SÉGUR DU NUMÉRIQUE EN SANTÉ en Normandie

Accompagnement en Cybersécurité

Septembre 2025

https://www.esegur-normandie/

SOMMAIRE

Financé par l'Union européenne
NextGenerationEU

Rappels

Micros coupés pendant le temps des interventions

Temps de questions / réponses à la fin

Questions à poser en levant la main (chat bloqué)

Session enregistrée

Ouverture du Comité Régional

Omar CHIBANE

Coordonnateur Collectif SI Normandie &
Référent régional Cyber ESMS

Ouverture du Comité Régional

Jenna DUFRENE

Responsable qualité et projets
Association LA RONCE

Ouverture du Comité Régional

Fabian RICHARD

Responsable e-Santé & Transformation Numérique
Référent régional Cyberdéfense du système de santé
Direction de l'Attractivité des Métiers et de la
Transformation Numérique du système de santé

La Cybersécurité en Normandie

Le Centre Régional de Ressources en Cybersécurité

Centre Régional de Ressources en Cybersécurité (CRRC)

Appui et accompagnement

Sécur'NeS est le Centre de Ressources Régional en Cybersécurité (CRRC) à destination des acteurs du sanitaire, médico-social et social.

Sécur'NeS est opéré par le GRADeS Normand'e-Santé et financé par l'ARS Normandie. Cette plateforme vise à accompagner les établissements au programme CaRE ainsi qu'à renforcer la sécurité des systèmes d'information en mettant à disposition des ressources et des outils en cybersécurité.

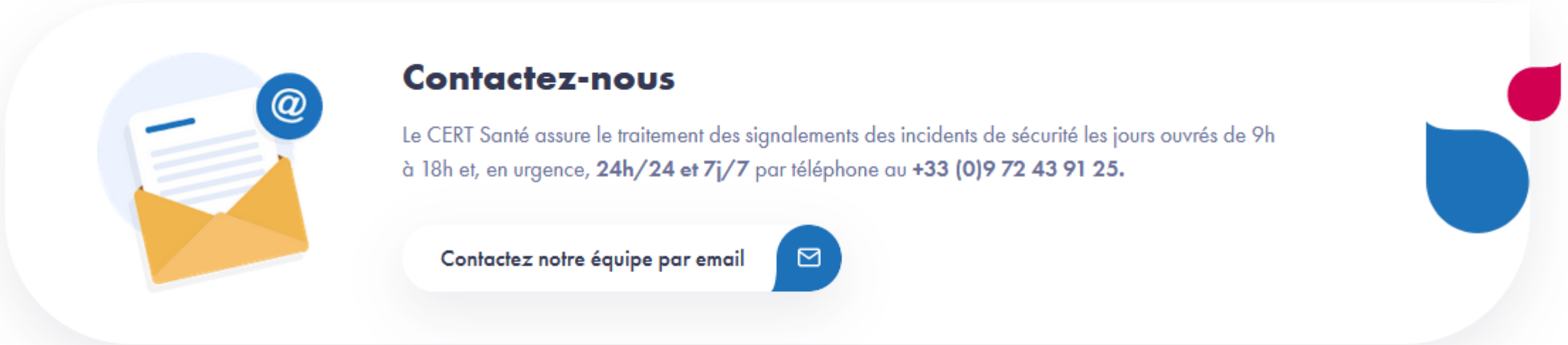
Et puis spécifiquement de :

- La **sensibilisation** au risque cyber ;
- **Accompagnement** aux respects de la réglementation ;
- **L'entraînement et l'organisation** aux incidents de cybersécurité (exercices de crise) ;
- L'accompagnement dans les programmes nationaux dédiés.

Réaction en cas d'incident cyber

Service d'appui à la gestion des cybermenaces 24h/24 et 7j/7

En premier lieu sur un incident => CERT-Santé : https://www.cyberveille-sante.gouv.fr/



Notifier une violation de données personnelles

La notification doit être transmise à la **CNIL dans les meilleurs délais (72h)** à la suite de la constatation d'une violation présentant un risque pour les droits et libertés des personnes.

https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles

Les moyens disponibles

CARE

- Entrée des ESMS dans Domaine 2 (PCRA)

