Auditabilité des SI

Retour sur l'expérience du CH Compiègne-Noyon

8 avril 2015 – DGOS

Rodrigue ALEXANDER

Le CH Compiègne-Noyon

- Territoire de santé Oise-Est (Picardie) issu d'une fusion au 1/01/2013
- 1195 lits et places (MCO, SSR, HAD, USLD, EHPAD)
- 166M€ d'exploitation – 7,3M€ d'investissement
- 2666 professionnels

- Informatique

✓ Direction de la performance et des SI

✓ 9,8 ETP (2 ingénieurs, 5,8 TSH, 1 OPQ, 1 secrétaire)

Lien entre certification des comptes et système d'information?

COMPIÈGNE NOYON Centre Hospitalier Intercommunal

1/ Pas de lien à priori…

- ✓ Formation majoritairement comptable à l'EHESP
- ✓ Peu de références à l'informatique dans les premiers documents édités
- ✓ Actualité nationale SI: Hôpital numérique, TSN,…
- ✓ Projet piloté par les DAF avec un accent fort sur les 6 cycles
- ✓ …
- ✓ *l'instruction du 21 février 2013 relative au guide méthodologique pour l'auditabilité des systèmes d'information dans le cadre de la certification des comptes des établissements publics de santé*

2/ Le SIH, essentiel à la certification des comptes

Des objectifs ambitieux!

Lecture des exigences du guide d'auditabilité

1e analyse → objectifs irréalistes et inatteignables…

- ✓Contexte institutionnel : Réorganisation d'équipe post fusion (organisation, infrastructure,…)
- ✓Effectif limité (9.8ETP théorique – 8.8 présents)
- ✓Contexte financier (IV, Fonctionnement)
- ✓Autres projets (DPI, MSS, PCI, SID, armoires sécurisées,…)

Recours à une AMO?

Audit flash et aide à l'élaboration d'un plan d'actions

- ✓ Cabinet découvrant le milieu hospitalier…
- ✓ approche maximaliste du guide
- ✓ Influence de certains acteurs internes souhaitant voir émerger leurs projets informatiques
- ✓ Plan d'actions sans rappels des points forts et insistant sur les écarts
  - ✓ Démotivation de l'équipe SI
  - ✓ Caractère peu opérationnel → Par quoi commencer?

