS5.9 Prévention, détection et correction des logiciels malveillants: Objectif visé identique

Bien que non formalisées, les pratiques en cours consistent à protéger les terminaux avec un Antivirus F-Secure fournis par le sous-traitant. Sur le serveur hébergé, cette pratique est de la responsabilité du fournisseur. Néanmoins, les services de mises à jour n'étant actifs que lorsque les terminaux sont connectés, il arrive que des virus soient déployés depuis un poste dont la base virale est obsolète. Cette pratique sera améliorée dans les prochaines itérations.

DS5.10 Sécurité du réseau: Objectif visé identique

Les réseaux locaux n'abritant aucun serveur ni aucune données sensibles sur les terminaux, cette pratique n'est pas améliorée dans la présente itération. Néanmoins, aucune intrusion ne peut être détectée en l'état actuel des mesures de protection. Ce point sera pris en compte dans la prochaine itération.

DS5.11 Transmission des données sensibles: Objectif visé Niveau 1

L'échange sécurisé de données sensibles entre les terminaux et le serveur d'hébergement est actuellement assuré par le système Citrix. Néanmoins, les établissements sanitaires sont peu sensibilisés aux risques de transmissions de données sensibles par mail. Le premier d'entre eux est l'absence d'identification forte du destinataire.

Les manquements expliquant l'écart actuel avec l'objectif concernent donc:

- Mise à disposition d'outils de communication sécurisés pour les établissements sanitaires,
- Absence de sensibilisation des utilisateurs aux règles de sécurité.

3 La mise en service du Référentiel COBIT

L'audit des 4 processus a révélé des écarts importants entre les attendues de la Direction et l'existant. Leurs analyses, réalisées conjointement entre les dirigeants et le RSI, a mis en évidence les points à améliorer.
A ce stade, COBIT n'étant pas prescriptif, l'Association doit déterminer, seule, les moyens à mettre en œuvre. Une fois ces actions engagées, le contrôle de leur efficacité sera réalisé en suivant la démarche PDCA. Cette dernière est bien sûr intégrée dans COBIT, mais aussi dans l'esprit de l'Association à travers sa méthodologie : Organiser, Agir et Evaluer (voir Figure 1 – Organisation hiérarchique de l'Association).

3.1 ETAPE 5 : Projets d'améliorations

3.1.1 Définitions des projets d'amélioration

Pour combler les écarts identifiés précédemment, 4 projets ont été discernés. Le premier, concerne la définition et la mise en place d'un service desk interne à l'Association, qui couvre les processus DS8 et DS3. Le second, concerne la gestion des projets SI de l'Association, qui couvre le processus DS3. Enfin les deux derniers, concernent la mise en place des plans de continuité et de sécurité de l'Association, ils couvrent respectivement les processus DS4 et DS5.

3.1.1.1 Service DESK

Ce service plus connu dans l'Association sous le nom de « l'informaticien », est chargé d'assister les utilisateurs du SI sur un plan matériel et applicatif. Bien qu'en grande partie délégué à la société ALFA, « l'informaticien » reste fortement utile pour gérer les blocages et pour toutes questions ayant un rapport évident, ou non, avec un ordinateur.

Le projet Service Desk doit amener à :

- Améliorer la communication des responsabilités du service desk interne aux utilisateurs,
- Fournir l'état d'avancement des requêtes aux utilisateurs,
- Fournir des engagements de délais de résolution,
- Mesurer la qualité des services rendus,

- Mesurer la charge consommée,
- Fournir les mesures de résultats attendues.

Ce projet couvre les processus DS3 et DS8.

3.1.1.2 Gestion de projets SI

Par projet SI, il convient d'entendre toute évolution du SI à mettre en œuvre pour répondre à de nouvelles exigences. L'acquisition de nouvelles applications, l'ouverture de nouveaux sites géographiques, en sont 2 exemples types.

Comme l'a montré l'audit, il n'existe aucun référentiel de gestion pour cette partie. Aussi, le projet « Gestion des projets SI » doit amener à :

- Référencer les projets SI de l'Association,
- Evaluer et maintenir la charge nécessaire à leurs réalisations,
- Outiller le suivi d'avancement.
- Mesurer la charge consommée,
- Fournir les mesures de résultats attendues.

Ce projet couvre le processus DS3.

3.1.1.3 Plan de continuité

L'audit a mis en évidence une gestion encore trop réactive face aux problèmes de ruptures de services. Les reprises d'activité et la communication associée ne sont pas reproductibles même si elles sont la plupart du temps assez efficaces.

Pour l'améliorer, un projet de planification doit être mis en place. Il permettra de :

- Améliorer les capacités de résistances du SI,
- Définir formellement un plan de continuité, de reprise et de communication,
- Définir une organisation sur chaque site pour supporter ces plans,
- Tester l'efficacité,
- Fournir les mesures de résultats attendues.

Ce projet couvre le processus DS4.

3.1.1.4 Plan de sécurité

L'audit a mis en évidence des lacunes dans les politiques de sécurité du SI. Actuellement elles reposent entièrement sur l'infrastructure informatique. Les

responsabilités des utilisateurs ne sont pas définies. Pour l'améliorer, un projet de mise en place d'un plan de sécurité permettra de :

- Définir formellement les exigences de sécurité,
- Diffuser et former les utilisateurs à une utilisation sûre du SI,
- Fournir des outils de communications conformes aux exigences du monde sanitaire,
- Fournir les mesures de résultats attendues.

Ce projet couvre le processus DS5 et DS8.

3.1.2 Ordonnancement des projets

La mise en place des 4 projets précités, doit permettre d'améliorer les résultats d'évaluation des 4 processus COBIT retenus. A la suite de ces réalisations, disposant d'un recul suffisant, il sera possible d'évaluer la charge nécessaire à la poursuite de l'activité.

Avant d'envisager ce déploiement, il convient de définir un programme d'entrée en vigueur aux projets déjà identifiés.

Puisque il est nécessaire de connaitre les capacités de la ressource RSI et de disposer d'outil de planning, les projets « Gestion de projets » et service Desk doivent être déployés conjointement.

A leurs suites viendront respectivement les projets « plan de sécurité » et « plan de continuité ». Les impacts de l'exploitation d'une faille de sécurité peuvent en effet être plus pénalisants qu'un arrêt des services et sont surtout moins facilement détectés.

3.1.3 Conception des projets d'amélioration

Pour les raisons indiquées dans le chapitre précédent, les projets « Gestion de projets » et service desk sont conçus en priorité et conjointement. Les deux autres seront étudiés une fois les capacités du RSI connues.

3.1.3.1 Service DESK

Avant d'organiser le service desk une première étude est décidée. Elle consiste à enregistrer et traiter les incidents comme ils viennent. De cette manière, il sera possible de définir les premières tendances concernant :

- Les types d'incidents,
- Le nombre d'incidents ouverts,
- Les capacités de traitement,
- Les délais de traitements moyens.

Système de mesure de résultat automatique

Une fois cet enregistrement réalisé, ce projet va être mis en place en 3 itérations. Chacune d'elles va couvrir une partie des objectifs identifiés lors de l'analyse des écarts.

Itération	Résultat de l'analyse des écarts	Identifiants
1	Création de la base de données de gestion des incidents	DS08-EX-04-00
2	Classification des incidents	DS08-EX-02-00
2	Définition des objectifs de délais de résolution	DS08-EX-03-00
2	Evaluation de la charge nécessaire au Service Desk et aux projets SI	DS08-EX-05-00
2	Statistiques de capacité de traitement d'incidents	DS08-EX-10-00
2	Suivi des mesures de résultats sélectionnés	DS08-EX-11-00
2	Projection des charges de résolutions et de suivi de projets SI	DS08-EX-12-00
2	Compte-rendu formalisé et périodique avec la Direction	DS08-EX-13-00
2	Définition des objectifs de délais de résolution	DS03-EX-02-00
2	Suivi du nombre d'incidents en cours	DS03-EX-03-00
2	Suivi du nombre d'incidents crées,	DS03-EX-05-00
2	Intégration des disponibilités du RSI dans les plans de charges	DS03-EX-09-00
2	Compte-rendu des capacités actuelles et à venir du Service Desk	DS03-EX-11-00
3	Définition du fonctionnement du Service Desk interne	DS08-EX-01-00
3	Définition d'une procédure d'escalade	DS08-EX-07-00
3	Accès aux utilisateurs des suivis de leurs incidents	DS08-EX-06-00
3	Suivi des incidents non résolus	DS08-EX-08-00
3	Suivi des problèmes connus sur le SI	DS08-EX-09-00

Figure 45 - Traçabilité du projet Service Desk avec l'analyse des écarts

Le présent document s'attache à la réalisation des 2 premières itérations.