Portail ANS

- Kits Exercices cyber
- Kits PCRA
- Documentation

CERT-Santé

- Réponse à incident
- Documentation
- Audits
- Alerting

ARS

- Veille et alerte
- Relai informationnel
- Appui à la crise
- Conseil et accompagnement

Centre Régional de Ressources Cybersécurité (CRRC)

- Plateforme régionale de sensibilisation
- Escape Game
- Jeu de gestion de crise
- Base documentaire
- Accompagnement aux exercices cyber (en développement)
- Appui au diagnostic cyber (en développement)
- Parcours de cybersécurité (en développement)

Partenaires régionaux

Centre Régional de Ressources en Cybersécurité (CRRC)

Appui et accompagnement

Un parcours Cyber ESMS en 5 étapes

Le **CRRC** propose un parcours structuré en **5 étapes** pour aider les **Établissements Sociaux et Médico-Sociaux (ESMS)** à renforcer leur cybersécurité.

Auto-Diagnostic Cyber

Première évaluation pour identifier les points forts et les vulnérabilités

Convention

Engagement des parties prenantes et définition du cadre d'accompagnement

Diagnostic de maturité

(3 niveaux)

Analyse approfondie pour situer l'établissement sur une échelle de maturité

Plan d'action personnalisé

Élaboration de mesures adaptées aux besoins spécifiques de l'établissement

Suivi

Accompagnement dans la mise en œuvre des actions et ajustements selon l'évolution des risques.

Structuration du SI

Association La Ronce

Présentation de La Ronce

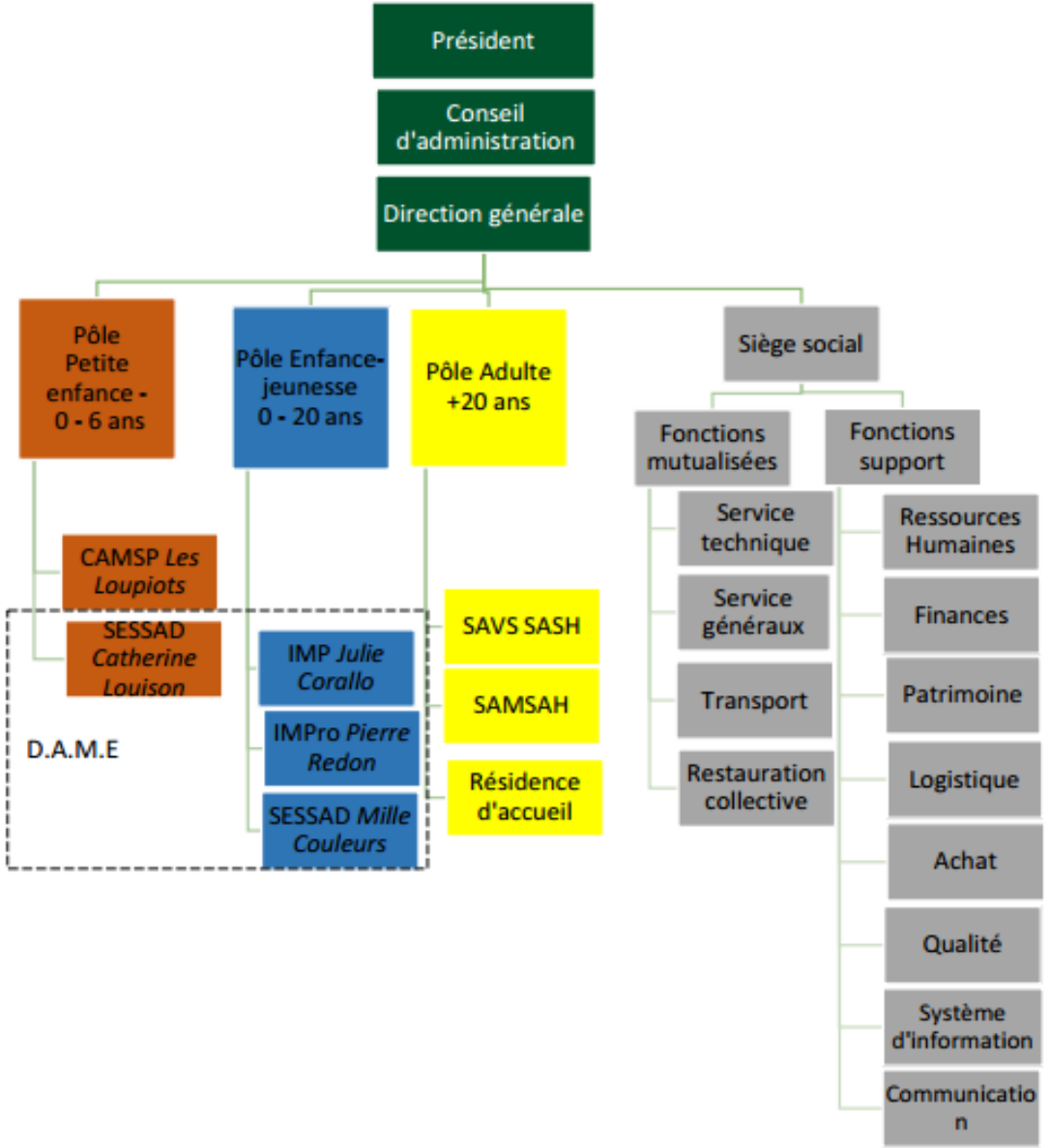
Qui est La Ronce ?

