TOUS CYBER VIGILANTS

JOURNÉE DE LA CYBERSÉCURITÉ

07 Avril 2026

sesan ÎLE-DE-FRANCE
Groupement d'Intérêt Public eSanté

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ars Agence Régionale de Santé Île-de-France

Conférence Institutionnelle **Établissements de santé**

Silvère RUELLAN
Chef du bureau cybersécurité santé et affaires sociales - ANSSI

Estelle NICAUD
Responsable de missions – ANS

Patrice BIGEARD
FSSI du Ministère de la Santé

Christian LEMAIRE
Chef de projet sénior numérique et cybersécurité Référent Programme Care – ARS IDF

sesan ILE-DE-FRANCE
Groupement d'Intérêt Public eSanté

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

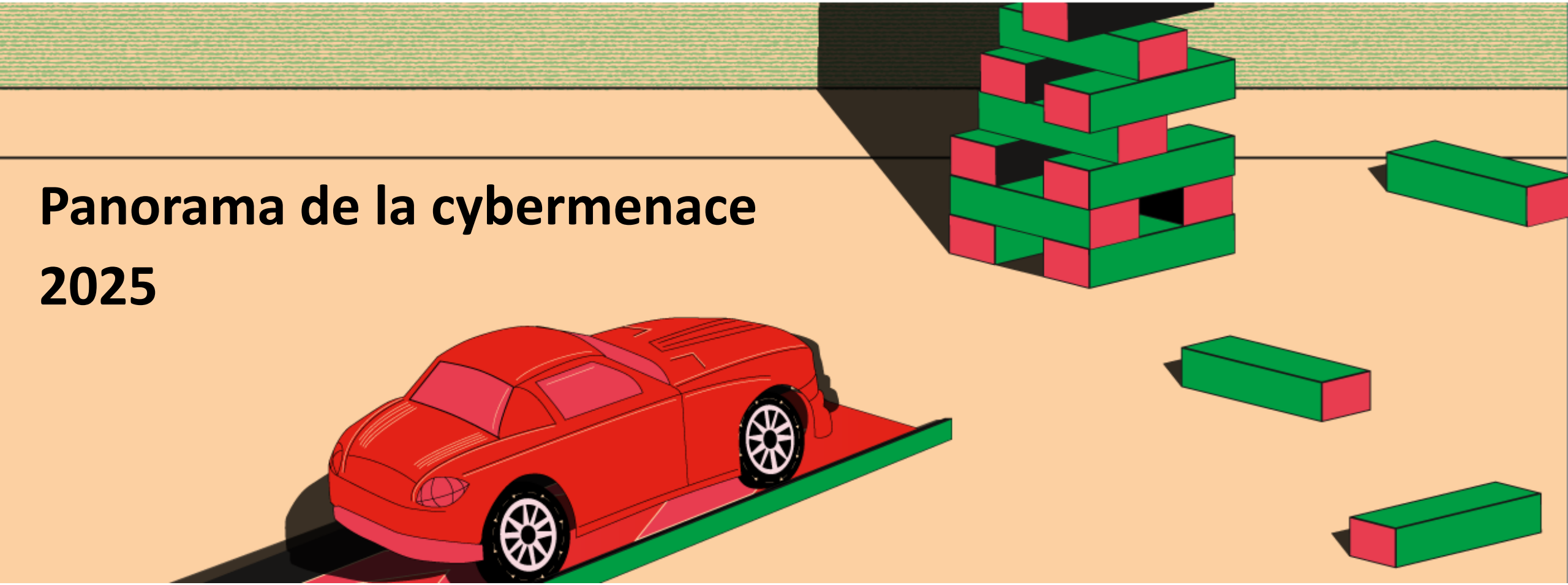
ars Agence Régionale de Santé Île-de-France

Conférence Institutionnelle
Établissements de santé

Silvère RUELLAN
Chef du bureau cybersécurité santé et affaires sociales - ANSSI

sesan Groupement d'Intérêt Public eSanté
RÉPUBLIQUE FRANÇAISE Liberté Égalité Fraternité
ars Agence Régionale de Santé Île-de-France

https://www.cert.ssi.gouv.fr/uploads/CERTFR-2026-CTI-002.pdf



Pour une résilience cyber de premier rang

PILIER 1 | FAIRE DE LA FRANCE LE PLUS GRAND VIVIER DE TALENTS CYBER D'EUROPE

PILIER 2 | RENFORCER LA RESILIENCE CYBER DE LA NATION

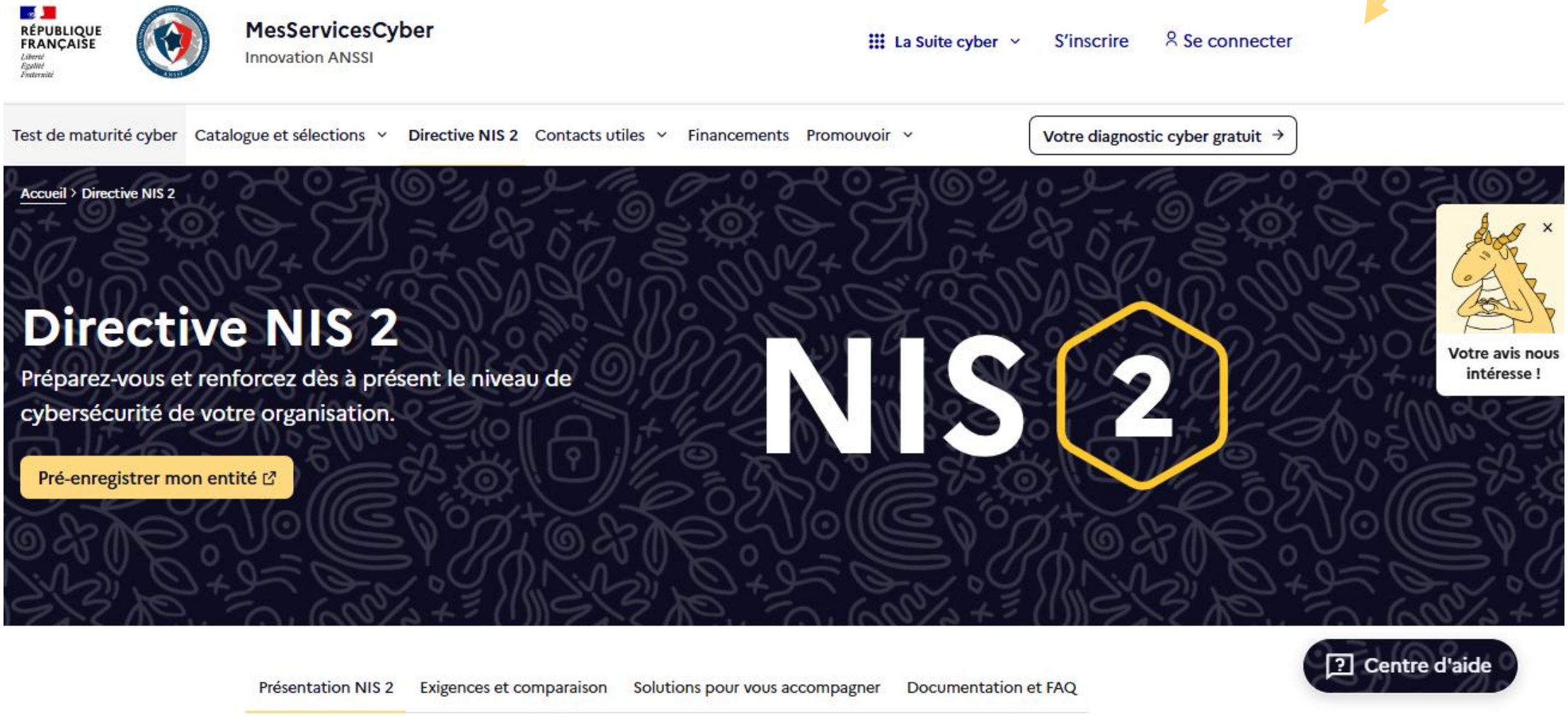
PILIER 3 | ENTRAVER L'EXPANSION DE LA CYBERMENACE

PILIER 4 | GARDER LA MAITRISE DE LA SECURITE DE NOS FONDEMENTS NUMERIQUES

PILIER 5 | SOUTENIR LA SECURITE ET LA STABILITE DU CYBERESPACE EN EUROPE ET A L'INTERNATIONAL

https://www.sgdsn.gouv.fr/publications/strategie-nationale-de-cybersecurite-2026-2030

www.messervices.cyber.gouv.fr/nis2



Conférence Institutionnelle
Établissements de santé

Patrice BIGEARD
FSSI du Ministère de la Santé

sesan
Groupement d'Intérêt Public eSanté
RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité
ars Agence Régionale de Santé Île-de-France

Conférence Institutionnelle
Établissements de santé

Estelle NICAUD
Responsable de missions – ANS

sesan Groupement d'Intérêt Public eSanté
RÉPUBLIQUE FRANÇAISE Liberté Égalité Fraternité
ars Agence Régionale de Santé Île-de-France

Le plan d'action CaRE

Une réponse collective, déterminée et coordonnée pour faire face à la menace

Les 4 axes du plan d'action CaRE :

01 **Gouvernance et résilience**

Structurer la gouvernance de la cybersécurité dans le secteur de la santé en impliquant les niveaux nationaux, régionaux et locaux.

02 **Ressources et mutualisation**

Prise en compte de la pénurie de talents et de ressources dans les établissements, et mise en avant du besoin de mutualiser et de pérenniser les ressources humaines.

03 **Sensibilisation**

Encourager un engagement fort de chacune des parties prenantes de la cybersécurité dans les établissements de santé.

04 **Sécurité Opérationnelle**

Soutenir financièrement les investissements jugés prioritaires via des « Domaines » (via des appels à financements et/ou appels à projets).

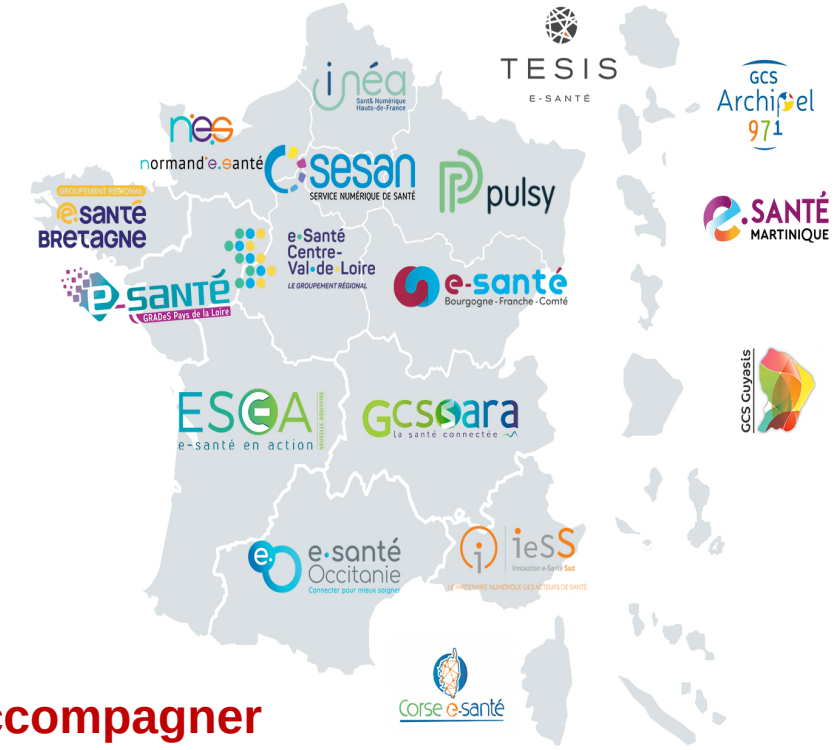
Mise à disposition du plan d'action

Cybersécurité accélération et Résilience des Etablissements (CaRE)

