



**HAL**  
open science

## Projet international de gestion des identités et des accès Singhakham Yang

► **To cite this version:**

Singhakham Yang. Projet international de gestion des identités et des accès. Cryptographie et sécurité [cs.CR]. 2014. dumas-01233651

**HAL Id: dumas-01233651**

**<https://dumas.ccsd.cnrs.fr/dumas-01233651>**

Submitted on 25 Nov 2015

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

**CONSERVATOIRE NATIONAL DES ARTS ET METIERS**  
**CENTRE REGIONAL ASSOCIE DE RHONE ALPES**

---

**MEMOIRE**

**présenté en vue d'obtenir**  
**le DIPLOME D'INGENIEUR CNAM**

**SPECIALITE : INFORMATIQUE**

**par**

**Singhakham YANG**

---

**Projet international de gestion des identités et des accès**

**Soutenu le 17 janvier 2014**

---

**JURY**

**PRESIDENT :**

Mr. Christophe PICOULEAU                      Professeur des Universités - Cnam Paris

**MEMBRES:**

Mr. Claude GENIER	Administrateur au CERN (E.R.) - Cnam Lyon
Mr. Bertrand DAVID	Professeur des Universités - Cnam Lyon
Mr. Fabrice BRIARD	Directeur de la Gouvernance Informatique - Ipsen
Mr. Soufiane ID BELLA	Directeur du Support Applicatif - Ipsen

## Remerciements

Je tiens en premier lieu à remercier Monsieur Fabrice BRIARD, Directeur de la Gouvernance Informatique du Groupe Ipsen, pour m'avoir intégré au sein de son département, en qualité de Chef de projet sécurité. Je le remercie tout particulièrement pour son aide et ses précieux conseils qui m'ont permis de réaliser le projet international de gestion des identités et des accès.

J'adresse aussi mes remerciements à toutes les personnes des différents comités de pilotage qui ont consacré de leur temps tout au long de ce projet : Laurent TOUZE (ancien Directeur de la Gouvernance Informatique), Isabelle MERIELLE (Directeur de la Transformation), Eliane TOSONI (Vice-Président Ressource Humaine Groupe), Dominique DUJARDIN (ancien Directeur du Centre de Compétence SAP), Sophie MARCHANDISE (Directeur du Contrôle Interne), Jérôme PICARD (Responsable de la relation client) et Soufiane ID BELLA (Directeur du support applicatif).

Ce travail n'aurait pu aboutir sans l'aide de nombreuses personnes, c'est pourquoi je tiens également à remercier tous les membres des comités opérationnels et équipes techniques pour leur aide.

Enfin, j'adresse un grand merci aux équipes informatiques locales pour avoir contribué au déploiement et support du système de gestion des identités et des accès dans les différents sites du Groupe Ipsen.

## Liste des abréviations

AD : Active Directory

BPF : Bonnes Pratiques de Fabrication

BT : British Telecom

EPROM : Enterprise Project Management

FDA : Food and Drug Administration

IAM : Identity and Access Management

IT : Information Technology

PMBOK : Project Management Body of Knowledge

PQP : Plan Qualité Projet

QI : Qualification d'Installation

QM : Qualification de Migration

QO : Qualification Opérationnelle

QP : Qualification de Performance

R&D : Recherche et Développement

RH: Ressources Humaines

SF : Spécifications Fonctionnelles

ST : Spécifications Techniques

# Table des matières

Remerciements .....	2
Liste des abréviations .....	3
Table des matières .....	4
Introduction .....	6
<b>CHAPITRE 1.....</b>	<b>8</b>
<b>PRESENTATION DU GROUPE IPSEN.....</b>	<b>8</b>
1.1 – LE GROUPE IPSEN.....	8
Profil et vocation .....	8
Historique du Groupe Ipsen .....	9
Ipsen dans le monde .....	10
Les principaux produits du Groupe.....	11
<b>CHAPITRE 2.....</b>	<b>13</b>
<b>L’INFORMATIQUE DU GROUPE IPSEN.....</b>	<b>13</b>
2.1 – PRESENTATION DE L’INFORMATIQUE.....	13
Les départements « informatiques métiers ».....	14
Le département « Infrastructure and Operation Services » .....	14
Le département « Enterprise Content Management » .....	14
Le département « Enterprise Performance Management ».....	15
Le département « CIO Office ».....	15
2.2 – LE SYSTEME D’INFORMATION IPSEN.....	15
2.3 – PRESENTATION DE LA METHODOLOGIE EPROM.....	15
Pourquoi EPROM ?.....	16
Objectifs et buts.....	16
Rôles et responsabilités.....	17
Le cycle de vie.....	18
La qualification et validation informatique.....	19
<b>CHAPITRE 3.....</b>	<b>22</b>
<b>LE PROJET IAM.....</b>	<b>22</b>
3.1 – LA PHASE DE CADRAGE.....	22
Le choix d’une solution et d’un intégrateur .....	22
La validation des nouveaux processus par les sites locaux.....	24
3.1 – LA PHASE DE DEMARRAGE .....	26
3.2 – LE PROJET DE GESTION DES IDENTITES .....	28
Le contexte.....	28
Les objectifs .....	30
Les processus d’identité IAM .....	30
Le plan projet .....	32
Les prérequis et contraintes.....	34
Phase projet – La conception .....	35
Phase projet – La qualification et validation du système .....	40
Phase projet – Le plan de communication et de formation.....	40
Phase projet – La mise en production.....	40
Les résultats.....	41
3.3 – LE PROJET DE GESTION DES ACCES .....	42

Le contexte .....	42
Les objectifs .....	43
Le processus de demande d'accès IAM.....	44
Le plan projet .....	45
Les prérequis et contraintes.....	47
Phase projet – Le plan de communication et de formation.....	47
Phase projet - La préparation des modèles de migration .....	48
Phase projet - La qualification et la validation.....	50
Phase projet - La mise en production .....	51
Les résultats.....	51
3.4 – LE PROJET DE CREATION AUTOMATIQUE DES ACCES INFORMATIQUES .....	54
Le contexte.....	54
Les objectifs .....	54
Le plan projet .....	56
Les prérequis .....	59
Phase projet - La conception.....	59
Phase projet – La qualification et validation du système .....	60
La mise en production .....	61
Les résultats.....	62
Conclusion.....	63
Bibliographie .....	65
Table des annexes.....	66
Annexe 1 : Evaluation du Gartner sur le niveau de maturité Ipsen.....	67
Liste des figures.....	68
Liste des tableaux .....	69

# Introduction

Ce mémoire s'inscrit dans le cadre de ma formation d'ingénieur en informatique de l'EICNAM (Ecole d'Ingénieurs du Conservatoire National des Arts et Métiers). Il a été réalisé au siège du Groupe Ipsen, localisé à Boulogne au sein du département de la Gouvernance Informatique.

L'évolution de la sécurité et des exigences réglementaires, nécessite le renforcement de la gestion des identités et des accès pour minimiser les risques de vol d'identité, d'erreurs, de fraudes et d'actes de malveillance. Dans ce but, Ipsen, groupe biopharmaceutique français de dimension mondiale, a lancé un projet pour mettre en œuvre de nouveaux processus et outils qui permettent de répondre à ces problématiques.

En effet, le Groupe Ipsen traitait les demandes de création d'identité et d'accès informatique à travers plusieurs référentiels et processus élaborés depuis 2001. Le nombre annuel de ces demandes ne cessant d'augmenter, il devenait difficile d'adapter ces processus aux nouvelles exigences en raison d'un manque de flexibilité des outils utilisés. Par ailleurs, il n'existait pas d'intégration entre les différents systèmes. Il en résultait donc un nombre important d'opérations réalisées manuellement sur les annuaires et comptes des systèmes, pouvant être générateur d'erreurs et source de non-conformités en cas d'audit.

C'est dans ce contexte que mon sujet de mémoire « Projet international de gestion des identités et des accès » a été défini. L'objectif a été de conduire en qualité de chef de projet de janvier 2012 au premier trimestre 2014, la mise en place du système IAM (Identity and Access management) sur l'ensemble de ces modules : gestion des identités, gestion des accès informatiques et création automatique des accès.

La structure du mémoire est la suivante :

- Le chapitre 1 présente de manière générale le Groupe Ipsen, son profil, son historique, sa place dans le monde et ses principaux produits.
- Le chapitre 2 décrit l'organisation de l'informatique du groupe et ses différents départements.

- Enfin le chapitre 3 présente de manière détaillée le projet IAM, ses différentes phases et itérations :
  - L'étude de cadrage qui a servi à la recherche d'une solution et d'un intégrateur.
  - Le projet de gestion des identités qui a consisté à implémenter le module de gestion des identités numériques et les nouveaux processus de cycle de vie du collaborateur.
  - Le projet de gestion des accès qui a consisté à mettre en place le module de gestion des accès informatiques avec le nouveau processus de demande d'accès aux applications du groupe.
  - Enfin le projet de création automatique des accès informatiques avec l'automatisation de la création des comptes et autorisations pour 13 systèmes majeurs du groupe.



# Chapitre 1

## Présentation du Groupe Ipsen

### 1.1 – Le Groupe Ipsen

#### Profil et vocation

Le mot « IPSEN » signifie "Institut des Produits de Synthèse et d'Extraction Naturelle". Toutefois, cet acronyme ne définit plus exactement les activités actuelles du Groupe, qui s'est largement diversifié. C'est en effet aujourd'hui un groupe pharmaceutique international qui commercialise actuellement des médicaments dans plus de 115 pays, et rassemble près de 4 900 collaborateurs dans le monde, qui ont permis de produire un Chiffre d'Affaires de plus de 1,2 milliards d'euros.

La stratégie de développement du Groupe Ipsen repose sur une complémentarité entre les produits des domaines thérapeutiques ciblés (oncologie, endocrinologie et désordres neuromusculaires), moteurs de sa croissance, et les produits de médecine générale qui contribuent notamment au financement de sa recherche. Cette stratégie est également complétée par une politique active de partenariats. La localisation de ses quatre centres de R&D (Paris, Boston, Barcelone, Londres) lui permet d'être en relation avec les meilleures équipes universitaires et d'accéder à un personnel de grande qualité.

En 2012, comme le démontre la figure 1 ci-après, les dépenses de Recherche et Développement ont augmenté de 5,9 % par rapport à l'année précédente pour atteindre environ 248,6 millions d'euros, soit 20% du Chiffre d'Affaires consolidé qui s'est élevé à 1,2 milliards d'euros, ce qui témoigne du caractère prioritaire accordé à la R&D. Plus de 900 personnes sont affectées aux activités de R&D, avec pour mission la découverte et le développement de médicaments innovants au service des patients.

**RECHERCHE ET DÉVELOPPEMENT**  
*en millions d'euros* **+5,9 %**



**Figure 1 : Evolution des dépenses en Recherche et Développement (en millions d'euros) [1]**

### **Historique du Groupe Ipsen**

L'histoire du Groupe Ipsen a débuté en 1929, lorsque pour le lancement de Romarène®, (produit d'origine naturelle à base de romarin destiné au traitement des troubles digestifs), le Docteur Henri Beaufour a créé les Laboratoires Beaufour à Dreux. Par la suite, ses deux fils, ont poursuivi l'œuvre de leur père et construit un groupe appuyé sur une recherche dynamique et performante.

À la suite de l'ouverture en 1969 de l'Institut Henri Beaufour, centre de recherche du Groupe Ipsen en France, les années 1970 ont constitué une période d'expansion des activités de l'entreprise en matière de produits d'origine naturelle. C'est en effet à cette époque que furent lancés Ginkor® Tanakan® qui sont tous deux à base de ginkgo biloba, et Smecta®. Ces médicaments constituent toujours des produits importants pour le Groupe Ipsen et font appel au savoir-faire spécifique de celui-ci.

Dès le début des années 1970, Ipsen s'est tourné vers la recherche biotechnologique avec l'implantation d'un centre de recherche sur les produits peptidiques à Boston. En 1986, l'un des médicaments issus de la biotechnologie, le Décapeptyl® a été commercialisé, ce qui a constitué la base de l'expansion internationale du Groupe.

C'est ainsi qu'à la fin des années 1980 et au début des années 1990, de nombreuses filiales et bureaux ont été implantés hors de France, et des sociétés étrangères ont été acquises par Ipsen. Hors d'Europe, le Groupe a créé une tête de pont commerciale en Asie du Sud- Est en ouvrant un bureau régional à Kuala Lumpur (Malaisie) en 1987.

En 1992, Ipsen a initié son développement en Chine et en 2000, un site industriel de fabrication du Smecta® a été ouvert tout particulièrement pour le marché chinois.

En décembre 2001 et janvier 2002, Ipsen a lancé Somatuline® Autogel® au Royaume-Uni et en France. Ce lancement a ensuite été étendu à de nombreux pays.

Depuis 2002, le Groupe a conclu de nombreux partenariats visant à enrichir son portefeuille de Recherche et Développement et à élargir sa gamme de produits. Actuellement, Ipsen est également implanté aux Etats-Unis qui représentent 50% du marché pharmaceutique mondial.

### Ipsen dans le monde

Le développement international est une priorité pour assurer l’avenir du Groupe avec 36% du Chiffre d’Affaires réalisé hors des principaux pays d’Europe de l’Ouest, et des produits commercialisés dans plus de 115 pays comme le montre la figure ci-dessous :

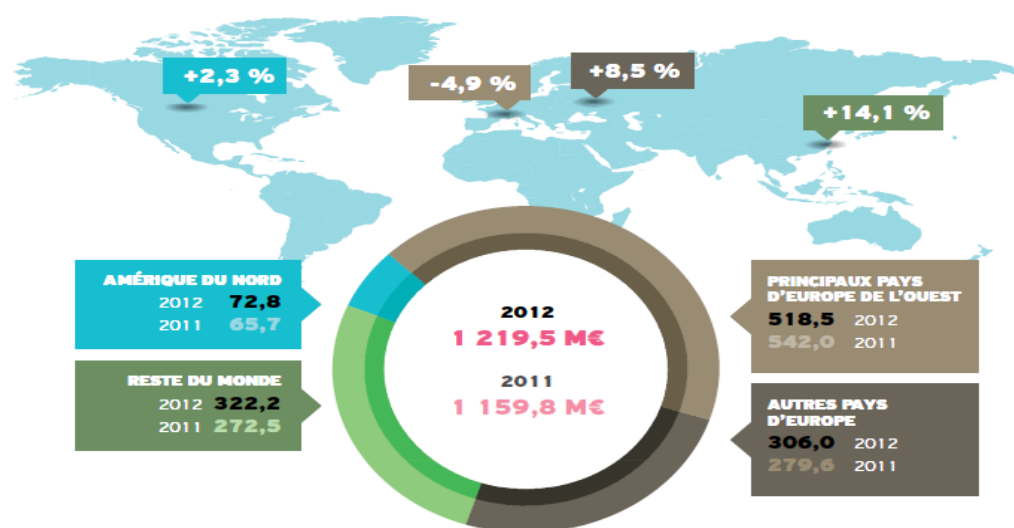
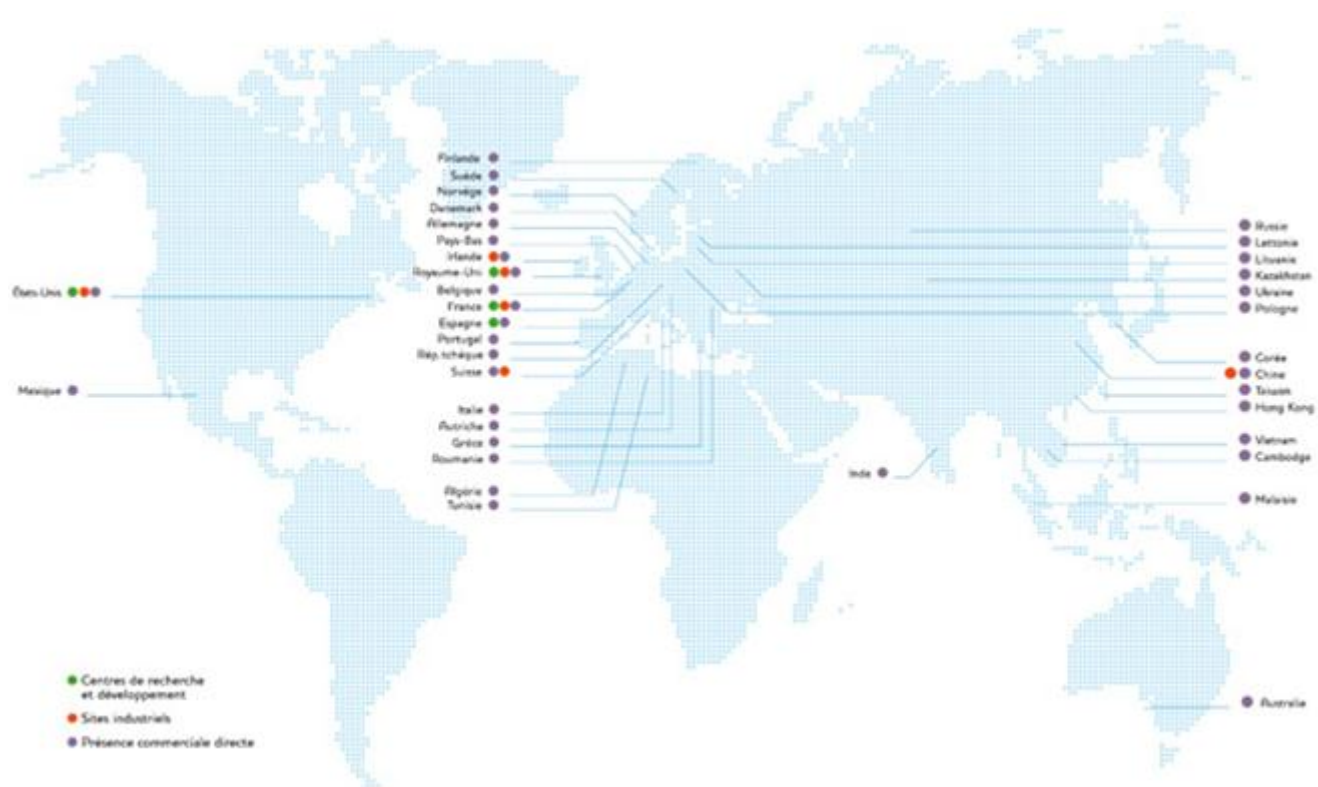


Figure 2 : Evolution du chiffre d’affaire par zone géographique (en millions d’euros) [1]

D'un point de vue géographique, la France continue à régresser (-4,9% de Chiffre d’Affaires) dans un contexte difficile qui correspond à un déclin des ventes de produits issues de la médecine générale cependant compensé par une solide croissance hors de France. La Chine et la Russie sont désormais les deux pays les plus importants du Groupe après la France.

Ipsen possède une présence commerciale directe dans plus de 30 pays. Ipsen dispose de sites de Recherche et Développement et de production en France, au Royaume-Uni, en Irlande, en Suisse, en Chine et aux Etats-Unis :



**Figure 3 : Répartition des centres de R&D, des sites industriels du Groupe dans le monde et des pays où Ipsen est présent commercialement directement [1]**

Chacun des sites de fabrication du Groupe est consacré à une technologie particulière afin d’optimiser son efficacité opérationnelle. Par exemple, le site de Dublin (Irlande) est dédié à la purification et la formulation des protéines, tandis que celui de Dreux (France) se consacre à la fabrication et au conditionnement de grands volumes de formulations orales.

