



Webinaire de présentation Domaine 1 Bis : Audits techniques : annuaires techniques et exposition sur internet

2 février 2026

**Programme CaRE : Cybersécurité accélération et Résilience
des Etablissements**

 **CaRE** Cybersécurité
accélération Résilience
des Etablissements

Webin- aire

Nos webinaires pour construire la
e-santé de demain !

• Nos intervenants



Christophe MATTLER
Directeur de programme



**MINISTÈRE
DU TRAVAIL, DE LA SANTÉ,
DES SOLIDARITÉS
ET DES FAMILLES**

*Liberté
Égalité
Fraternité*

Délégation au numérique
en santé



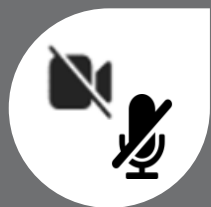
Steven GARNIER
Directeur de
domaine



Estelle NICAUD
Responsable de
mission



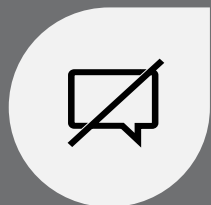
Webinaire, les bonnes pratiques



Le micro et la caméra sont automatiquement coupés sauf pour les intervenants.



Je pose mes **questions** dans l'espace Questions/Réponses.



Je ne pose **pas mes questions** dans l'espace conversation. Celles-ci ne seront pas traitées.

Déroulé du webinar

1. Introduction – Présentation du programme CaRE
2. Le Domaine 1 bis – Audits techniques : annuaires techniques et exposition sur internet
3. Comment candidater ?
4. Quels sont les objectifs à atteindre ?

1. Introduction – Présentation du programme CaRE



Ambition du programme

A court terme,
accompagner les
établissements à **être
plus résilients et
préparés** pour qu'ils
puissent faire face et
puissent s'organiser en
cas de cyberattaque.

A moyen terme, les
soutenir dans le
**renforcement de leur
sécurité opérationnelle.**

Axes du plan d'action



Gouvernance et résilience

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



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.



Sensibilisation


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



Sécurité Opérationnelle

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

• L'axe 4 : Sécurité opérationnelle



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.

Les domaines de financement

Domaine « Annuaire 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

2. Le Domaine 1 bis – Audits techniques : annuaires techniques et exposition sur internet

DOMAINE 1 bis

Candidature accessible
à tous

Valider les 2 prérequis cyber de SUN-ES

Des financements sur
atteinte d'objectifs

Atteindre les objectifs et en fournir les preuves

3 ACTEURS

ES

- Dépose officiellement sa candidature auprès de son ARS
- Travaille sur l'atteinte de ses objectifs
- Déclare à l'ARS l'atteinte des objectifs

ARS

- Vérifie la complétude des candidatures
- Favorise le développement des offres dans les CRRC
- Vérifie la complétude du dossier d'atteinte des objectifs déposé par les ES
- Sollicite l'ANS pour les opérations de contrôle

ANS

- Atteste de l'atteinte des objectifs d'un ES en effectuant des opérations de contrôle
- Finance l'ES si atteinte des objectifs



Pour chaque candidature validée, une convention sera signée entre l'ES candidat et l'ANS. Elle définit les droits et obligations réciproques des parties au titre du programme de financement.

- Critères d'éligibilité pour candidater

Je suis un ...

GHT



- Candidature unique portée par l'ES support pour l'ensemble des entités juridiques (EJ) du GHT



- La candidature nécessite le respect de la convention ou une validation en instance.