Rôle des CRRC

Les CRRC (Centres Régionaux de Ressources Cyber) proposent des services mutualisés et personnalisables, pour mieux prévenir et gérer la cybersécurité des établissements de santé

- **Aider les structures sanitaires et médico-sociales à renforcer leur cybersécurité**
- **Concevoir des services pour prévenir et réagir aux cyberattaques**
- **Proposer des formations et sensibiliser aux bonnes pratiques en cybersécurité**
- **Mobiliser les capacités de soutien nécessaires en cas d'incident cyber**



Cartographie des GRADeS

Prenez contact avec votre CRRC pour vous accompagner dans le renforcement de votre cybersécurité

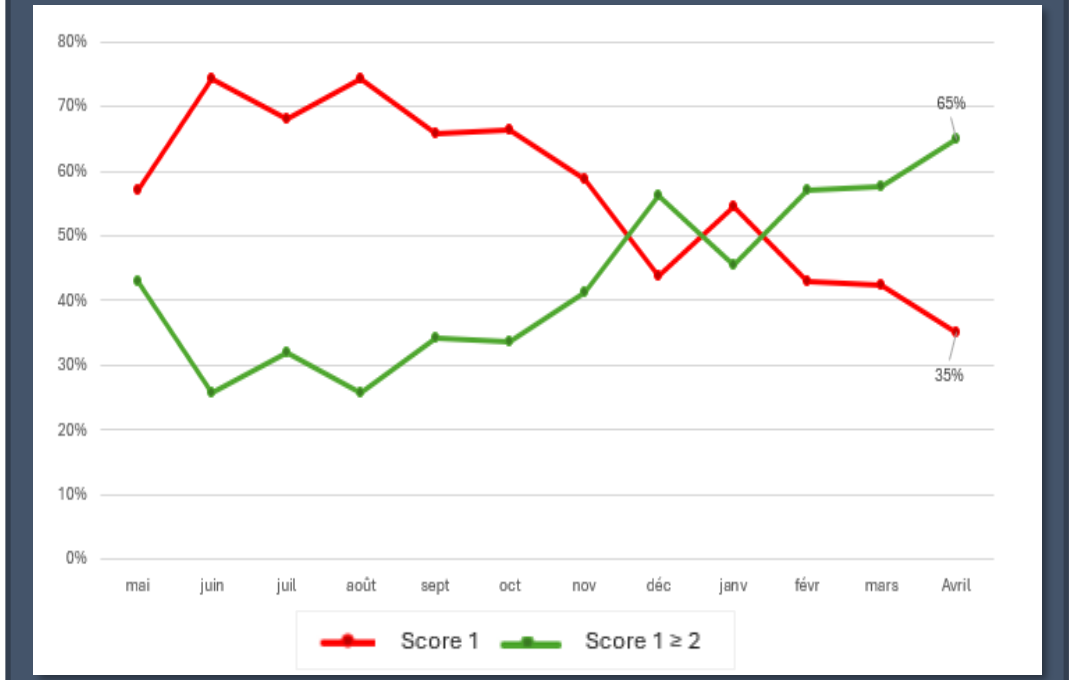
Les appels à financement de l’axe 4

L'axe 4 du programme CaRE, consacré à la **sécurité opérationnelle**, est décliné en plusieurs domaines spécifiques. Chacun de ces domaines vise à **traiter une problématique technique précise** et **à combler les lacunes existantes en matière de cybersécurité**, afin de renforcer la protection des systèmes d'information des établissements de santé.

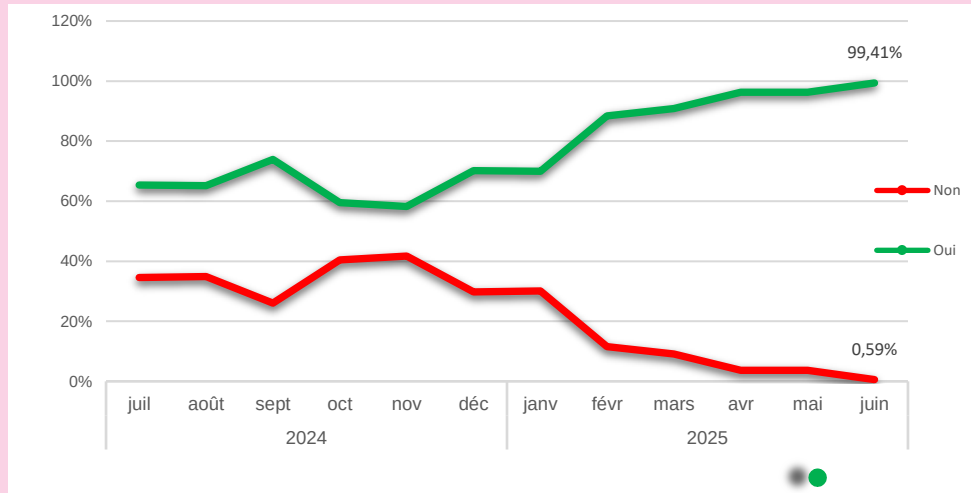
- **Domaine « Annuaires techniques et exposition internet »**
- **Domaine « Stratégie de continuité et de reprise d’activité »**
- **Domaine « Sécurisation des accès distants »**
- **Domaine « Supervision des postes de travail »**
- **HospiConnect**

Appels à financement – Annuaires techniques et exposition internet

Un score supérieur ou égal à 2 doit être obtenu lors des 2 derniers audits ADS des différents AD [objectif D1.O1.B]



Un score inférieur à 3, indiquant l'absence de vulnérabilité critique (niveau rouge CVSS ≥ 9) doit être obtenu lors des 2 derniers audits industriels [objectif D1.O2.B]



Appel à financement – Stratégie de continuité et de reprise de reprise d'activité

Phase de candidature
02 septembre – 02 décembre 2025

La phase opérationnelle court depuis la publication de l'arrêté, jusqu'à la fermeture du portail de déclaration des objectifs

Phase d'atteinte des objectifs et paiement
16 janvier 2026 – 15 septembre 2027

16 janvier 2026 — **Ouverture du portail de déclaration d'atteinte des objectifs**

Les structures peuvent débuter la complétion des documents et déposer les justificatifs attendus

16 février 2026 — **Ouverture du guichet de paiement**

Le versement des subventions débutera pour les établissements ayant atteint les objectifs du domaine.

18 novembre 2026 — **Fermeture du portail de déclaration d'atteinte des objectifs**

Date limite de dépôt de l'ensemble des éléments justificatifs attendus pour valider l'atteinte des objectifs du domaine.

15 septembre 2027 — **Fermeture du guichet de paiement**

Date limite de paiement des fonds alloués, sous réserve de l'atteinte des objectifs.

HospiConnect

Volet matériel

CaRE Cybersécurité accélération et Résilience des Établissements

Financer les moyens d'authentification électroniques physiques et les composants nécessaires à leur lecture pour permettre aux établissements de santé la mise en œuvre d'une **authentification à deux facteurs (2FA)** conforme au RIE

Arrêté du 27/01/2026

Volet transformation

HOP'EN 2

Donner l'impulsion et financer les établissements dans leur projet de **sécurisation de la chaîne d'identification électronique** permettant l'accès au système d'information hospitalier et la consultation du DMP

Instruction n°DNS/2025/180 du 29/12/2025

Quelle réponse pour le secteur médico-social ?

Une réponse spécifique pour le secteur médicosocial

- **Un appel à projet adapté au secteur MS**
- **Publication du cahier des charges d'une phase exploratoire le 30 mars 2026**

Différents parcours

- Trois parcours ont été définis dans les travaux précédents :
  - Parcours 1 : Maturité cyber faible, sans ressource dédiée
  - Parcours 2 : Maturité cyber faible, avec quelques ressources partiellement dédiées
  - Parcours 3 : Maturité cyber intermédiaire
- Pour chaque parcours :
  - Des prérequis
  - Des objectifs obligatoires et des objectifs à la carte

Conférence Institutionnelle **Établissements de santé**

Christian LEMAIRE
Chef de projet sénior numérique et cybersécurité
Référent Programme Care – ARS IDF

sesan Groupement d'Intérêt Public eSanté
RÉPUBLIQUE FRANÇAISE Liberté Égalité Fraternité
ars Agence Régionale de Santé Île-de-France

Domaine 1

Analyse de l'atteinte de cibles et attribution des financements encore en cours (**30 juin 2026**)

Structures éligibles 280, pour un total de 11 691 702,20 €

Candidats 227

Candidatures Validées par l'ARS, répondant au prérequis 219

Dossiers déposés d'atteinte des objectifs : 219

Au 31 mars 2026

84 Dossiers financés par l'ANS pour 3 714 113,73 € de dépenses justifiées, (éligibles :4 330 309,04 €)

Candidatures D2 – Région Ile de France

Total : 222 candidatures sur 284, soit **78,2 %**

	Montants €	% montants	Activité €	% activité
non Candidats	647 929	7,6	1 180 053	5,2
Candidat	7 933 145	92,4	21 460 502	94,8
Total éligible	8 581 074		22 640 555	

Malgré les 78,2% de candidatures, on a 92,4% des montants engagés

Représentant 94,8% de l'activité combinée

D2 Care : **18 novembre 2026**, fermeture du portail de dépôt des éléments preuves

Hospiconnect

287 structures éligibles

250 candidatures

249 candidatures validées

1 candidature refusée

Montant plafond annuel 5 354 840€

HOSPICONNECT /HOPEN2 : **26 Juin 2026,** date de fin de dépôt des éléments preuves pour les cibles 2026

Convergence Care/Instruction ministérielle du 22 janvier 2025

Une instruction ministérielle du 22 Janvier 2025, **pérennise** les actions portées par le programme Care, également dans la perspective de la NIS2 (Directive Européenne) avec, en particulier, les actions suivantes à mener dans les établissements sanitaires :

- Réaliser au moins un **exercice de crise cyber annuel** (D1 Care)
- **Réaliser régulièrement des audits de l'annuaire active directory**, et être **inscrit à SILENE** de l'ANSSI pour contrôler son exposition sur internet (D1 Care)
- **Formaliser** un Plan de Continuité et de Reprise d'Activité (**PCRA**) en cas de cyberattaque ou incident en lien avec la sécurité du système d'information et le **tester** régulièrement, en intégrant l'ensemble des risques SSI dans le plan d'assurance qualité de l'établissement. (D2 Care)
- Se conformer au référentiel d'identification et d'authentification, devant aboutir à **une sécurisation renforcée des accès au SI et services nationaux comme le DMP, par une double authentification** (HOSPICONNECT)

Signalements

A noter, les signalements SSI (incidents et attaques)

2025 : Total : 85 signalements

Sanitaire : 50

EMS : 19

Autre : 16

2026 : Total : 9 signalements

Sanitaire : 7

EMS : 2

Signalements

Les établissements sanitaires doivent obligatoirement faire un **signalement** de tout incident de sécurité, cyber ou non, au **cert sante** selonl' Article L. 1111-8-2 du code de la santé publique

09 72 43 91 25-

https://signalement.social-sante.gouv.fr/espace-declaration/guidage?profil=PROFESSIONNEL_SANTE

En cas de suspicion de fuite de données, faire une **déclaration préalable** sur le site de la **CNIL dans les 72 heures** (https://notifications.cnil.fr/notifications/index)

Porter plainte

TOUS CYBER VIGILANTS

JOURNÉE DE LA CYBERSÉCURITÉ

07 Avril 2026

sesan ÎLE-DE-FRANCE
Groupement d'Intérêt Public eSanté

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ars Agence Régionale de Santé Île-de-France