Structure médico-sociale

L'association est, dans une organisation classique, articulée autour d'une Assemblée générale, d'un Conseil d'administration et d'un Bureau.

- 160 salariés au sein de 8 établissements et services.

- Le budget global avoisine 11 millions d'euros, financés par l'ARS de Normandie et le Conseil Départemental de l'Eure et la Direction Départementale de l'Emploi, du Travail et des Solidarités (DDETS) de l'Eure.



Structuration du SI

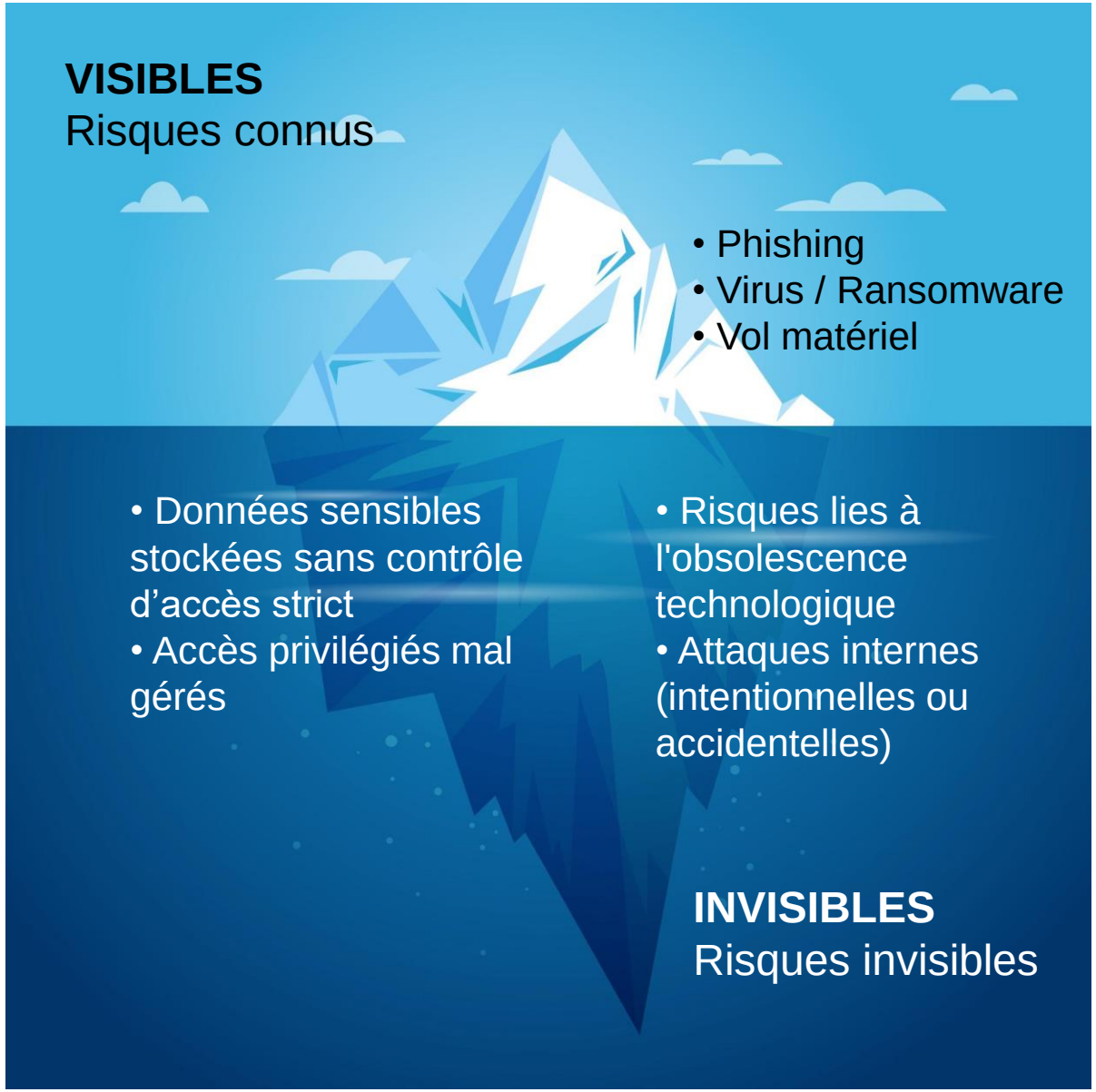
Stéphane LASNIER (Directeur Général),
Maxime GAUTHIER (DSI – Externalisé)
Cyril LAMY, Achat Logistique SI (Association LA RONCE)
Nino MARTEL, Administrateur Systèmes et Réseaux (Association LA RONCE)
Jenna DUFRENE, Responsable qualité et projets (Association LA RONCE)