ES privé (EBNL et Lucratif)

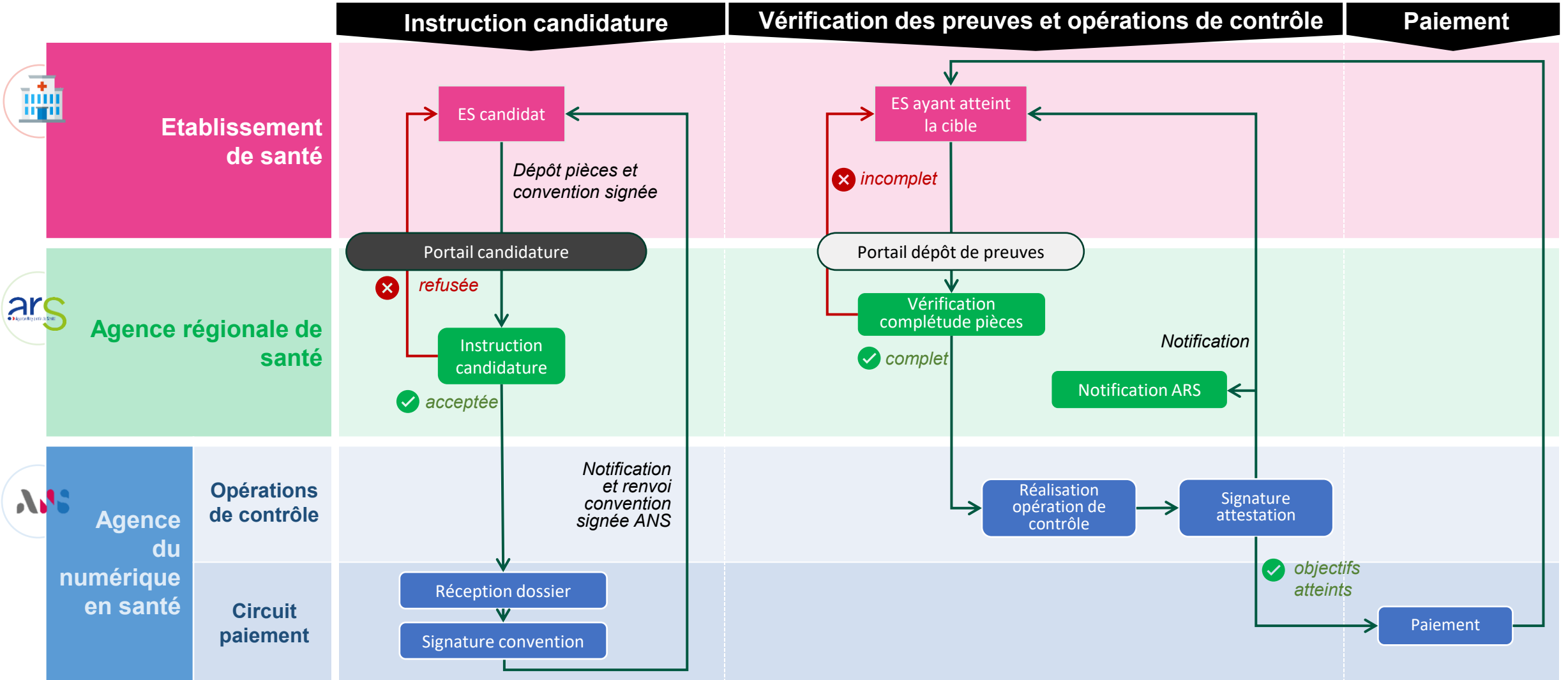


- Candidature unique portée par l'entité juridique (EJ) pour l'ensemble de ses ES-géographiques (EG)