3.1.3.1.1 Organisation des données

Dans le contexte de l'Association les informations nécessaires pour suivre un incident sont les suivantes :

La classification :

La classification suivante, issue du contexte de l'Association, a été retenue :

- ALFA

  Les incidents de type ALFA englobent les demandes d'assistantes sur tous les logiciels et matériels du parc. Ils peuvent être ou non édités par cette société.

- COMPTES

  Les demandes de ce type concernent, la création, la modification ou la fermeture de comptes utilisateurs sur tous les systèmes du SI.
- FAI

  Toutes interruptions ou dégradation des connexions Internet entrent dans cette catégorie.
- INTERNET

  Toute demande de modification ou de restauration des sites Internet de l'Association est de cette catégorie.
- MAIL

  Toute demande de création, modification, suppression est de ce type. Les interruptions de service mail en font également partie.
- MOBILE

  Toute demande de création, modification ou suppression de ligne mobile est de ce type. Les incidents matériels sur les terminaux mobiles entrent également dans cette catégorie.
- PARC

  Tous les incidents se produisant sur les réseaux locaux ou nécessitants une intervention sur site sont de ce type.
- TELEPHONIE

  Toutes les demandes de création, modification ou suppression de systèmes téléphonique font partie de cette catégorie.
- AUTRES

  Cette catégorie englobe tous les incidents ne pouvant être classés dans les types précédents.

Les incidents concernant la sécurité pouvant être de tous types, ce caractère est identifié indépendamment de la catégorie.

<u>Le statut :</u>

4 états ont été retenus :

- En cours : L'incident est enregistré et peut être traité.
- En attente : La progression de l'incident est stoppée car une information ou une action de la part d'un tiers est attendue.
- Annulée : L'incident a été annulé. Une justification est obligatoire.
- Clos : L'incident est fermé avec succès ou pas. En cas d'échec, une donnée ECHEC supplémentaire est marquée comme vraie.

Le suivi par établissement :

Un incident est lié à un établissement ou à un des 2 groupes suivants :

- SANITAIRE : qui englobe les 4 établissements sanitaires,
- TOUS : qui englobe tous les établissements.

3.1.3.1.2 IMPLEMENTATION DE LA BASE DE DONNEES

ACCESS de Microsoft, est un SGBD simple à mettre en place et ouvert, raison pour laquelle il a été retenu. Le schéma relationnel à implémenter est le suivant :

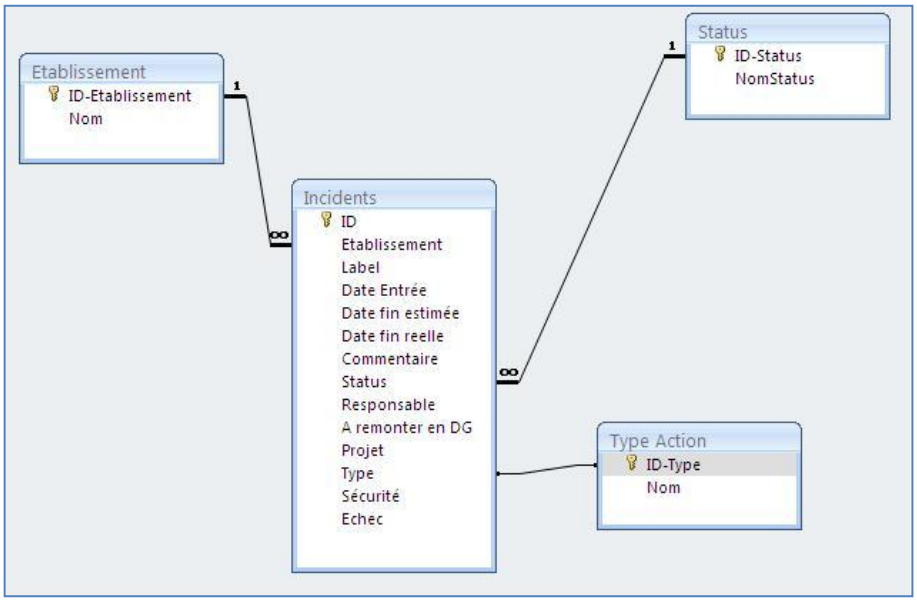


Figure 46 - Structure de la base de données du Service Desk

3.1.3.2 Gestion des projets SI

Avant toute chose, il est nécessaire de réaliser un inventaire des projets SI en cours et à venir. Ensuite, une charge de travail doit être estimée pour chacun d'eux. Elle est principalement allouée au RSI.

Pour simplifier la gestion du planning, le Service Desk est considéré comme un projet de 3 ans, utilisant 30 % de la ressource RSI.

Le plan de charge ainsi établi est intégré dans un logiciel de planification. Le choix de l'Association se porte sur le logiciel OpenProject sous licence GPL.

Les priorités de chaque projet SI sont définies avec la Direction Générale et communiquées aux Directeurs d'établissements.

L'établissement du plan de charge est la première itération du présent projet. L'intégration dans l'outil « Open Project » est la seconde. Ces 2 étapes couvrent tous les objectifs identifiés dans l'analyse des écarts.

Itération	Résultat de l'analyse des écarts	Identifiants
1	Inventaire des projets SI en cours	DS03-EX-04-00
1	Inventaire des projets SI à venir	DS03-EX-08-00
2	Intégration des disponibilités du RSI dans les plans de charges	DS03-EX-09-00
2	Statistiques sur la gestion des projets SI réalisés	DS03-EX-07-00
2	Outils de planification des charges du Service Desk et des projets	DS03-EX-01-00
2	Compte-rendu de l'avancement des projets SI en cours	DS03-EX-10-00

Figure 47 - Traçabilité du projet "Gestion des projets SI" avec l'analyse des écarts

3.2 ETAPE 6 : Réalisation des améliorations

Les projets Service Desk et « Gestion des projets SI » ont été conduits simultanément. En décembre 2011 les deux premières itérations de chacun d'eux a pont pu être presque totalement réalisées. Le paragraphe suivant présente les premiers résultats observés sur la période de juin à décembre 2011.