### **Les principaux produits du Groupe**

Ipsen dispose, tant dans ses domaines thérapeutiques ciblés qu'en médecine générale, d'un portefeuille diversifié de médicaments de premier plan qui ont fait la preuve de leur bon profil de tolérance. Ses produits comprennent des médicaments commercialisés dans :

- des domaines thérapeutiques ciblés tels que l’oncologie (Décapeptyl®), l’endocrinologie (Somatuline®, NutropinAq®, Testim®) et les troubles neuromusculaires (Dysport®). Ces médicaments sont commercialisés dans le

monde auprès de médecins spécialistes et représentent ses axes prioritaires de développement.

- d'autres domaines thérapeutiques dans lesquels Ipsen bénéficie d'une compétence historique, principalement destinés à la médecine générale en France. Il s'agit de la gastro-entérologie (Smecta®, Forlax®), des problèmes cardio-vasculaires (Ginkor Fort®, Nisis® et Nisisco®) et des troubles cognitifs (Tanakan®).

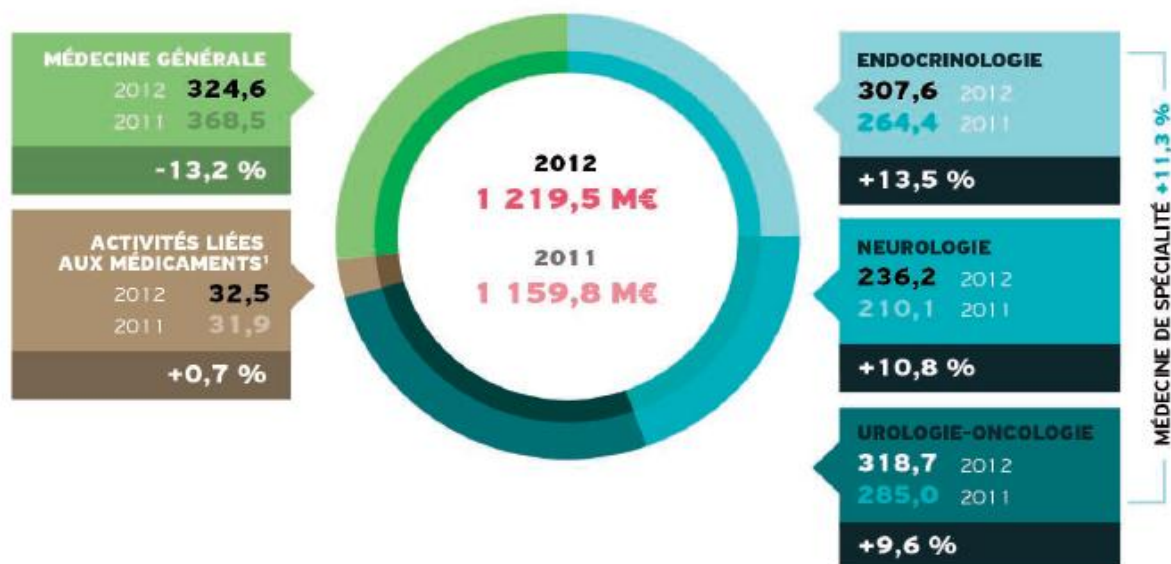


Figure 4 : Evolution du Chiffre d’Affaires par domaine thérapeutique (en millions d’euros) [1]

## Chapitre 2

### L'informatique du Groupe Ipsen

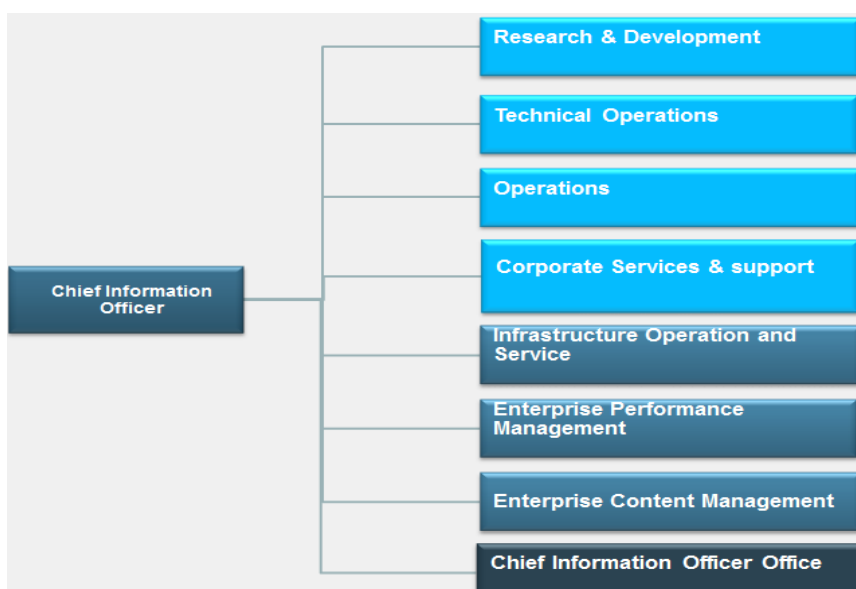
#### 2.1 – Présentation de l'informatique

L'informatique du groupe est directement rattachée au Vice-Président Directeur Général :



**Figure 5 : Place de l'informatique dans l'organisation Ipsen**

L'organisation de l'informatique du groupe a été établie afin de répondre aux besoins des clients internes en s'alignant avec les objectifs métiers. Elle est composée de 8 départements, chacun assurant une mission spécifique :



**Figure 6 : Organisation de l'informatique du groupe**

## **Les départements « informatiques métiers »**

Les départements informatiques métiers sont au nombre de 4 :

- « Research and Development »
- « Technical Operations »
- « Operation »
- « Corporate Services and support »

Chacun a pour mission de :

- définir la stratégie informatique en conformité avec la stratégie globale du domaine métier concerné
- gérer le portefeuille de projets et de demandes de mise à niveau des systèmes informatiques
- gérer les projets pour la mise en place de nouveaux systèmes informatiques
- aider dans la spécification et la hiérarchisation des besoins des utilisateurs
- développer et / ou configurer, et intégrer de nouvelles applications dans le cadre des contraintes réglementaires applicables

## **Le département « Infrastructure and Operation Services »**

Ce département assure pour l'informatique du groupe les missions suivantes :

- l'installation et la maintenance des équipements de l'infrastructure informatique
- le suivi des équipements de l'infrastructure informatique
- le fonctionnement des applications et des services
- le diagnostic et le traitement des incidents
- la sauvegarde et la restauration des systèmes et des données
- l'aide et le soutien pour le support informatique des sites

## **Le département « Enterprise Content Management »**

Les missions du département sont les suivantes :

- coordonner efficacement les sites et les services d'entreprise au travers d'outils collaboratifs
- encourager la formation des utilisateurs de la meilleure utilisation des ressources informatiques du groupe

- coordonner et promouvoir la communication informatique avec les utilisateurs et services informatiques des différents sites

### **Le département « Enterprise Performance Management »**

Les missions du département sont les suivantes :

- mettre à disposition aux différents domaines métiers, des outils et rapports permettant la prise de décision.

### **Le département « CIO Office »**

Le département « CIO Office » ou Gouvernance Informatique définit et structure des méthodes de gestion et d'exploitation d'entreprise. Il coordonne la définition de la stratégie informatique et surveille sa mise en œuvre. Les principales missions sont de contribuer à l'optimisation de la stratégie et de l'urbanisation des systèmes d'information au service des métiers, et de mettre en œuvre les meilleures pratiques de gestion (processus de prise de décision, le suivi, la gestion stratégique, la gestion de projet) à tous les niveaux. Le département de la gouvernance est sous-divisé en 5 services : Gestion du portefeuille projet, Architecture d'Entreprise, Finance IT, Assurance Qualité et enfin Sécurité dans lequel j'ai œuvré en qualité de chef de projet.

## **2.2 – Le système d'information Ipsen**

Le système d'information Ipsen est basé essentiellement sur des applications d'entreprise utilisant des solutions du marché (SAP, SQL LIMS, Trackwise, etc.). Il est composé de plus de 250 systèmes répartis sur les différents départements informatiques.

## **2.3 – Présentation de la méthodologie EPROM**

L'informatique du groupe Ipsen utilise la méthodologie EPROM (Excellence in Project Management) basé sur le PMBOK (Project Management Body of Knowledge) pour la gestion des projets informatiques. Celle-ci doit être appliquée par l'ensemble des chefs de projets. Elle comprend une stratégie de validation intégrée aux activités du projet, conforme aux différentes règles imposées par les instances réglementaires : FDA (Food



and Drug administration) et ANSM (Agence Nationale de Sécurité du Médicament). En effet, de par son domaine d'activité, Ipsen doit pouvoir prouver que toutes implémentations de systèmes informatisés ont été conduites selon les standards établis.

## **Pourquoi EPROM ?**

Avant cette méthodologie, il n'existait au sein de l'informatique aucune règle commune sur les livrables, le vocabulaire et les pratiques de projets. C'est pourquoi il arrivait de manière courante que les chefs de projet se retrouvent dans les situations suivantes :

- se sentir mal à l'aise avec ce qui est attendu d'eux
- être en confusion fréquente sur les rôles et les responsabilités (métier et informatique)
- avoir des difficultés à mettre en place de bonnes pratiques (la gouvernance du projet, les rapports, la formalisation des livrables)

De manière globale, du fait de l'absence de gouvernance, il en résultait un mauvais contrôle sur la gestion du portefeuille de projets, et des résultats inégaux en termes de réussite des projets. En effet, ceux-ci dépendaient fortement du contexte et des compétences du chef de projet.

## **Objectifs et buts**

Les objectifs de cette méthodologie mise en place par le département Gouvernance sont donc de :

- définir un cadre de gestion de projet global
- formaliser les actions et les livrables clés
- clarifier les rôles et responsabilités des acteurs

Dans le but de fournir à l'ensemble des chefs de projet informatique :

- une compréhension commune des phases clés de la gestion de projet et de bonnes pratiques connexes
- une "façon Ipsen" avec un vocabulaire commun des livrables, des rôles et des responsabilités
- un moyen d'améliorer leurs compétences de gestion de projets informatiques

- un cadre pour être aligné avec le système de management qualité du département Assurance Qualité, afin de permettre une implémentation de système en conformité avec les exigences réglementaires.

### **Rôles et responsabilités**

Les rôles et la responsabilité standards sont donc définis clairement et répartis en deux entités qui sont :

- Le Comité de Pilotage:
  - Il se réunit une fois par mois et a pour objectif de suivre l'avancée du projet et de prendre les décisions stratégiques importantes (budget, ressources et choix fonctionnel).
- Le Comité Opérationnel :
  - Il se réunit une fois toutes les deux semaines et a pour objectif de suivre l'avancée du projet, de prendre les décisions stratégiques importantes (budget, ressources et choix fonctionnel) et de les remonter au Comité de Pilotage pour arbitrage.

En dehors de ces deux comités, des réunions techniques ou processus sont nécessaires pour approfondir des sujets ou régler des points en suspens. A l'issue de ces réunions, les points importants sont consignés dans un rapport et reportés au comité opérationnel pour décision. La figure ci-après présente le cycle de décision entre les deux comités, les différents acteurs ainsi que leurs rôles et responsabilités.

## Two project committees must be set up for any project



**The Steering Committee must include at least one business representative having the authority to validate committee decisions.**

**Figure 7 : Rôles et responsabilités des acteurs des comités projets [2]**

### Le cycle de vie

Le cycle de vie d'un projet EPROM est constitué de 6 phases (identification, scoping, launch, design, build and test, et roll out) avec pour chacun des livrables attendus à chaque étape du processus :

Phase	Objectifs et contenu	Livrables clés
Identification	Décrit et hiérarchise les besoins métier qui justifient le lancement d'un projet potentiel. Formalise les objectifs, la justification et les coûts.	Formulaire projet
Scoping (étude de cadrage)	Détaille les besoins métiers, planifie les phases et les besoins en ressources. Evalue les impacts sur les processus et système. Evalue les coûts et bénéfices attendus. Fournie l'ensemble des éléments nécessaires à la décision	Formulaire de criticité du système Charte projet Décision d'investissement
Launch (démarrage)	Prépare l'implémentation en finalisant l'organisation et la mobilisation des acteurs ainsi que le planning.	Plan Qualité Projet
Design (conception)	Définit en détail les processus et la solution cible.	Spécifications fonctionnelles Analyse de risque

Phase	Objectifs et contenu	Livrables clés
Build & test (développement et test)	Développe le système et lance les tests. Finalise la communication et les matériels de formation.	Qualification Opérationnelle Fichier d'exploitation
Roll-out (démarrage)	Forme les utilisateurs et les équipes techniques. Installe le système dans l'environnement de production. Migre des données existantes vers le nouveau système. Surveille le système pendant un mois.	Rapport de mise en production Qualification de Performance

**Tableau 1 : Rôle et responsabilité des acteurs du projet [3]**

En fonction du périmètre du projet, les livrables peuvent être en français ou en anglais. Le système de gestion des identités et des accès étant utilisé au niveau mondial, l'ensemble des documents ont été rédigés en anglais afin de faciliter l'accès et la compréhension de la documentation du système IAM aux :

- inspecteurs d'organisme internationaux en cas d'audit
- support informatique des sites non français

### **La qualification et validation informatique**

De par son domaine d'activité et en vertu des instances réglementaires, le Groupe Ipsen est tenu de définir le travail de validation à effectuer en vue de démontrer le contrôle des aspects critiques des opérations spécifiques et les changements importants apportés aux installations, équipements, systèmes et procédés susceptibles d'influencer la qualité du produit. C'est pourquoi sont également intégrées à chacune des phases de projet, les étapes de qualification et de validation définies par la Plan Qualité Projet du service Assurance Qualité pour autoriser la mise en production du système.

La qualification d'un système neuf ou ayant subi des modifications a lieu généralement suivant les quatre étapes suivantes :

- Qualification de la Conception (QC)
  - La Qualification de la Conception est en général le premier élément de validation de tout nouveau système. Elle fournit une preuve documentée que le système a été conçu en conformité avec les spécifications consignées dans le cahier des charges, qui exprime les attentes de l'entreprise auprès de

l'intégrateur. Cette étape permet également de vérifier que les éléments définis dans le cahier des charges sont en adéquation avec les réglementations en vigueur.

- Qualification d'Installation (QI)
  - La Qualification d'Installation est réalisée sur tout système neuf ou ayant subi des modifications. Elle est la vérification documentée que le système est correctement installé; c'est-à-dire que les différents éléments du système sont correctement identifiés, installés et configurés, conformément à la conception approuvée et aux spécifications de l'intégrateur, aux normes et aux réglementations en vigueur, ainsi qu'aux besoins de l'utilisateur.
- Qualification Opérationnelle (QO)
  - La QO fait suite à la QI une fois que celle-ci a été réalisée, examinée et approuvée. La QO est la preuve documentée que tous les différents éléments du système fonctionnent bien comme prévu. Cela implique de tester tous les témoins du fonctionnement normal, tous les points d'alerte, tous les écrans, tous les témoins d'interaction et toute autre indication du fonctionnement.
- Qualification de la Performance (QP)
  - La QP intervient seulement après le passage réussi de la QO. Cette étape est la vérification documentée du bon fonctionnement et de la performance de l'équipement dans sa globalité, dans les conditions normales d'utilisation prévue, et le cas échéant dans les situations les plus défavorables (conditions du « pire cas »).

Le passage d'une des étapes à une autre ne peut se faire que si toutes les anomalies jugées bloquantes de l'étape en question ont été résolues. La qualification/validation est donc un des outils de l'Assurance Qualité qui permet :

- d'avoir confiance dans le système
- de prouver que le système est sous contrôle
- d'avoir une meilleure connaissance du système
- de réduire les coûts dus aux pannes
- de maîtriser la maintenance préventive
- d'être en conformité avec les exigences réglementaires

Le principe de validation est donc l'établissement de la preuve documentée, en conformité avec les référentiels réglementaires que la mise en œuvre ou l'utilisation de tout processus et système permet réellement d'atteindre les résultats escomptés. En d'autres termes, la validation consiste à vérifier qu'une opération, menée selon une procédure écrite donnée, conduit automatiquement au résultat attendu. Quant au principe de qualification, c'est une opération destinée à démontrer qu'un matériel ou système fonctionne correctement et donne réellement les résultats attendus. Le schéma ci-dessous présente les différentes phases d'un projet EPROM couplées aux différents livrables demandés par le département qualité :

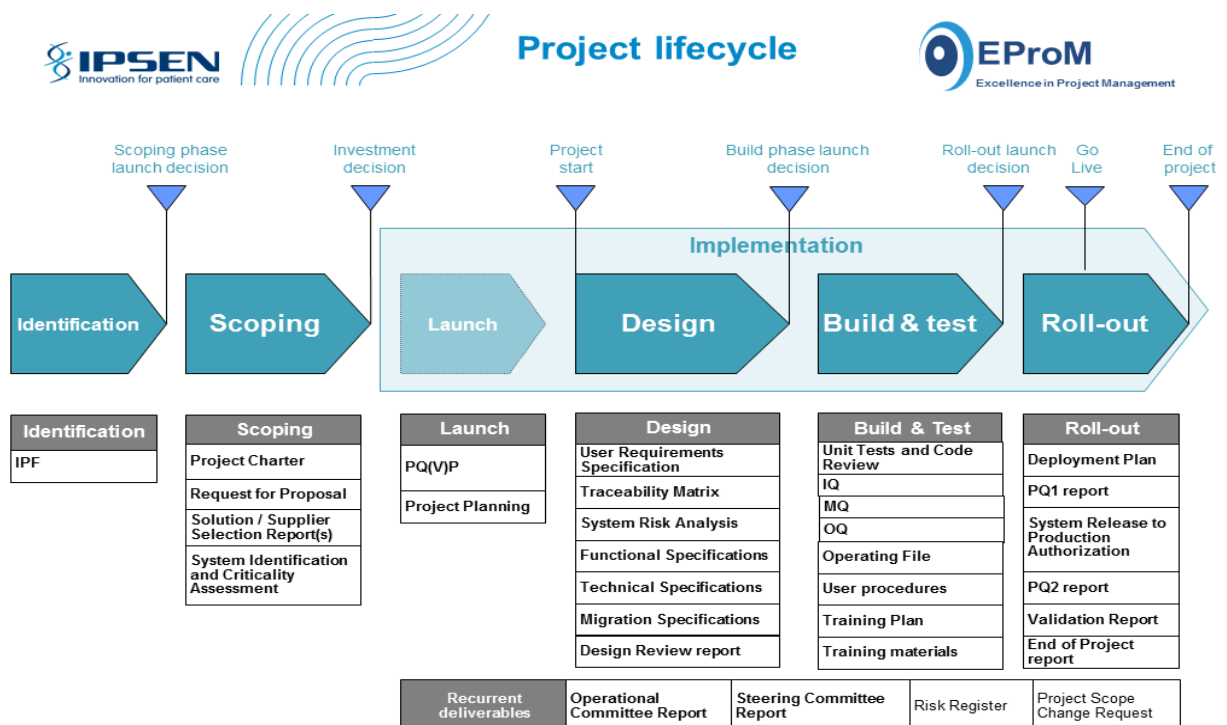


Figure 8 : Cycle de vie d'un projet EPROM avec les livrables associés [2]

Donc conformément aux bonnes pratiques initiées par le département Gouvernance, le projet IAM a été piloté selon la méthodologie EPROM sur l'ensemble de son périmètre :

1. L'étude de cadrage de janvier 2012 à mars 2012
2. Le projet de gestion des identités d'avril 2012 à décembre 2012
3. Le projet de gestion des accès de janvier 2013 à mai 2013
4. Le projet de création automatique des accès de juin 2013 à avril 2014

## Chapitre 3

### Le projet IAM

Le projet IAM a démarré en 2009, par une étude de cadrage menée par Fabrice BRIARD à l'époque « Directeur de la Sécurité de l'information Groupe », et Kernel Networks, société experte en Conseil et Intégration de solutions IAM (fédération d'identités, gestion des comptes et des autorisations). Cependant, il a été demandé de le suspendre, suite au lancement d'un projet jugé prioritaire : Le système d'information RH du groupe. Néanmoins cette étude de cadrage a abouti à la cartographie de l'existant et à la modélisation des processus cibles. Après la mise en place du système d'information RH en 2011, le projet IAM a été relancé avec les objectifs suivants :

- Implémenter le nouveau système IAM avec une interface avec le système d'information RH
- Implémenter le processus de demandes d'accès aux systèmes informatiques
- Automatiser la création des comptes et autorisations sur les systèmes informatiques

C'est dans ce contexte que j'ai intégré le poste de chef de projet au sein de la Gouvernance Informatique, pour mener à bien ce projet selon la méthodologie EPROM de janvier 2012 au premier trimestre 2014.