Sécuriser les identités et les accès

Quentin LE THIEC
Cybersecurity Engineer du CERT Santé – ANS

Thierry WEY
Directeur Système d'Information - HOPITAL LA PORTE VERTE

Thomas SAVATIER
Directeur des Services Numériques - Centre Hospitalier d'Arles

Adeline LEMBRE
Responsable de projets - ANS

Florian CATTEAU
Directeur de Programme - ANS

sesan ILE-DE-FRANCE
Groupement d'Intérêt Public eSanté

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ars Agence Régionale de Santé Île-de-France

Sécuriser les identités et les accès

Quentin LE THIEC
Cybersecurity Engineer du CERT Santé
ANS

sesan
Groupement d'Intérêt Public eSanté
RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité
ars Agence Régionale de Santé Île-de-France

Sécuriser les identités et les accès

Thierry WEY
Directeur Système d'Information
HOPITAL LA PORTE VERTE

sesan
ILE-DE-FRANCE
Groupement d'Intérêt Public eSanté

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ars
Agence Régionale de Santé
Île-de-France

Sécuriser les identités et les accès

Thomas SAVATIER
Directeur des Services Numériques
Centre Hospitalier d'Arles
Hôpitaux de Provence

sesan
Groupement d'Intérêt Public eSanté
RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité
ars Agence Régionale de Santé Île-de-France

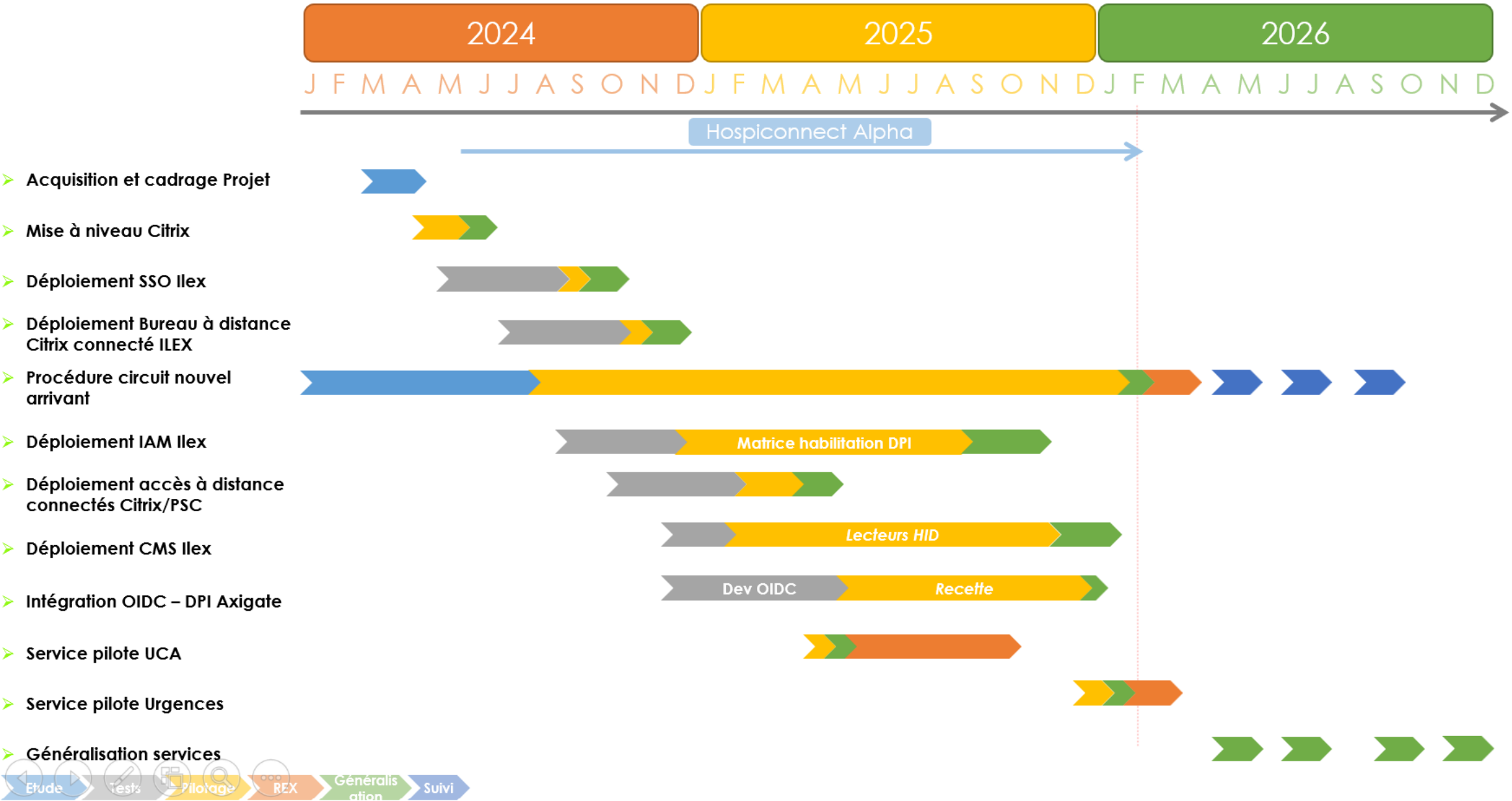
DIRECTION DES SERVICES NUMÉRIQUES

07 Avril 2026

CENTRE HOSPITALIER D'ARLES – HÔPITAUX DE PROVENCE

Vidéo de démonstration

CHRONOLOGIE DU PROJET



Retour d'expérience : Difficultés et Contournements

Application de gestion de cartes CMS

Bien vérifier les pré requis des outils d'encodage DESFire pour s'assurer qu'ils sont biens compatibles avec tous les usages (contrôle d'accès physique/logique, imprimantes, distributeurs, …)

Lecteurs de cartes - tarifs et CPSV3

Augmentation forte du prix des lecteurs de cartes pendant le projet (+50%)

La technologie DESFire a évolué entre la CPSv3 et la CPSv4, s'assurer de la compatibilité de toute la chaîne (encodage, lecture)

Vérifier la compatibilité CPSv3, CPSv4 et carte blanche avec le lecteur poste de travail choisi

Ordres, perte et délai de réception des cartes

Les professionnels à ordre peuvent avoir un usage de leur carte CPS (activité libérale) ou avoir des difficultés pour les retrouver s'ils ne s'en servent pas

Les situations d'exercice et coordonnées ne sont pas forcément à jour dans le SI des ordres

Délais de livraisons importants des CPSv4 en phase pilote pour les professionnels au RPPS+ (prévu par l'ANS)

Spécificité des cartes blanches multi-technologiques avec des délais de livraisons important (DESFire et 125Khz)

Réconciliation d'identité GRH/DPI

Anticiper les usages de l'identifiant unique de l'agent dans les différentes applications métiers (facturation, DPI, LAD, …)

Retour d'expérience : Perspectives

Choisir le(s) MIE(s) définitif

Activer l’authentification poste de travail en e-cps lors de l’oubli de la carte

Confirmer que la carte blanche est compatible avec tous les usages envisagés (identification du professionnel sur sa blouse, distributeurs divers, délivrance de documents sur les imprimantes)

Disposer d’une carte blanche identique à la carte CPSv4 pour des questions de compatibilités

➔ En attente du marché centrale d’achat

Renforcer le processus de recrutement

Se connecter à Pro Santé Identité pour faciliter la mise à jour des SI Ordre

Traiter les circuits spécifiques : Vacataires, Intérimaires, Mobilité Interne

Délégation de droits

Permettre la réinitialisation de mot de passe par un tiers autorisé en authentification multi facteurs

Fournir un formulaire de génération de comptes temporaires compatible avec le projet

SONS-2

Connecter toutes les applications métiers certifiées à notre fournisseur d’identité

➔ Intégrer le pré requis OpenID Connect et API pour la gestion des identités et des accès à nos marchés

Sécuriser les identités et les accès

Adeline LEMBRE
Responsable de Projets – ANS
Florian CATTEAU
Directeur de Programme – ANS

sesan ILE-DE-FRANCE
Groupement d'Intérêt Public eSanté
RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité
ars Agence Régionale de Santé Île-de-France

Ressources méthodologiques – Le guide IE

> Issu de la phase d'expérimentation HospiConnect, ce guide interactif structure la démarche de transformation en établissement. Il s'articule autour de volets complémentaires.

https://sante-gouv-9827.slite.page/p/sVKcP-ZTcdZ_vH/Guide-pour-la-securisation-et-la-simplification-de-l-identification-electronique-des-professionnels-en-structure

1 - Comprendre pourquoi agir

Enjeux, contexte, cadre de référence

2 - Cadrer son projet

État des lieux, cible, gouvernance, trajectoire

3 - Mettre en œuvre les chantiers

Organisation, technique, déploiement, support

4 - S'appuyer sur les retours d'expérience

Points de vigilance, bonnes pratiques, enseignements terrain

Ressources méthodologiques – Le questionnaire IE

> Un support pour aider chaque établissement à couvrir l'ensemble des sujets à adresser et objectiver sa situation de départ.

Faire un état des lieux structuré

Processus, organisation, SI, pratiques existantes.

Couvrir tout le périmètre IE

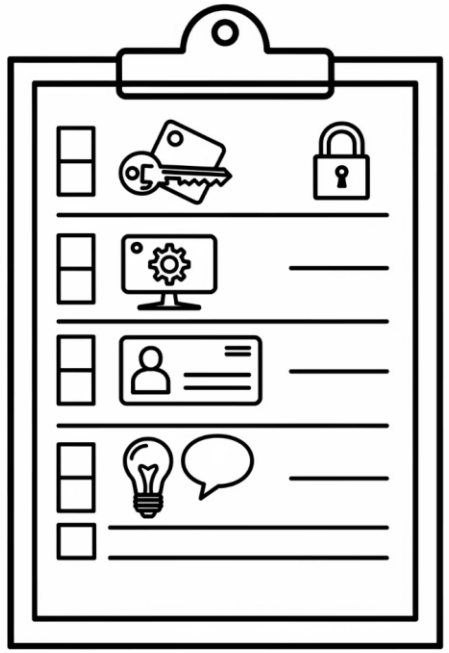
L'ensemble des sujets à adresser dans la démarche.

Identifier les priorités de transformation

Repérer les sujets à traiter en priorité.

Préparer la suite de la démarche

Alimenter la réflexion, le cadrage et la trajectoire de l'établissement.

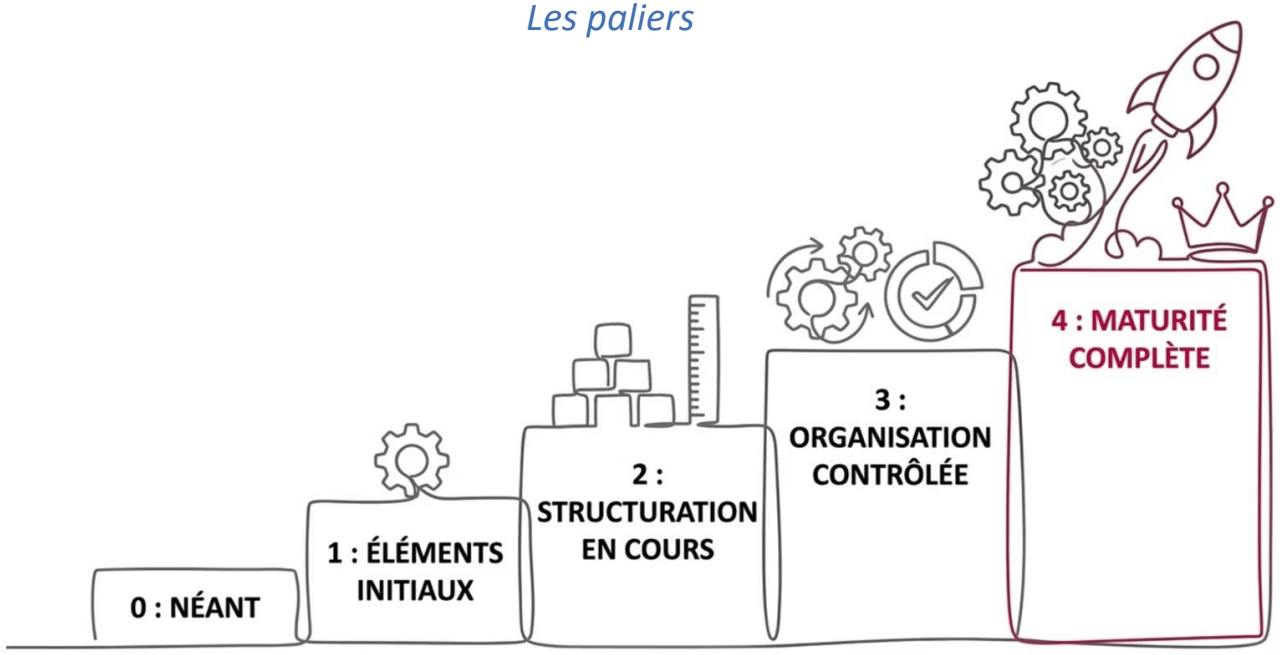


https://sante-gouv-9827.slite.page/p/hGi5scrMIHDhch/Focus-sur-l-etat-des-lieux-de-la-gestion-electronique-des-identites

Ressources méthodologiques – Le dispositif d'évaluation et de suivi de la maturité IE

> Un support pour mesurer la progression, définir une trajectoire cible et suivre l'avancement du projet de transformation IE.