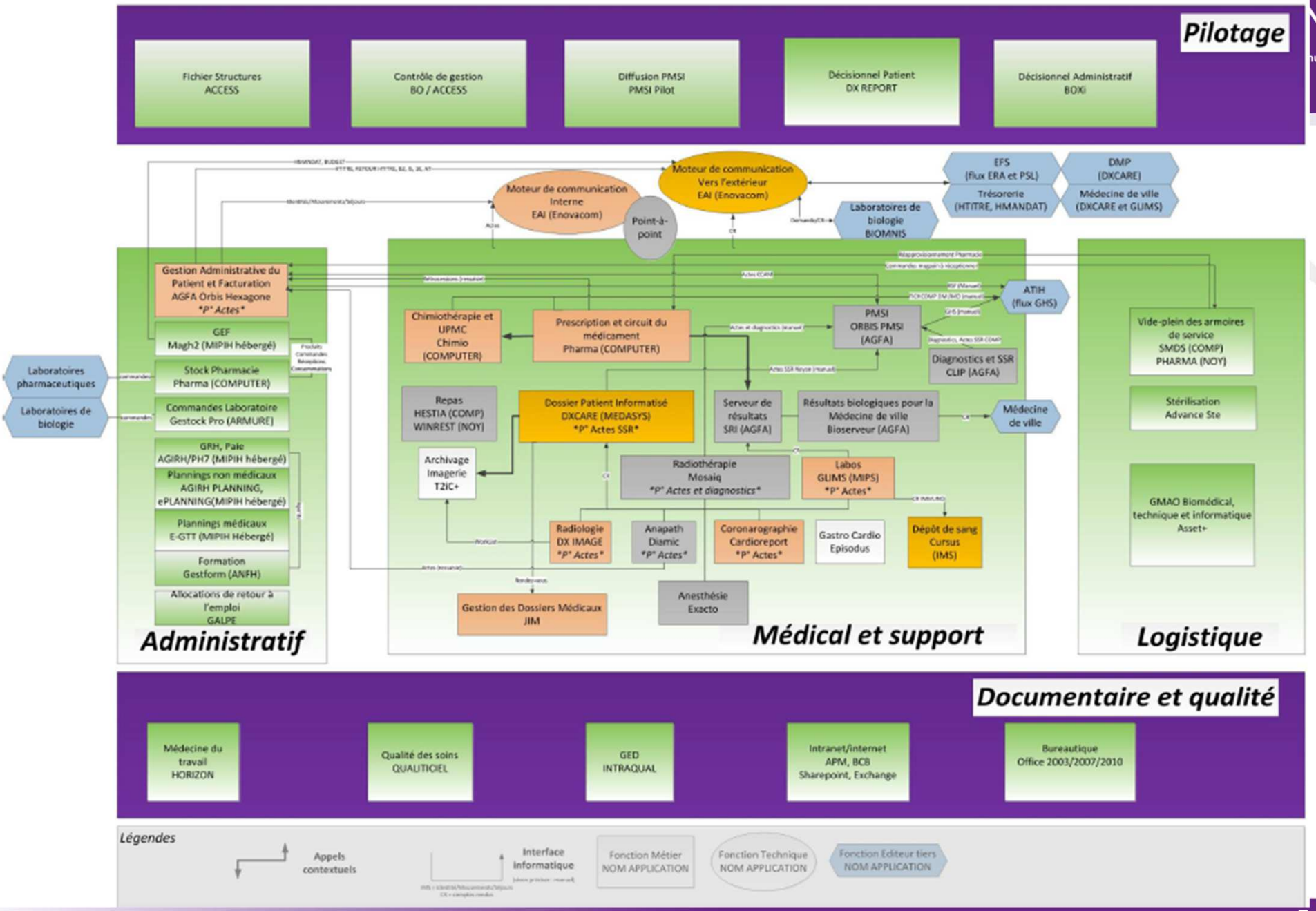
Approche finalement pragmatique

COMPIÈGNE NOYON
Centre Hospitalier Intercommunal

1/ Effort de production des éléments nécessaires à la prise de connaissance par CAC *(fiche pratique 1 – DGOS)*

- ✓ Organigramme hiérarchique et fonctionnel
- ✓ Description des principales applications et interfaces
- ✓ Cartographie applicative
- ✓ Définition d'un périmètre d'application
- ✓ Description des principaux contrats (maintenance, service,…)
- ✓ Schéma directeur SIH

➢ *Approche similaire aux démarches qualité (COBIT, ITIL,…)*


Pilotage
Fichier Structures ACCESS
Contrôle de gestion BO / ACCESS
Diffusion PMSI PMSI Pilot
Décisionnel Patient DX REPORT
Décisionnel Administratif BOXi
Moteur de communication Interne EAI (Enovacom)
Moteur de communication Vers l'extérieur EAI (Enovacom)
Point-à-point
EFS (flux ERA et PSL)
DMP (DXCARE)
Trésorerie (HTITRE, HMANDAT)
Médecine de ville (DXCARE et GLIMS)
Laboratoires de biologie BIOMNIS
Laboratoires pharmaceutiques
Laboratoires de biologie
Gestion Administrative du Patient et Facturation AGFA Orbis Hexagone *P* Actes*
GEF Magh2 (MIPIH hébergé)
Stock Pharmacie Pharma (COMPUTER)
Commandes Laboratoire Gestock Pro (ARMURE)
GRH, Paie AGIRH/PH7 (MIPIH hébergé)
Plannings non médicaux AGIRH PLANNING, ePLANNING(MIPIH hébergé)
Plannings médicaux E-GTT (MIPIH Hébergé)
Formation Gestform (ANFH)
Allocations de retour à l'emploi GALPE
Administratif
Chimiothérapie et UPMC Chimio (COMPUTER)
Prescription et circuit du médicament Pharma (COMPUTER)
PMSI ORBIS PMSI (AGFA)
ATIH (flux GHS)
Diagnostics et SSR CLIP (AGFA)
Repas HESTIA (COMP) WINREST (NOY)
Dossier Patient Informatisé DXCARE (MEDASYS) *P* Actes SSR*
Serveur de résultats SRI (AGFA)
Résultats biologiques pour la Médecine de ville Bioserveur (AGFA)
Médecine de ville
Archivage Imagerie T2IC+
Radiothérapie Mosaiq *P* Actes et diagnostics*
Labos GLIMS (MIPS) *P* Actes*
Radiologie DX IMAGE *P* Actes*
Anapath Diamic *P* Actes*
Coronarographie Cardioreport *P* Actes*
Gastro Cardio Episodus
Dépôt de sang Cursus (IMS)
Gestion des Dossiers Médicaux JIM
Anesthésie Exacto
Médical et support
Vide-plein des armoires de service SMDS (COMP) PHARMA (NOY)
Stérilisation Advance Ste
GMAO Biomédical, technique et informatique Asset+
Logistique
Documentaire et qualité
Médecine du travail HORIZON
Qualité des soins QUALITOIEL
GED INTRAQUAL
Intranet/internet APM, BCB Sharepoint, Exchange
Bureautique Office 2003/2007/2010
Légendes
Appels contextuels
Interface informatique
Fonction Métier NOM APPLICATION
Fonction Technique NOM APPLICATION
Fonction Editeur tiers NOM APPLICATION