#### 3.1 – La phase de cadrage

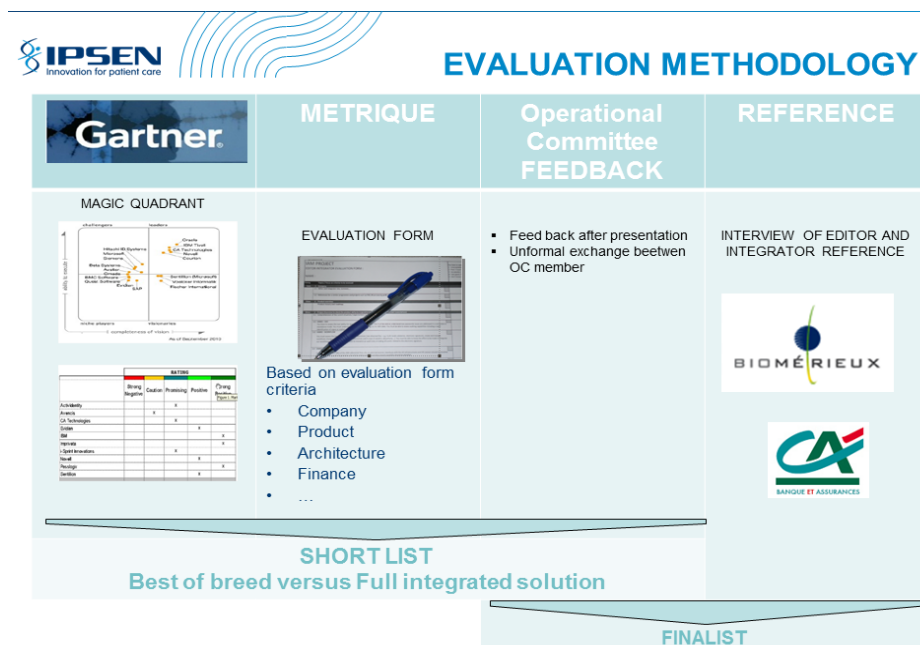
Avec le Directeur de la sécurité de l'information, nous avons lancé une nouvelle étude de cadrage de janvier 2012 à mars 2012, afin de trouver une solution du marché et un intégrateur pour aider au développement et à l'implémentation du système IAM.

##### **Le choix d'une solution et d'un intégrateur**

Notre première tâche a été de créer un cahier des charges regroupant l'ensemble des besoins sur la base des processus modélisés en 2009. Nous avons appliqué à ce document un circuit de vérification et de validation auprès de plusieurs acteurs techniques (architectes, experts applicatifs, etc.) et métiers tels que les achats ou la qualité. En parallèle de la rédaction de ce document, un travail de recherche a été fait sur Internet

(Gartner, Forster, etc.) et sur les partenaires historiques, dans l'objectif de trouver une liste d'éditeurs et d'intégrateurs pouvant répondre au cahier des charges. Des présentations ont donc été organisées en présence d'acteurs clefs (architecte, acheteur, expert, membre du comité opérationnel, etc.). Afin de mener à bien la sélection de l'outil et du partenaire, une méthodologie d'évaluation basée sur les critères ci-dessous a été mise en place :

- Le positionnement de ces acteurs par rapport au marché
- Les références clients avec entretien
- La solution technique proposée
- L'organisation proposée pour mener à bien le projet à son terme
- Les conditions de la maintenance et assistance après démarrage
- Les engagements du prestataire
- Les conditions financières



**Figure 9 : Méthodologie d'évaluation des offres commerciales**

L'acteur et le produit retenus pour accompagner Ipsen dans ce projet étaient la société BT (British Telecom) avec le produit Tivoli Identity Manager de l'éditeur IBM. En effet, l'offre éditeur/intégrateur proposée était la plus compétitive en matière de prix et répondait aux besoins décrits dans le cahier des charges. Une fois la sélection finale effectuée, nous avons mis en place un rapport de sélection de fournisseurs afin de le présenter au comité de pilotage, pour valider la solution retenue et obtenir un feu vert sur le budget et le démarrage du projet en avril 2012.



## **La validation des nouveaux processus par les sites locaux**

Afin d'avoir une adhérence des sites au projet, des déplacements et vidéoconférences sur les sites majeurs d'Ipsen (Irlande, Angleterre, Etats Unis, Chine et France) ont été organisés de janvier 2012 à avril 2012. Nous avons rencontré les représentants des départements impactés par l'implémentation du système IAM (ressources humaines, services généraux, informatique locale et qualité). L'objectif de ces réunions était de préparer les sites aux changements générés par l'implémentation du nouveau système, en confrontant les processus locaux avec les processus IAM. Toute cette analyse a été consignée sur un plan d'action de changement et dès lors qu'un écart important était identifié, une solution devait être proposée, arbitrée et validée par le Comité de Pilotage projet.

Ce plan d'action était un document Excel mis à disposition sur un espace de travail collaboratif accessible par tous les sites. Celui était composé de plusieurs colonnes permettant de faire le lien entre les besoins utilisateurs initiaux, les risques inhérents au changement et la décision finale :

- N° : numéro de l'écart identifié
- URS : numéro du besoin utilisateur
- DOMAIN : domaine métier impacté (ressource humaine, service généraux, etc.)
- PROCESS : processus impacté (arrivé, cycle de vie et départ)
- DESCRIPTION : description de l'écart
- RISKS : risque généré par l'écart
- SOLUTION OR DECISION : solution ou décision du comité de pilotage
- STATUS : statut de l'écart (ouvert, en cours et non clôturé)

N°	URS	DOMAIN	PROCESS	DESCRIPTION	RISKS	SOLUTION OR DECISION	STATUT	POST DECISION COMMENT FROM SITE
1	NA	HR	Transversal expectation	The email address is required within the HR IS. The HR IS will not be the reference. The IAM would be able to send the email address to the HR IS.	Today, HR put manually email address in HR CONNECT, we could have risk of error in email address in HR CONNECT, the information is not always available.	OC & SC Decision : Send the email address in the HR - IS system via IAM, an integration between IAM and HR CONNECT must be performed, this point is out of IAM234 scope and must be studied and budgeted with IT HR CONNECT TEAM in 2013	Closed and accepted	ML-C: numero telephone
2	URS-500-03	HR	Transversal expectation	Update of email address must not be automatic : it must be managed case by case depending on user decision (eg: the	Risk to do it automatically in spite of user needs. Risk to create new mail box if nothing is	Non automatic email change. A programme exists to change email address in GMAIL. Its integration must be considered by BT (our integrator) to automatically provision the coporate	Closed and accepted	
3	URS-301.4-9	QA	Transversal expectation	The delegation must be possible for the hierarchical manager	User can be absent and access request locked. User could delegate to anybody the	This IAM URS is specified : a manager can delegate the access request approval to equivalent grade or higher. Note : IAM administrators can approve any request. This	Closed and accepted	
4	URS-301.3-11	HR	Transversal expectation	Reminder 3 days instead of 7 during 10 days instead of 60	User could forget to perform tasks	OC DECISION: The IAM workflow will have send a reminder every 3 days during 10 days	Closed and accepted	
5	URS-301.3-13	Project OC	Transversal expectation	The request approval must be made by grade 11th minimum	Manager less than grade 11 could validate access request on critical or sensitive applications	OC & SC DECISION: The request approval must be made by the hierarchical manager of grade 11th minimum	Closed and accepted	

**Figure 10 : Plan d'action de changement IAM**

Les écarts pouvant être considérés gênants par les sites mais non bloquants par l'équipe projet, il était donc essentiel d'avoir la présence de parties prenantes importantes (Vice-Président RH, Directeur de la transformation, etc.) au comité de pilotage, pour statuer sur les différents points à imposer aux sites.

### 3.1 – La phase de démarrage

Après une sensibilisation des consultants BT sur la méthodologie EPROM et ses livrables, la première réunion de travail s’est articulée sur deux points importants :

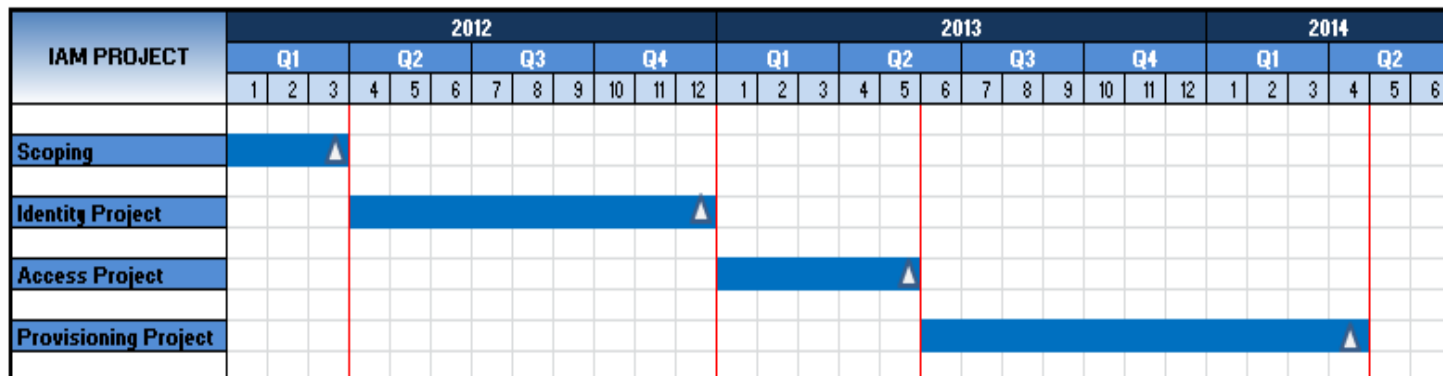
1. la clarification des rôles et responsabilités entre BT et Ipsen : En plus du contrat standard client-fournisseur validé par le service juridique des deux parties, nous avons demandé à BT de signer le Plan Qualité Projet dans lequel est définie la responsabilité de chacun :

	Sponsor	System Owner/ Project Leader	IT Governance Representative	Quality/Validation Representative	Technical Contributors	 Supplier
W = Write R = Review A = Approve						
<u>System architecture</u>			W		W	W
<u>Solution Selection Report</u>	A	A	W	A	W	A
<u>System Identification &amp; Criticality Assessment</u>		A	W		A	
<u>Project Quality &amp; Validation Plan</u>		A	W	A	W	
<u>Project Plan</u>			W		R	W
<u>Supplier Selection Report</u>	A	A	W	A	W	A
<u>User Requirements Specification</u>		A	W		R	R
<u>Functional Specifications</u>		A	A		A	A
<u>Technical Specifications</u>		A	A		A	A
<u>System Risk Analysis</u>		A	W		W	W
<u>Traceability Matrix</u>		A	R		W	W
<u>Migration Specifications</u>		A	A		A	A
<u>Design Review</u>		A	W		W	
<u>IQ Protocol</u>		A	A		A	A
<u>OQ Protocol</u>		A	A		A	A
<u>MQ Protocol</u>		A	A		A	A
<u>PQ Protocol</u>		A	A		A	A
<u>IQ Report (Development)</u>		A	A		A	A
<u>IQ Report (Qualification)</u>		A	W		W	A
<u>IQ Report (Production)</u>		A	W		W	A
<u>OQ Report (Development)</u>		A	A		A	A
<u>OQ Report (Qualification)</u>		A	W		W	A
<u>MQ Report</u>		A	A		A	A

	Sponsor	System Owner/	Project Leader	IT Governance Representative	Quality/Validation Representative	Technical Contributors	BT	
							Supplier	
	W = Write							
	R = Review							
	A = Approve							
<b>(Development)</b>								
<b>MO Report (Qualification)</b>		A	W		W	A		
<b>MO Report (Production)</b>		A	W		W	A		
<b>Training Plan</b>		A	W		R			
<b>Deployment Plan</b>		A	W			W		
<b>Operating File</b>			W		A	WA		
<b>User Procedures</b>		A	A		A	A	W	
<b>PQ Report</b>		A	W		W	A		
<b>System Release to Production</b>	A	A	W	A	W	R	A	
<b>Go-Live Announcement</b>		WA	W					
<b>System review check list</b>		A	W		W	A		
<b>Validation Report</b>	A	A	W	A	WA			
<b>End of Project Report</b>	A		W	A				

Tableau 2 : Rôles et responsabilités sur les livrables projets [3]

2. Le planning du projet, après concertation entre les deux parties, a été découpé en 3 projets distincts, et réparti de manière chronologique de 2012 à 2014 :



▲ End of project

Figure 11 : Planning général du projet IAM

- Projet 1 (avril 2012 - décembre 2012) :
  - Implémentation du module de gestion d'identité intégré au système d'information des Ressources Humaines
- Projet 2 (janvier 2013 - mai 2013) :
  - Implémentation du module de gestion des accès informatique intégrant un self-service utilisateur
- Projet 3 (juin 2013 - avril 2014)
  - Implémentation du module de création automatique de compte et autorisation pour 13 systèmes informatiques

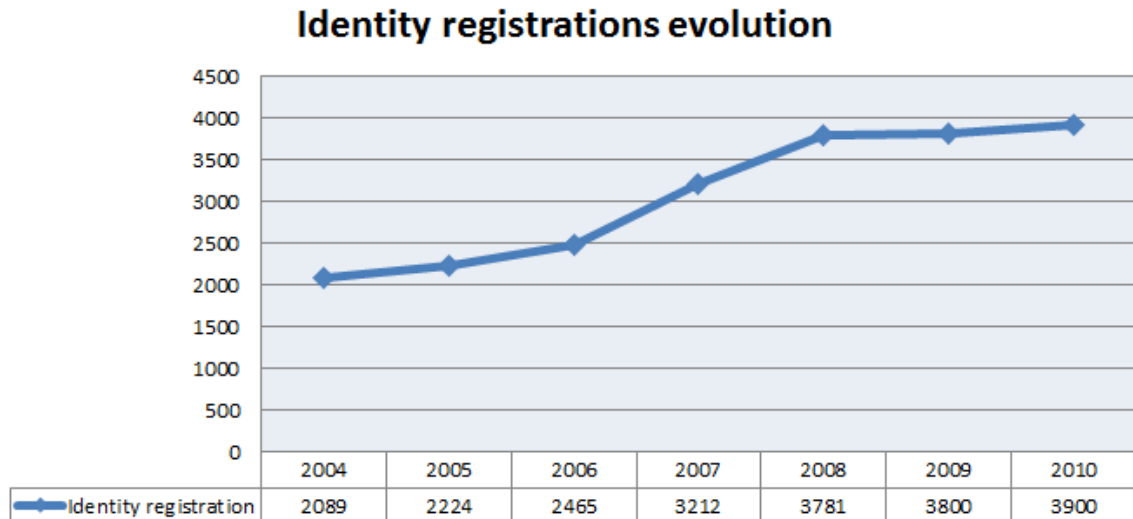
Le passage d'un projet à un autre n'a pu se faire que si le précédent était terminé sans non-conformité majeure. Chaque projet a contribué à des résultats visibles aussi bien qualitatifs que quantitatifs :

- Amélioration de l'efficacité opérationnelle et satisfaction utilisateur accrue
- Amélioration de la conformité
- Réduction des risques

## **3.2 – Le projet de gestion des identités**

### **Le contexte**

Pour gérer l'identité d'un collaborateur, Ipsen utilisait plusieurs outils vieillissants (créés en 2001), non intégrés entre eux, ainsi que des processus faisant intervenir plusieurs acteurs de différents départements : le support informatique local, l'équipe de gestion des accès et les Ressources Humaines. Au vu de l'évolution du groupe, ces outils et processus ne répondaient plus au besoin de flexibilité et de réactivité d'aujourd'hui, du fait d'une absence de centralisation des données d'identité et d'une augmentation d'actes techniques.



**Figure 12 : Evolution du nombre d’actes de gestion d’identité**

Parmi ces outils, « Ipsen registration » servait à déclarer l’arrivée, le transfert et le départ d’un collaborateur. Cette application était utilisée sur les sites par différentes personnes, les rôles et responsabilités pouvant être différents d’un site à un autre. Dans le cas d’une arrivée, une fois la demande effectuée par le site, le service de gestion des accès réceptionnait la demande par mail et procédait à la génération de l’identifiant numérique unique du collaborateur, via une autre application « UMAN ». Il créait ensuite le compte active directory sur l’annuaire technique puis renvoyait par mail l’information aux RH et aux supports informatiques locaux. L’ensemble des processus de cycle de vie d’un utilisateur faisaient donc intervenir au minimum trois personnes et s’appuyait sur plusieurs outils vieillissants, cloisonnés et non intégrés avec le système d’information des Ressources Humaines. Il en résultait donc les problématiques suivantes :

- non conformités en cas de non-respect des processus
- possibilité d’incohérence sur une même donnée due au cloisonnement des systèmes
- temps de délivrance d’un identifiant pouvant être supérieur à deux jours en fonction de la charge de l’équipe de gestion des accès
- rôles et responsabilités non définis sur les sites locaux
- pas de suspension automatique de l’identité numérique lorsqu’un utilisateur quitte la société
- pas d’outils de reporting et d’audit pour suivre le cycle de vie des utilisateurs

## Les objectifs

Les objectifs de ce premier projet étaient de remplacer les systèmes existants par le système IAM, avec une intégration aux différents référentiels d'identité (système d'information RH et annuaire technique Active Directory) et de faire adopter par l'ensemble des sites, les processus de cycle de vie d'identité modélisés en 2009.

## Les processus d'identité IAM

Les processus IAM liés à la gestion des identités sont au nombre de 3 : arrivé, mise à jour d'identité et départ.

Dans le cadre du processus d'arrivée IAM, il suffit au représentant RH d'effectuer seulement deux tâches pour déclarer un nouvel utilisateur :

1. Créer l'identifiant sur le module de gestion des identités du système IAM.
  - a. Par cette action, le système IAM crée automatiquement le compte active directory dans l'annuaire technique.
2. Créer la fiche employée dans le système d'information RH avec le même identifiant.
  - a. Par cette action, le système d'information RH synchronise ses données avec le système IAM.