La Ronce
Faire association

Structuration du SI

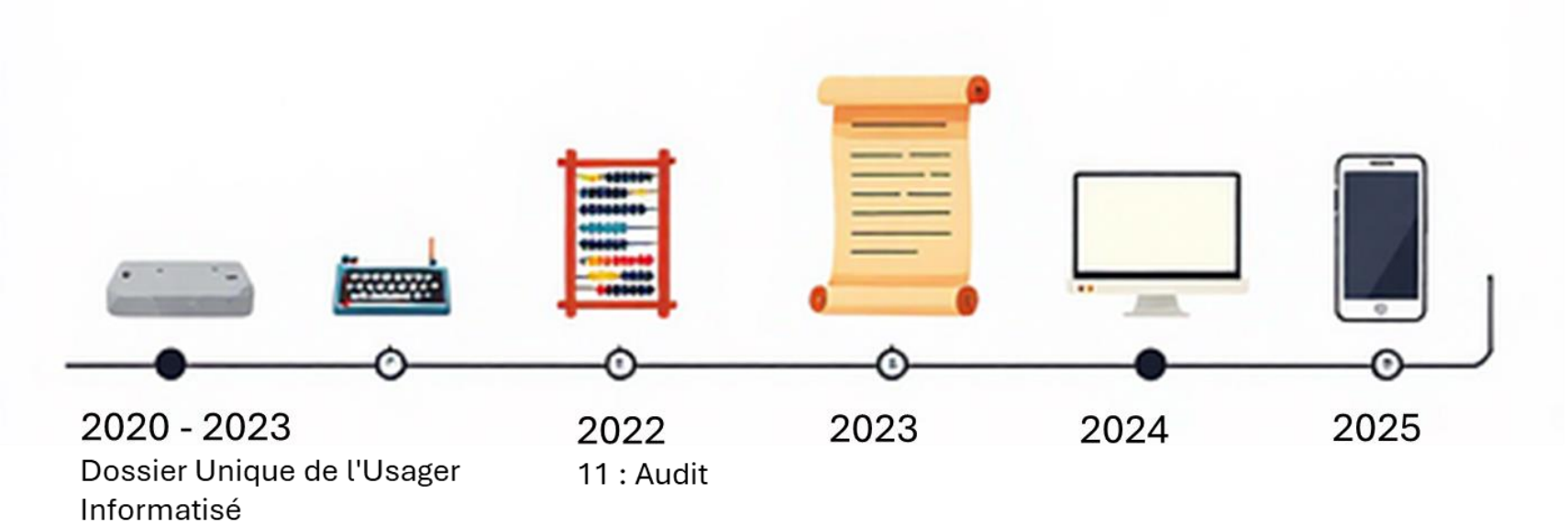
Introduction

- Diagnostic
- Projet d'orientation stratégique 2023-2026 sécuriser le SI (feuille de route SI, DSI temps partagé, solution CEGI…)
- Projet de rapprochement LRS