3.2.1 Délais de traitement et classification des incidents

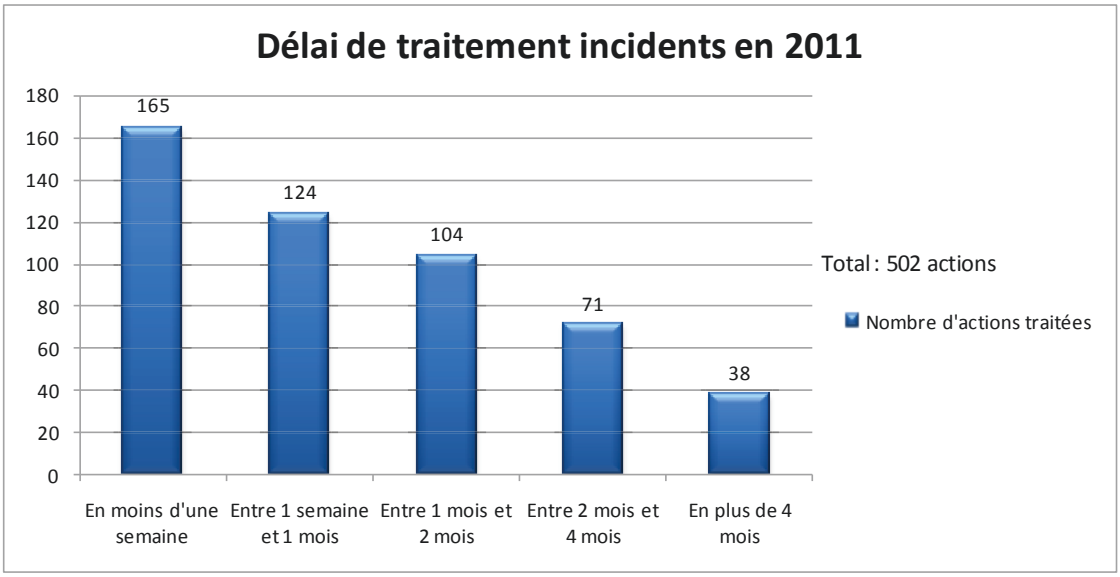


Figure 48 - Délai de traitement des incidents en 2011

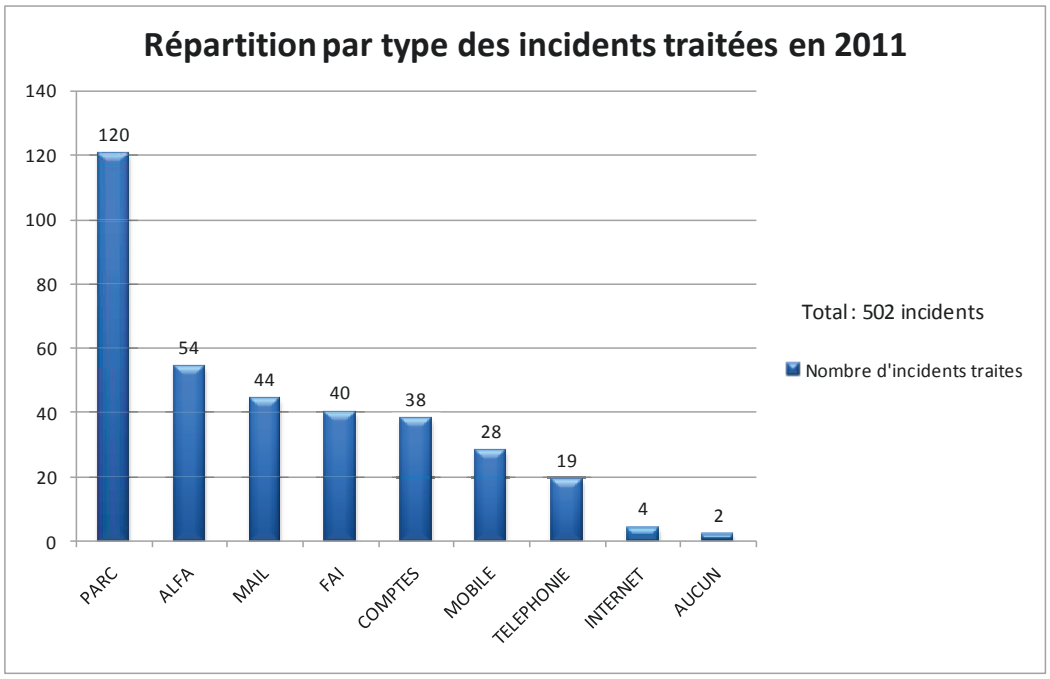


Figure 49 - Répartition des délais de traitement des incidents

Observations et Analyse :

La moitié des incidents déclarés est traitée en plus d'un mois. L'expérience a montré que 3 types de problèmes doivent être pris en compte en priorité : FAI, COMPTES et MAIL. La répartition des délais observés dans ces catégories est :

- FAI : 50 % des incidents sont traités en 20 jours.
- COMPTES : Plus de 50 % des incidents sont clos en une semaine mais 20 % en plus d'un mois.
- MAIL : Moins de 60% des incidents sont fermés en un mois.

Fort des ces constatations, il a été décidé de fixer 3 objectifs de délai de résolution pour ces types de demandes :

- FAI <= 7 jours ouvrés,
- COMPTES <= 7 jours ouvrés,
- MAIL <= 30 jours ouvrés.

3.2.2 Capacité de traitement du service DESK

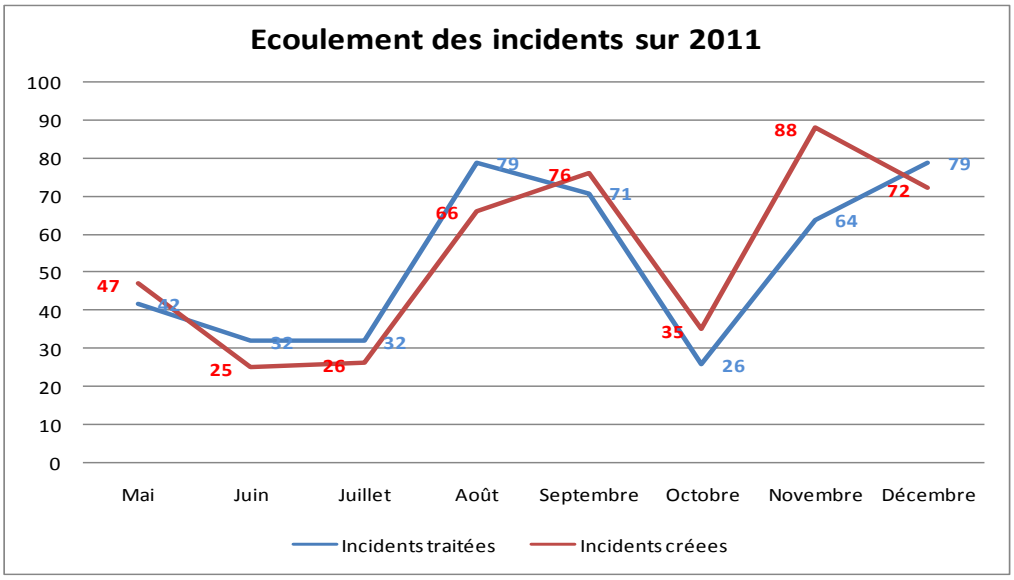


Figure 50 - Ecoulement des incidents sur 2011

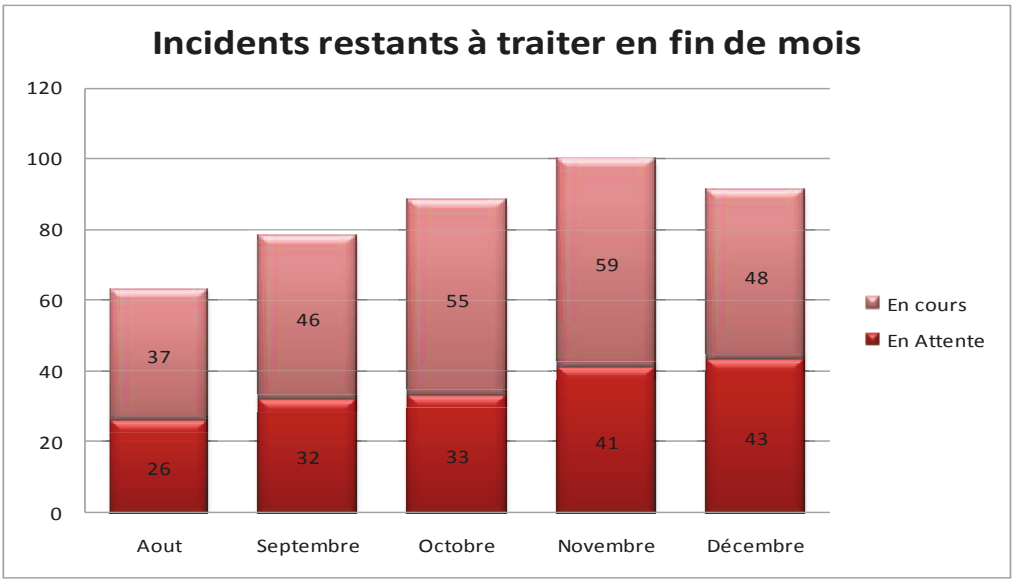


Figure 51 - Evolution du nombre d'incidents à traités en fin de mois

Observations et analyse :

L'enregistrement des incidents est en phase de production à partir du mois d'août 2011. La baisse observée au mois d'octobre correspond à une absence de 3 semaines du RSI. La forte augmentation le mois suivant correspond à son retour.

En décembre le nombre d'actions ouvertes ne retrouve pas son niveau de septembre. Le retard accumulé pendant l'absence du RSI en explique une partie. La sous-estimation du traitement des renouvellements des terminaux pour l'année 2011, explique l'autre partie. La charge nécessaire pour résoudre ce type d'incident est en effet importante.