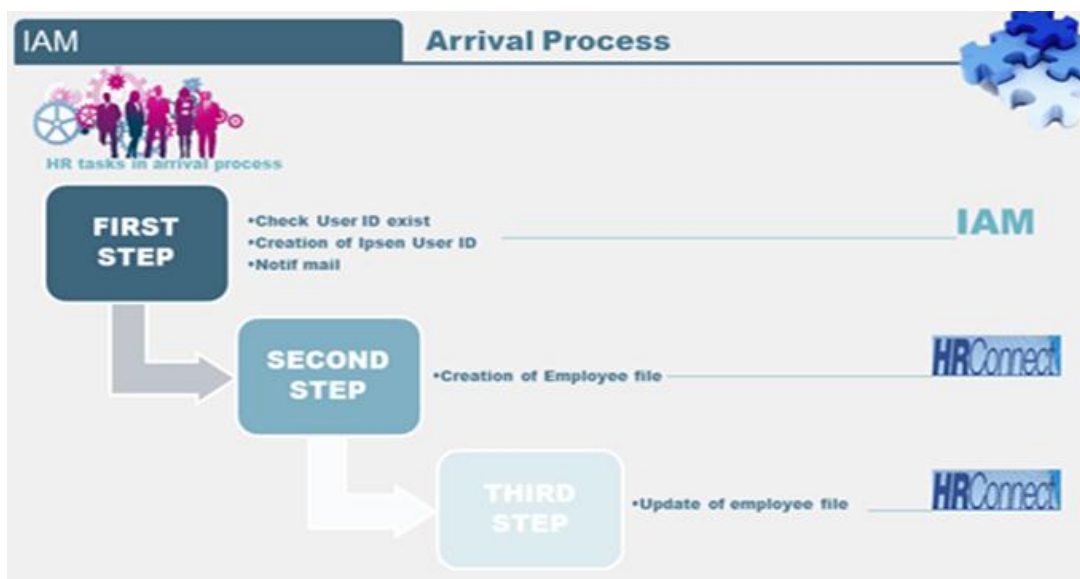
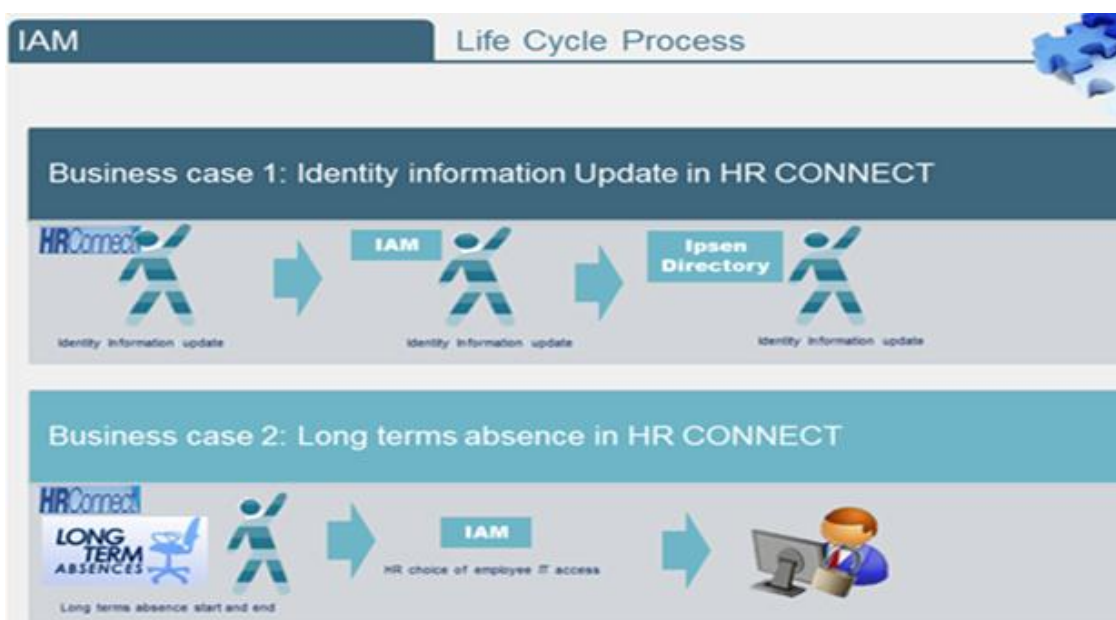


Figure 13 : Processus d'arrivée IAM

La valeur ajoutée du processus d'arrivée IAM était de réduire le nombre de personnes et le temps de délivrance d'un identifiant numérique.

Dans le cadre du processus de mise à jour d'identité, il n'existait qu'un seul référentiel : le système d'information RH. L'intégration avec le module d'identité IAM permettait de diffuser les mêmes informations (nom, prénom, date départ, etc.) sur tous les systèmes connectés à IAM.



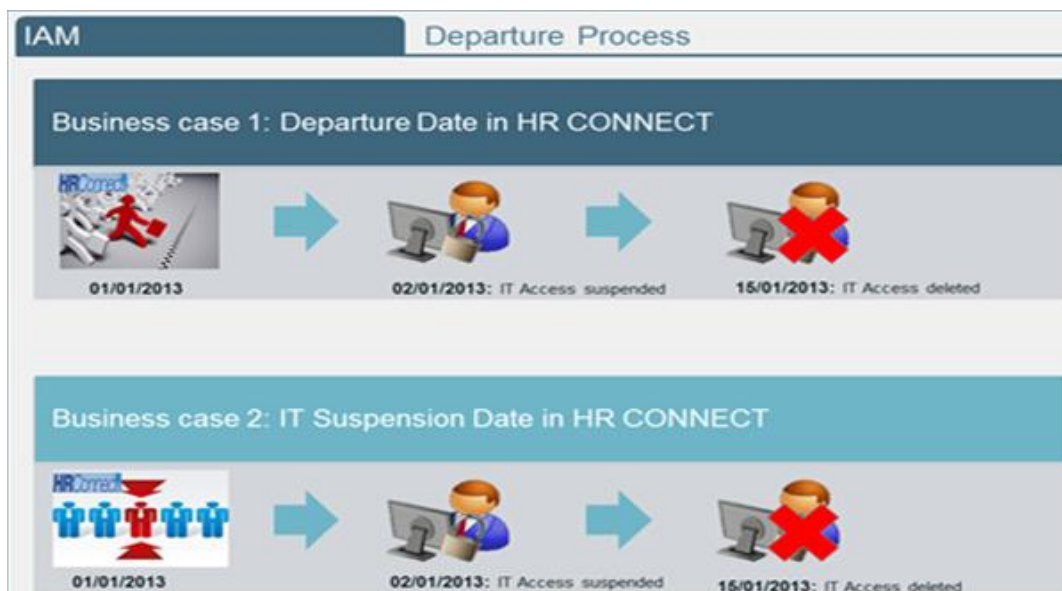
**Figure 14 : Processus de mise à jour d'identité IAM**

La valeur ajoutée attendue du processus de mise à jour d'identité IAM était l'uniformité de l'information quel que soit le système.

Dans le cadre processus de départ, le point essentiel était la gestion de la suspension automatique de l'identité de l'utilisateur. Le système IAM a donc basé ses politiques de sécurité sur la date de départ du collaborateur :

- A la date de départ plus 1 jour : le compte de l'utilisateur est suspendu, lui empêchant de se connecter au système d'information.
- A la date de départ plus 15 jours : le compte de l'utilisateur est supprimé ainsi que ses accès informatiques sur les différentes applications.





**Figure 15 : Processus de départ IAM**

La valeur ajoutée attendue du processus de départ IAM était une meilleure sécurisation du système d'information par la suspension automatique des identités en cas de départ.

### Le plan projet

Comme tout projet informatique, le projet de gestion d'identité a suivi la méthodologie EPROM, en appliquant l'enchaînement logique des phases de Design (conception), Build & Test (développement et test) et Roll Out (démarrage). L'avancement de ces phases était présenté à chaque comité projet.

IAM	Phase	Activity	Begin	End	% Plan.	% Comp.	Risk
	<b>Design</b>	Workshops & Documents	12/04/2012	05/07/2012			
	<b>Build &amp; Test</b>	Customization & Configuration & Packaging	09/07/2012	28/09/2012			
		Documentation	28/09/2012	23/10/2012			
		BT Qualification	23/10/2012	02/11/2012			
		Ipsen QA & Validation	02/11/2012	23/11/2012			
	<b>Rollout</b>	Training	06/12/2012	13/12/2012			
Deployment & Support		06/12/2012	07/02/2013				

**Figure 16 : Tableau d'avancement des phases du projet d'identité**

# Identity and access project plan

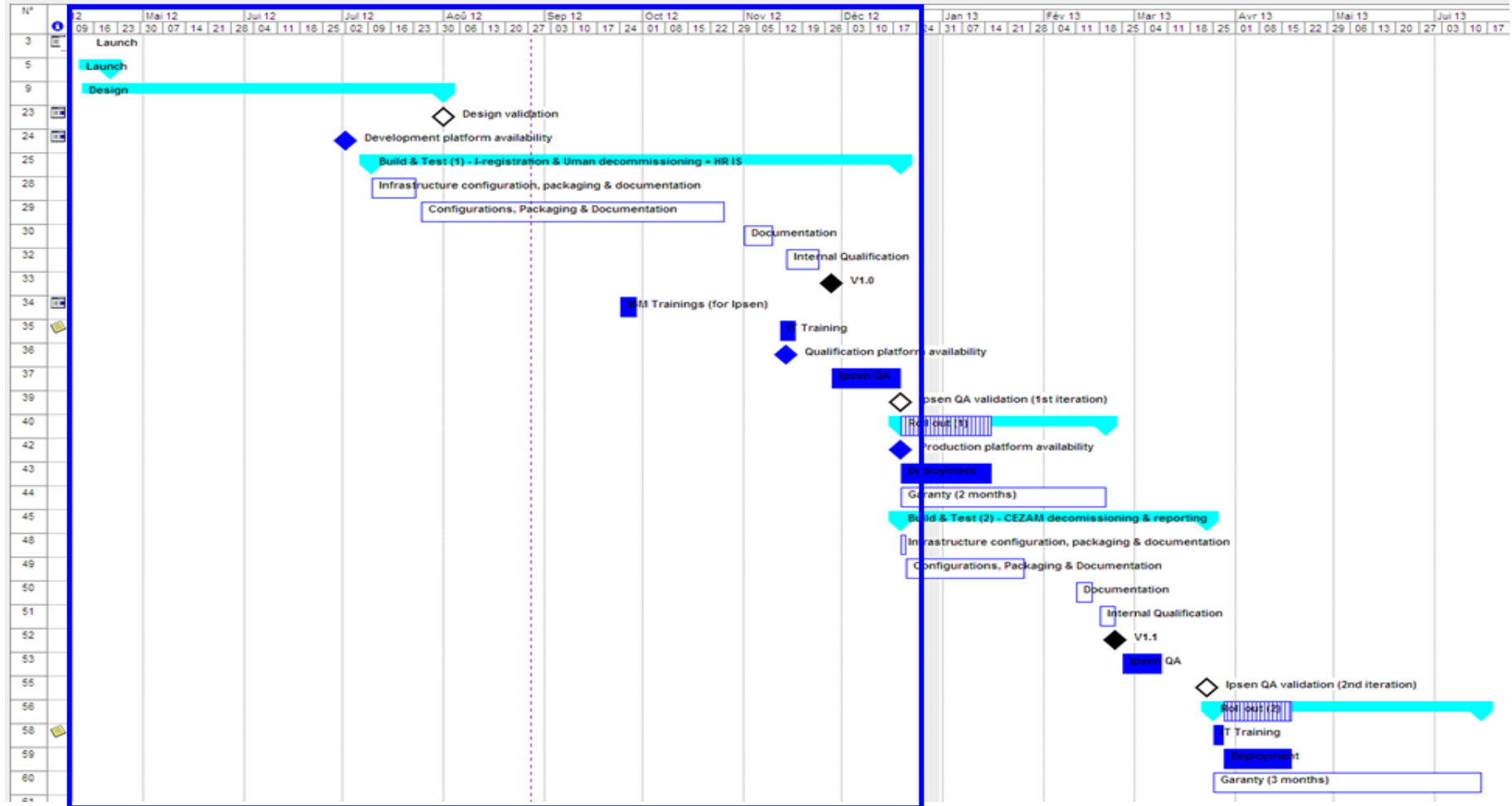


Figure 17 : Planning du projet de gestion des identités

## Les prérequis et contraintes

Le périmètre de ce premier projet ayant un impact fort sur les processus RH et sur l'architecture technique, il a fallu bâtir une équipe projet avec des acteurs représentatifs tant sur le plan métier que sur le plan technique. Côté métier, nous avons intégré le Vice-Président RH Groupe, le Directeur de la Transformation et le Directeur du Contrôle Interne dans le comité de pilotage pour valider les ressources métiers nécessaires aux tâches suivantes :

- Validation des nouveaux processus et outils
- Communication du projet IAM à tous les représentants RH au niveau monde
- Participation de l'équipe en charge du système d'information RH pour le travail d'interfaçage avec le système IAM

Côté technique, nous avons intégré au comité opérationnel des représentants des services Infrastructure et système d'information RH pour les tâches suivantes :

- Participation aux ateliers de Design de la solution technique
- Participation aux ateliers de mise au rebus des systèmes remplacés par IAM
- Travail sur les différentes interfaces et référentiels techniques

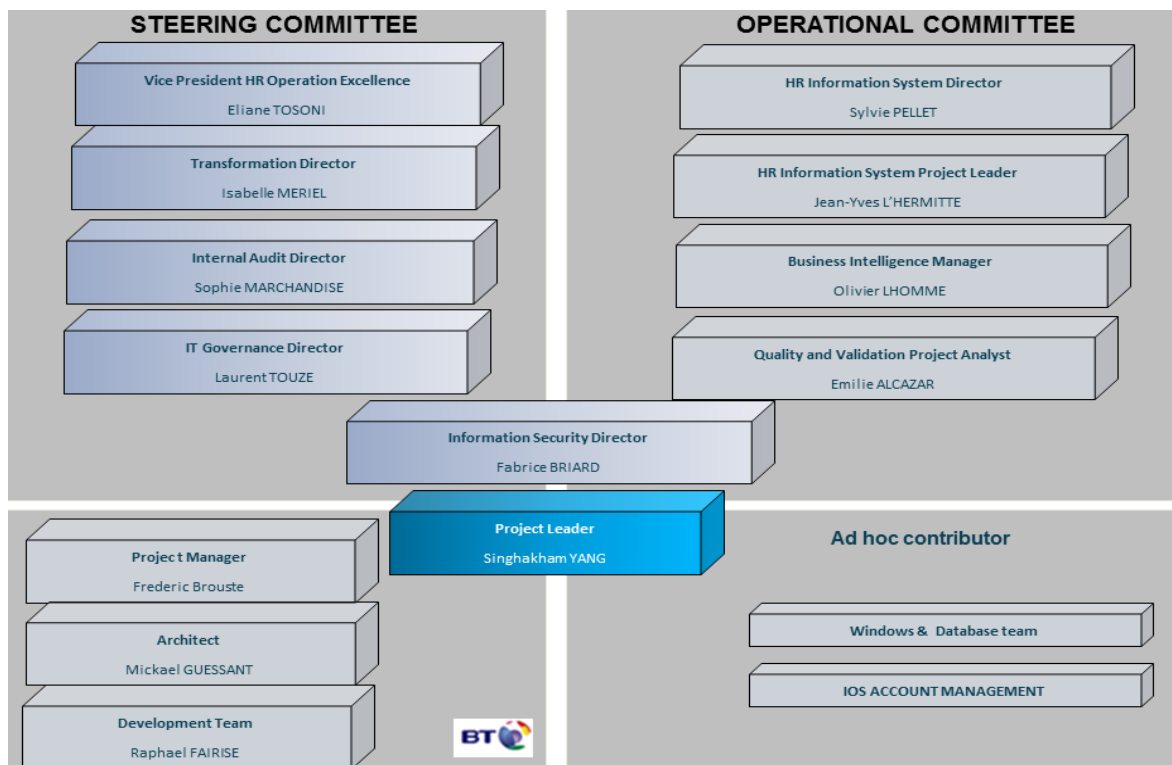


Figure 18 : Organisation du projet de gestion des identités

## **Phase projet – La conception**

Afin de maîtriser au mieux cette phase de conception, avec le chargé de qualification et de validation, nous avons mis en place les prérequis documentaires :

- Les spécifications des besoins utilisateurs de l'ensemble des phases
- La matrice de traçabilité permettant de faire les liens entre les différents documents : spécifications fonctionnelles, techniques et scripts de test
- L'analyse de risque

Plusieurs ateliers et plusieurs experts informatiques ont été nécessaires pour arriver à modéliser l'architecture cible du système IAM, ainsi que ses interfaces avec le système RH et l'annuaire technique Active Directory. Le résultat de ces ateliers a été formalisé sur deux documents majeurs : les spécifications fonctionnelles et techniques :

Le document de spécifications fonctionnelles comprend les éléments suivants :

- La définition des données (type et format)
- La fréquence des batchs (procédures automatiques de lancement de tâches)
- La liste des référentiels de données autoritaires
- La modélisation des différents flux de données

En ce qui concerne les différents flux de données, le système IAM fait intervenir deux systèmes majeurs : le système d'information RH et le DATAHUB (référentiel de donnée entreprise). Le flux d'identité principal est le suivant :

1. Le système d'information RH dépose une fois par nuit une extraction de sa base de données dans un espace d'échange avec le DATAHUB
2. Le DATAHUB dispose de ses données brutes RH et fournit les données transformées dans un espace d'échange avec le système IAM
3. Le système IAM récupère tous les matins les données du DATAHUB

# IAM DATA FLOW – DataHub and IAM General Overview

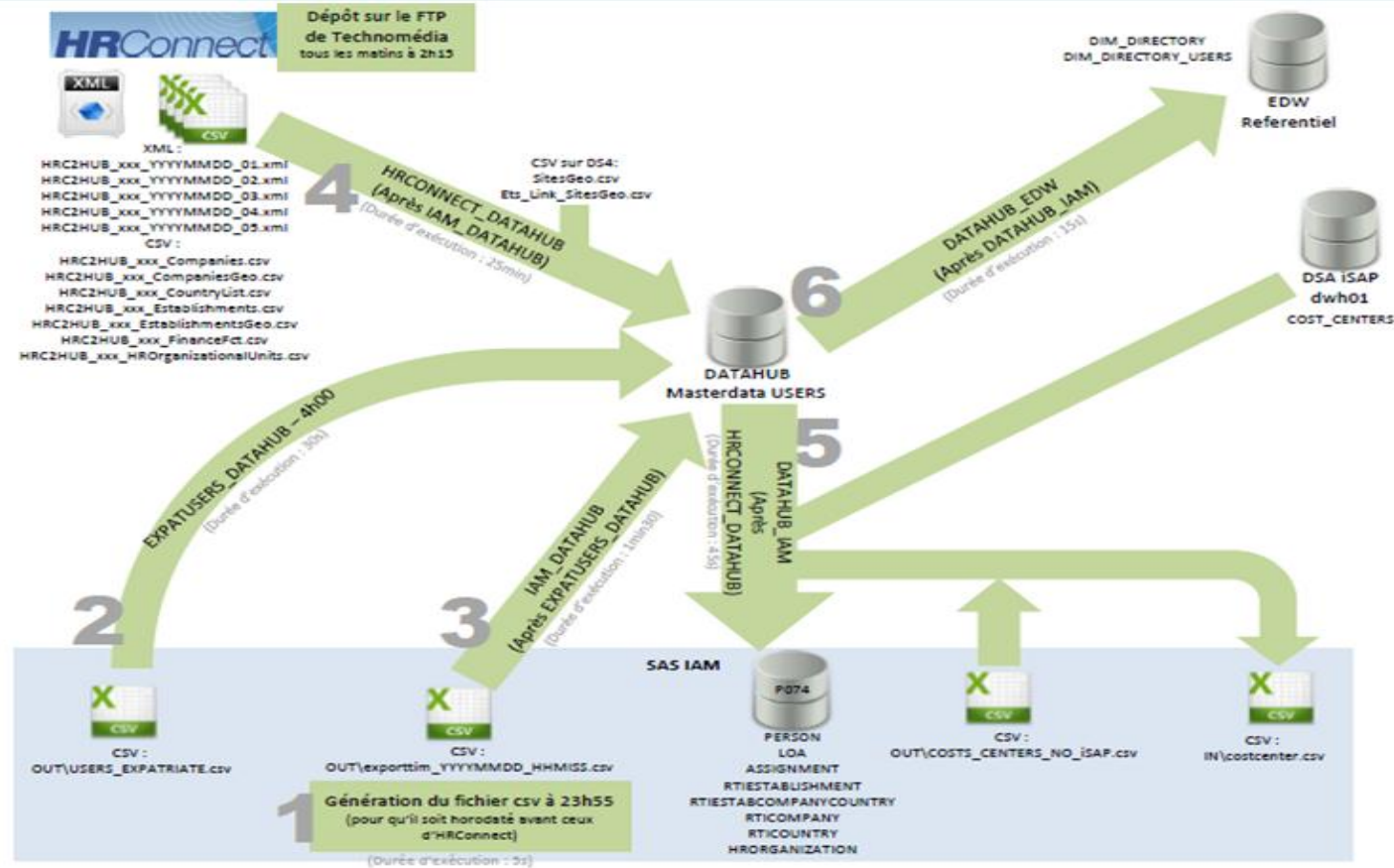


Figure 19 : Liste des flux de donnée entre les différents systèmes et IAM

Le document de spécifications techniques comprend les éléments suivant :