La Ronce....avant

- L'informatique
- L'artisanat
- L'état des lieux

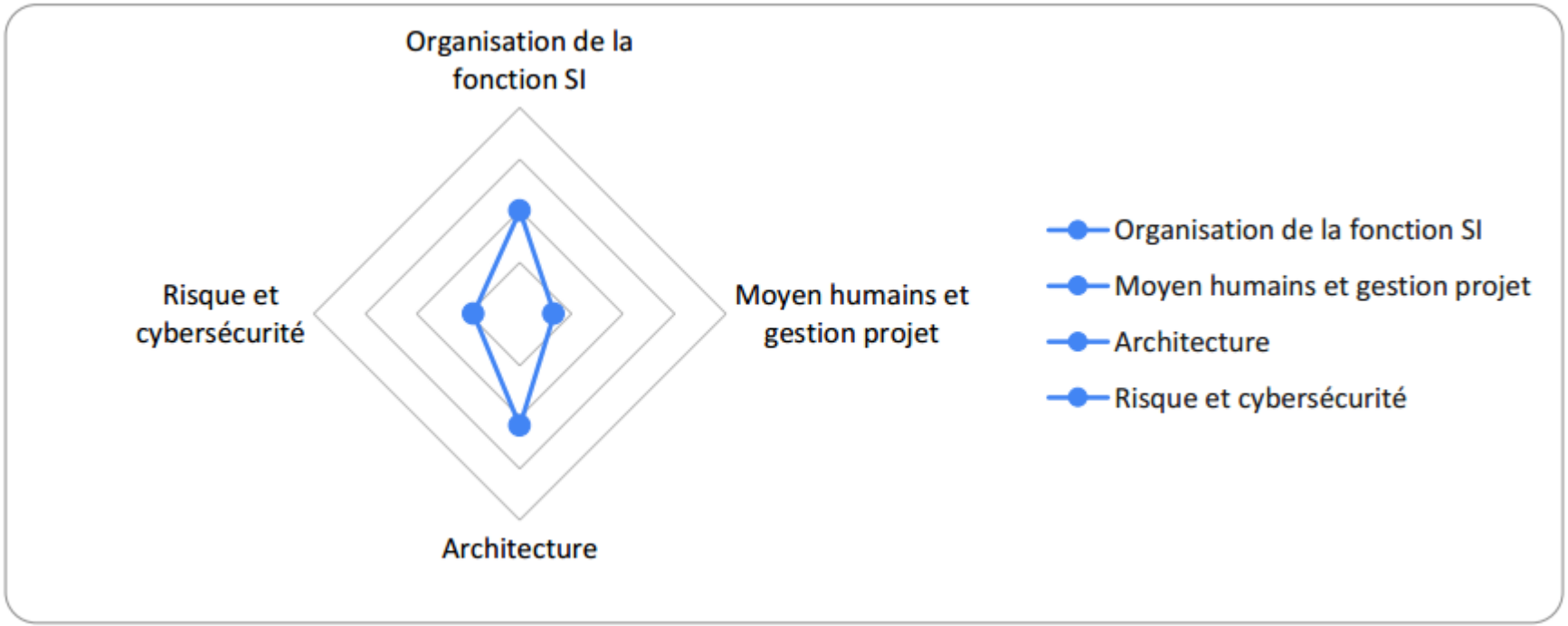


Structuration du SI

Etape 1 : Audit

Ratio du budget SI par rapport au budget global 1,43% (consensus 2%)

SI en grande fragilité



Source : Audit Ressourcial

Les 7 objectifs de la stratégie d'information

1

Organisation et stratégie
Élaborer une feuille de route SI permettant d'établir une fiche CPOM sur le numérique