3.2.3 Répartition de la charge entre service DESK et Gestion des projets SI

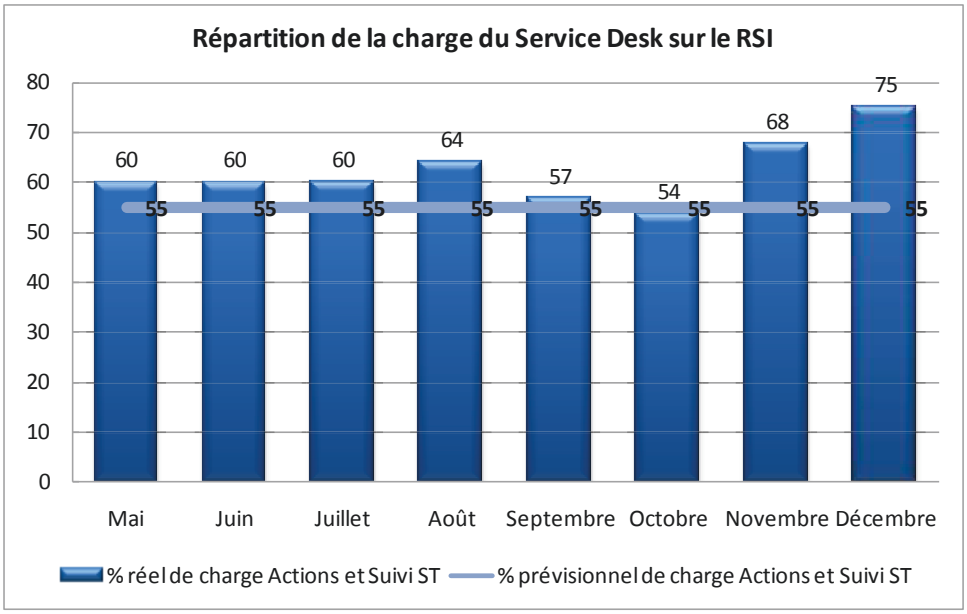


Figure 52 - Répartition de la charge de travail Service Desk / Gestion des projets SI

Observations et analyse :

Une répartition de 60% Service Desk et 40% Gestion des projets RSI semblent plus appropriées pour atteindre les objectifs de délais de résolutions évoqués précédemment.

Les pics de charges observés en novembre et décembre correspondent au retour d'absence du RSI et à une sous-estimation du temps de traitement des commandes de matériel.

Ainsi la répartition initiale de 30 %/70% pour le Service Desk et la gestion des projets SI est revue dans les proportions 60%/40%.

3.2.4 Planification des projets SI

L'inventaire, l'évaluation du reste à faire et la priorisation des priorisations des projets avec la Direction a permis de mettre en place le planning présenté en annexe 5.1

3.3 ETAPE 7 : Contrôle et Actions

Les paragraphes suivants présentent le suivi des performances sur le premier trimestre 2012.

3.3.1 Respect des délais de traitement

Les indicateurs de performances sont positionnés sur les 3 catégories FAI, COMPTES et MAIL. Dans le cadre de ce chapitre, seul sera abordé le type FAI. Les analyses sont sensiblement les mêmes sur les deux autres.

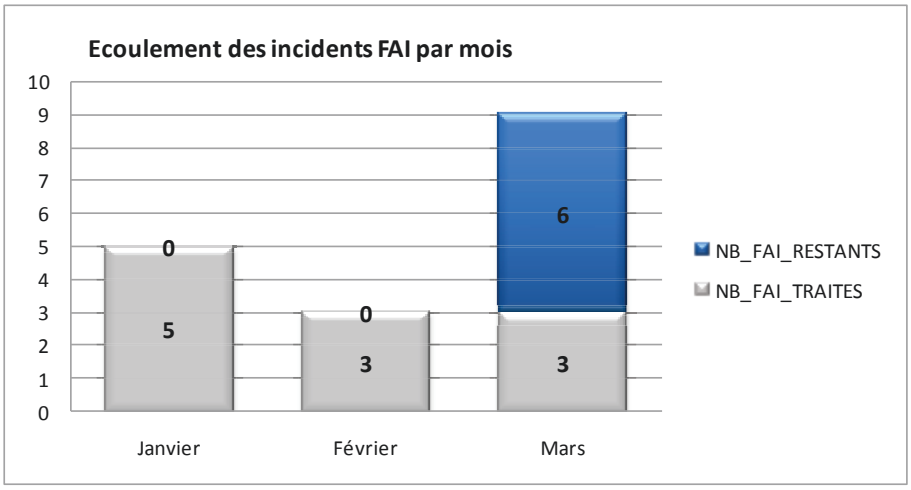


Figure 53 - Ecoulement des incidents FAI au premier trimestre 2012

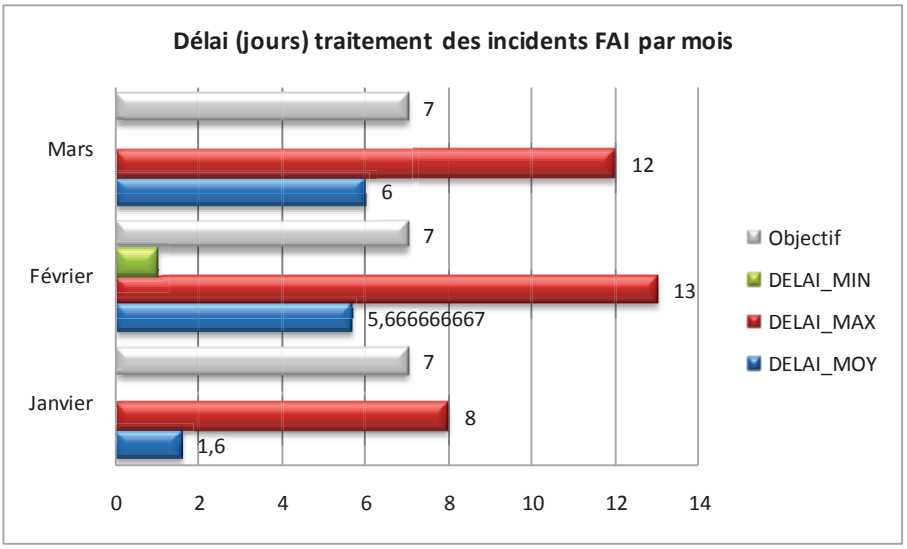


Figure 54 - Respect du délai de traitement des incidents FAI

Observations et analyse :

Sur le premier trimestre on constate un délai moyen de traitement en dessous de l'objectif de délai de 7 jours. Néanmoins, chaque mois, des incidents n'ont pu être

traités dans les délais. Une analyse détaillée des incidents en causes révèlent qu'ils ne sont pas à l'origine d'un blocage ou d'un dysfonctionnement de la connexion mais d'un problème de facturation du FAI. Il apparait donc un manque de finesse dans la catégorisation de ces incidents.