- La liste de serveurs avec leurs caractéristiques techniques
- La liste des bases de données associées avec leurs caractéristiques techniques
- Le schéma d'architecture du système IAM

En ce qui concerne l'architecture du système IAM, celui est composé de plusieurs éléments dont les principaux sont les suivants:

- Un serveur d'application permettant de lancer l'application utilisateur
- Un serveur d'annuaire permettant de stocker les identités des collaborateurs
- Une base de données Oracle pour les transactions spécifiques au système IAM
- Une base de données Oracle pour l'interface avec le DATAHUB
- Un connecteur Active Directory pour s'interfacer avec l'annuaire technique

# IAM COMPONENT – General Architecture

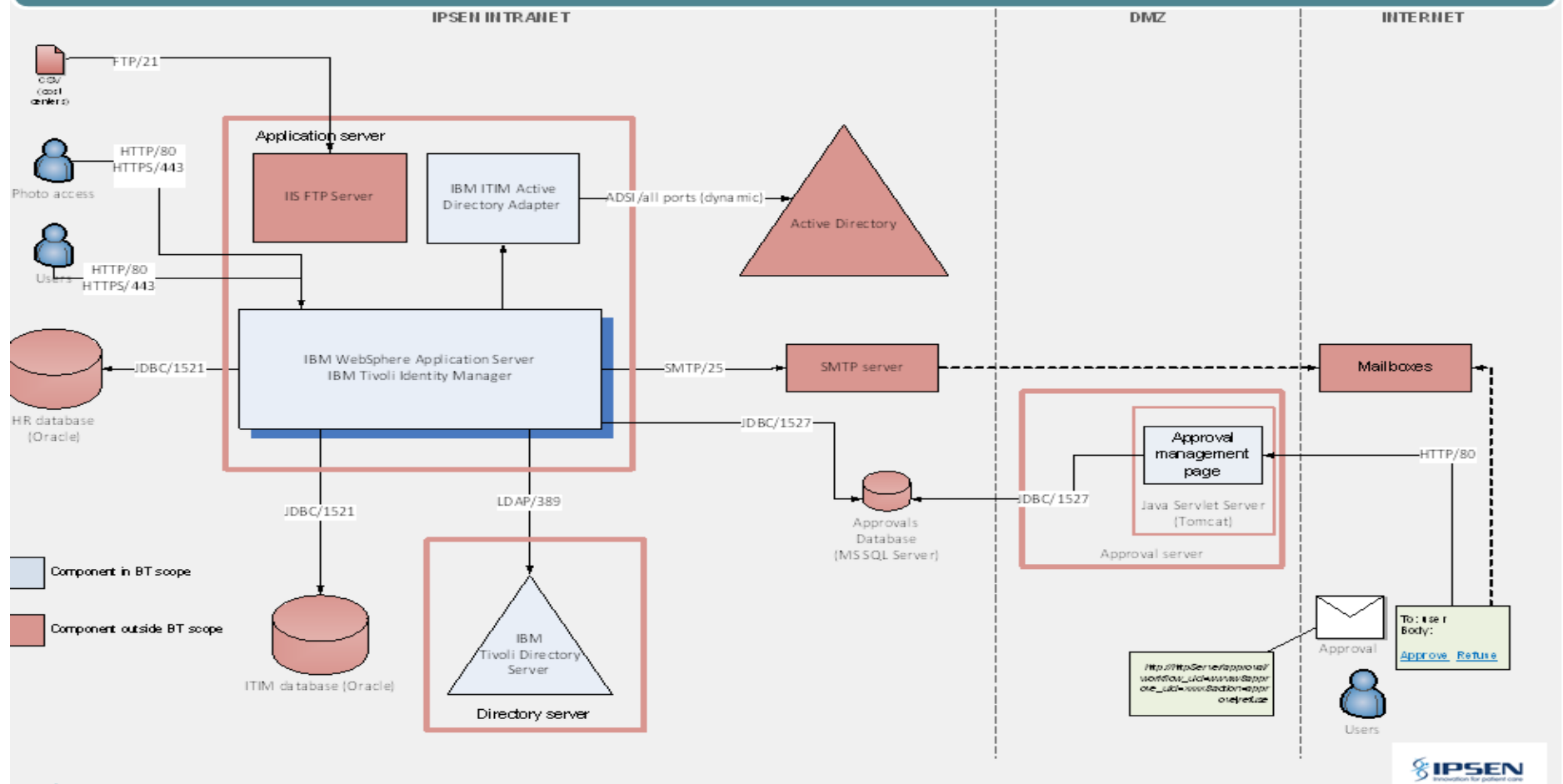
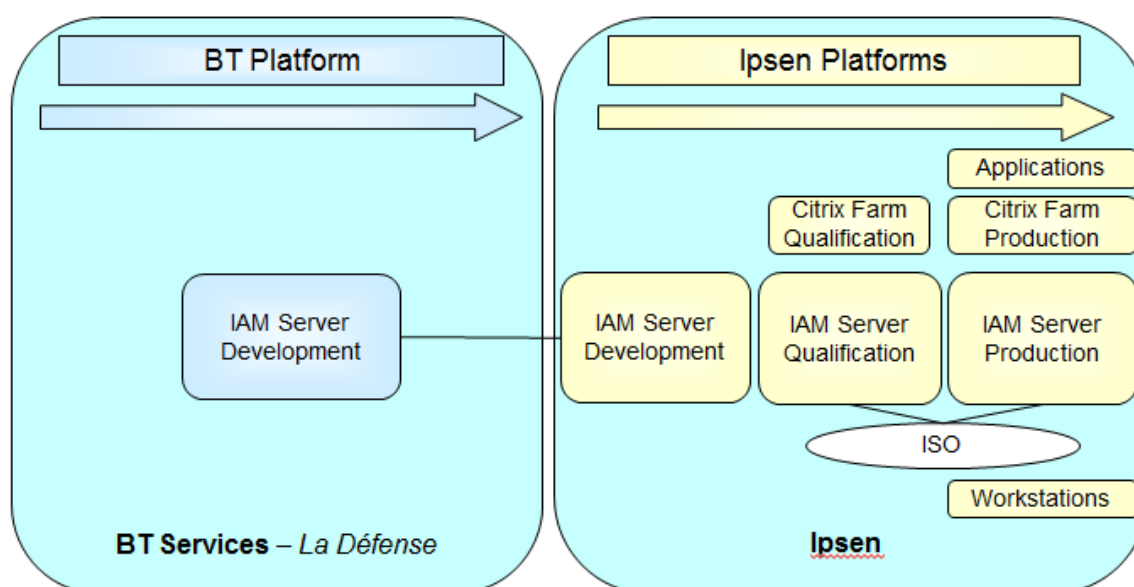


Figure 20 : Architecture technique du système IAM

Les spécifications fonctionnelles et techniques ont été fournies par l'intégrateur et ont suivi un circuit de vérification auprès des acteurs techniques sollicités dans les ateliers. Une fois ces documents validés, nous nous avons donné le feu vert pour démarrer le développement de la solution. Afin de cloisonner les différentes activités projets (développement, test et formation), plusieurs environnements techniques ont été créés :

- La plateforme de développement, dédiée à l'intégrateur pour le développement de la solution et ses tests fournisseur.
- La plateforme de qualification, dédiée à la qualification interne (recette client) et à la formation des utilisateurs.
- La plateforme de production pour la solution finale.



**Figure 21 : Les différents environnements du système IAM**

Ces ateliers ont également mis en évidence le travail de préparation nécessaire pour démarrer le nouveau système : à savoir un nettoyage, ou plutôt une mise en conformité du référentiel d'identité présent dans l'annuaire technique. En effet, de par la conception voulue dans l'interface entre les systèmes (le système d'information RH est autoritaire sur tous les autres), il fallait obligatoirement une parfaite osmose des données, sous peine de voir une suspension ou une suppression des compte active directory. Une campagne de sensibilisation avec des relances hebdomadaires a donc été menée auprès des services



informatiques et RH locaux, pour mettre en conformité le type des utilisateurs (interne ou externe) dans l'annuaire technique.

### **Phase projet – La qualification et validation du système**

La phase de qualification et de validation a suivi le processus standard EPROM. Après la recette fournisseur, nous avons déroulé avec le chargé de validation projet, les scripts de test sur l'environnement de qualification :

- La Qualification d'Installation qui atteste que l'implémentation du module de gestion des identités a été déroulée selon les documents d'installation approuvés
- La Qualification de Migration qui atteste que le chargement des informations d'identité migrées dans le système IAM est bien conforme aux fichiers de migration
- La Qualification Opérationnelle qui atteste que les processus de gestion des identités, ainsi que le flux entre les différentes interfaces, sont opérationnels

### **Phase projet – Le plan de communication et de formation**

Ce premier projet impactant directement les RH et les IT locaux, l'organisation des formations a donc été répartie en deux :

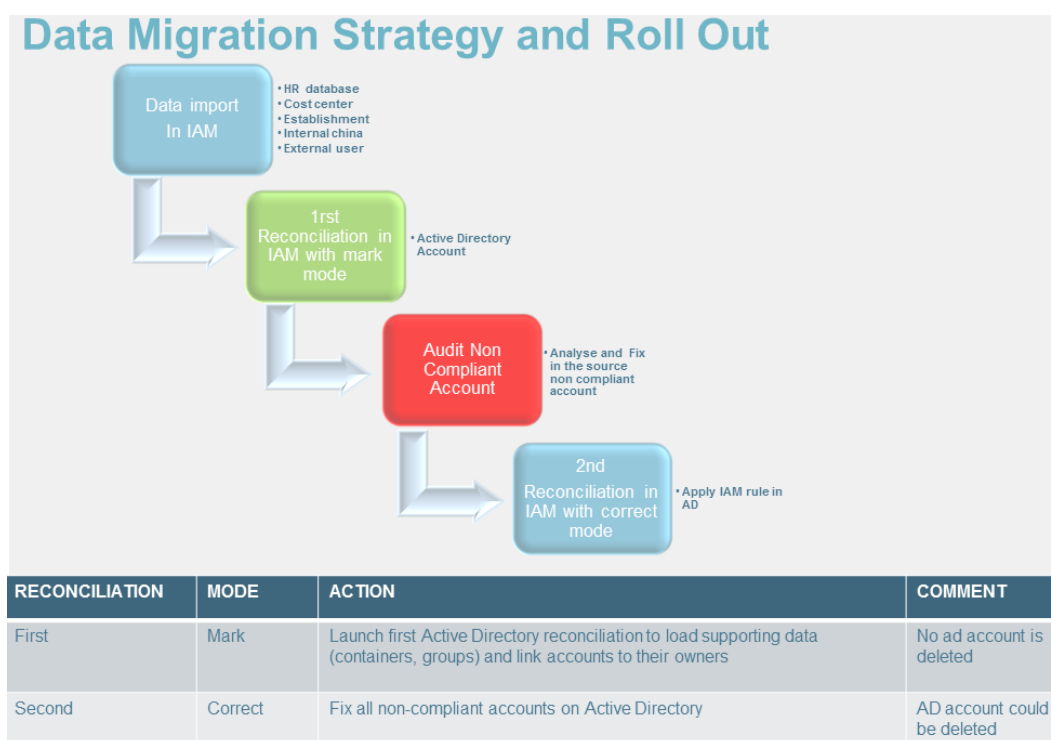
- Toute l'organisation des formations et la communication des RH site ont été pilotées par le service système d'information RH.
- Avec le responsable de la sécurité de l'information, nous avons pris en charge la population des services informatiques locaux.

Le système et l'interface étant simples d'utilisation, la formation d'une durée d'une heure comprenait une partie théorique sur les processus (arrivée, mise à jour d'identité et départ) et une démonstration de l'interface.

### **Phase projet – La mise en production**

La mise en production a été lancée le 19 décembre 2012. Cependant, malgré un travail de communication en amont sur la mise en conformité des référentiels, et une simulation des interfaces avant activation, un incident a été remonté par les sites des Etats Unis. Certains utilisateurs n'arrivaient plus à se connecter au système d'information. Après investigation, il s'avérait que les comptes actives directory de ces personnes avaient été supprimés par les

politiques de sécurité IAM car évalués non conformes : sur le référentiel du système d'information RH, ces personnes avaient quitté le Groupe. Toutefois sur l'annuaire technique, leur compte existait toujours en tant qu'employé interne. En activant le connecteur, IAM n'a fait que respecter la source autoritaire RH ; à savoir, supprimer le compte d'une personne ayant quitté la société. Après discussion avec le support informatique du site américain, il s'est avéré que ces personnes avaient quitté Ipsen et étaient revenus en tant qu'externes. Les actions demandées lors de la campagne de mise en conformité n'avaient donc pas été réalisées sur ces personnes.



**Figure 22 : Stratégie de mise en production du module de gestion des identités**

## Les résultats

Après le démarrage du système, les résultats ont été très vite perçus. La rapidité de délivrance d'un identifiant et d'un compte active directory était un parfait exemple : le temps d'attente en nombre de jours est passé de l'ordre d'une journée minimum, à seulement 5 minutes. Au niveau rapport, il était désormais possible d'avoir un état des lieux de l'ensemble des employés et partenaires, sans passer par un travail de réconciliation fastidieux de plusieurs référentiels.

	Avant	Après
Nombre de systèmes utilisés	3	1
Nombre de personnes impliquées dans la création d'un identifiant numérique	3	1
Temps de délivrance d'un identifiant numérique et création d'un compte Active Directory	1 à 3 jours	5 minutes
Notification mail aux acteurs concernés	manuel	automatique
Temps de génération d'un rapport pour avoir la population Ipsen	2h	5 mn

**Tableau 3 : Gain du projet de gestion des identités**

Le module de gestion des identités du système IAM ayant été délivré le 19 décembre 2012 comme prévu dans le planning, nous avons donc lancé le deuxième projet de gestion des accès, première semaine de janvier 2013 avec un objectif de démarrage à fin Mai 2013.

### 3.3 – Le projet de gestion des accès

#### Le contexte

Ipsen disposait d'un système appelé CEZAM pour faire des demandes d'accès informatique (création et suppression) à l'ensemble des applications du groupe. Celui-ci était utilisé par les services informatiques locaux qui recevaient les demandes métiers par différents canaux (présentiel, téléphone, mail ou formulaire papier). Cet outil permettait de cocher sur une fiche descriptive en format texte, le rôle demandé. Une fois la demande effectuée, une notification était envoyée à l'équipe de gestion des accès pour le traitement de ces demandes. Les faiblesses de cet outil étaient les suivantes :

- Aucune intégration avec d'autres systèmes.
- La fiche applicative en mode texte pouvait être modifiée par n'importe quelle personne ayant les droits pour faire une demande d'accès.

- La fiche applicative en mode texte ne permettait pas au final la consolidation de données et d'exploitation de donnée.
- Pas de gestion de séparation de pouvoir : un collaborateur pouvait demander des rôles incompatibles.
- Pas de circuit d'approbation par le manager ou de contrôle de formation de l'utilisateur.
- Des processus différents, voire redondants, en fonction des sites.
- En cas de départ du collaborateur, les suppressions n'étaient pas demandées par le service informatique, par manque de communication avec le service RH.

Application	
<b>Title :</b> Corporate Systems - SEAS	
<b>Identification code :</b> SEAS	
<b>Application form :</b>	
REQUEST DESCRIPTION	
_____	
Please put an "X" before the following request :	
<input type="checkbox"/> : Grant access to user	
<input type="checkbox"/> : Remove access from user	
For NEW access please enter the following information :	
Line manager's name..... : _____	
Sector (add an "X" where relevant)	
<input type="checkbox"/> : R&D	
<input type="checkbox"/> : Other	
<b>System owners :</b> AMANDINE PASCAL MARIA PAOLA FOPELLI SOLVEIG DE RANCOURT CHANTAL PETIT BOIS	
<b>Application administrators :</b> SOLVEIG DE RANCOURT AMANDINE PASCAL CHANTAL PETIT BOIS	

**Figure 23 : Exemple de fiche applicative disponible sous CEZAM**

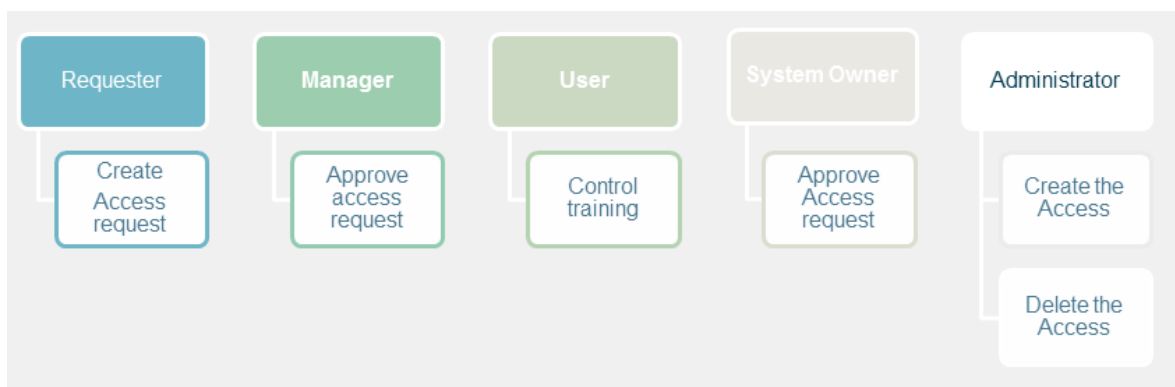
## Les objectifs

L'objectif de ce deuxième projet était de répondre aux faiblesses de l'outil CEZAM, en déployant le module de gestion des accès et de faire adopter par l'ensemble des sites, le processus de demande d'accès IAM modélisé en 2009.