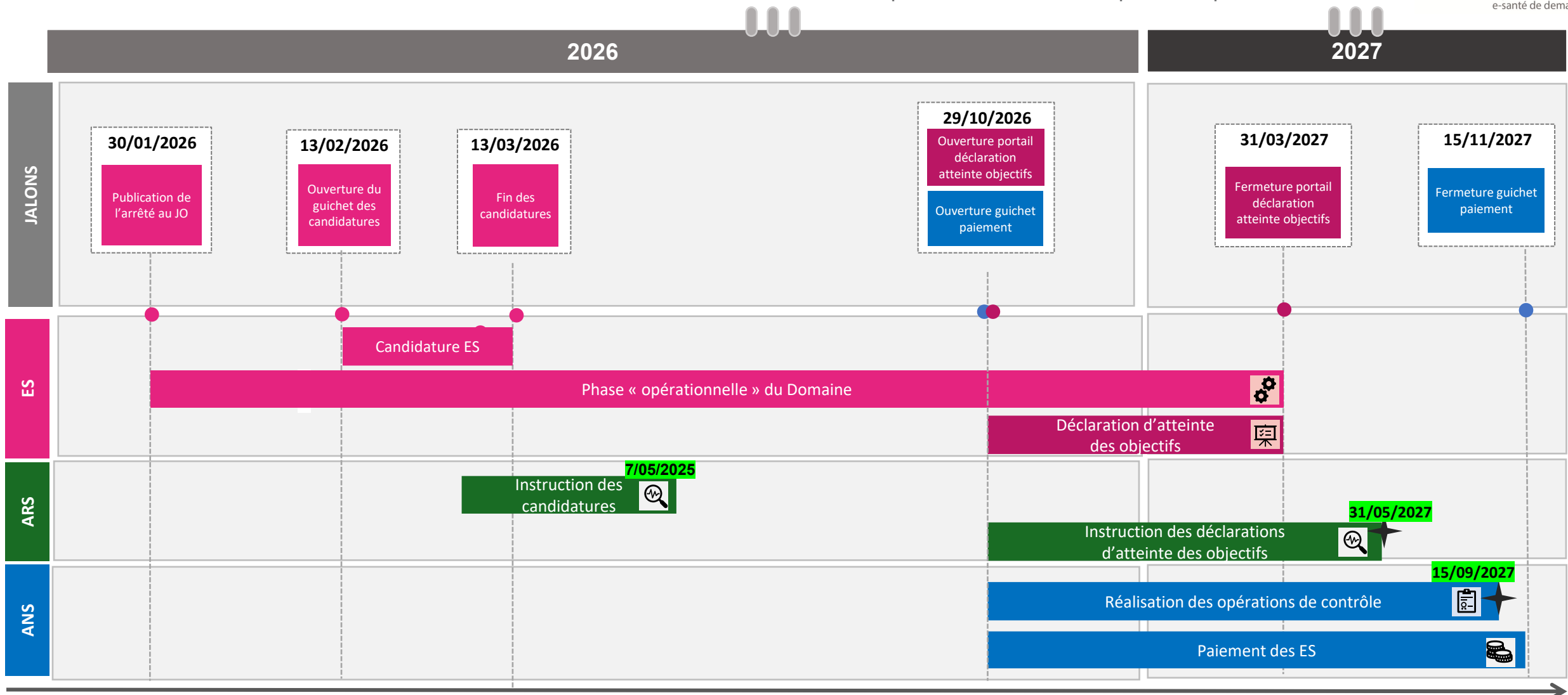


- Mon EJ à des EG localisées dans différentes régions => la candidature sera instruite par l'ARS de la région de l'EJ candidate

• Processus de candidature et de paiement



● Calendrier du domaine « Audits techniques : annuaires techniques et exposition sur internet »



3. Comment candidater ?



• Qui peut candidater ?



Rappel

Les structures **concernées** par le domaine D1 bis sont :

- **Le GHT des îles du Nord (Saint Martin et Saint Barthelemy)**
- **Les structures d'alternative à la dialyse en centre (code FINESS 146 – 82 entités juridiques au total)**

Le domaine 1 bis s'adresse **uniquement aux établissements définis répondant aux conditions fixées par l'arrêté.**
Il **n'adresse pas** les établissements éligibles au domaine 1 n'ayant **pas** candidaté ou soumis leur dépôt d'atteinte des objectifs.

Cas 1

Structures « nouvelles » qui n'étaient pas éligibles au D1

➤ Ces structures sont **éligibles**.