3.3.2 Capacité de traitement du service DESK

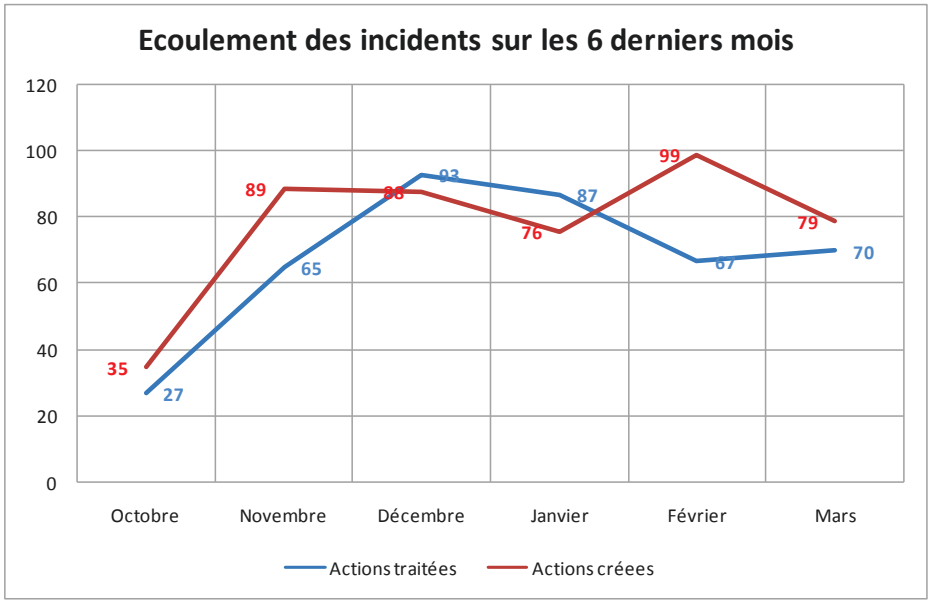


Figure 55 - Ecoulement des incidents au premier trimestre 2012

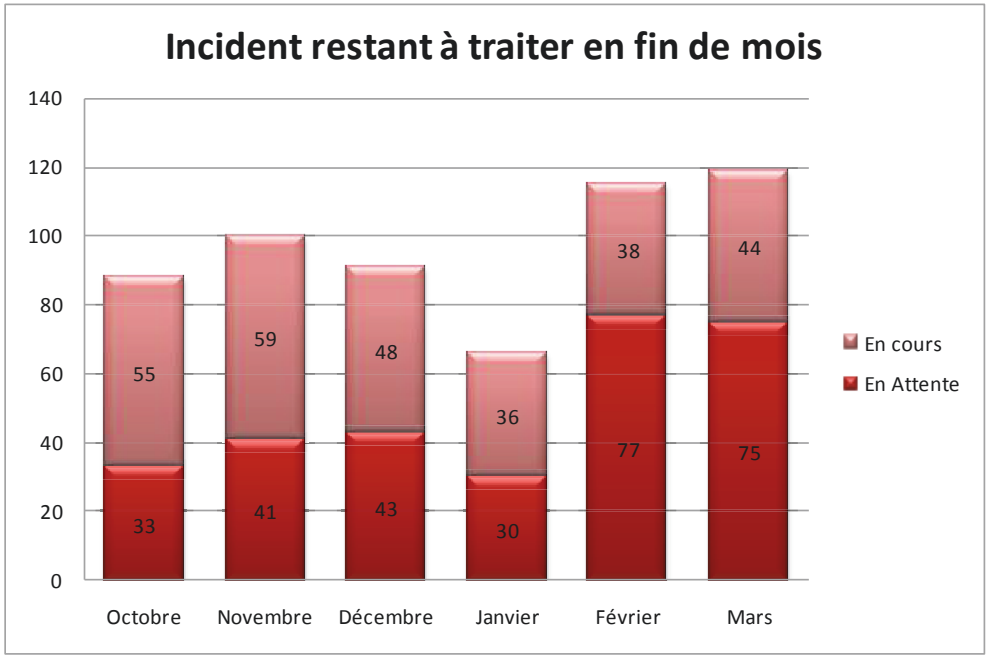


Figure 56 - Evolution du nombre d'incidents à traités en fin de mois au premier trimestre 2012

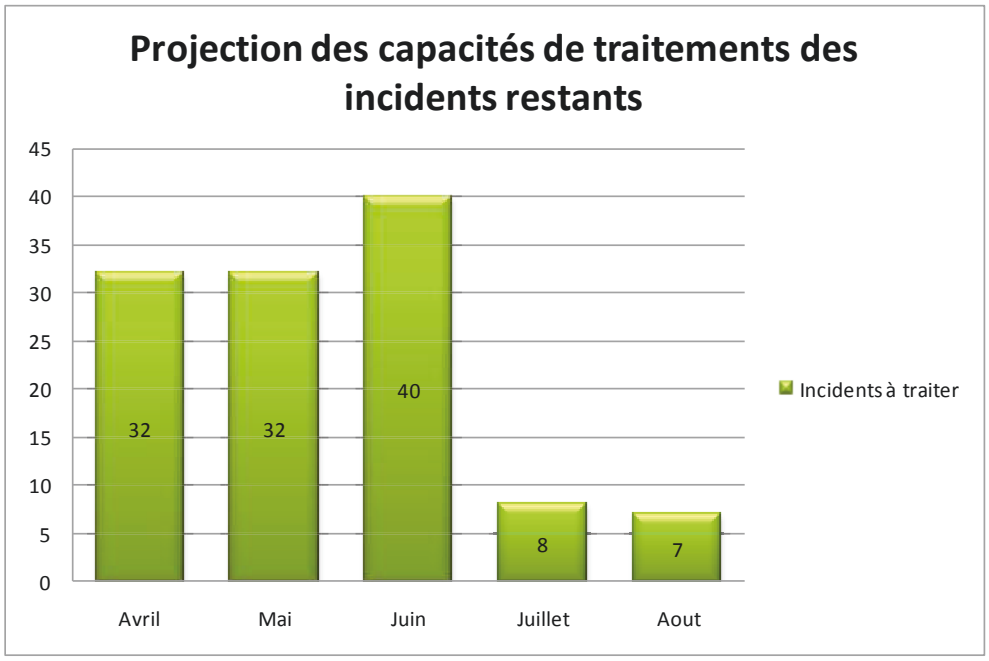


Figure 57 - Prévision des délais de traitement des incidents ouverts

Observations et analyse :

Une charge de travail avoisinant les 60 % permet d'écouler les incidents sans prendre de retard. Les pics de création constatés sont en effet sous-contrôle. Au mois de février et mars, des incidents destinés à gérer la totalité du renouvellement du parc informatique sur 2012, ont été créés. La plupart d'entre eux sont en attente. En mars, malgré une absence d'une semaine du RSI, 70 incidents ont pu être traités ne laissant apparaitre qu'un retard de 9 incidents.

En s'appuyant sur les capacités de traitement constatées ces derniers mois, il est possible de projeter les dates de résolutions des incidents restants à traiter. Les hypothèses sont les suivantes :

- Capacité de traitement mensuelle: 64 incidents,
- Capacité de traitement mensuelle des incidents restants: 32.

Cette marge respecterait les objectifs de délais de résolutions des incidents à venir.

3.3.3 Répartition de la charge entre service DESK et gestion des projets SI

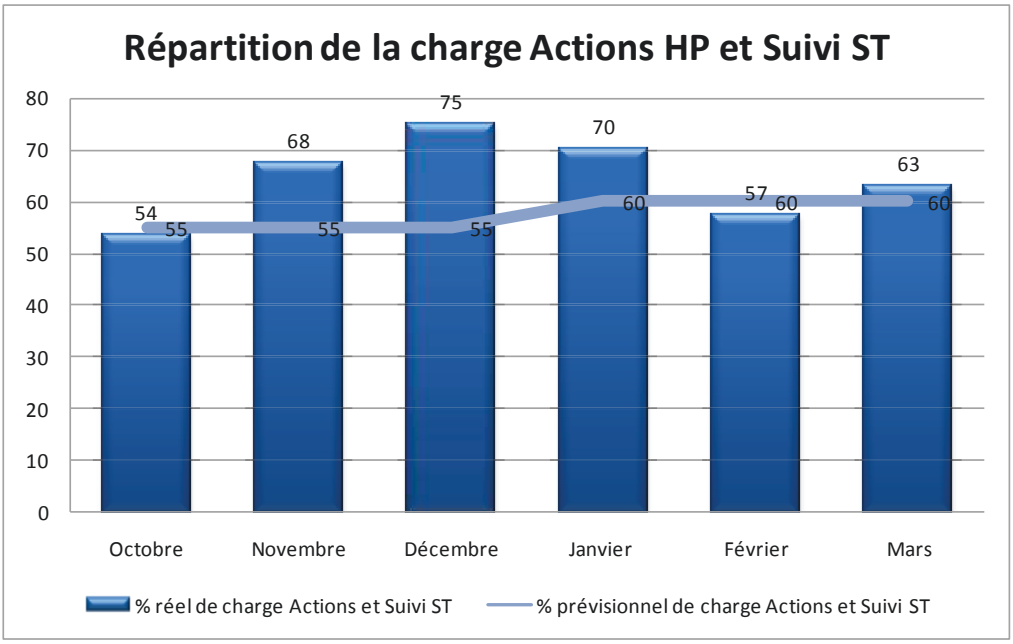


Figure 58 - Répartition de la charge de travail Service Desk / Gestion des projets SI au premier trimestre 2012

Observations et analyse :

La répartition de la charge commence à tendre vers 60 % sur les 2 derniers mois. La surconsommation en janvier s'explique par les installations de matériels commandés en 2011.

3.3.4 Planification des projets SI

La planification des projets est effective et revue mensuellement avec le Directeur Général. La communication aux Directeurs d'établissements est encore effectuée au cas par cas.