## Le processus de demande d'accès IAM

Le processus de demande d'accès IAM fait intervenir plusieurs acteurs ayant des responsabilités différentes :

- Le demandeur
  - crée la demande d'accès informatique pour lui-même
- Le responsable de service
  - vérifie la légitimité de la demande de son collaborateur
  - approuve la séparation de pouvoir en cas de demande incompatible
  - approuve la demande d'accès
- Le responsable du système :
  - vérifie que l'utilisateur a suivi la formation
  - approuve la demande d'accès
- L'utilisateur
  - approuve le fait qu'il a suivi la formation adéquate à l'accès demandé
- L'administrateur
  - crée les comptes et autorisations d'accès sur le système informatique demandé



**Figure 24 : Processus de demandes d'accès sur IAM**

La valeur ajoutée attendue du processus de demande d'accès IAM était une meilleure sécurisation de la demande par l'enchaînement des étapes d'approbation et une autonomie de l'utilisateur vis-à-vis du support informatique pour créer les demandes d'accès.

## Le plan projet

Le projet de gestion des accès a suivi la méthodologie EPROM, en appliquant l'enchaînement logique des phases de Build & Test (développement et test) et Roll Out (démarrage). Le module de gestion des accès se basant sur la même plateforme technique que le module de gestion des identités, il n'a pas été nécessaire de mettre en place une phase de Design (conception). L'avancement de ces phases était présenté à chaque comité projet.

IAM	Phase	Activity	Begin	End	% Plan.	% Comp.	Risk
	<b>Build &amp; Test</b>	Customization & Configuration & Packaging	02/01/2013	22/03/2013			
		Documentation	25/03/2013	29/03/2013			
		BT Qualification	02/04/2013	15/04/2013			
		Ipsen QA & Validation	16/04/2013	29/04/2013			
	<b>Rollout</b>	Training	20/05/2013	27/05/2013			
		Deployment & Support	28/05/2013	12/06/2013			

**Figure 25 : Avancement des phases du projet d'identité**

# Identity and access project plan

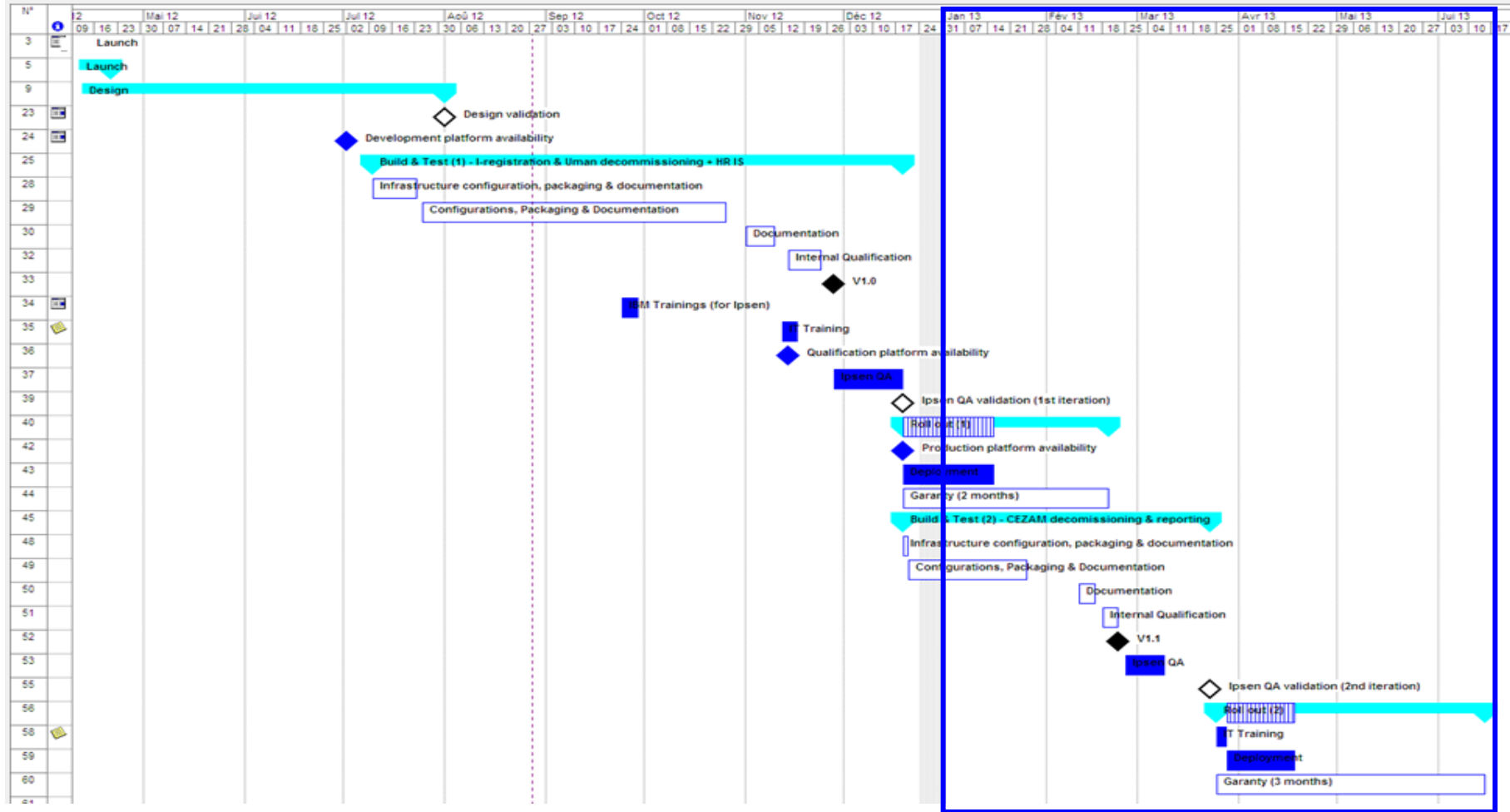


Figure 26 : Le planning projet du module de gestion des accès

## Les prérequis et contraintes

Le périmètre de ce deuxième projet touchant toute la population des utilisateurs ainsi que l'ensemble du paysage applicatif Ipsen, il a fallu garder une équipe projet avec des acteurs représentatifs du métier et de l'informatique. Côté métier, le comité de pilotage IAM a pu garder du premier projet le Directeur de la Transformation et le Directeur du contrôle interne, acteurs nécessaires pour imposer le processus de demandes d'accès aux différents sites. Côté technique, le comité opérationnel a intégré une personne de l'équipe de gestion des accès et de manière ad hoc les experts applicatifs des systèmes.

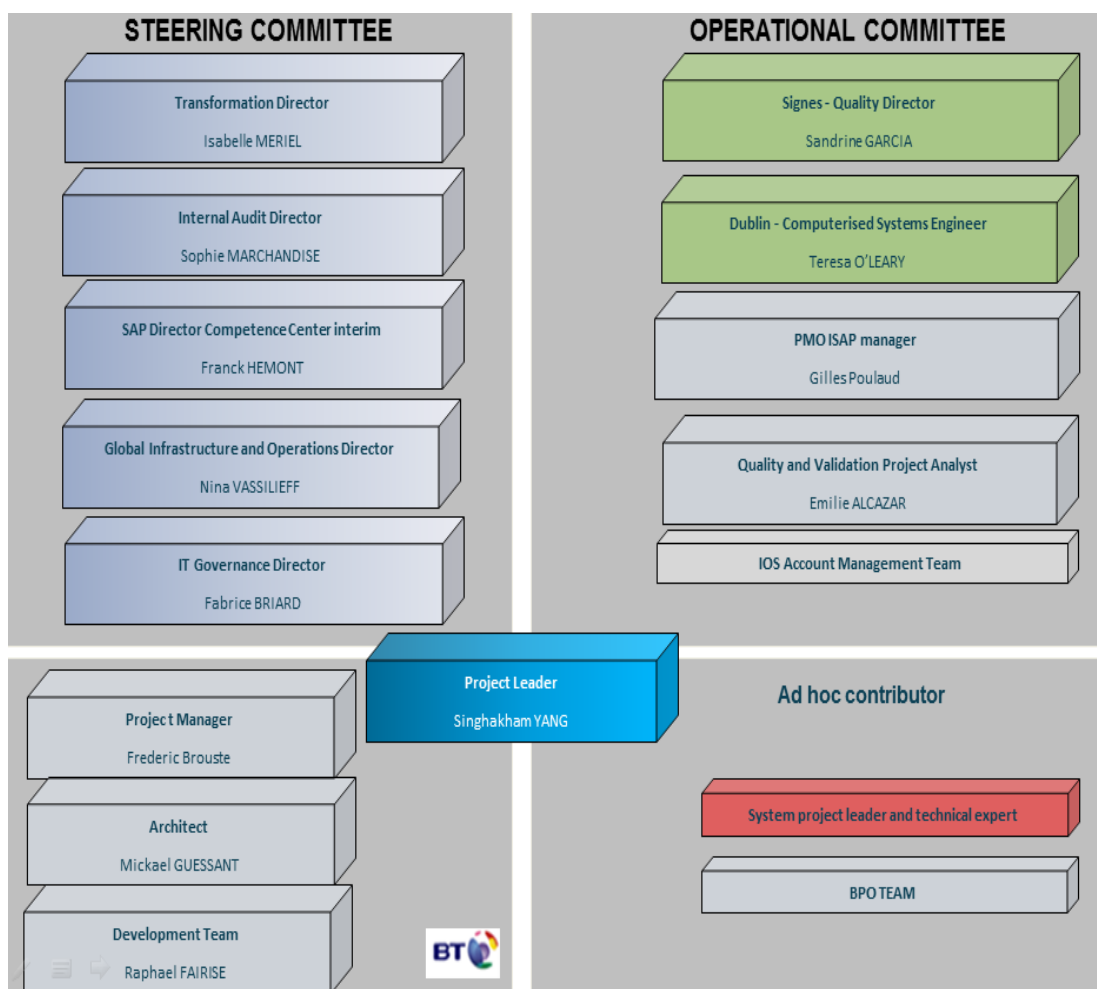


Figure 27 : Organisation du deuxième projet

## Phase projet – Le plan de communication et de formation

A la problématique « comment former plus de 5000 collaborateurs au vu du timing et des ressources limitées de l'équipe projet ? », nous avons décidé en comité de pilotage de partir sur une stratégie d'autoformation de l'utilisateur. C'est pourquoi nous avons fait intervenir



le cabinet EMS Conseil. Cette société est spécialisée dans le domaine de la communication, et nous à accompagner pour la création de tutoriels vidéo et de guides utilisateurs en trois versions (française, anglaise et chinoise). Nous avons donc calé le planning de réalisation de ces différents livrables, par rapport au planning de livraison des développements de la solution. Une fois que la qualification fournisseur de BT était terminée, EMS a pu disposer de la plateforme de test et faire des captures d'écran des différentes interfaces. Les guides utilisateurs et tutoriels vidéo ont fait l'objet de vérification et d'approbation par le comité opérationnel et contributeurs ad hoc (utilisateurs finaux et services informatiques locaux).



**Figure 28 : Cinématique du tutoriel vidéo de demandes d'accès (version chinoise)**

Concernant les guides utilisateurs et tutoriels vidéo chinois, l'équipe projet a mis à contribution l'équipe informatique locale chinoise du site de Tianjin pour la vérification et l'approbation des matériels de formation.

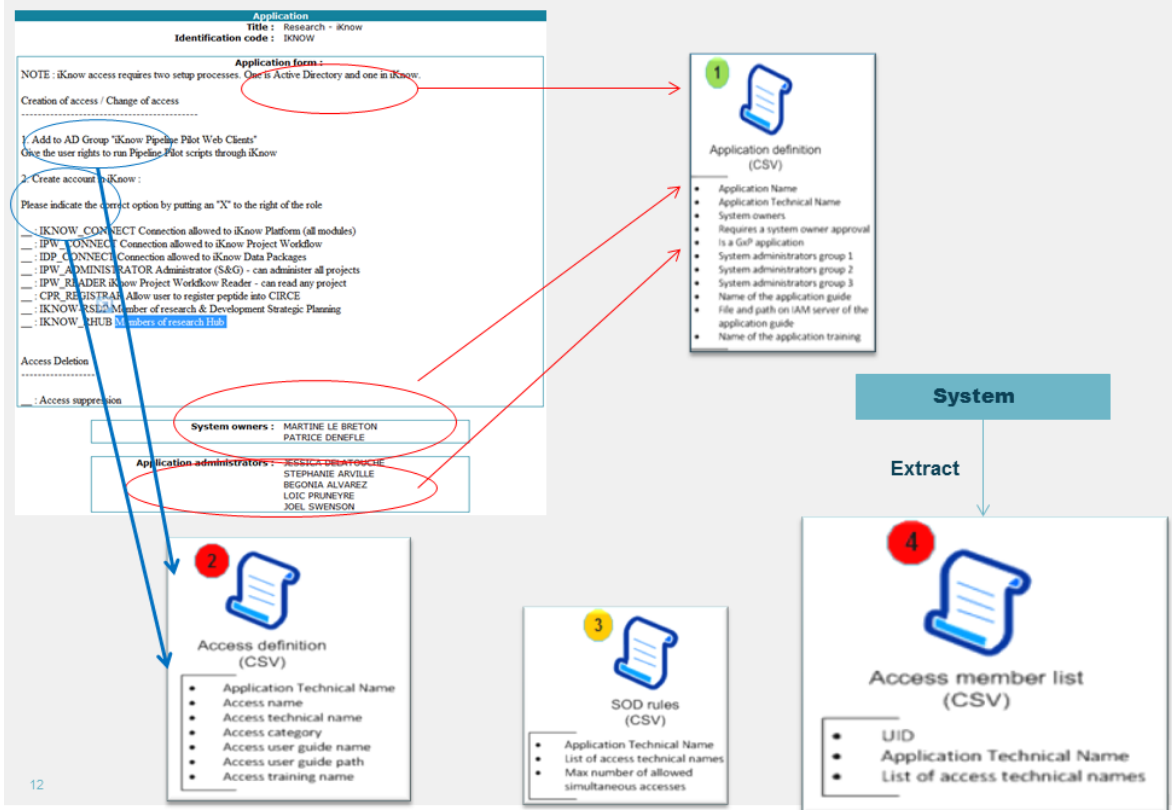
### **Phase projet - La préparation des modèles de migration**

La préparation des modèles de migration était une étape clef du projet faisant intervenir l'ensemble des experts applicatifs de chaque système. En effet, le challenge était de modéliser au mieux les droits et autorisations disponibles sur CEZAM vers le modèle du

nouveau système IAM. Afin d'aider aux mieux les experts dans cette tâche de modélisation, des modèles de fichier ont été créés :

- Modèle 1 : Description de l'application
  - Nom de l'application
  - Description de l'application
  - Le système est-il critique ?
  - Le système a-t-il un responsable ?
  - Liste des responsables du système
  - Liste des administrateurs du système
- Modèle 2 : Liste des accès de l'application
  - Nom de l'accès
  - Description de l'accès
  - Cet accès fait il l'objet d'une formation ?
- Modèle 3 : Règle de séparation des pouvoirs
  - Liste des accès incompatible de l'application
- Modèle 4 : Liste des utilisateurs avec leurs accès
  - Liste des identités numériques couplées aux accès de l'application

## Migration Template Methodology – CEZAM to IAM



**Figure 29 : Méthodologie de modélisation des applications sur le module Access Management**

Afin de couvrir les 250 systèmes à modéliser sur le temps imparti, nous avons dû organiser avec les experts applicatifs plusieurs sessions en vidéoconférence, pour présenter la méthodologie de modélisation et fixer la date limite de livraison.

### Phase projet - La qualification et la validation

La phase de qualification a suivi le processus standard EPROM. Après la recette fournisseur, nous avons déroulé avec le chargé de validation projet, les scripts de test sur l'environnement de qualification :

1. La Qualification d'Installation qui a attesté que l'implémentation du module de gestion des accès été déroulée selon les documents d'installation approuvés.
2. La Qualification de Migration qui a attesté que le chargement des modèles applicatifs migrés dans le système était bien conforme aux fichiers de migration.
3. La Qualification Opérationnelle qui a attesté que les processus de demandes d'accès étaient opérationnels.

## **Phase projet - La mise en production**

La mise en production du module de gestion des accès a eu lieu le 27 mars 2013 comme défini dans le planning projet. Cependant, suite à un bug technique de la solution non identifié pendant la phase de qualification, le démarrage pour la partie collaborateur a été suspendu. Après correction du bug par notre intégrateur fin juin, le Comité de Pilotage s'est prononcé sur une nouvelle stratégie de déploiement. Il a été décidé de lancer une phase pilote sur l'ensemble des collaborateurs de 3 sites majeurs (Angleterre, France et Chine) de septembre à octobre 2013. Le but était de disposer d'une base de donnée suffisante pour, d'une part avoir un indicateur représentatif sur la création des demandes d'accès faites par le métier, et d'autre part un nombre d'utilisateurs suffisant pour le lancement d'un sondage de satisfaction sur le mois de novembre. Le sondage a été axé sur les fonctionnalités principales de l'outil :

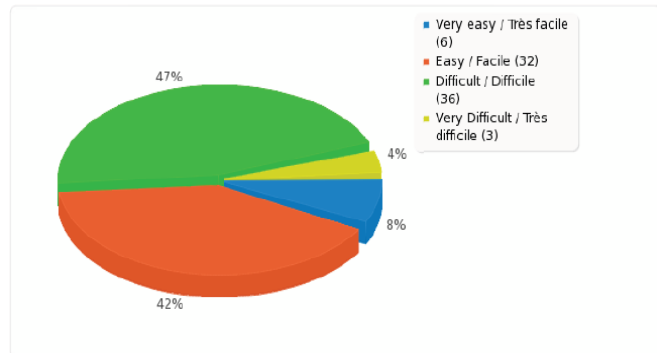
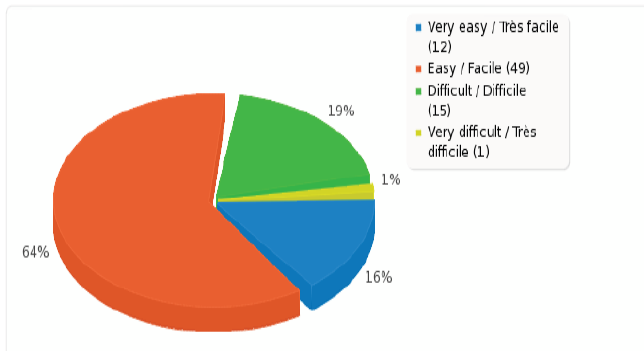
- La création d'une demande d'accès informatique
- La facilité de voir le statut de sa demande
- La facilité de recherche d'une application ou d'un accès informatique
- Le niveau de support du service informatique sur l'outil

## **Les résultats**

Concernant le sondage, les résultats ont remonté une difficulté des utilisateurs à trouver la bonne application, et un manque de visibilité sur le statut des demandes en cours. Ces remarques ont été prises en compte et rapportées à notre intégrateur pour l'amélioration de l'interface.