Cas 3

Structures hybrides ayant candidaté au D1 et atteint les objectifs pour l'ensemble de ses activités (y compris 146)

➤ Ces structures ne sont **pas éligibles**.

Cas 2

Structures hybrides avec une activité 146, et qui n'avaient pas candidaté au D1

➤ Ces structures sont **éligibles**.

Cas 4

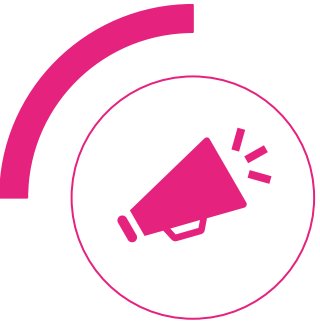
Structures hybrides candidates au D1 n'ayant pas intégré les structures portant une activité 146 dans leurs travaux.

➤ Ces structures sont **éligibles**.

- Modèle financier de l'appel à financement



Le modèle financier du domaine « Annuaire Technique et Exposition internet » est un modèle linéaire qui se base sur l'Activité Combinée et le nombre d'EJ composant le GHT pour les GHT et d'EG composant le candidat pour les autres établissements.

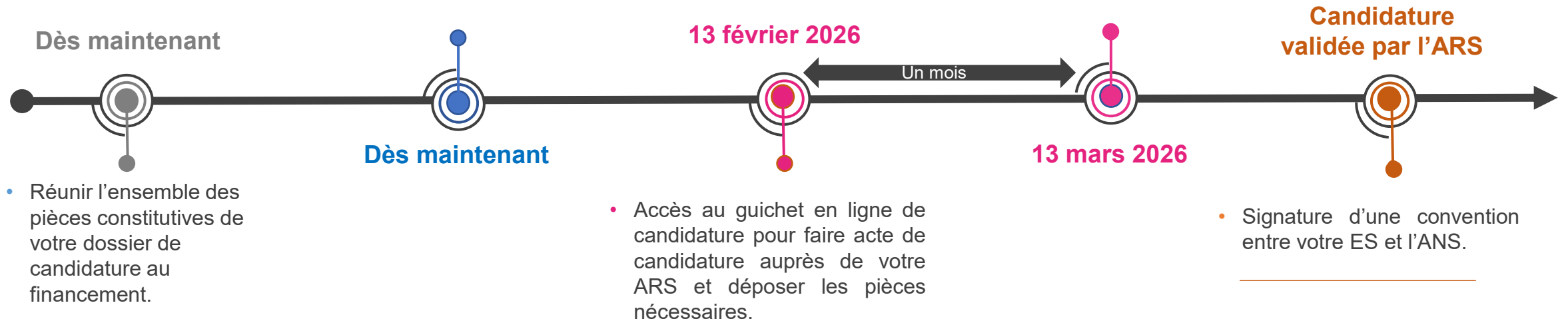


- Pour les **établissements ayant déjà candidaté dans le cadre de l'appel à financement initial**, le montant maximal de la subvention sera calculé avec la méthode présentée au paragraphe précédent, tenant compte des activités nouvellement éligibles, dont sera déduit le montant calculé sur la première candidature.
- Pour les établissements ayant déjà candidaté **dans le cadre de l'appel à financement initial**, le montant de financement pour le D1 bis peut être nul (0€) si le montant plafond cumulé D1 et D1 bis est inférieur ou égal au montant plafond défini pour le D1
- Le montant du financement alloué aux candidats sera calculé sur la base des **coûts réellement engagés** par l'établissement, à compter de la date de publication de l'arrêté au Journal Officiel, soit le **27 janvier 2026**, jusqu'à la déclaration d'atteinte des objectifs.
- Ce financement sera accordé dans la limite du montant plafond prévu, et ne pourra excéder les dépenses effectivement engagées sur la période concernée.

• Procédure de candidature

- Lancement des travaux nécessaire et possible dès à présent pour se préparer à atteindre les objectifs (inscription ANSSI, saisie OPSSIES...)