3.3.5 Compte-rendu

Des comptes-rendus mensuels présentant les indicateurs ci-dessus sont fournis au Directeur Général. Une fois validés, ils sont transmis pour information aux Directeurs d'établissements.

En mai 2012, un projet de mise en place d'un site Intranet va aboutir à la mise à disposition pour tous :

- Des indicateurs de performance,
- Du suivi des incidents déclarés au Service Desk.

3.3.6 Les améliorations

Les objectifs de répartition doivent être revus à la baisse pour le Service Desk dès qu'une stabilisation des tendances actuelles est constatée.

Ces améliorations pourront s'appuyer en fonction des catégories à diminuer sur :

- Une délégation plus efficace au Service Desk ALFA,
- Une définition précise et une diffusion des responsabilités du Service Desk interne,
- Des améliorations de solutions applicatives,
- L'aboutissement de projet SI en cours.

4 Conclusion

L'étude des référentiels COBIT, CMMI et ITIL dans le contexte de l'Association a permis de conclure que COBIT était le choix le mieux adapté.

Pour la Direction Générale, l'implémentation de COBIT a permis de mettre en place un compte-rendu périodique faisant état des performances et des capacités du Service informatique. Sur ce point, le référentiel ITIL aurait conduit au même résultat.

COBIT offre également une bonne vision des projets en cours, de leurs avancements et de leur planification. CMMI aurait également était un bon candidat sur cette partie.

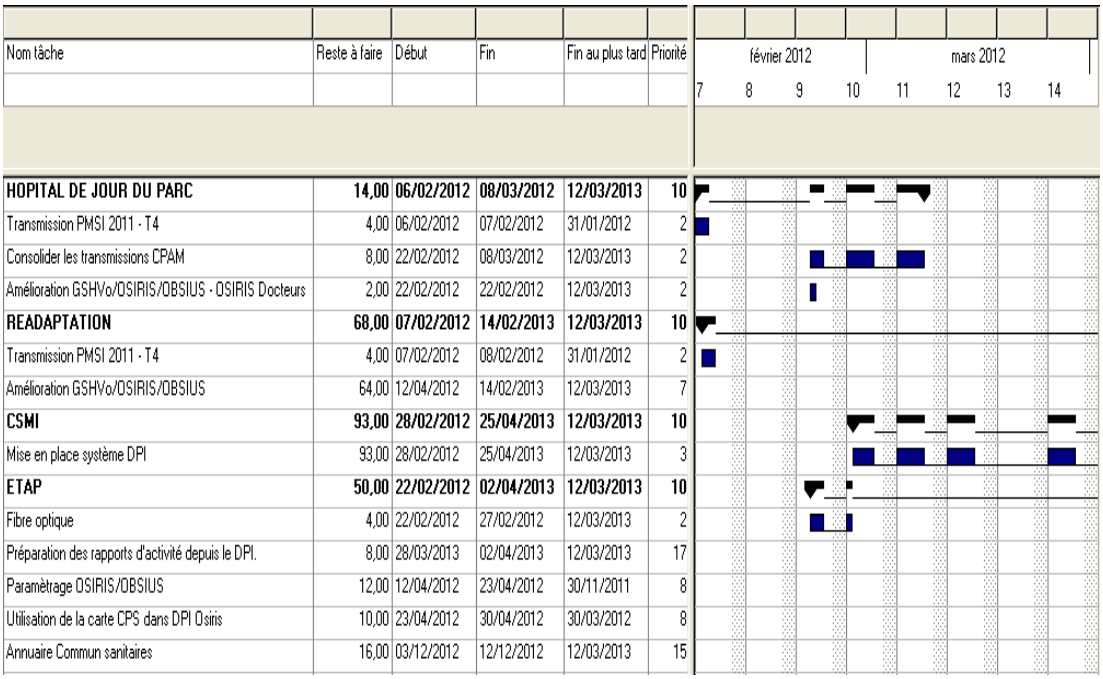
Pour les utilisateurs, la mise à disposition de l'état de leurs demandes au Service Desk sera une réalité en août 2012 avec la mise à disposition d'un Intranet répondant au nom de Picasso. Là encore, ITIL aurait conduit au même résultat.

Pour le RSI, les capacités de planification sont devenues réelles. Ainsi, les mises en place des plans de sécurité et de continuité ne sont plus perçues comme l'affaire de « l'informaticien » et sont intégrés dans le planning du Service.

Concernant le plan de sécurité, COBIT et ITIL semblent tous les deux capables d'apporter une réponse satisfaisante. Un référentiel est pourtant capable de détailler d'avantage ce point : ISO27001. Dans la mesure du possible, un seul référentiel sera retenu.

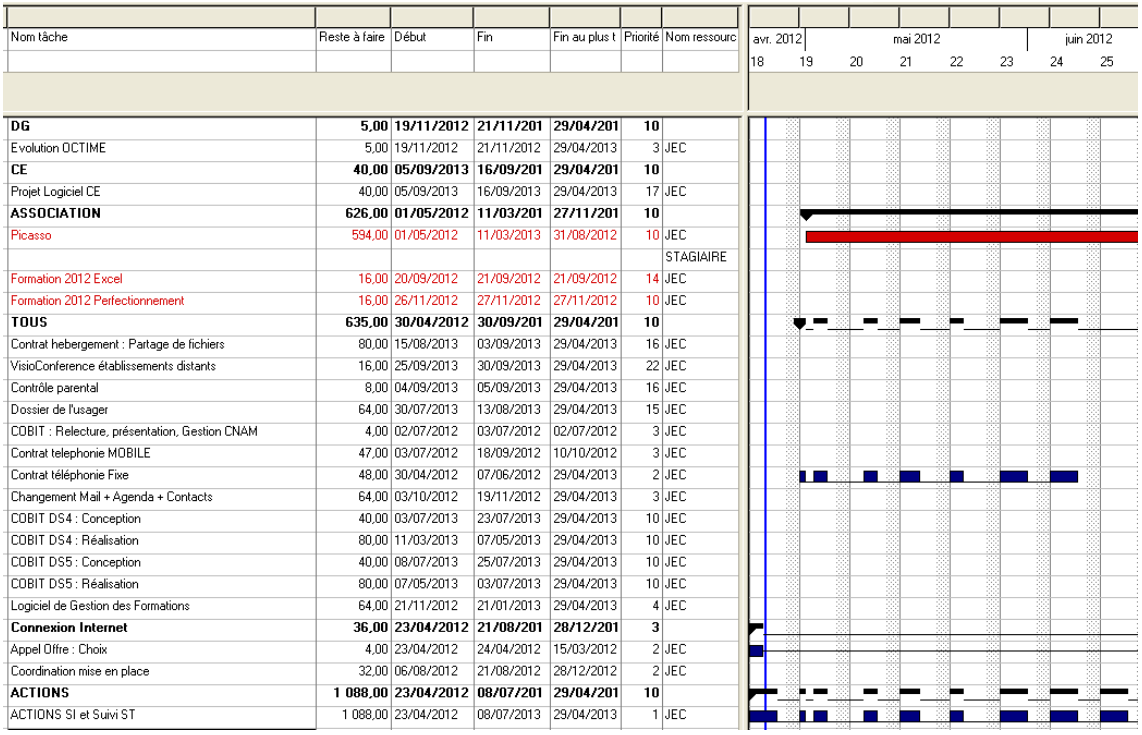
5 Annexes

5.1 Compte-rendu de l'outil de planification Open Project



Nom tâche	Reste à faire	Début	Fin	Fin au plus tard	Priorité
HOPITAL DE JOUR DU PARC	**14,00**	**06/02/2012**	**08/03/2012**	**12/03/2013**	**10**
Transmission PMSI 2011 - T4	4,00	06/02/2012	07/02/2012	31/01/2012	2
Consolider les transmissions CPAM	8,00	22/02/2012	08/03/2012	12/03/2013	2
Amélioration GSHVo/OSIRIS/OBSIUS - OSIRIS Docteurs	2,00	22/02/2012	22/02/2012	12/03/2013	2
READAPTATION	**68,00**	**07/02/2012**	**14/02/2013**	**12/03/2013**	**10**
Transmission PMSI 2011 - T4	4,00	07/02/2012	08/02/2012	31/01/2012	2
Amélioration GSHVo/OSIRIS/OBSIUS	64,00	12/04/2012	14/02/2013	12/03/2013	7
CSMI	**93,00**	**28/02/2012**	**25/04/2013**	**12/03/2013**	**10**
Mise en place système DPI	93,00	28/02/2012	25/04/2013	12/03/2013	3
ETAP	**50,00**	**22/02/2012**	**02/04/2013**	**12/03/2013**	**10**
Fibre optique	4,00	22/02/2012	27/02/2012	12/03/2013	2
Préparation des rapports d'activité depuis le DPI.	8,00	28/03/2013	02/04/2013	12/03/2013	17
Paramètrage OSIRIS/OBSIUS	12,00	12/04/2012	23/04/2012	30/11/2011	8
Utilisation de la carte CPS dans DPI Osiris	10,00	23/04/2012	30/04/2012	30/03/2012	8
Annuaire Commun sanitaires	16,00	03/12/2012	12/12/2012	12/03/2013	15