Les paliers



Les type d'indicateurs

Process → Couverture → Gouvernance → Pilotage

Les axes

- Cycle de vie des identités
- Droits et accès
- Services numériques
- MIE
- Gouvernance & sensibilisation

Les objectifs

Piloter dans le temps

Suivre l'avancement du projet de transformation IE

Construire sa trajectoire

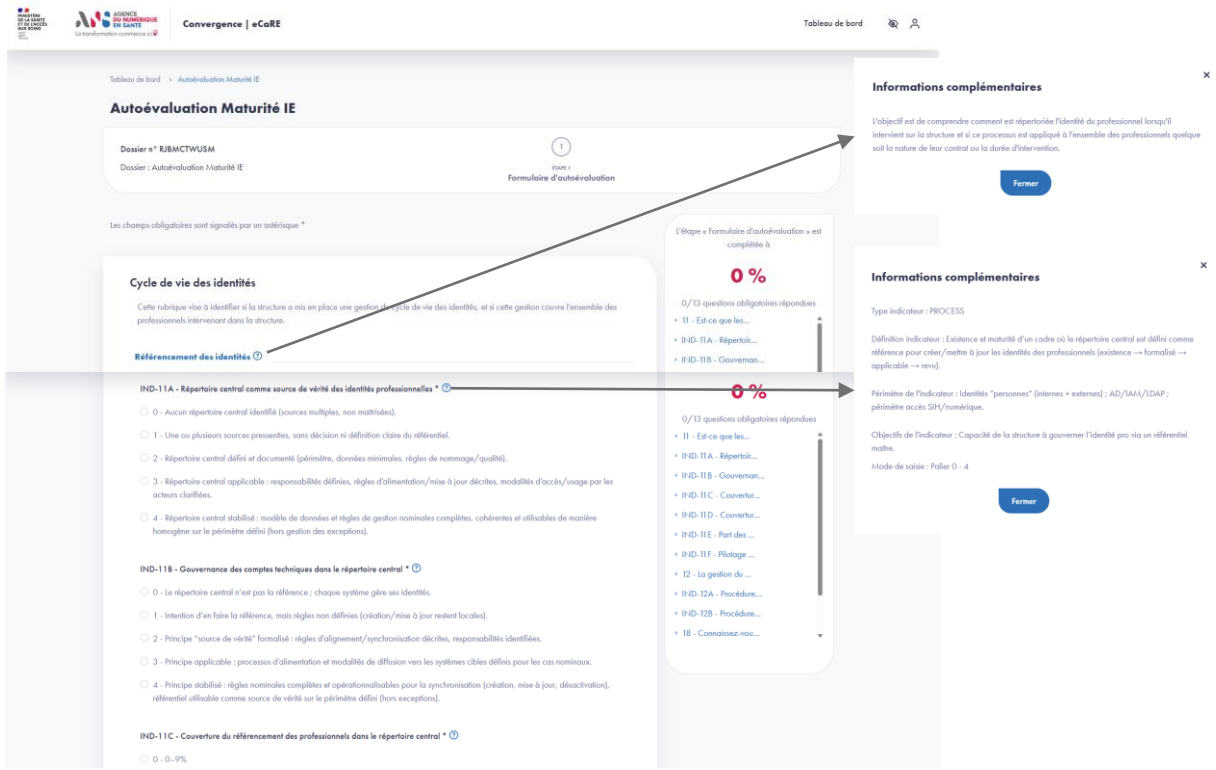
Définir des paliers cibles et un chemin de progression

S'auto-évaluer

Mesurer objectivement son niveau de maturité IE

Ressources méthodologiques – Le dispositif d'évaluation et de suivi de la maturité IE

> Un support pour mesurer la progression, définir une trajectoire cible et suivre l'avancement du projet de transformation IE.



Les axes

- Cycle de vie des identités
- Droits et accès
- Services numériques
- MIE
- Gouvernance & sensibilisation

Les objectifs

Piloter dans le temps

Suivre l'avancement du projet de transformation IE

Construire sa trajectoire

Définir des paliers cibles et un chemin de progression

S'auto-évaluer

Mesurer objectivement son niveau de maturité IE

Ressources méthodologiques – document d'aide à la définition de la trajectoire et plan projet

> Fournir un socle commun de réflexion, de décision et de pilotage, directement réutilisable par les équipes projet. Il peut être repris, allégé, enrichi ou réorganisé selon le contexte local.

Proposer une trame de référence

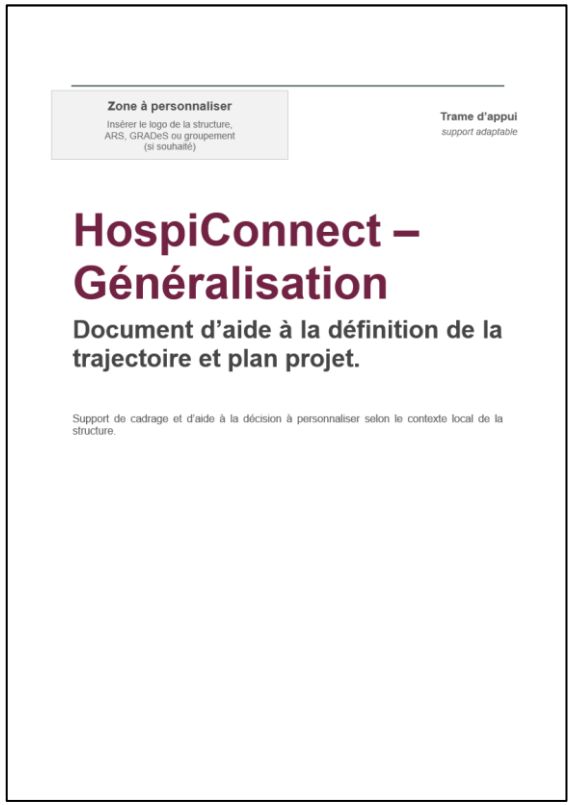
aider à cadrer, documenter et piloter une trajectoire locale de transformation de la chaîne d'identification électronique des professionnels.

Fournir au sponsor une vision claire

vision claire de la cible, des décisions à arbitrer, des risques majeurs, des dépendances et des jalons de gouvernance

Repère opérationnel du chef de projet

un repère opérationnel pour structurer la trajectoire, découper les travaux, organiser les livrables et suivre la progression de maturité.



Zone à personnaliser

Insérer le logo de la structure, ARS, GRADeS ou groupement (si souhaité)

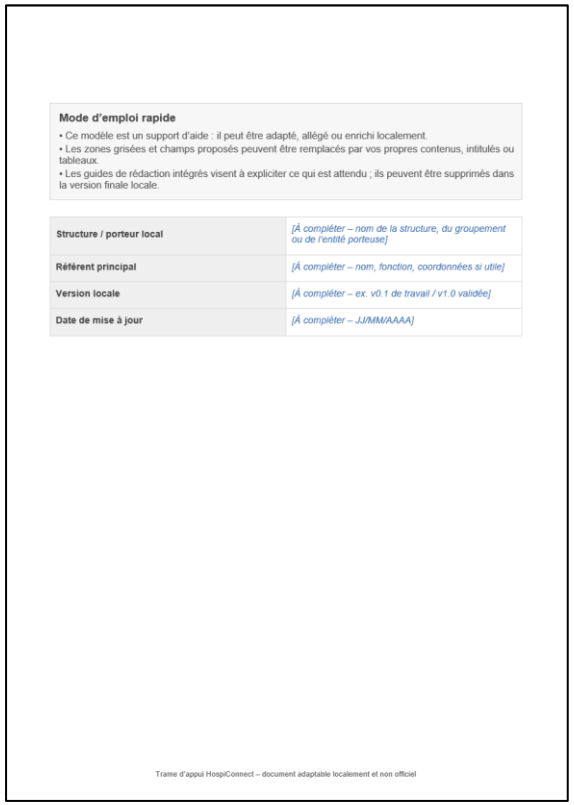
Trame d'appui

support adaptable

HospiConnect – Généralisation

Document d'aide à la définition de la trajectoire et plan projet.

Support de cadrage et d'aide à la décision à personnaliser selon le contexte local de la structure.



Mode d'emploi rapide

- Ce modèle est un support d'aide : il peut être adapté, allégé ou enrichi localement.
- Les zones grisées et champs proposés peuvent être remplacés par vos propres contenus, intitulés ou tableaux.
- Les guides de rédaction intégrés visent à expliciter ce qui est attendu ; ils peuvent être supprimés dans la version finale locale.

Structure / porteur local	*[À compléter – nom de la structure, du groupement ou de l'entité porteuse]*
Référent principal	*[À compléter – nom, fonction, coordonnées si utile]*
Version locale	*[À compléter – ex. v0.1 de travail / v1.0 validée]*
Date de mise à jour	*[À compléter – JJ/MM/AAAA]*

Trame d'appui HospiConnect – document adaptable localement et non officiel

Ressources méthodologiques – Des supports simples pour accompagner les chefs de projet

> Selon les besoins, quelques trames ou modèles pourront être proposés pour faciliter la structuration de la démarche.

Structurer certains travaux

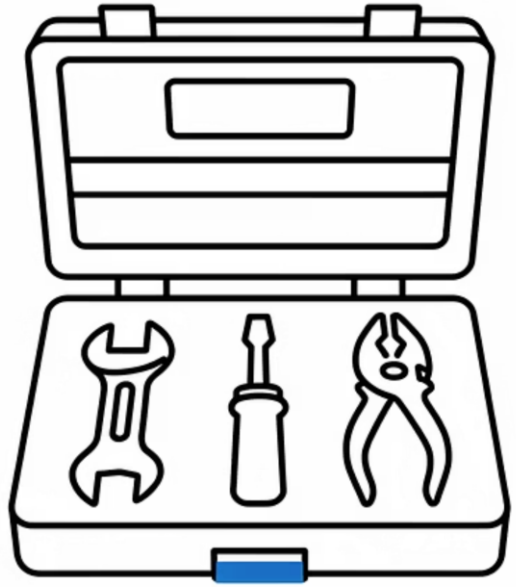
Par exemple : trame simple de formalisation ou de cadrage.

Faciliter l'organisation de la démarche

Par exemple : support simple de recensement ou de suivi.

Proposer des repères réutilisables

Par exemple : modèle adaptable selon le contexte de l'établissement.



TOUS CYBER VIGILANTS

JOURNÉE DE LA CYBERSÉCURITÉ

07 Avril 2026

sesan ÎLE-DE-FRANCE
Groupement d'Intérêt Public eSanté

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ars Agence Régionale de Santé Île-de-France

Pitch SESAN :

Quelles actions pour les établissements de santé ?