- Fermeture du guichet de dépôt des candidatures



- Réunir l'ensemble des pièces constitutives de votre dossier de candidature au financement.

- Accès au guichet en ligne de candidature pour faire acte de candidature auprès de votre ARS et déposer les pièces nécessaires.

- Signature d'une convention entre votre ES et l'ANS.



Pièces à fournir

- **Éléments administratifs** : Points de contact (DSI, RSSI, référent CaRE), informations bancaires pour le paiement
- Pièces justificatives pour les prérequis CaRE **si prérequis SUN-ES non atteints**

Prérequis pour candidater

Atteindre les deux prérequis liés à la sécurité des systèmes d'information prévus par le programme SUN-ES :

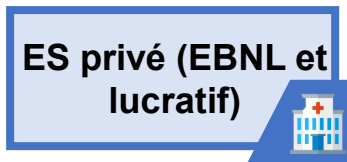
- ✓ **Prérequis PS2.1** - Présence d'une politique de sécurité et plan d'action SSI réalisé, existence d'un responsable sécurité
- ✓ **Prérequis PS2.2** - Cybersécurité : réalisation d'un audit externe de cybersurveillance

Je suis un ...



Prérequis SUN-ES pour :

- l'ES Support
- Les autres ES du GHT (dont l'activité combinée cumulée correspond à 90% de l'activité combinée du GHT)



Prérequis SUN-ES pour :

- Les EG composant l'EJ candidate (dont l'activité combinée cumulée correspond à 90% de l'activité combinée de l'EJ)

Liste des pièces à fournir

✓ **Vous avez déjà validé les prérequis SUN-ES ?**
Aucune pièce justificative à fournir



✓ **Vous n'avez pas validé les prérequis / candidaté SUN-ES :**

- Document présentant la **politique de sécurité des SI**
- **Procédure de remontée des incidents de sécurité**
- Organigramme incluant le RSSI
- Fourniture d'une attestation de la tenue d'au moins 2 rendez-vous annuels RSSI/Direction de l'établissement
- Fourniture d'une **attestation de réalisation de l'audit de cybersurveillance** (exposition sur internet) datant de moins de 2 ans.

- Un guichet de candidature unique : la plateforme eCaRE



Le guichet de candidature du Domaine 1 bis sera ouvert à partir du 13 février !

Les candidats qui souhaitent déposer leur candidature doivent se connecter à la plateforme eCaRE en utilisant le compte de la personne habilitée à représenter l'établissement dans le cadre de cette démarche.

Les infos importantes sur la plateforme eCaRE

- ▶ Pour rappel, pour des raisons de sécurité, un seul référent principal est autorisé par dossier. Il est toutefois possible d'ajouter des référents techniques et DAF/RH pour la phase de dépôt d'atteinte des objectifs.
- ▶ Si, au cours du dépôt ou après le dépôt du dossier, l'établissement souhaite modifier le référent dossier :
 - ▶ Le nouveau référent doit créer son compte sur la plateforme eCaRE en remplissant le formulaire d'inscription
 - ▶ Le référent actuel doit sélectionner ce collaborateur en tant que nouveau référent depuis la page "Votre compte" et confirmer le transfert du dossier. Suite à cette confirmation, le nouveau référent aura accès au dossier.



En cas de départ du référent initial sans transfert préalable du dossier au nouveau référent, la modification du référent dossier ne pourra plus être réalisée par l'établissement. Il sera nécessaire de contacter le support Convergence à l'adresse ans-support-convergence@esante.gouv.fr en indiquant le nom d'utilisateur du nouveau référent et la référence du dossier

Des difficultés à utiliser la plateforme ? Suivez le guide !