Figure 59 - Planning des établissements sanitaires



Nom tâche	Reste à faire	Début	Fin	Fin au plus t	Priorité	Nom ressourc
DG	**5,00**	**19/11/2012**	**21/11/201**	**29/04/201**	**10**	
Evolution OCTIME	5,00	19/11/2012	21/11/2012	29/04/2013	3	JEC
CE	**40,00**	**05/09/2013**	**16/09/201**	**29/04/201**	**10**	
Projet Logiciel CE	40,00	05/09/2013	16/09/2013	29/04/2013	17	JEC
ASSOCIATION	**626,00**	**01/05/2012**	**11/03/201**	**27/11/201**	**10**	
Picasso	594,00	01/05/2012	11/03/2013	31/08/2012	10	JEC
						STAGIAIRE
Formation 2012 Excel	16,00	20/09/2012	21/09/2012	21/09/2012	14	JEC
Formation 2012 Perfectionnement	16,00	26/11/2012	27/11/2012	27/11/2012	10	JEC
TOUS	**635,00**	**30/04/2012**	**30/09/201**	**29/04/201**	**10**	
Contrat hebergement : Partage de fichiers	80,00	15/08/2013	03/09/2013	29/04/2013	16	JEC
VisioConference établissements distants	16,00	25/09/2013	30/09/2013	29/04/2013	22	JEC
Contrôle parental	8,00	04/09/2013	05/09/2013	29/04/2013	16	JEC
Dossier de l'usager	64,00	30/07/2013	13/08/2013	29/04/2013	15	JEC
COBIT : Relecture, présentation, Gestion CNAM	4,00	02/07/2012	03/07/2012	02/07/2012	3	JEC
Contrat telephonie MOBILE	47,00	03/07/2012	18/09/2012	10/10/2012	3	JEC
Contrat téléphonie Fixe	48,00	30/04/2012	07/06/2012	29/04/2013	2	JEC
Changement Mail + Agenda + Contacts	64,00	03/10/2012	19/11/2012	29/04/2013	3	JEC
COBIT DS4 : Conception	40,00	03/07/2013	23/07/2013	29/04/2013	10	JEC
COBIT DS4 : Réalisation	80,00	11/03/2013	07/05/2013	29/04/2013	10	JEC
COBIT DS5 : Conception	40,00	08/07/2013	25/07/2013	29/04/2013	10	JEC
COBIT DS5 : Réalisation	80,00	07/05/2013	03/07/2013	29/04/2013	10	JEC
Logiciel de Gestion des Formations	64,00	21/11/2012	21/01/2013	29/04/2013	4	JEC
Connexion Internet	**36,00**	**23/04/2012**	**21/08/201**	**28/12/201**	**3**	
Appel Offre : Choix	4,00	23/04/2012	24/04/2012	15/03/2012	2	JEC
Coordination mise en place	32,00	06/08/2012	21/08/2012	28/12/2012	2	JEC
ACTIONS	**1 088,00**	**23/04/2012**	**08/07/201**	**29/04/201**	**10**	
ACTIONS SI et Suivi ST	1 088,00	23/04/2012	08/07/2013	29/04/2013	1	JEC

Figure 60 - Planning des projets associatifs dont COBIT

5.2 Objectifs prioritaires

Objectif métier, OBJ1 : Contrôler les risques liés à l'utilisation du SI dans le contexte sensible de l'Association.

Objectif métier, OBJ2 : Garantir l'adéquation entre la charge de travail et les missions confiées.

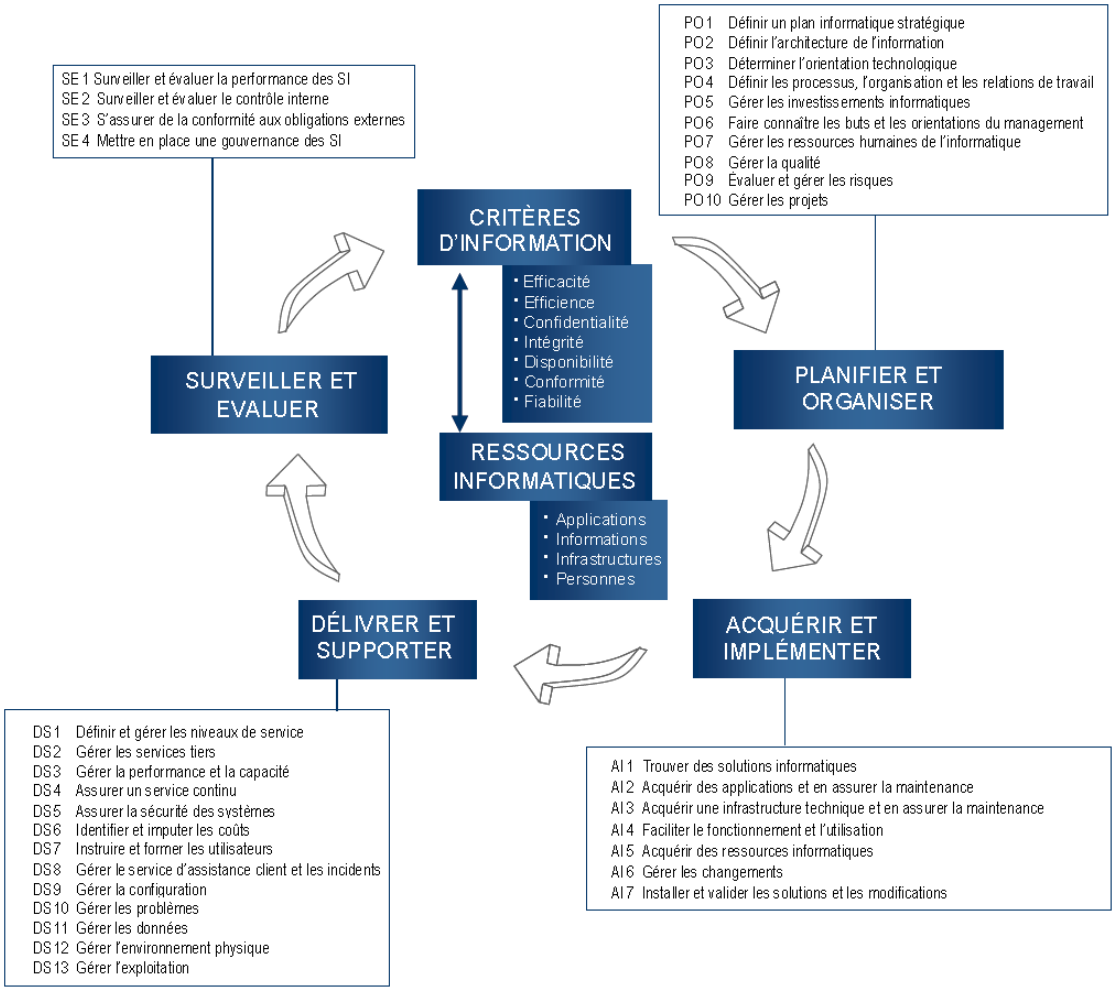
Objectif métier, OBJ3 : Maintenir la performance du service informatique de l'Association.

5.3 Stratégies de choix des processus à auditer

Stratégie d'évaluation STRAT1 : Approche Ascendante.

Stratégie d'évaluation STRAT2 : Approche Descendante.