Sébastien BALTHAZAR
Consultant SSI – SESAN

sesan ILE-DE-FRANCE
Groupement d'Intérêt Public eSanté

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ars Agence Régionale de Santé Île-de-France

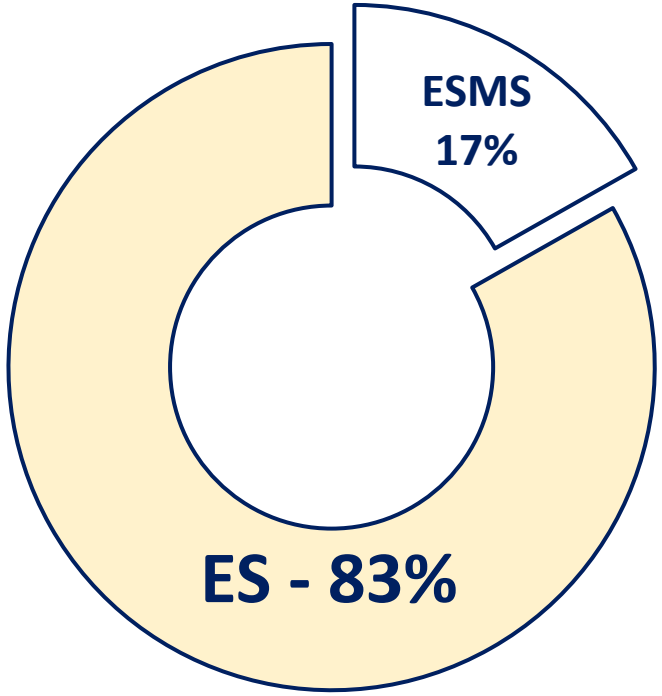
PANORAMA DE LA CYBERMENACE 2025

La Santé 3ème secteur ciblé

PANORAMA DE LA CYBERMENACE 2025

SESAN est le Groupement Régional d'Appui au Développement de l'eSanté (GRADeS) d'Île-de-France.

- 7 Consultants en SSI et RGPD
- Plus de 130 adhérents



ÉTUDE SUR LA CYBERSÉCURITÉ DES ÉTABLISSEMENTS DE SANTÉ

Resultats-enquete-cyber-ANS

32% **des établissements ayant subi un incident cyber estiment être « insuffisamment préparés ».**

ÉTUDE SUR LA CYBERSÉCURITÉ DES ÉTABLISSEMENTS DE SANTÉ

SENSIBILISATION

Comment sensibiliser les professionnels à la cybersécurité ?

Test de Phishing / Campagne de sensibilisation

Jeu de carte PRA*

Exercice de Cybercrise
(Embarquer la Direction)

*Plan de reprise d'activité

Initier vos réflexions sur le Plan de Reprise d'Activité "PRA" en cas de cyberattaque, de manière ludique.

Temporalité

- 3 PREMIÈRES HEURES
- 3 PREMIERS JOURS
- 3 PREMIÈRES SEMAINES
- 3 PREMIERS MOIS

Cellules

- CELLULE SUPPORT
- CELLULE SECURITE
- CELLULE INFRASTRUCTURE
- CELLULE APPLICATIVE

Actions

- Isoler les zones réseau impactées par l'attaque.
- Produire de nouveaux masters sains pour les postes de travail.
- Identifier le vecteur de compromission initial (email, accès VPN...).
- PC sain isolé du réseau
- Evaluer les pertes financières
- Envoyer les résultats pharma par fax/coursiers

DÉTECTION

Comment détecter les vulnérabilités du SI de l'établissements ?

Audit d'exposition

Cybersurveillance

Test d'intrusion

Test d’intrusion

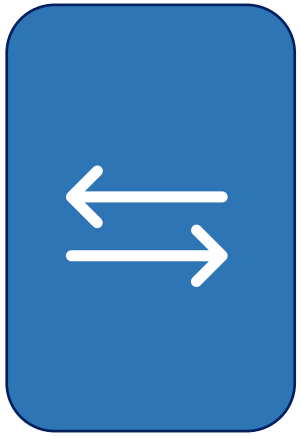
Test d'intrusion interne

Test d'intrusion externe

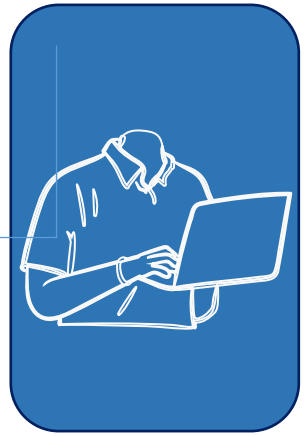
Audit de contrôle ou contre-audit

PROTECTION

Comment protéger les informations ?



Echange sécurisé



Expert Technique

Expert Technique

Sécurisation de Microsoft

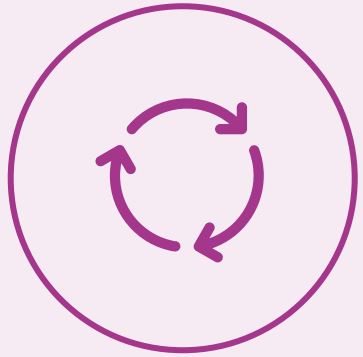
Sécurisation des stockages et sauvegardes

Sécurisation des réseaux

RÉSILIENCE

Comment se préparer et réagir en cas d'incident majeur ?

Continuité d'Activité

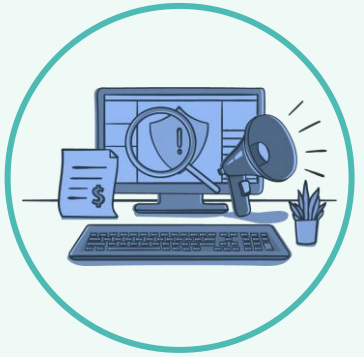


Solution de Continuité d'Activité

Expert Continuité d'Activité

Assistance en cas de crise

Expert Gestion de crise



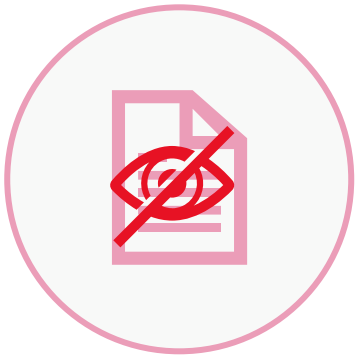
Prestataire de réponse à incident de sécurité PRIS

CONFORMITE

Comment se conformer aux exigences de sécurité ?

RSSI

(Resp Sécurité des systèmes d'information)



DPO

(Délégué à la protection des données)

Cartographie du SI

Banque documentaire

Banque documentaire

Exemple de Charte Utilisateur

1. Objet du document

La présente Charte a pour objet de décrire les règles d'accès et d'utilisation des ressources informatiques et des services Internet du *[indiquer le nom de l'établissement de santé]* et rappelle à ses utilisateurs les droits et les responsabilités qui leur incombent dans l'utilisation du système d'information.

Elle pose des règles permettant d'assurer la sécurité et la performance du système d'information de l'établissement, de préserver la confidentialité des données dans le respect de la réglementation en vigueur et des droits et libertés reconnus aux utilisateurs, conformément à la politique de sécurité du système d'information définie par l'établissement.

Cette Charte a été validée par la Direction générale de l'établissement. Préalablement, elle a été notifiée à sa mise en œuvre au Comité d'Etablissement et à la Commission médicale d'Etablissement. Elle constitue une annexe au Règlement Intérieur de l'établissement. Les membres du personnel et les personnels extérieurs sont invités à en prendre connaissance. La Charte est mise à leur disposition sur l'Intranet et affichée dans les locaux de l'établissement de santé.

La Charte d'accès et d'usage du système d'information doit être validée conjointement par la Direction générale et la Commission médicale de l'établissement. Elle constitue une annexe au Règlement intérieur.

2. Champ d'application

Cette section décrit le périmètre d'application de la présente Charte et précise les utilisateurs du système d'information de l'établissement qui sont concernés par celle-ci.

La présente Charte concerne les ressources informatiques, les services internet et téléphoniques du *[indiquer le nom de l'établissement de santé]*, ainsi que tout autre moyen de connexion à distance permettant d'accéder, via le réseau informatique, aux services de communication ou de traitement électronique interne ou externe.

Il s'agit principalement des ressources suivantes :

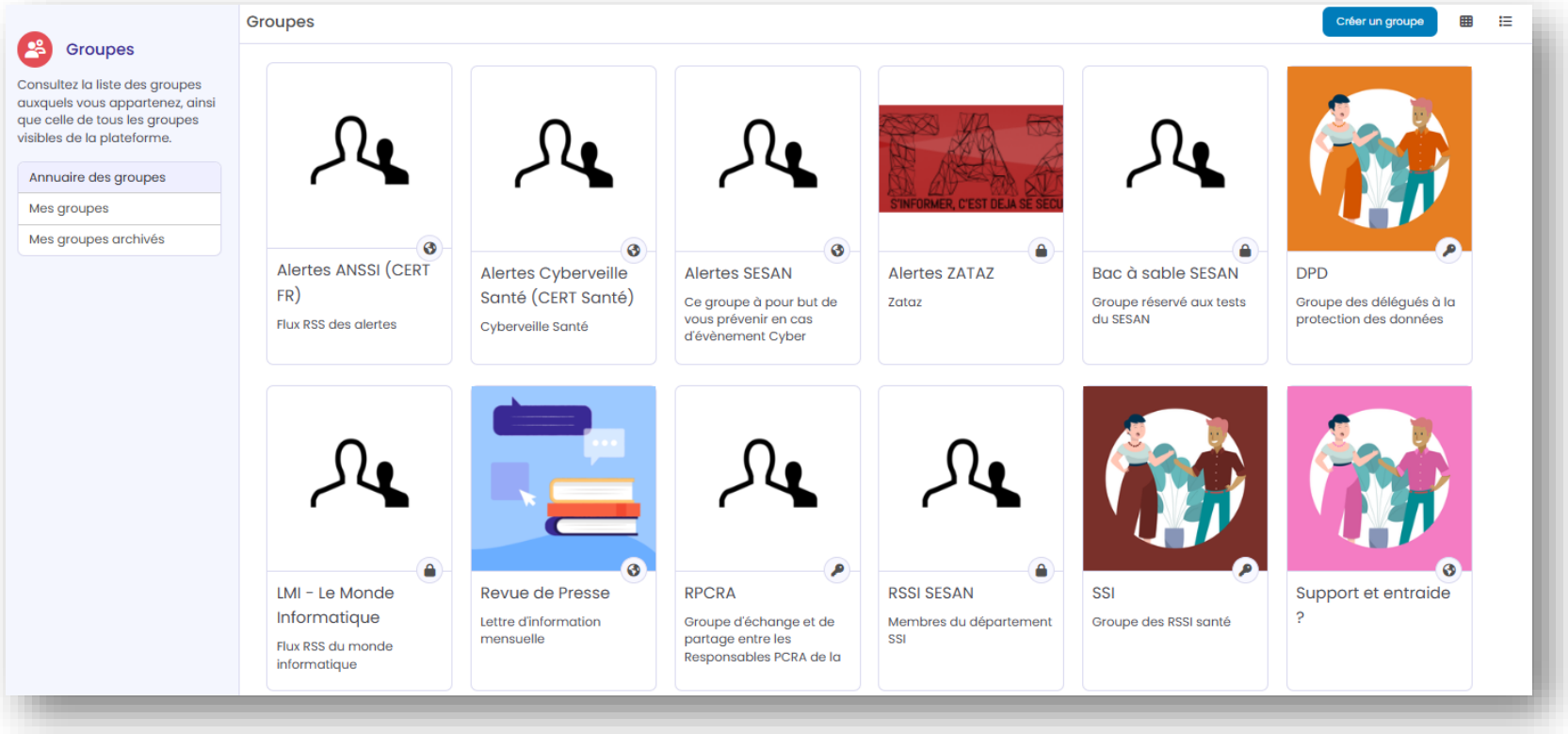
- Ordinateurs de bureau ;

Fiche Réflexe

Forum d'échanges : Jamespot

(compris dans l'adhésion)

Un réseau social communautaire piloté par le GRADeS à destination des référents sécurité des structures de santé de la région.