2/ Création d'une grille d'analyse sous Excel à partir des attendus des fiches pratiques

- Recensement de l'existant
- Lien vers les procédures internes
- Commentaires
- Appréciation sur l'état d'avancement

Indicateur Auditabilité	Lien documentaire	Etat d'avancement	Commentaire
FICHE 1 : PRESENTATION DU SYSTEME D'INFORMATION			
- Cartographie applicative :	Cliquer ICI	100%	
o Préciser les applications liées au périmètre			
o préciser les interfaces sur la cartographie			
- Schéma directeur (projet d'établissement + PPI)	Cliquer ICI	100%	
o Projet d'établissement			
o Portefeuille Projets			
- Organigramme DSI	GED N2-1150-V1	100%	
- Revue des applications (catalogue de service ITIL)	Cliquer ICI	100%	
- Effectifs internes et externes DSI			
o Données CABESTAN	Cliquer ICI	100%	
- Contrats/Mutualisation (pharmacie, laboratoire, imagerie, DAG/DDP, Dsoins, DAF, DAETB, DRH, IFSI, Crépy-en-Valois)	Cliquer ICI	50%	
FICHE 2 : MECANISMES D'IDENTIFICATION			

31% d'atteinte de la cible

3/ Rapprochement de l'auditabilité et de la stratégie du CHCN

- Attente des utilisateurs
  - ✓ Ne pas saisir son identifiant
  - ✓ Ne plus se loguer plusieurs fois
  - ✓ Disposer d'un compte actifs sans recours à la DSI pour les contractuels, stagiaires,…
  - ✓ Optimiser les recettes
- Autres exigences nationales
  - ✓ Exigences CNIL → Pilote projet MSSanté (août2014)
  - ✓ HN (prérequis) → dépôt d'un dossier de financement pour le SID (août 2014)
  - ✓ Certification HAS V2014 (Références E1, E2 et E3) → Visite sur site des experts visiteurs (janvier 2015)

4/ Capitaliser sur les points forts

- ✓ Sécurité des applicatifs en lien avec le soins (DPI avec identifiant personnel, gestion de profil, procédures dégradées,…)
- ✓ infrastructure géo clustérisée,
- ✓ référentiels uniques (patients, séjours-mouvements, structure)
- ✓ documentation de la revue des traitements d'exploitation sur Sharepoint
- ✓ sécurisation de l'accès physique aux locaux techniques (badge ou clé)

5/ Recherche de « quick wins »

- ✓ Utilisation de la « boite à outil » HN : Procédure CIV, Procédure gestion du FICOM, Amélioration du plan de reprise d'activité (PRA), Charte d'accès et d'usage,…
- ✓ Extraction de la liste des comptes (génériques, administrateurs)
- ✓ Revue des accès physiques aux locaux techniques