5.4 Catégories et Processus COBIT



5.5 Modèle de maturité générique

Modèle de Maturité Générique
0 Inexistant : Absence totale de processus identifiables. L'entreprise n'a même pas pris conscience qu'il s'agissait d'un problème à étudier.
1 Initialisé/Cas par cas : On constate que l'entreprise a pris conscience de l'existence du problème et de la nécessité de l'étudier. Il n'existe toutefois aucun processus standardisé, mais des démarches dans ce sens tendent à être entreprises individuellement ou cas par cas. L'approche globale du management n'est pas organisée.
2 Reproductible mais intuitif : Des processus se sont développés jusqu'au stade où des personnes différentes exécutant la même tâche utilisent des procédures similaires. Il n'y a pas de formation organisée ni de communication des procédures standard et la responsabilité et laissée à l'individu. On se repose beaucoup sur les connaissances individuelles, d'où un risque d'erreurs.
3 Processus défini : On a standardisé, documenté et communiqué des processus *via* des séances de formation. Ces processus doivent impérativement être suivis ; toutefois, des écarts seront probablement constatés. Concernant les procédures elles-mêmes, elles ne sont pas sophistiquées mais formalisent des pratiques existantes.
4 Géré et mesurable : La direction contrôle et mesure la conformité aux procédures et agit lorsque certains processus semblent ne pas fonctionner correctement. Les processus sont en constante amélioration et correspondent à une bonne pratique. L'automatisation et les outils sont utilisés d'une manière limitée ou partielle.
5 Optimisé : Les processus ont atteint le niveau des bonnes pratiques, suite à une amélioration constante et à la comparaison avec d'autres entreprises (Modèles de Maturité). L'informatique est utilisée comme moyen intégré d'automatiser le flux des tâches, offrant des outils qui permettent d'améliorer la qualité et l'efficacité et de rendre l'entreprise rapidement adaptable.

5.6 Traçabilité Objectifs métiers / Processus

		Business Goals	IT Goals							
Financial Perspective	1	Provide a good return on investment of IT-enabled business investments.	24							
	2	Manage IT-related business risk.	2	14	17	18	19	20	21	22
	3	Improve corporate governance and transparency.	2	18						
Customer Perspective	4	Improve customer orientation and service.	3	23						
	5	Offer competitive products and services.	5	24						
	6	Establish service continuity and availability.	10	16	22	23				
	7	Create agility in responding to changing business requirements.	1	5	25					
	8	Achieve cost optimisation of service delivery.	7	8	10	24				
	9	Obtain reliable and useful information for strategic decision making.	2	4	12	20	26			
Internal Perspective	10	Improve and maintain business process functionality.	6	7	11					
	11	Lower process costs.	7	8	13	15	24			
	12	Provide compliance with external laws, regulations and contracts.	2	19	20	21	22	26	27	
	13	Provide compliance with internal policies.	2	13						
	14	Manage business change.	1	5	6	11	28			
	15	Improve and maintain operational and staff productivity.	7	8	11	13				
Learning and Growth Perspective	16	Manage product and business innovation.	5	25	28					
	17	Acquire and maintain skilled and motivated people.	9							

Figure 61 - Lien entre objectifs métiers et objectifs IT

IT Goals		Processes										
1	Respond to business requirements in alignment with the business strategy.	PO1	PO2	PO4	PO10	AI1	AI6	AI7	DS1	DS3	ME1	
2	Respond to governance requirements in line with board direction.	PO1	PO4	PO10	ME1	ME4						
3	Ensure satisfaction of end users with service offerings and service levels.	PO8	AI4	DS1	DS2	DS7	DS8	DS10	DS13			
4	Optimise the use of information.	PO2	DS11									
5	Create IT agility.	PO2	PO4	PO7	AI3							
6	Define how business functional and control requirements are translated in effective and efficient automated solutions.	AI1	AI2	AI6								
7	Acquire and maintain integrated and standardised application systems.	PO3	AI2	AI5								
8	Acquire and maintain an integrated and standardised IT infrastructure.	AI3	AI5									
9	Acquire and maintain IT skills that respond to the IT strategy.	PO7	AI5									
10	Ensure mutual satisfaction of third-party relationships.	DS2										
11	Ensure seamless integration of applications into business processes.	PO2	AI4	AI7								
12	Ensure transparency and understanding of IT cost, benefits, strategy, policies and service levels.	PO5	PO6	DS1	DS2	DS6	ME1	ME4				
13	Ensure proper use and performance of the applications and technology solutions.	PO6	AI4	AI7	DS7	DS8						
14	Account for and protect all IT assets.	PO9	DS5	DS9	DS12	ME2						
15	Optimise the IT infrastructure, resources and capabilities.	PO3	AI3	DS3	DS7	DS9						
16	Reduce solution and service delivery defects and rework.	PO8	AI4	AI6	AI7	DS10						
17	Protect the achievement of IT objectives.	PO9	DS10	ME2								
18	Establish clarity of business impact of risks to IT objectives and resources.	PO9										
19	Ensure that critical and confidential information is withheld from those who should not have access to it.	PO6	DS5	DS11	DS12							
20	Ensure that automated business transactions and information exchanges can be trusted.	PO6	AI7	DS5								
21	Ensure that IT services and infrastructure can properly resist and recover from failures due to error, deliberate attack or disaster.	PO6	AI7	DS4	DS5	DS12	DS13	ME2				
22	Ensure minimum business impact in the event of an IT service disruption or change.	PO6	AI6	DS4	DS12							
23	Make sure that IT services are available as required.	DS3	DS4	DS8	DS13							
24	Improve IT's cost-efficiency and its contribution to business profitability.	PO5	DS6									
25	Deliver projects on time and on budget, meeting quality standards.	PO8	PO10									
26	Maintain the integrity of information and processing infrastructure.	AI6	DS5									
27	Ensure IT compliance with laws, regulations and contracts.	DS11	ME2	ME3	ME4							
28	Ensure that IT demonstrates cost-efficient service quality, continuous improvement and readiness for future change.	PO5	DS6	ME1	ME4							

Figure 62 - Lien entre objectifs IT et Processus

6 Table des Figures

7 Bibliographie

- [1] COBIT MAPPING: Mapping of CMMI V1.2 With COBIT® 4.1, édité par l'ISACA (ISBN 978-1-60420-180-2)

- [2] COBIT MAPPING : Mapping of ITIL v3 With COBIT®4.1, édité en 2008 par l'ISACA (ISBN 978-1-60420-035)

- [3] IT Governance Implementation Guide: Using COBIT and VALIT edité par l'ISACA (ISBN 1-933284-75-7)

- [4] COBIT QuickStart 2nd Edition édité par l'ISACA (ISBN 978-1-893209-54-1)

- [5] COBIT 4.1 édité par l'ISACA en 2007 (ISBN 1-933284-72-2)

Résumé

L'association Rénovation gère de nombreux sites dans les domaines sociaux, médico-sociaux et sanitaires. Pour dégager des économies, le ministère de la santé, son principal financeur, incite de plus en plus le domaine sanitaire à s'appuyer sur un SI performant pour gérer et communiquer des informations fiables.

Pour atteindre ces objectifs et en faire profiter ses établissements médico-sociaux et sociaux, la Direction souhaite s'appuyer sur les référentiels SI existants. Ils doivent permettent d'évaluer puis d'améliorer l'adéquation entre les résultats fournis par le SI en place et ses exigences.

Les 3 référentiels candidats retenus sont le COBIT, le CMMI et ITIL. Un processus de sélection permet de désigner le COBIT comme le plus apte à répondre aux spécifications de l'Association.

Un plan de déploiement est élaboré. Son application permet d'obtenir les premiers résultats sur les performances et les capacités de son service SI.

Mots clés : COBIT, ITIL, CMMI, objectifs métiers, objectifs SI.

Summary

The Association "Renovation" manages several entities in social, medical and social and health areas. Its main contributor, the French Department of health, exhorts health sector to improve theirs IT services to manage and communicate reliable information to, in the end, collect financial savings.

To allow all his entities to reach these objectives, the organization wants to evaluate his IT performance against the current best practices. This comparison must lead to design improvement processes to align IT products and her objectives.

COBIT, CMMI and ITIL are investigated and, finally, COBIT is elected as the best mean to improve IT services in health sector.

An implementation plan is designed and realized. The first results are delivered and deal with the performance and capacity of the IT department.

Key words : COBIT, ITIL, CMMI, business goal, IT Goal.