Statistique de satisfaction

94% **satisfaction sur l'ensemble des services SSI et RGPD en 2025**

96% **satisfaction sur la réactivité de l'équipe SSI à vous répondre à vos questions.**

Pourquoi pas vous ?

Pause & visite des stands

TOUS CYBER VIGILANTS

JOURNÉE DE LA CYBERSÉCURITÉ

07 Avril 2026

sesan ÎLE-DE-FRANCE
Groupement d'Intérêt Public eSanté

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ars Agence Régionale de Santé Île-de-France

Sous-traitants : Comment imposer et contrôler les exigences cyber ?

Vincent THAU
Key Account Manager - Board of Cyber

Thomas AUBIN
RSSI du CHRU de Lille et du GHT Hôpitaux Publics Grand Lille, Président du Club des RSSI Santé

Patrice DRUEZ
Consultant Mission Sécurité et Urbanisation Référent RGPD - Région Ile-de-France

sesan Groupement d'Intérêt Public eSanté
RÉPUBLIQUE FRANÇAISE Liberté Égalité Fraternité
ars Agence Régionale de Santé Île-de-France

Sous-traitants :

Comment imposer et contrôler les exigences cyber ?

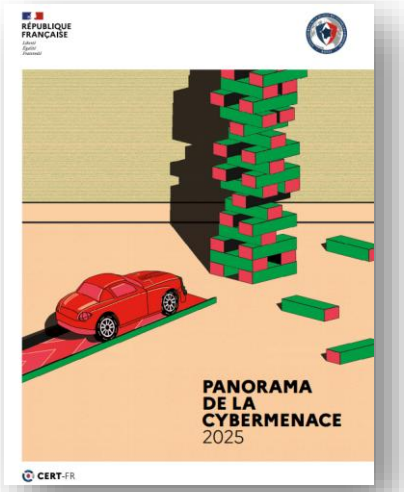
Vincent THAU
Key Account Manager - Board of Cyber

sesan
ILE-DE-FRANCE
Groupement d'Intérêt Public eSanté

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ars
Agence Régionale de Santé
Île-de-France

Risque systémique et réglementaire



PANORAMA DE LA CYBERMENACE 2025 ANSSI

C
LE CIBLAGE DES SOUS-TRAITANTS COMME VECTEUR DE COMPROMISSION

→ Les attaques contre la chaîne logistique ou d'approvisionnement (*supply-chain attack*) consistent à compromettre un tiers, comme un fournisseur de services logiciels ou un prestataire, afin de cibler la victime finale. Cette technique est éprouvée et exploitée par plusieurs acteurs étatiques et cybercriminels depuis au moins 2016. Cette méthode présente un risque de propagation rapide d'une attaque qui peut parfois concerner un secteur d'activité entier ou une zone géographique précise notamment lorsque l'attaque cible un fournisseur de logiciels largement répandus ou une entreprise de service numérique (ESN) locale ou spécialisée dans un secteur d'activité particulier [91]. Les attaquants à l'origine de ces attaques peuvent chercher à exfiltrer des informations via un tiers, réaliser des attaques lucratives ou alors paralyser de manière temporaire ou pérenne un secteur ou un ensemble d'entités données.

Avec le développement de la sous-traitance, assortie d'une délégation de compétences au sein de certains secteurs d'activités, les entreprises peuvent ne plus maîtriser l'intégralité des équipements qu'elles incorporent dans leurs réseaux. Cette situation de fait affaiblit le niveau de sécurisation des environnements, et les attaquants peuvent exploiter cette moindre maîtrise pour réaliser leurs compromissions.

Plusieurs acteurs étatiques réputés russes, chinois ou iraniens ont pu mener des attaques via la chaîne d'approvisionnement ces dernières années.

Les attaques via la chaîne d'approvisionnement ne sont cependant pas uniquement l'apanage des MOA réputés étatiques. Entre janvier et juin 2025, l'ANSSI a observé la compromission par rançongiciels de plusieurs entités industrielles impliquées dans la chaîne d'approvisionnement de la Base Industrielle et Technologique de Défense (BITD) française. Ces entreprises, à l'origine de la conception et de la fabrication de systèmes, de pièces et de logiciels liés aux secteurs de l'armement et de l'aéronautique peuvent disposer d'informations sensibles, potentiellement exposées lors de ces attaques. Si l'ANSSI ne considère pas que ces attaques ont été menées de manière coordonnée (les entreprises ont été compromises par des opérateurs de rançongiciels différents), ces événements de sécurité rappellent ainsi l'importance d'identifier ces sous-traitants essentiels et de les aider à améliorer leur sécurité informatique. Le secteur de la défense a également fait l'objet en 2025 d'actions de reconnaissance, de tentatives de compromissions et de compromissions par des modes opératoires réputés étatiques à des fins d'espionnage stratégique et de renseignement.

En 2025, l'ANSSI a été témoin de nombreuses compromissions d'entités par des attaquants en mesure de se latéraliser depuis les systèmes d'information de prestataires vers des clients. À titre d'exemple, un attaquant a compromis et exfiltré des ressources clientes chez un prestataire de nombreuses entités françaises. En tirant parti des interconnexions existantes avec les systèmes d'information des clients et grâce à des authentifiants volés, l'attaquant est parvenu à se latéraliser sur le système d'information de plusieurs clients.

Dans d'autres cas observés par l'Agence, les attaquants ont réalisé des attaques par rebond en compromettant une victime initiale et en utilisant les ressources de celle-ci pour réaliser de nouvelles compromissions, sans qu'il ne s'agisse forcément de sous-traitant. Les ressources internes de la première entité compromise peuvent alors servir à forger ou utiliser des éléments crédibles permettant de mieux cibler une deuxième entité [92], [93].

Par ailleurs, l'ANSSI a été témoin de plusieurs compromissions par rançongiciel de prestataires causant des impacts forts sur les clients. Au cours de l'année, les ressources d'une entité française ont été

48

« Les attaques par la chaine d'approvisionnement permettent de compromettre par rebond les organisations clients d'un prestataire commun »

Panorama 2024

« En 2025, l'ANSSI a été témoin de nombreuses compromissions d'entités par des attaquants en mesure de se latéraliser depuis les systèmes d'information de prestataires vers des clients. »

Panorama 2025

Article 21, paragraphe 2, de la Directive NIS 2 (Directive (UE) 2022/2555)

(d) *la sécurité de la chaîne d'approvisionnement*, y compris les aspects de sécurité liés aux relations entre chaque entité et ses fournisseurs directs ou prestataires de services

NIS2 Directive

Observatoire 2025

Extrait de l'observatoire réalisé par Board of Cyber en partenariat avec le CESIN

Novembre 2025 – 174 répondants

82%

des entreprises jugent le risque fournisseurs « très important » ou « important »

84%

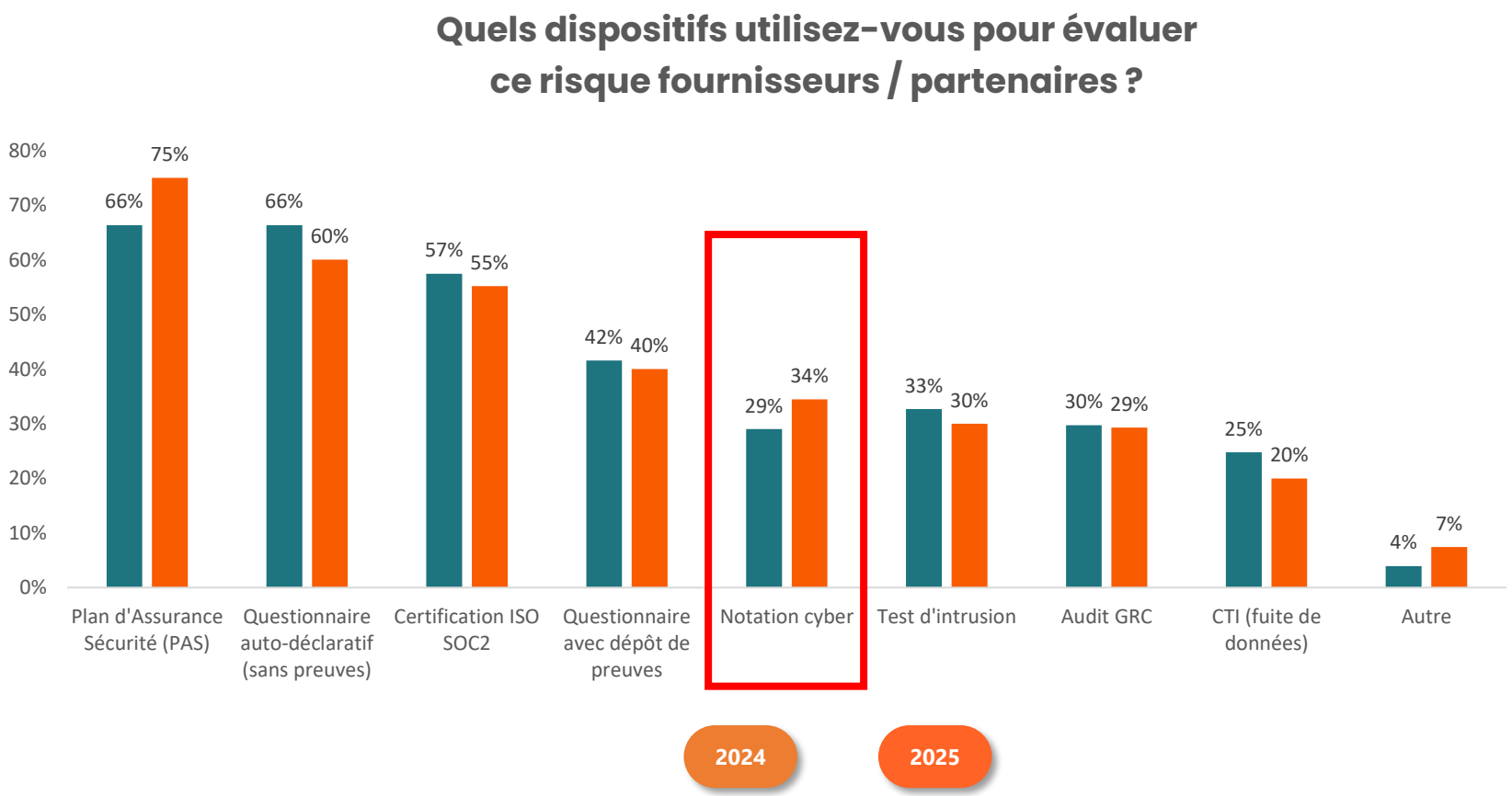
des entreprises sont soumises à une réglementation

82%

des entreprises seraient prêtes à mutualiser leurs évaluations

Source : Observatoire des risques cyber liés aux fournisseurs (TPRM) 2025

La notation cyber, nouveau levier d'efficacité?



Et si une baguette magique TPRM existait ?

" Disposer d'un **« Cyberscore »** (comme le nutriscore) de toutes les entreprises ayant des activités en Europe, basé sur un **référentiel d'évaluation unique** et **une plateforme** pour connaitre le niveau des entreprises. "

RSSI d'un établissement de santé

Source : Observatoire des risques cyber liés aux fournisseurs (TPRM) 2025

Sous-traitants :

Comment imposer et contrôler les exigences cyber ?