Atteintes des cibles Mode projet

I. Accès aux programmes et aux données → Sécurité (9 fiches)

Fait	A développer
• **RSSI nommé au sein de la DSI** ✓ fiche de poste, objectifs dans l'évaluation annuelle, ✓ formations gratuites (ANSI et éditeurs) ✓ Autoévaluation (politique de l'Etat) ✓ Test PRA • **Procédure « nouvel arrivant »** • **Création d'un Comité sécurité**	• Généralisation des **comptes Windows nominatifs** • **IAM** pour un meilleur contrôle des entrées-sorties • **Authentification par carte CPS** • **SSO** pour réelle contrainte des mots de passe *« Utiliser une carte CPS ou des mots de passe, conservés confidentiellement, composés de chiffres et de lettres, d'une longueur de 8 caractères au moins… et changés à la première connexion et au moins tous les 6 mois »*

II. Gestion des changements

Fait	A développer
• **Base de test** pour le SIL • Traçabilité des demandes via une **GMAO** (Asset +)	• **Traçabilité des tests de recette** • **Visibilité les applicatifs hébergés** • **Clarifier le circuit de décision** (comité de gestion!) • **Test de conformité au CCTP** • Procédure pour les changements en urgence

III. Gestion des acquisitions et des migrations

Fait	A développer
• **Formation institutionnelle sur la gestion de projet (3j)** • **Cadrage des projets via** la « **fiche opportunité ANAP »**	• **Traçabilité de la conduite de projet** (CR réunions, document de spécification, jeux d'essais,…)

IV. Gestion de l'exploitation → démarche qualité

Fait	A développer
• **Optimisation du classement documentaire** (TRAPEC) • Sensibilisation à la **démarche qualité ITIL** • Restructuration du service vers la **spécialisation** • **Contractualisation** avec nos clients internes	• Procédures de **contrôle des interfaces** • Procédure de **contrôle des référentiels** → non correspondance des référentiels CCAM de deux bases! • **Indicateurs de pilotage** (satisfaction des utilisateurs, temps de traitement des tickets,…) • PRA financier, procédures dégradées,….

V. Séparation des tâches

Fait	A développer
• Procédure de gestion des droits et **matrice de séparation des tâches** (GEF) • Identification de **référents fonctionnels**	• A poursuivre pour les autres applications (GAM, GRH, PMSI particulièrement)

Difficultés rencontrées

1. **Isolement de la DSI…**
2. **Périmètre de l'auditabilité ?** (fichiers Excel)
3. **Temps agents**
4. **Coût** des projets → Financement 111k€ de l'ARS Picardie
5. **Mobilisation des référents fonctionnels**
   - ✓ Matrice de séparation des tâches
   - ✓ Profils des applications
   - ✓ Gestion des pré-production (test et recette fonctionnelle)
   - ✓ Contrôle des interfaces

Facteurs de réussite

1. **Valoriser les équipes**

   Points forts, dépôt d'un dossier HN pour s'en servir en communication interne

2. **Mode projet avec implication du DG**

   COPIL, macroplanning, chiffrage en € et en temps-homme …

3. **Utiliser les outils nationaux**

   Boîte à outil HN, fiches pratiques auditabilité, Publications ANAP,…)

4. **Prioriser en ciblant des gains rapides**

5. **Responsabiliser les éditeurs via les CCTP**

6. **Répertoire informatique partagé par les référents**

   ✓ Procédures, logigrammes, règles et méthodes comptables, présentations en COPIL,

Propositions

- **Création d'une boîte à outil DGOS**
  - apports des établissements de la vague 1 dont la documentation a été approuvée par des CAC
- **Lobbying de la DGOS auprès des éditeurs**
  - Certification/accréditation/labellisation à l'instar des LAP
  - Profils types par applicatif
  - Visibilité sur l'infogérance (PRA? Recette fonctionnelle avant mise en production? Taux de disponibilité? Gestion des incidents?)
- **Identifier un RSSI auprès des MOA régionales**

En conclusion

- **Auditabilité à mener dans l'intérêt du CH**

  « bonnes pratiques attendues quant à l'organisation, le fonctionnement et le contrôle du SI »

- A inscrire dans une logique plus générale de **démarche qualité** si:

  ✓ Ressources (effectifs, moyens financiers)

  ✓ Analyse d'une trajectoire par le CAC

- **Traçabilité des opérations et contrôles réalisés**

  Les contrôles non-documentés sont réputés non réalisés!

- **Merci de votre attention**