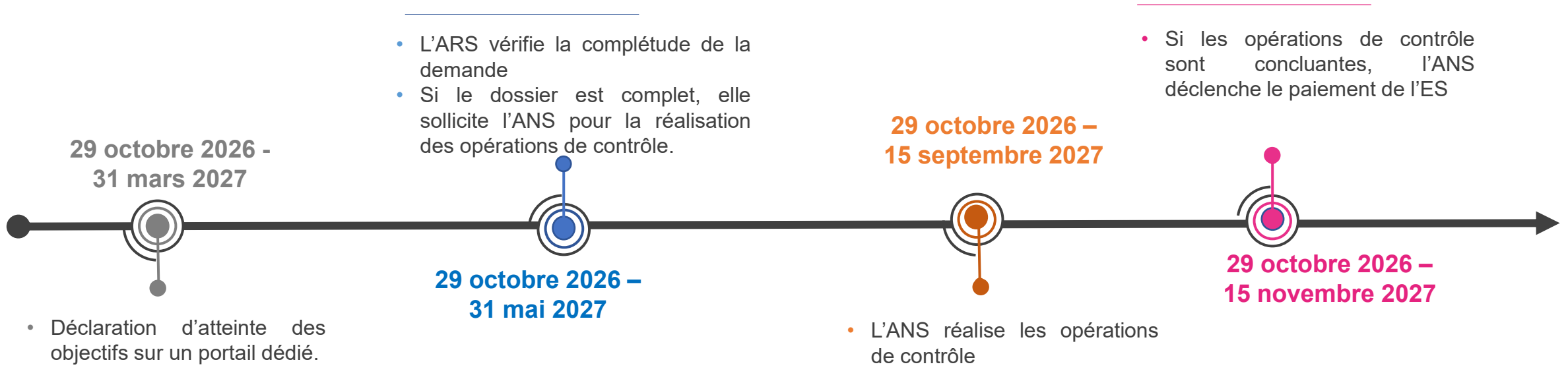
- ▶ Le guide d'utilisation eCaRE détaille toutes les étapes à suivre sur la plateforme
- ▶ Il est disponible sur la [page d'accueil de la plateforme Convergence](#) dans la section « Assistance »



4. Objectifs à atteindre



• Vérification des atteintes des objectifs



Les opérations de contrôle réalisées par l'ANS visent à vérifier que les ES candidats ont bien atteint les objectifs fixés, mais aussi à **l'éligibilité et la conformité des dépenses déclarées**.

Elles seront réalisées **via un contrôle sur pièces principalement**, possiblement accompagné d'échanges (à distance) avec l'établissement si **besoin de réaliser une analyse plus poussée**

• Objectifs à atteindre



Sont définies, pour chaque objectif, les valeurs cible et autres conditions minimales à réunir pour valider l'atteinte des objectifs.
Le détail des objectifs sera présenté ultérieurement dans le webinaire.

	Maîtrise de l'annuaire d'établissement	D1.O1.A	<ul style="list-style-type: none"> • Réaliser régulièrement des audits de tous les AD (Active Directory)
		D1.O1.B	<ul style="list-style-type: none"> • Atteindre un niveau de sécurisation minimum des AD (Active Directory)
	Maîtrise de l'exposition internet	D1.O2.A	<ul style="list-style-type: none"> • Réaliser régulièrement des audits de l'exposition internet
		D1.O2.B	<ul style="list-style-type: none"> • Atteindre un niveau de sécurisation minimum de son exposition sur internet
	Exercices Cyber	D1.O3	<ul style="list-style-type: none"> • Se préparer au risque cyber en réalisant un exercice de crise cyber
	Auto-évaluation en matière de maturité vis-à-vis des risques cyber	D1.O4	<ul style="list-style-type: none"> • S'auto-évaluer en matière de maturité vis-à-vis des risques cyber en remplissant tous les volets de l'oSIS
	Calculer la part du numérique dans le budget	D1.O5	<ul style="list-style-type: none"> • Calculer la part du budget dédiée au numérique dans le budget général de l'ES
	Convergence des GHT <i>(spécifique ES publics)</i>	D1.O6.A	<ul style="list-style-type: none"> • Piloter au niveau du GHT la réponse au programme et le suivi de l'atteinte des objectifs
		D1.O6.B	<ul style="list-style-type: none"> • Formaliser la stratégie du GHT en matière de convergence des AD

- **Objectif D1.O1 : Maitriser l'annuaire d'établissement**
Objectif D1.O1.A : Réaliser régulièrement des audits de tous les AD



Pourquoi ?