2

Infrastructure
Poursuivre l'urbanisation de vos serveurs

3

Ressources humaines
Renforcer les compétences internes & expertise DSI

4

Espace de travail Numérique
DUI
Travail en mode projet

5

Protection des données
DPO – pratiques RGPD

6

Sécurité
Définir PCA PRA incluant les évolutions du système de sauvegarde

7

Communication et formation
Numérique aux bénéfices des usagers

Etape 2 : Mise en œuvre : 5 axes opérationnels – Pratique de management du SI

Axe 1 : Pratique de management du SI

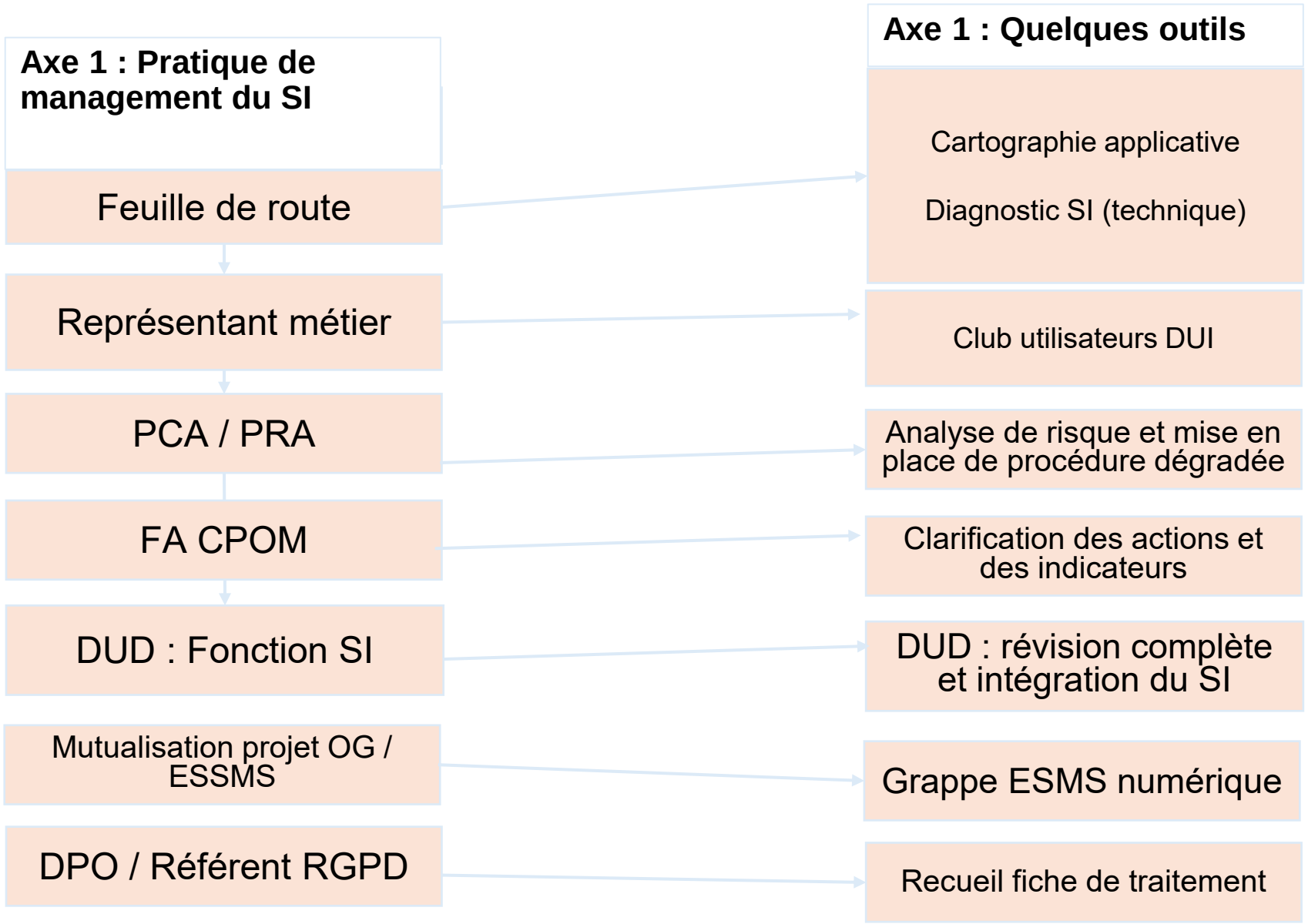
Axe 2 : Adéquation fonctionnelle

Axe 3 : Qualité de service

Axe 4 : Sécurité des SI

Axe 5 : Performance, usage et satisfaction

Etape 2 : Mise en œuvre : 5 axes opérationnels – Pratique de management du SI



Etape 2 : Mise en œuvre : 5 axes opérationnels – Pratique de management du SI

Zoom sur certains documents

Feuille de route

PCA / PRA

Plan n°	PCRA – Gestion des médicaments
Elaboré par : Maxime GAUTHIER et Jenna DUFRENE	Date mise à jour : 24/04/2025

Situations possibles :
Indisponibilité du système d'information de plus de **1 heure** impactant le processus de gestion du flux des médicaments (commande, suivi des stocks, traçabilité, dispensation)

Enjeux et impacts de l'événement
En cas de coupure réseau, internet, attaque cyber malveillante, électrique ou tout autre indisponibilité informatique ayant comme impact l'indisponibilité du dossier usager informatisé (DUI).