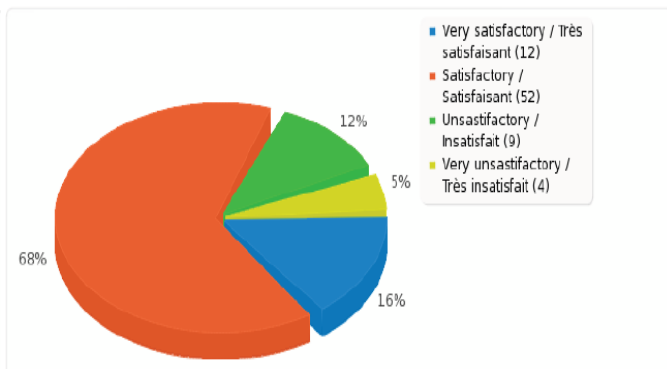
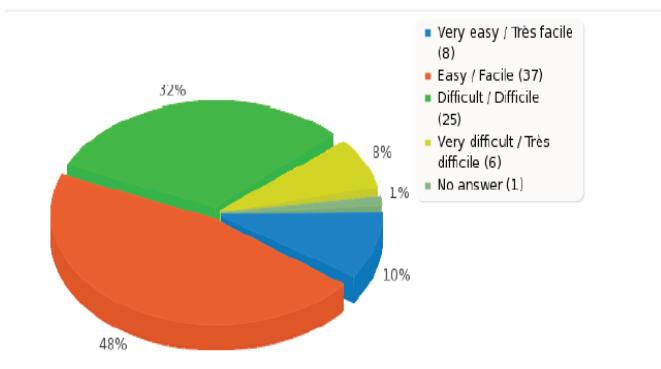
Question 2/12EN. Please rate the ease of creating an access request with the toolFR. Merci d'évaluer la facilité de création d'une demande d'accès avec l'outil

Question 3/12EN. Please rate the search facility to find application with the tool ?FR. Merci d'évaluer la facilité de recherche d'une application ou d'un accès avec l'outil



Question 4/12EN. How do you rate the ability of the tool to see the status of your pending access requests ?FR. Comment évaluez vous la facilité de visualiser le statut de vos demandes en cours ?

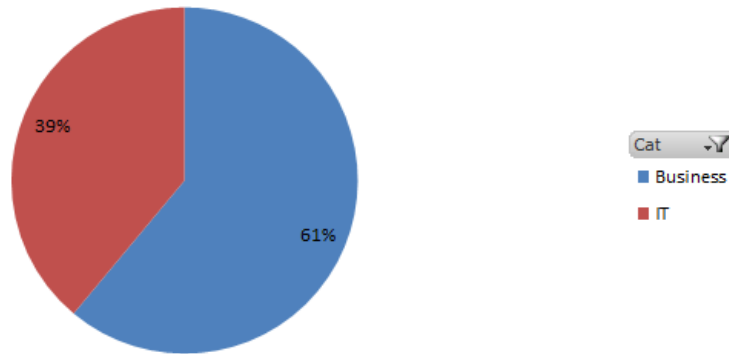
Question 11/12EN. How do you rate the IT helpdesk on the support for the Access Management tool ?FR. Comment évaluez vous le niveau du service IT sur le support de l'outil Access Management ?



**Figure 30 : Résultat du sondage collaborateur sur le module de gestion des accès**

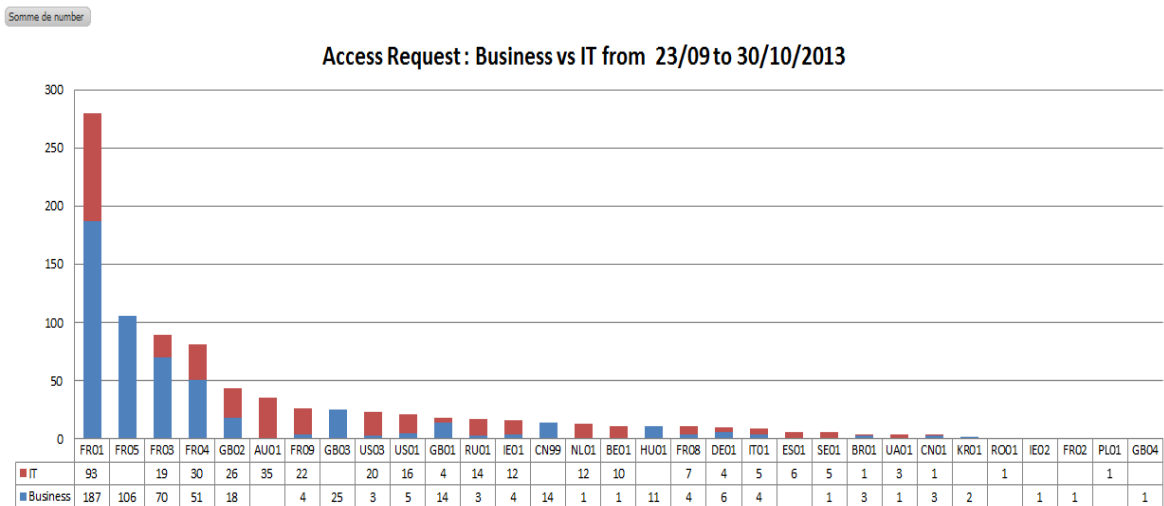
Concernant l'appropriation de l'outil par les métiers, un indicateur pour jauger le taux d'utilisation a été mis en place. Le pourcentage des demandes de création faites par les métiers par rapport à celui des services informatiques locaux, était de 60 % contre 40 %. Les résultats étaient donc encourageants au vu de l'impact sur le changement des habitudes des utilisateurs.

### Access Request: Business VS IT



**Figure 31 : Nombre de demandes d'accès créées par les utilisateurs par rapport au support informatique**

La figure ci-dessous montre le niveau d'appropriation de l'outil de gestion des accès par site. Cet indicateur nous a permis de cibler nos efforts de communication et de sensibilisation et d'être plus efficace en évitant une communication massive.



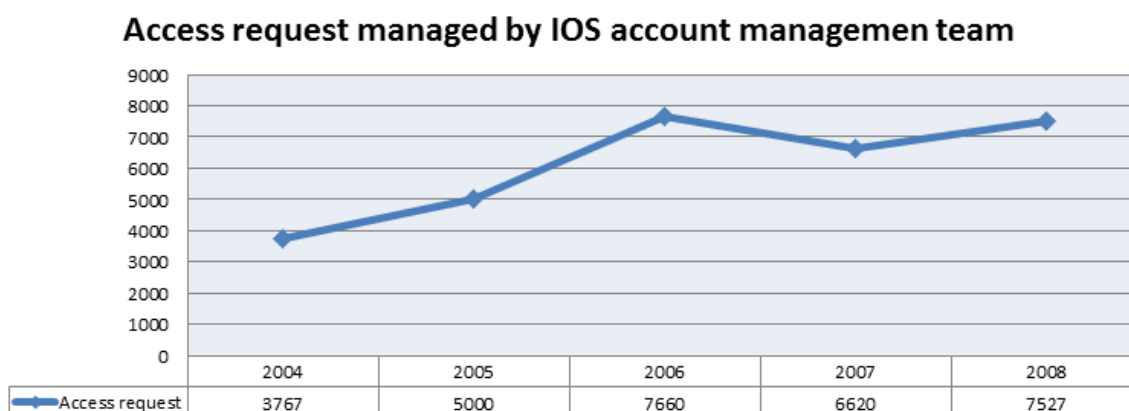
**Figure 32 : Comparatif de création de demandes d'accès par établissement**

Le module de gestion des accès du système IAM ayant été implémenté le 27 mai 2013 comme prévu sur le planning, le dernier projet de création automatique des accès informatique a donc été démarré en juin 2013 avec la particularité suivante : la mise en production de manière itérative du module de création automatique sur 13 systèmes.

### 3.4 – Le projet de création automatique des accès informatiques

#### Le contexte

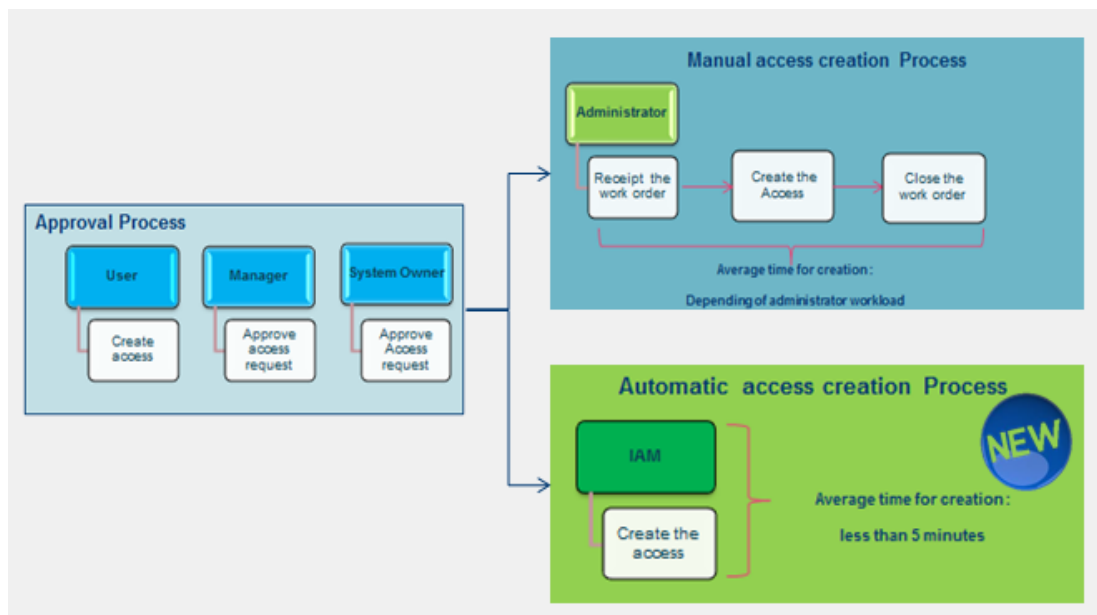
Le service de gestion des accès est composé de 3 personnes. Celui-ci gérait les accès (création, modification et suppression) de plus de 250 systèmes. A cela se rajoutaient des experts applicatifs pour la création de comptes sur des référentiels spécifiques. Le nombre de systèmes augmentait d'année en année ainsi que le nombre de collaborateurs avec leur cycle de vie (arrivée, transfert et départ). C'est la raison pour laquelle il était difficile sur certaines périodes, d'assurer un niveau de service réactif au niveau de la délivrance des accès, et ce sans non-conformité. La figure ci-dessous montre une augmentation de 100% de 2004 à 2008 du nombre de demandes traitées par le service de gestion des accès sans augmentation d'effectif sur cette période.



**Figure 33 : Nombre de demandes d'accès traitées par le service de gestion des accès de 2004 à 2008.**

#### Les objectifs

L'objectif de ce troisième et dernier projet était de répondre à cette problématique de délivrance des accès informatiques. Ceci en fournissant à 13 systèmes majeurs du Groupe Ipsen, un module de création automatique. Par ce biais, la gestion manuelle des comptes assurée par le service de gestion des accès et des experts applicatifs était désormais assurée par le système IAM lui-même. La figure ci-dessous montre le parallèle entre le traitement d'une tâche de création effectuée manuellement par un administrateur et le traitement automatique effectuée par le système IAM. L'opérateur humain doit réceptionner la tâche, la prioriser en fonction de sa charge puis procéder à la création de l'accès. Le système IAM lui reçoit la demande et la traite tout de suite.



**Figure 34 : Processus de demandes d'accès avec mise en place du module de création automatique**

Ce nouveau mode de fonctionnement présentait comme principaux avantages :

- Une rapidité de délivrance des accès informatiques
- La suppression des non conformités réglementaires dues à des erreurs humaines
- Une satisfaction utilisateur accrue
- Une sécurisation de la gestion des accès informatiques couplée aux processus de cycle de vie des collaborateurs (arrivée, mise à jour et départ)

La liste des 13 systèmes inclus dans le périmètre projet a été établie sur la base du nombre de demandes d'accès traitées sur l'année 2012.



Target System	Number of requests in 2012	Target repository
Office 365	1703 (mail)	Office 365
Internet	1230	Active Directory
SAP	835	SAP
Easidoc	662	DOCUMENTUM / AD
BO report	340	Active Directory
Secure Client VPN	245	RSA
iProject	233	Active Directory
Trackwise	149	SPARTA
Lighthouse	117	Active Directory
iReview	49	SAS BI
Bird	25	DOCUMENTUM / AD
Lims	4	LABVANTAGE
IAM	NA	TIVOLI

**Figure 35 : Liste des systèmes inclus dans le périmètre projet**

## **Le plan projet**

En termes de planning projet, nous avons décidé avec le comité de pilotage, de mettre en place un mode itératif, en répartissant les 13 systèmes sur 6 lots pour les raisons suivantes :

- Eviter un effet tunnel sur les livrables attendus.
- Délivrer les bénéfices du module de création aux utilisateurs finaux de manière séquencée.
- Répartir la charge des experts applicatifs sollicités.

Scope	Application	Adapter/Connector
Lot 1	IAM	ITIM API adapter
	BO	ITIM Active Directory Agent
	Easidoc	ITIM Active Directory Agent
	Internet	ITIM Active Directory Agent
	Lighthouse	ITIM Active Directory Agent
Lot 2	Ireview	SAS Adapter: Driver SAS Sharenet JDBC (SAS Foundation Services)
Lot 3	iSAP	ITIM SAP Netweaver (R/3) Adapter (ITDI based)
Lot 4	iProject	ITIM Active Directory Agent + other target
	AD Mixed applications	ITIM Active Directory Agent + Work Orders
Lot 5	Trackwise	JAVA based API (custom)
	Lims	JAVA based API (custom)
Lot 6	Mail	ITIM Office 365 Adaptor (coming up Q4 2013)
	Secure Client VPN	IBM RSA adapter

**Figure 36 : Liste des systèmes par lots**

Chaque lot a suivi la méthodologie EPROM, en appliquant l'enchaînement logique des phases de Design (conception), Build & Test (développement et test) et Roll Out (démarrage).

### Project Macro Gantt

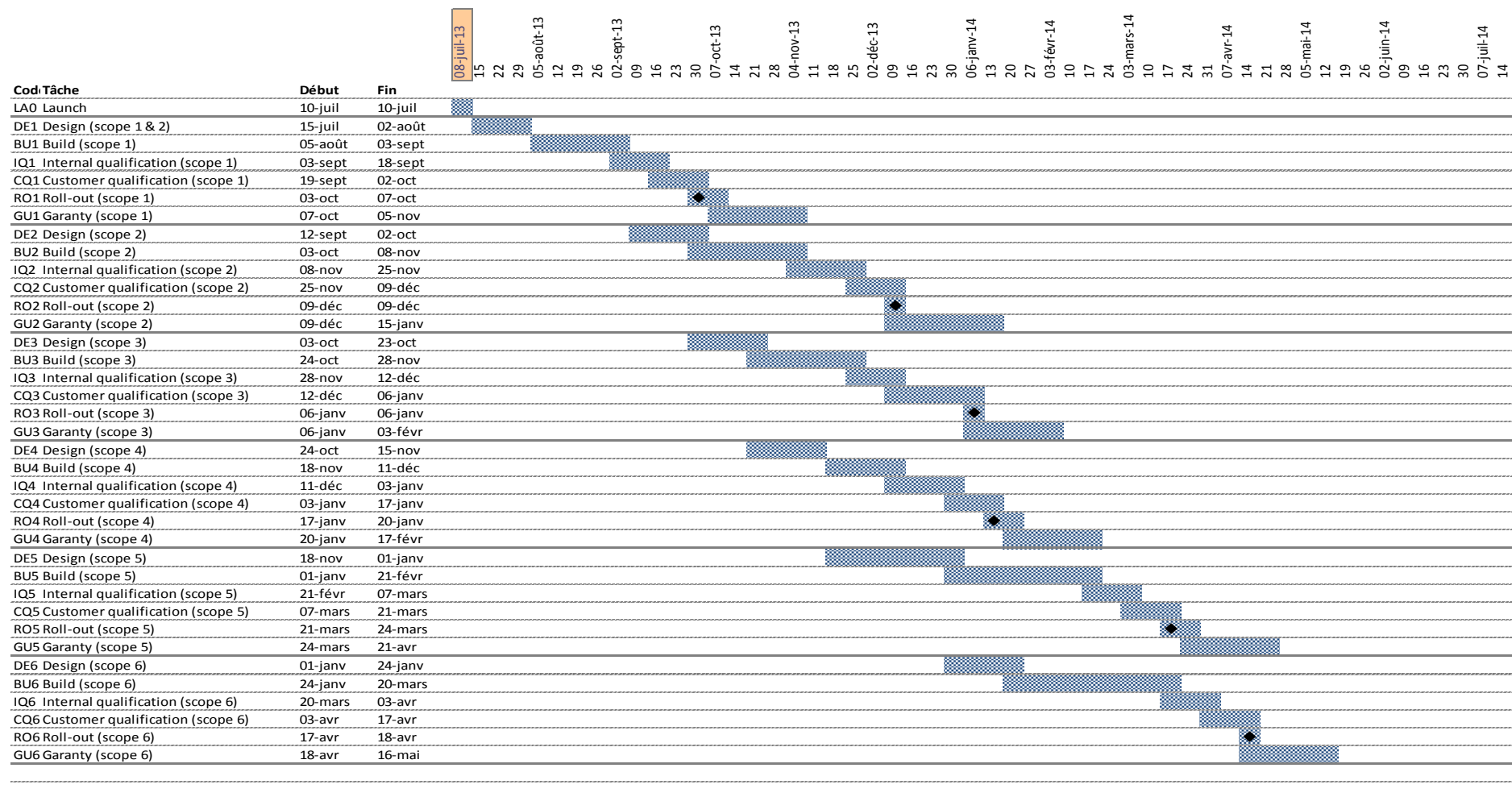


Figure 37 : Planning du projet de création automatique des accès

## Les prérequis

Ce projet étant essentiellement technique, les instances projet ont été entièrement remodelées. La différence majeure par rapport aux deux premiers projets, a été l'absence totale d'acteurs métier (RH, Transformation et Contrôle Interne) sur les deux comités (pilotage et opérationnel).