Thomas AUBIN
RSSI du CHRU de Lille et du GHT Hôpitaux Publics Grand Lille, Président du Club des RSSI Santé

sesan
Groupement d'Intérêt Public eSanté
RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité
ars Agence Régionale de Santé Île-de-France

Le Clausier Conformité Numérique

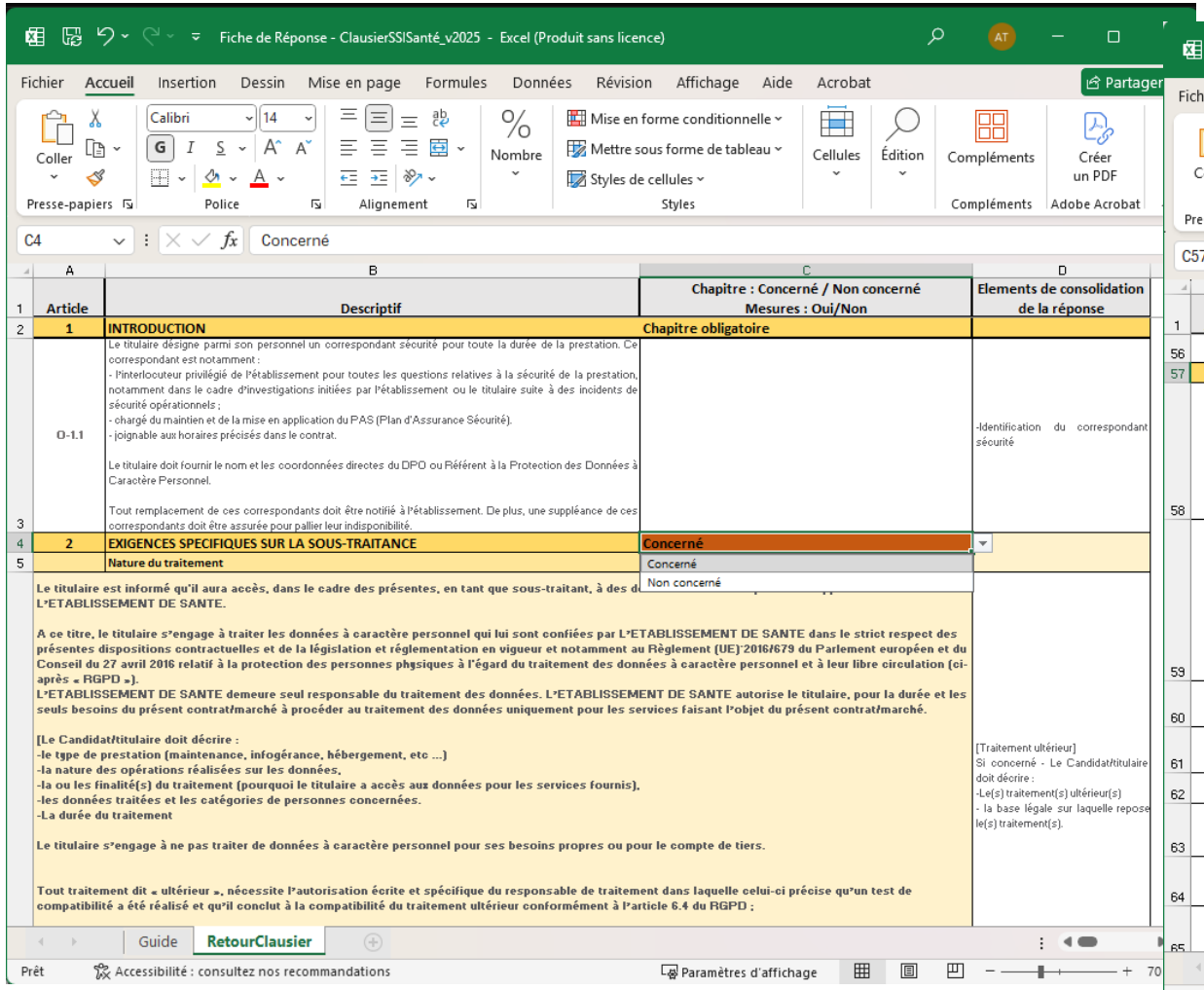
CLAUSIER
CONFORMITÉ
NUMÉRIQUE
2025

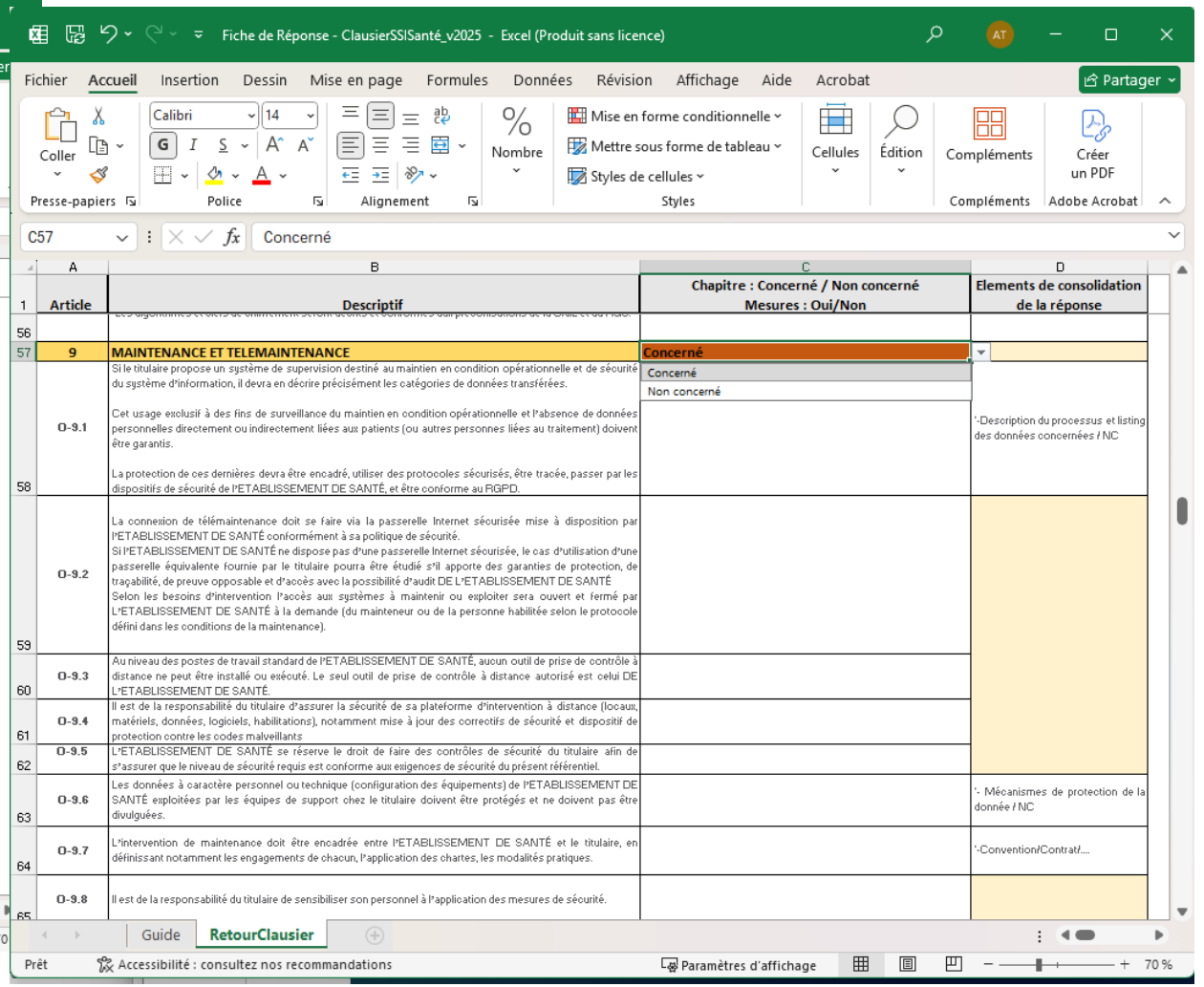
Sommaire

1. Introduction 4
2. Exigences spécifiques sur la sous-traitance 6
3. Exigences générales sur les logiciels 10
4. Identités 12
5 . Authentification, Single Sign On et habilitations 13
6. Tracabilité 15
7. Protection des systèmes 16
8. Cryptographie 17
9. Maintenance et Télémaintenance 18
10. Spécifications wi-fi 21
11. Protection des données médicales 22
12. Cas particulier selon périmètre 23
12.1 Cas de dispositifs mobiles 23
12.2 Cas des dispositifs médicaux connectés 23
12.2.1 Conformité 24
12.2.2 Gestion des accès 24
12.2.3 Connectivité et sécurité des réseaux 24
12.2.4 Exploitation et communication 25
12.2.5 Maintenance et télémaintenance des dispositifs médicaux 26
12.2.6 Protection des données 27
12.2.7 Sécurité physique 28
12.2.8 Résilience 28
12.2.9 Gestion des licences 29
12.2.10 Protection des secrets 30
12. 3 Cas de service hébergé en dehors du SI de l'établissement de santé et de prestation de type SaaS/IaaS 30
12. 4 Cas de service hébergé par l'établissement de santé et intégralement administré par le titulaire 32
12. 5 Cas du fournisseur de service de développement 33
12. 6 Cas de service utilisant des technologies d'intelligence artificielle 36
Références documentaires 38
Glossaire des termes employés 39

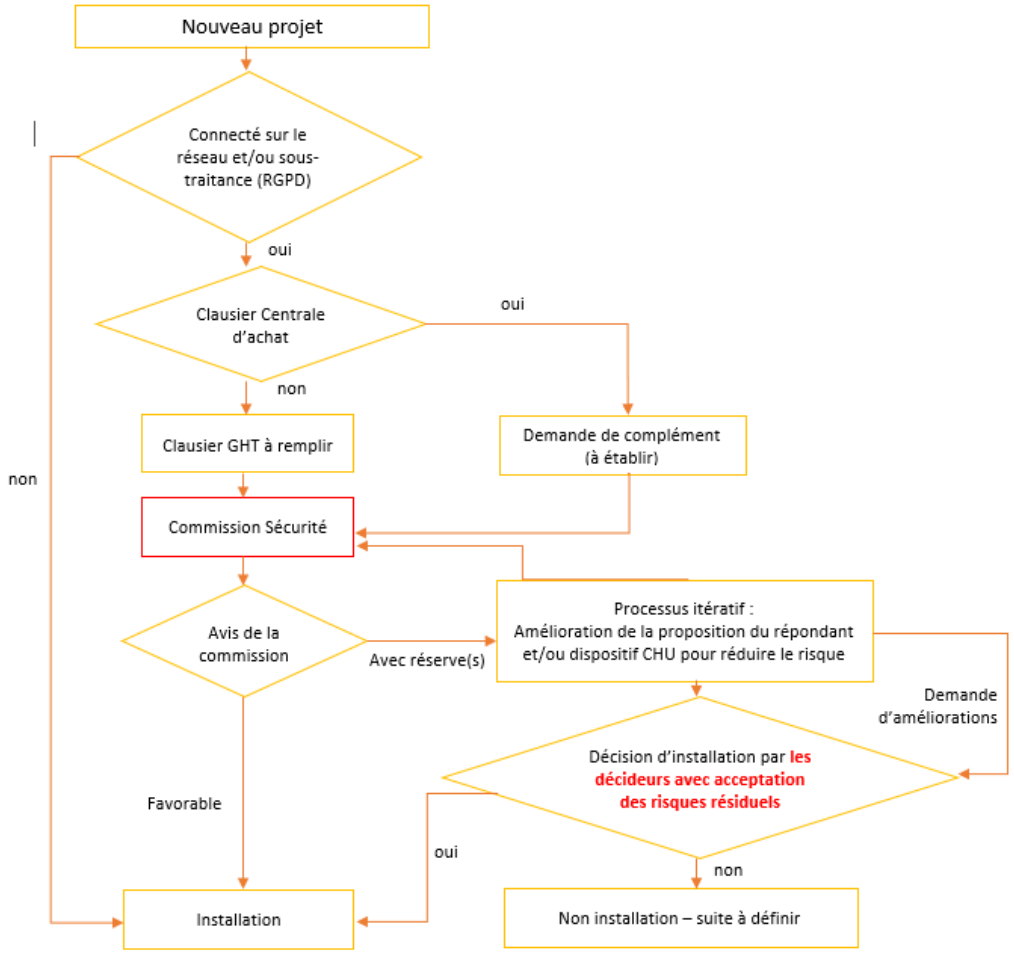
https://www.rssi-sante.fr/clausier-securite-ssi