- *Impacts :*
1. *Usager : non dispensation ou erreur de distribution des médicaments*
2. *Opérationnel : retard dans les commandes, déplacements à prévoir*
3. *Juridique / médiatique / financier : procédure judiciaire, préjudice financier et* couverture médiatique négative

Actions en prévention
1.Assurer la haute disponibilité du logiciel du dossier usager informatisé : *VIVALITY est hébergé sur un seul serveur au siège* (contrat à l'étude pour le faire héberger dans un DATA CENTER certifié HDS).
2. Réaliser des sauvegardes journalières du DUI : sauvegarde réalisée sur un disque dur externalisé
3. Protection cyber du système d'information (anti-virus, anti-spam)
4. Tenir un dossier de liaison d'urgence à jour : pour chaque personne accompagnée un dossier papier est tenu à jour (rangé dans l'armoire sécurisée de la salle de soin – mise à jour à chaque évolution, contrôle mensuel)
5. Tenir un classeur des prescriptions en cours

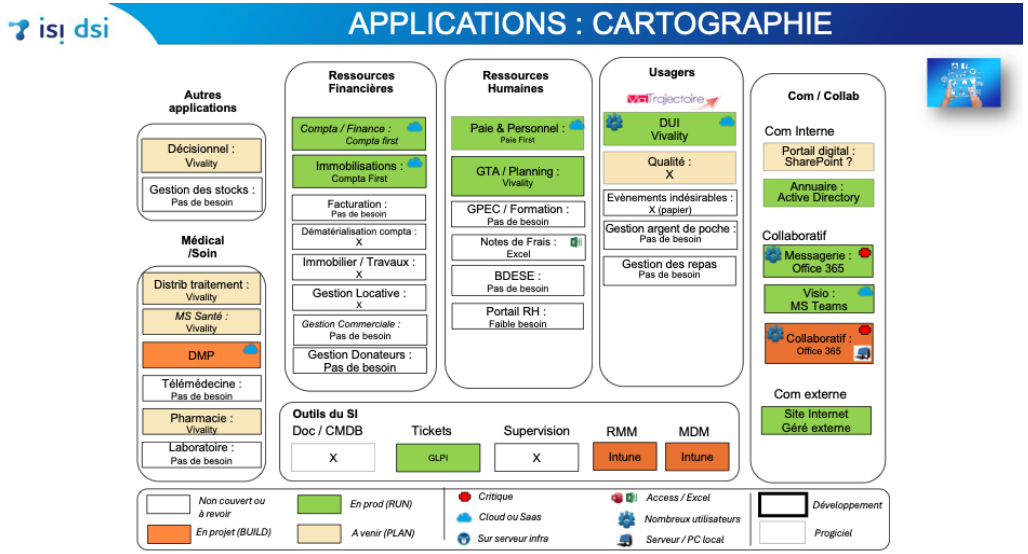
Action à réaliser en cas de crise

Pour le service soin :
Utiliser les classeurs et les dossiers papiers
Contacter la pharmacie
Réaliser les pluiliers
Assurer la distribution, la dispensation et la tracer sur une feuille libre
Réaliser les comptes rendus sur papier libre (dans l'attente de l'opérationnalité du logiciel)

Pour la direction générale
Prévenir les directions d'établissement et les instances de représentation (CSE)
Prévenir ou non les autorités (URSSAF, impôts, etc.) du retard des déclarations obligatoires.
Déclencher la procédure EI EIG EIGS

Pour la DSI :
Restauration du DUI à J-1

En cas de cyber attaque :