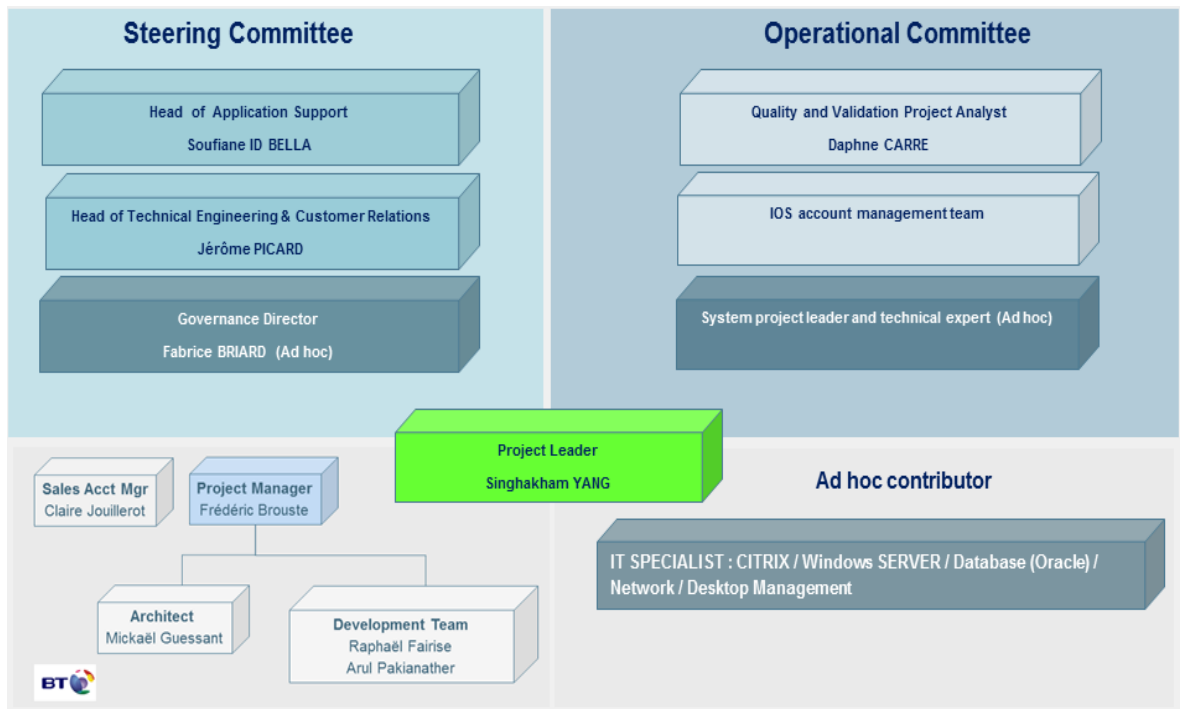


Figure 38 : Organisation du projet création automatique des accès

## Phase projet - La conception

Des ateliers de conception ont donc été réalisés pour chaque système. Le but était d'évaluer la faisabilité technique de mise en place des connecteurs entre le système IAM et les référentiels des systèmes à automatiser. Les acteurs présents étaient nécessairement les experts applicatifs, un membre de l'équipe de gestion des accès, l'équipe de consultants BT (architecte et consultants IAM), et moi-même. Les points abordés en atelier étaient :

- le modèle de compte et d'autorisation de chaque système
- le nombre de référentiels existants pour l'activation d'un compte
- les actes techniques des différents administrateurs nécessaires à la création d'un compte

- la technologie du système (base de données, service, etc.)

Divers problèmes ont été rencontrés, certains nécessitaient une réévaluation du projet en termes de planning, ou voire même de périmètre :

- Malgré l'expertise des experts applicatifs, certaines questions restaient en suspens, et nécessitaient le recours aux différents éditeurs et intégrateurs des solutions, ce qui avait un impact sur le planning projet.
- La gestion des accès des systèmes complexes à modéliser sur le connecteur du fait de l'absence de matrice, pouvait conduire à une automatisation partielle du connecteur, avec encore des tâches manuelles.

L'ensemble de ces points ont été remontés au comité de pilotage qui nous a challengés pour maintenir les dates de démarrage, en rognant sur les marges de sécurité du planning. De plus, il nous a été demandé de refaire des ateliers pour atteindre la cible en matière de création automatique, à savoir plus d'actions manuelles des administrateurs.

### **Phase projet – La qualification et validation du système**

La phase de qualification a suivi le processus standard EPROM. Après la recette fournisseur, nous avons déroulé avec le chargé de validation projet, les scripts de test sur l'environnement de qualification :

1. La Qualification d'Installation qui a attesté que l'implémentation du connecteur a été déroulée selon les documents d'installation approuvés.
2. La Qualification de Migration qui a attesté que le chargement des données migrées dans le système était bien conforme aux fichiers de migration.
3. La Qualification Opérationnelle qui a attesté que le connecteur et les flux de création et de suppression étaient opérationnels entre le système IAM et le système cible.

Pour ce dernier projet, une attention particulière a été portée sur la phase de migration qui s'était portée sur 100% des données, et sur la qualification opérationnelle qui comportait un échantillonnage des données à 15%. Cette méthodologie permettait de s'assurer du bon paramétrage du connecteur pour chaque système. En cas d'anomalie rencontrée pendant les tests, une fiche de non-conformité était générée et envoyée à l'intégrateur pour résolution.

Toutes les non-conformités devaient être levées avant l'autorisation de mise en production par le chargé de validation qualité.

## La mise en production

La mise en production pour chaque lot respectait également le même schéma :

1. Une sauvegarde du référentiel applicatif était obligatoirement effectuée la veille, pour permettre un retour arrière en cas de problème de déploiement.
2. La Qualification d'Installation sur l'environnement de production qui attestait que l'implémentation du connecteur a été déroulée selon les documents d'installation approuvés.
3. La Qualification de Migration sur l'environnement de production qui attestait que le chargement des données migrées dans le système était bien conforme aux fichiers de migration.
4. Une activation du connecteur en deux temps :
  - a. Lancement du mode prévisualisation, permettant la simulation de l'effet du connecteur sur le référentiel cible. Cela présentait comme sérieux avantage la détection de comptes non conformes ou anomalies.
  - b. Activation du connecteur après correction des anomalies.

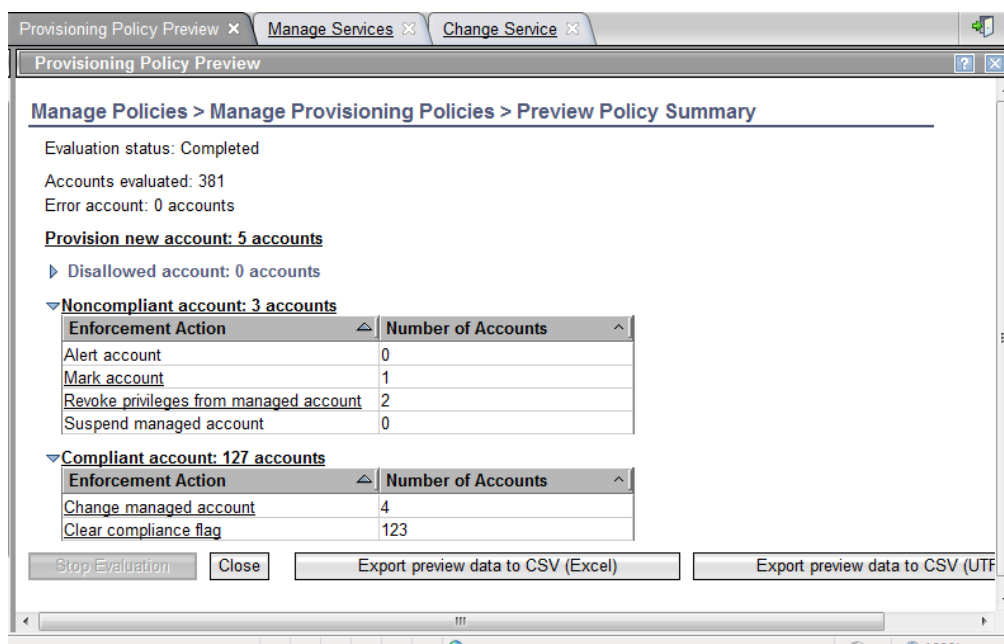


Figure 39 : Mode de simulation du connecteur IAM sur les systèmes cibles

## Les résultats

Afin d'avoir une visibilité sur le temps moyen de délivrance des accès, un indicateur de type écart-type a été calculé sur la période de mai à juillet 2013. Après un retour d'expérience sur les mois de novembre et décembre 2013, le module de création automatique a pris en charge 30% de l'activité de gestion des accès. La rapidité de délivrance des accès a été accrue de 1,6 jours à 5 minutes, et sans non-conformité.

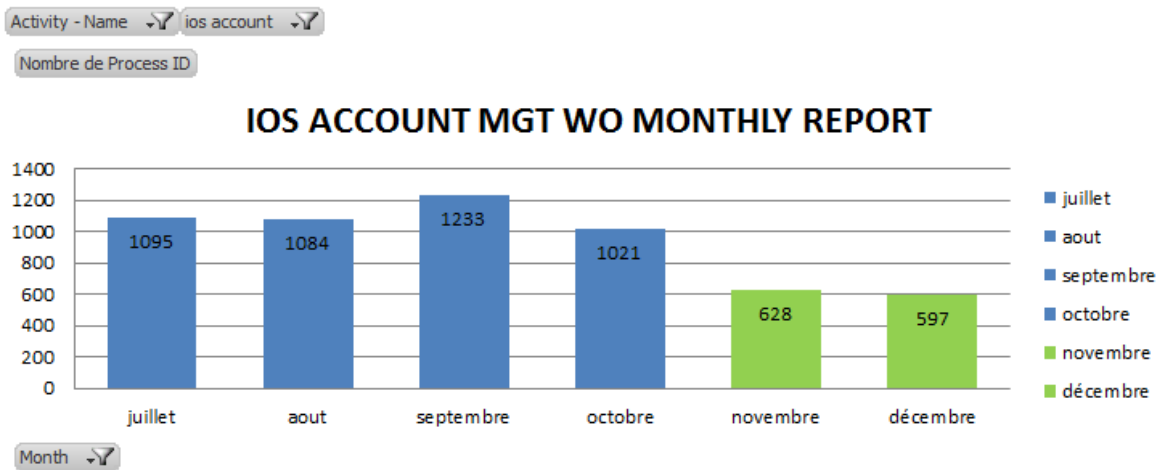


Figure 40 : Charge de l'équipe de gestion des accès

## Conclusion

Actuellement, le troisième et dernier projet est toujours en cours. Il reste à délivrer le module de création automatique pour 4 systèmes (Lims, Trackwise, VPN et Office 365). Les précédents lots ont été terminés selon le planning défini. D'après moi, un projet de gestion des identités et des accès sort du périmètre strict de l'informatique pour couvrir d'autres domaines métier. Il est donc nécessaire d'avoir, d'une part un engagement fort des parties prenantes métier, et d'autre part l'implication, la disponibilité et une parfaite coordination des experts techniques des différents domaines (annuaire, base de données, Windows, etc.).

Les difficultés auxquelles j'ai été confronté sont diverses. Cependant, deux majeures retiennent mon attention :

- La première a été ma charge de travail, je gérais en même temps le support du projet terminé et la gestion du projet qui suivait. En effet, du fait d'une réorganisation informatique, aucune ressource n'a pu être affectée au support des différents modules après mise en production. Malgré une formation à l'outil et aux processus dispensée aux supports informatique des différents sites, de nombreux tickets informatiques étaient générés et escaladés à mon niveau. Il m'a donc fallu adapter mon planning afin d'assurer un niveau de service correct, tout en ne mettant pas en danger la gestion du nouveau projet. J'ai également dû fournir aux supports informatique des sites, des guides et bonnes pratiques afin qu'ils puissent assurer un support correct de premier niveau.
- La deuxième difficulté, était la gestion du changement, inhérente à l'implémentation de ces nouveaux outils et processus. Certains sites percevaient le nouveau processus comme un transfert de tâche de l'informatique vers leurs activités quotidiennes. Il a donc fallu communiquer avec les représentants RH de certains sites sur les valeurs d'autonomie et de responsabilité, et insister sur la rapidité de délivrance des accès d'une manière globale.

Ce projet a été très enrichissant tant d'un point de vue technique que d'un point de vue humain car j'y ai pu :



- découvrir les processus RH, achat et financier et renforcer mes connaissances sur ces domaines respectifs
- élargir mon réseau au sein même d'Ipsen en travaillant en étroite collaboration avec des acteurs métiers hors IT
- élargir mes compétences techniques sur les différentes technologies abordées dans le cadre de ce projet (WebSphere, annuaire, base de données)
- gérer la conduite et le déroulement d'un projet de grande envergure pour le Groupe Ipsen et ce dans un contexte international

Afin de démontrer la valeur ajoutée d'un tel projet, Ipsen a fait l'objet d'une évaluation du Gartner (entreprise américaine de conseil et de recherche dans le domaine des techniques avancées) en juin 2013 (cf. annexe 1). Les résultats ont montré qu'Ipsen avait atteint un certain niveau de maturité sur les processus de gestion des identités et des accès. Afin d'élever ce niveau dans le cadre de l'amélioration continue du système, la prochaine étape serait une étude de définition de rôle qui optimiserait le processus de demandes d'accès en amont de la création de l'identité. Cela consisterait à définir à partir du profil métier d'un utilisateur, l'ensemble des rôles ou accès informatiques nécessaires à l'exécution de son travail. Par ce biais, on pourrait imaginer le scénario suivant : lors de la déclaration d'un nouvel arrivant par les services RH, une création automatique de ses accès se produirait par le simple fait de l'avoir intégré dans un service et un corps de métier.

## Bibliographie

### Sites web

- [1] Ipsen. Ipsen Innovation for patient care, [en ligne]. Disponible sur : <<http://www.ipsen.com> >.

### Documents Ipsen

- [2] Eprom framework, Ipsen IT project management framework, Département de la Gouvernance Informatique Ipsen, version 3
- [3] Project Quality and Validation Plan, Département Assurance Qualité, version 3

## **Table des annexes**

Annexe 1 : Evaluation du Gartner sur le niveau de maturité Ipsen.....	67
---	----

## Annexe 1 : Evaluation du Gartner sur le niveau de maturité Ipsen

### Your Results

Wednesday, June 05, 2013

## ITScore for Identity and Access Management

Your role score is 3.3 and your role maturity is Level 3: Defined

This ITScore report was created for Fabrice Briard on 05-Jun-13.

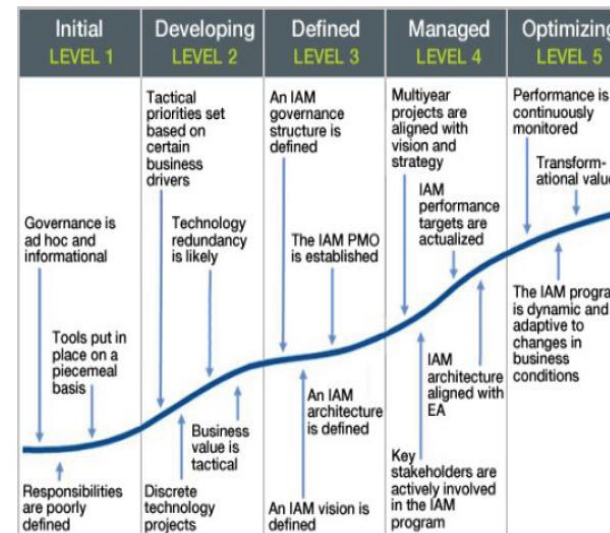
Assessment name: CIO Office

### Overview

Gartner's ITScore for Identity and Access Management (IAM) enables IAM leaders to identify shortcomings, determine priorities and establish goals for improving their organizations. This maturity model is intended to support IAM activities enterprise-wide. This assessment will help you determine your level of maturity, based on a scale from Level 1-5.

The results and recommendations from this survey are based upon your responses and common issues discovered within those responses. These results and recommendations, while tending to be accurate, will vary based upon each organization's unique conditions.

For a more accurate assessment and interpretation of your assessment maturity, contact a Gartner Analyst.



## Liste des figures

Figure 1 : Evolution des dépenses en Recherche et Développement (en millions d'euros) [1].....	9
Figure 2 : Evolution du chiffre d'affaire par zone géographique (en millions d'euros) [1] .....	10
Figure 3 : Répartition des centres de R&D, des sites industriels du Groupe dans le monde et des pays où Ipsen est présent commercialement directement [1] .....	11
Figure 4 : Evolution du Chiffre d'Affaires par domaine thérapeutique (en millions d'euros) [1]....	12
Figure 5 : Place de l'informatique dans l'organisation Ipsen.....	13
Figure 6 : Organisation de l'informatique du groupe .....	13
Figure 7 : Rôles et responsabilités des acteurs des comités projets [2].....	18
Figure 8 : Cycle de vie d'un projet EPROM avec les livrables associés [2] .....	21
Figure 9 : Méthodologie d'évaluation des offres commerciales .....	23
Figure 10 : Plan d'action de changement IAM.....	25
Figure 11 : Planning général du projet IAM.....	27
Figure 12 : Evolution du nombre d'actes de gestion d'identité .....	29
Figure 13 : Processus d'arrivée IAM.....	30
Figure 14 : Processus de mise à jour d'identité IAM.....	31
Figure 15 : Processus de départ IAM .....	32
Figure 16 : Tableau d'avancement des phases du projet d'identité .....	32
Figure 17 : Planning du projet de gestion des identités .....	33
Figure 18 : Organisation du projet de gestion des identités .....	34
Figure 19 : Liste des flux de donnée entre les différents systèmes et IAM.....	36
Figure 20 : Architecture technique du système IAM.....	38
Figure 21 : Les différents environnements du système IAM .....	39
Figure 22 : Stratégie de mise en production du module de gestion des identités .....	41
Figure 23 : Exemple de fiche applicative disponible sous CEZAM .....	43
Figure 24 : Processus de demandes d'accès sur IAM.....	44
Figure 25 : Avancement des phases du projet d'identité .....	45
Figure 26 : Le planning projet du module de gestion des accès .....	46
Figure 27 : Organisation du deuxième projet .....	47
Figure 28 : Cinématique du tutoriel vidéo de demandes d'accès (version chinoise).....	48
Figure 29 : Méthodologie de modélisation des applications sur le module Access Management....	50
Figure 30 : Résultat du sondage collaborateur sur le module de gestion des accès .....	52
Figure 31 : Nombre de demandes d'accès créées par les utilisateurs par rapport au support informatique .....	53
Figure 32 : Comparatif de création de demandes d'accès par établissement .....	53
Figure 33 : Nombre de demandes d'accès traitées par le service de gestion des accès de 2004 à 2008.....	54
Figure 34 : Processus de demandes d'accès avec mise en place du module de création automatique .....	55
Figure 35 : Liste des systèmes inclus dans le périmètre projet .....	56
Figure 36 : Liste des systèmes par lots .....	57
Figure 37 : Planning du projet de création automatique des accès .....	58
Figure 38 : Organisation du projet création automatique des accès .....	59
Figure 39 : Mode de simulation du connecteur IAM sur les systèmes cibles .....	61
Figure 40 : Charge de l'équipe de gestion des accès .....	62

## Liste des tableaux

Tableau 1 : Rôle et responsabilité des acteurs du projet [3] .....	19
Tableau 2 : Rôles et responsabilités sur les livrables projets [3] .....	27
Tableau 3 : Gain du projet de gestion des identités .....	42

## **Projet international de gestion des identités et des accès**

**Mémoire d'Ingénieur C.N.A.M., Rhône Alpe 2013**

---

### **RESUME**

L'évolution de la sécurité et des exigences réglementaires, nécessite le renforcement de la gestion des identités et des accès pour minimiser les risques de vol d'identité, d'erreurs, de fraudes et d'actes de malveillance. Dans ce but, Ipsen, groupe biopharmaceutique français de dimension mondiale, a lancé un projet de gestion des identités et des accès qui a permis de mettre en œuvre de nouveaux processus et outils répondant à ces problématiques. Ce projet inclue dans son périmètre l'ensemble des collaborateurs internes et externes et les processus suivants : arrivée, demande d'accès, cycle de vie et départ. La solution retenue par Ipsen pour couvrir l'ensemble du projet est un produit IBM appelé TIM (TIVOLI IDENTITY MANAGER).

**Mots clés : Identité, accès, processus, cycle de vie, système, sécurité, compte, autorisation.**

---

### **SUMMARY**

The evolution of safety and regulatory requirements requires the strengthening of identity access management to minimize the risks of identity theft, errors, frauds and malfeasance. To achieve this goal, Ipsen, a French biopharmaceutical group, has launched a global identity and access management project, which allows new processes and tools to be implemented and to comply with these issues. This project includes on its scope all IPSEN employees and external partners and the following processes: arrival, access request, life-cycle and departure. The solution chosen by Ipsen to cover this entire project is an IBM product called TIM (TIVOLI IDENTITY MANAGER).

**Key words: Identity, access, process, life cycle, system, security, account, authorization.**