Le Clausier Conformité Numérique





Un exemple au CHU de Lille : la Commission Sécurité



HÔPITAUX PUBLICS Grand Lille	Contrat d'interface entre la Direction du Système d'Information (DSI) et la Direction des Achats (DA)	Code du document : [P_TYPE] / [P_UNIT] / [P_REF] Date d'application : [P_APPLICATION_DATE] Version : [P_REVISION] Page 1 sur 5

Rédaction	Validation
Nom / Prénom et fonction : **RENIAU Marine** Chargée de mission méthodologie, communication, RSE du GHT HPGL **BOUZIDI Anthony** Délégué à la protection des données (DPO) du GHT HPGL **AUBIN Thomas** Responsable de la Sécurité des Systèmes d'Information du GHT HPGL	Nom / Prénom : **TAINE Michael** - **CARESMEL Frédérique** Fonction : Directeur des Ressources Numérique et du Système d'Information du GHT HPGL - Directrice des Achats du GHT HPGL

Périmètre d'application :
Ce document s'applique à toutes les procédures achats concernées par de la gestion de données personnelles ou pouvant avoir une incidence sur la sécurité du système d'information du GHT.

Pourquoi ?

Le présent contrat d'interface est établi entre la Commission de Sécurité et la Direction des Achats du GHT Hôpitaux Publics Grand Lille. Il repose sur un contrat de partenariat compris et partagé par l'ensemble des acteurs. Il a une double finalité :
- la fluidité du circuit entre la Direction des Achats et la Commission de Sécurité
- la prise en charge optimale des sujets relatifs aux protections des données et à la sécurité informatique.

Ce contrat définit les obligations réciproques, concrètes et mesurables que se fixent les signataires.

Qui ?

La Direction des Ressources Numériques et du Système d'Information du GHT HPGL, représentée par Monsieur Michael TAINE d'une part, et la Direction des Achats du GHT HPGL, représentée par Madame Frédérique CARESMEL d'autre part.
Les contacts opérationnels pour la Direction des Ressources Numériques pour le suivi de cette interface sont :
- Le Délégué à la Protection des Données : Anthony BOUZIDI, dpo@chu-lille.fr
- Le Responsable de la Sécurité du Système d'Information : Thomas AUBIN, thomas.aubin@chu-lille.fr

Pour la Direction des Achats, les contacts sont les pilotes des filières achats suivantes :
- Produits de santé
- Biomédical-Laboratoires
- Travaux et infrastructures
- Achats généraux
- Nouvelle Technologie d'Information et de Communication (NTIC)

Annuaire Achats GHT HPGL.xlsx

HÔPITAUX PUBLICS Grand Lille	Contrat d'interface entre la Direction du Système d'Information (DSI) et la Direction des Achats (DA)	Code du document : [P_TYPE] / [P_UNIT] / [P_REF] Date d'application : [P_APPLICATION_DATE] Version : [P_REVISION] Page 2 sur 5

Les rôles sont établis comme suit :

Commission de Sécurité	Achats
Conseille les achats sur l'insertion du clausier numérique	Peuvent solliciter la commission de sécurité, au moment du lancement d'une procédure, pour avoir un avis sur la nécessité ou non de faire compléter le clausier numérique
Analyse le risque via le clausier numérique complété par le pressenti attributaire d'un marché, pour un ou plusieurs établissements du GHT	Transmettent le clausier numérique aux soumissionnaires via le dossier de consultation des entreprises (DCE)– Peuvent transmettre le clausier numérique au fournisseur en amont du lancement de la procédure dans le cadre d'un marché négocié sans mise en concurrence
Informe les achats du suivi des procédures internes à la commission	Vérifient la complétion du clausier numérique et le transfèrent à la commission de sécurité
Émet un avis sur la conformité de la solution au clausier numérique et indique des réserves si besoin	Informent la Commission de Sécurité de la notification des marchés concernés par des avis
Le cas échéant, révise le niveau de risque des réserves émises après un réexamen	

Quand ?

Le contrat entre en vigueur dès validation des 2 parties.
Il s'applique lorsqu'une procédure d'achat est concernée par de la gestion de données personnelles par le prestataire et/ou embarquant une solution numérique.

Comment ?

Pré-requis : Pour solliciter la Commission Sécurité , la procédure achat doit être concernée :

- par des questions de **gestion de données personnelles** (= lorsque le prestataire a à minima accès à des données à caractère personnel au sens du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données)
- et/ou de mise à disposition d'une solution numérique (= lorsque l'équipement est connecté au réseau du Centre Hospitalier ou qu'il implique une connexion du prestataire au système d'information du Centre Hospitalier).

En cas de doute, la Commission Sécurité doit être saisie.

La commission de sécurité s'engage à partager un tableau de suivi des dossiers en cours avec la Direction des Achats. Ce tableau indiquera également l'historique des avis et des réserves déjà émis.

Seule la version informatique du logiciel de gestion documentaire est valide
© Document interne, propriété du C.H.U de Lille

Sous-traitants :

Comment imposer et contrôler les exigences cyber ?

Patrice DRUEZ

Consultant Mission Sécurité et Urbanisation Référent RGPD - Région Ile-de-France

sesan Groupement d'Intérêt Public eSanté

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ars Agence Régionale de Santé Île-de-France

UN CONSTAT

- **OBSERVATOIRE DES COMMUNES**
  Juin 2023
  Accompagnement à la maturité cyber des collectivités

- **CSIRT Urgence CYBER**
  novembre 2023
  Réponse aux incidents cyber sécurité Collectivité PME, ETI, ASSOC

- **Gestion mutualisée du risque Fournisseurs**
  Novembre 2025
  Regrouper les processus d'identification et d'évaluation de la chaîne d'approvisionnement liées aux partenaires commerciaux.

COMMENT IMPOSER ET CONTROLER LES EXIGENCES CYBER ?

❑ **S'APPUYER SUR LA REGLEMENTATION :** Selon le contexte, certaines obligations peuvent être ou doivent être **légalement imposées** :

Le client est **responsable du traitement et du niveau de sécurité de ses sous-traitants**

- RGPD (protection des données personnelles)
- NIS2 (gestion des risques fournisseurs)

❑ **EVALUER LES FOURNISSEURS (avant contractualisation)**

Classer les fournisseurs par niveau de risque (critique, sensible, standard).

- Analyse de maturité cyber
- Questionnaire de sécurité
- Demande de preuves :
  - certificats (ISO, SOC2)
  - politiques internes
  - résultats d'audits

❑ **IMPOSER LES EXIGENCES CYBER (cadre réglementaire)**

Formaliser des obligations via :

Clauses contractuelles (sécurité, confidentialité, notification d'incident)

Références à des standards reconnus comme

- ISO/IEC 27001
- NIST Cybersecurity Framework

Exigences concrètes : MFA obligatoire , chiffrement des données , gestion des accès , tests de vulnérabilité réguliers , délai de notification d'incident

COMMENT IMPOSER ET CONTROLER LES EXIGENCES CYBER ?

❑ **OPTIMISER LES COUTS ET LES EFFORTS** Évaluer un fournisseur demande beaucoup de ressources. (audit, conformité, cybersécurité, etc.)

Une entreprise seule aurait du mal à maintenir un niveau d'analyse aussi élevé

En mutualisant on :

- Evite de faire les mêmes audits plusieurs fois
- Partage les bases de données et analyses
- Diminue les coûts globaux

❑ **AMELIORER LA QUALITE DE L'INFORMATION** Un acteur isolé voit seulement une partie du risque.

À plusieurs le risque est mieux anticipé.

Groupé on :

- Croise les expériences (incidents, retards, défauts)
- Détecte plus vite les signaux faibles
- Obtient une vision plus complète et fiable

❑ **MIEUX GERER LES RISQUES SYSTEMIQUES** Certains fournisseurs sont critiques pour tout un secteur (ex : cloud, matières premières).

On passe d'une logique individuelle à une logique collective de résilience.

Mutualiser permet

- Identifier les risques partagés
- Anticiper les ruptures de chaîne d'approvisionnement
- Coordonner les réponses en cas de crise

COMMENT IMPOSER ET CONTROLER LES EXIGENCES CYBER ?

- **RENFORCER LE POUVOIR VIS-À-VIS DES FOURNISSEURS** Une seule entreprise a peu de poids face à un gros fournisseur.

  On contribue à la création d'un effet de levier.

En groupe les :

- Exigences sont plus crédibles (sécurité, éthique, conformité)
- Fournisseurs sont incités à s'améliorer
- Standards deviennent plus homogènes

- **STANDARDISER LES PRATIQUES** Chaque entreprise peut avoir ses propres critères

  Une complexité inutile.

La mutualisation permet :

- Harmoniser les méthodes d'évaluation
- Simplifier les échanges avec les fournisseurs
- Faciliter la conformité réglementaire

ACCEDER A DES EXPERTISES AVANCEES Certaines analyses demandent des compétences pointues. (cybersécurité, etc)

Même les petites structures montent en maturité.

En mutualisant on:

- Accède à des experts spécialisés
- Bénéficie d'outils plus sophistiqués

EN RESUME

- **La gestion mutualisée du risque fournisseurs répond à un besoin simple :**
  - Faire mieux, plus vite et à moindre coût face à des risques de plus en plus complexes et interconnectés.

- **Elle transforme la gestion du risque**

D’une approche isolée et redondante ⇨ vers une approche collaborative, efficace et stratégique

TOUS CYBER VIGILANTS

JOURNÉE DE LA CYBERSÉCURITÉ

07 Avril 2026

sesan ÎLE-DE-FRANCE
Groupement d'Intérêt Public eSanté

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ars Agence Régionale de Santé Île-de-France

Quels moyens pour la cyber en période de restriction ?

Christophe MATTLER
Directeur de projet - DNS

Thomas AUBIN
RSSI du CHRU de Lille et du GHT Hôpitaux Publics Grand Lille, Président du Club des RSSI Santé

Rémi TILLY
Directeur du département Sécurité des Systèmes d'Information - SESAN

sesan
ILE-DE-FRANCE
Groupement d'Intérêt Public eSanté

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ars
Agence Régionale de Santé
Île-de-France

Quels moyens pour la cyber en période de restriction ?

Christophe MATTLER
Directeur de projet - DNS

sesan
Groupement d'Intérêt Public eSanté
RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité
ars Agence Régionale de Santé Île-de-France

Quels moyens pour la cyber en période de restriction ?

Thomas AUBIN
RSSI du CHRU de Lille et du GHT Hôpitaux Publics Grand Lille, Président du Club des RSSI Santé

sesan
Groupement d'Intérêt Public eSanté
RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité
ars
Agence Régionale de Santé
Île-de-France

Quels moyens pour la cyber en période de restriction ?

Rémi TILLY
Directeur du département Sécurité des Systèmes d'Information - SESAN

sesan
ILE-DE-FRANCE
Groupement d'Intérêt Public eSanté

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ars
Agence Régionale de Santé
Île-de-France

Clôture de la journée

Rémi TILLY
Directeur du département Sécurité des Systèmes d'Information - SESAN

sesan
ILE-DE-FRANCE
Groupement d'Intérêt Public eSanté

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ars
Agence Régionale de Santé
Île-de-France

MERCI
Pour votre participation