Activités du processus métier											
Objectif :	Faire l'inventaire des activités principales qui font le quotidien du processus métier. Puis, au regard du seuil de criticité défini pour chaque typologie d'impact, évaluer si l'arrêt de cette activité est critique selon les temporalités. Cela est le point de départ qui permet de définir le périmètre à traiter dans le PCRA.										
Activités	Echelle de mesure de criticité de l'arrêt de l'activité					Impacts					
	1h	3h	24h	3 jours	2 semaines	Personnel	Usager	Opérationnel	Juridique	Médiatique	
Suivi des usagers dans leurs besoins médicaux (bobologie)	Non critique	Non critique	Non critique	Critique	Critique		x	x			
Programmation et consultation médicale	Non critique	Non critique	Non critique	Non critique	Critique		x	x			
Accompagnement dans les rdv exterieur	Non critique	Non critique	Non critique	Non critique	Non critique		x	x			
Bilan médicaux avec les médecins	Non critique	Non critique	Non critique	Non critique	Critique		x	x			
Suivi des documents et des ordonnances / Relance parents / Reccueil des données médical / Ordonnances si médecin extérieur	Critique	Critique	Critique	Critique	Critique						
Gestion du flux de médicament (commande pharmacie, tracabilité des médicaments, suivi des stocks armoire à pharmacie)	Critique	Critique	Critique	Critique	Critique						
Echange et communication avec les autres corps de métier de l'association et parents / famille / autre prise en charge externe	Non critique	Non critique	Non critique	Critique	Critique						
Suivi du Dossier de Liaison d'Urgence	Critique	Critique	Critique	Critique	Critique						
Animation d'atelier avec les usagers	Non critique	Non critique	Non critique	Non critique	Non critique						

Etape 2 : Mise en œuvre : 5 axes opérationnels

Axe 2 : Adéquation fonctionnelle

Nouvelles fonctions DUI

Services socles

Mise à niveau du SI RH

Demain ?

Axe 3 : Qualité de service

Niveaux de service (SLA) - Organiser les services SI en conséquence

Etape 2 : Mise en œuvre : 5 axes opérationnels

Axe 4 : Sécurité des SI	Axe 4 : Quelques outils
Charte SI et mener des actions de sensibilisation et de formation régulières	Accompagnement Cybersécurité Securnes
Comptes génériques d'accès au SI et politique de gestion de l'annuaire et des authentifications	Référentiel unique, mise en place d'une politique d'authentification (mot de passe, double authentification, …)
Habilitations et registre d'accès	Process « RH » Onboarding/Offboarding
Mises à jour des systèmes et des logiciels antiviraux	Choix d'un MDM/RMM afin de gérer les mises à jour des postes de travail
Séparation des comptes systèmes (y compris administration) et les comptes utilisateurs	Charte SI « administrateur » et généralisation de compte spécifique aux tâches d'administration
Authentification individuelle systématique	Cf : Process « RH » Onboarding/Offboarding
Identification conforme au référentiel d'identitovigilance	INS usagers et gestion des non-conformités

Demain ?

Axe 5 : Performance, usage et satisfaction

- Evaluation annuelle de la satisfaction des prestations informatiques
- Analyses sur le taux d'usage des sous-fonctions du DUI
- Actions pour accompagner les utilisateurs dans les usages numériques
- Bilans de compétence SI/Numérique à destination des utilisateurs
- Appels à projet Innovation Numérique/SI

La Ronce
Faire association

Difficultés rencontrées

Financière : Contrainte budgétaire

Budget alloué – Coûts

Transformation numérique – accompagnement au changement

« Ce n'est pas mon métier d'être derrière un ordinateur »

« Je passe plus de temps que si je faisais en papier »

Humaines : Disponibilité des professionnels – contrainte opérationnelle

Exemple : Sécurisation des espaces documentaire

Managérial : Effet pelote de laine -> Un projet en entraine un autre. Il faut finir le projet C pour commencer le projet A …

Exemple : sécurisation du circuit du médicament

Et demain…

- L'hébergement de nos applicatifs métiers (RH-Compta-DUI) par un fournisseur certifié HDS
- Outils collaboratifs
- En fil rouge : Cybersécurité -> Communication/Sensibilisation
- Rapprochement LRS -> Structuration de l’équipe SI

Reprise des ateliers à 14h

La Cybersécurité en Normandie

Clôture et prochaines étapes

Clôture du comité régional

Stéphane LASNIER

Directeur
Association LA RONCE

Merci de votre attention

contact@securnes.fr

www.securnes.fr