L'annuaire d'établissement est un élément critique permettant la gestion centralisée de l'ensemble des permissions sur les différents domaines qui composent un système d'information. **L'obtention de privilèges élevés sur l'annuaire entraîne par conséquent une prise de contrôle instantanée et complète de tout le SI.**

Un audit régulier des annuaires permet de contrôler les effets des actions de remédiation engagées et du maintien du niveau obtenu.

Détails de l'objectif

Réaliser régulièrement des audits de tous les AD

- Un **audit ADS** doit être réalisé **pour l'ensemble des annuaires des établissements** du candidat **en moyenne tous les 60 jours durant la phase opérationnelle, avec un intervalle d'au plus 100 jours entre deux audits consécutifs.**
- ***Phase opérationnelle** : Phase débutant sur une date comprise entre la date de publication de l'arrêté portant l'appel à financement et la date de validation de la candidature par l'ARS et finissant au dépôt de la déclaration d'atteinte des objectifs.*

Liste des pièces à fournir

- Description exhaustive des infrastructures AD et de leurs interconnexions
- Rapports des audits ADS réalisés

OUTIL D'AUDIT À UTILISER

Service Active Directory Security ADS ORADAD proposé par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI). **Ces audits sont disponibles pendant 6 mois et doivent être téléchargés par le candidat.**



- **Objectif D1.O1 : Maitriser l'annuaire d'établissement**
Objectif D1.O1.B : Atteindre un niveau de sécurisation minimum des AD



Pourquoi ?

L'annuaire d'établissement est un élément critique permettant la gestion centralisée de l'ensemble des permissions sur les différents domaines qui composent un système d'information. **L'obtention de privilèges élevés sur l'annuaire entraîne par conséquent une prise de contrôle instantanée et complète de tout le SI.**

Détails de l'objectif

Atteindre un score supérieur ou égal à 2 pour les 2 derniers audits ADS des différents AD.

Je suis un ...

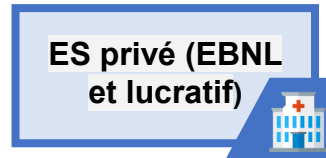


Pour tous les AD du GHT : absence de vulnérabilité critique et application des correctifs de sécurité associés.

Score des 2 derniers audits successifs ADS ≥ 2 pour tous les AD de l'établissement support

Si le GHT à plusieurs entités juridiques :

Score des 2 derniers audits successifs ADS ≥ 2 pour tous les AD d'au moins 2 établissements (FINESS EJ) pour un nombre d'établissement représentant au moins 66% de l'activité combinée du GHT



Pour tous les AD de l'EJ : absence de vulnérabilité critique et application des correctifs de sécurité associés.

Score des 2 derniers audits successifs ≥ 2 pour tous les AD de l'entité juridique (FINESS EJ)

Si l'EJ à plusieurs entités géographiques :

Score des 2 derniers audits successifs ≥ 2 pour tous les AD d'au moins 2 établissements (FINESS EG) pour un nombre d'établissements représentant au moins 66% de l'activité combinée de l'entité juridique

Liste des pièces à fournir

- 2 (ou 3) derniers rapports des audits ADS pour l'ensemble des AD du candidat

Remarque : le dernier audit doit être réalisé au plus 60 jours avant la soumission du dossier.

Remarque : si l'avant dernier n'est pas à la cible, l'antépénultième audit peut être soumis s'il a été réalisé dans les 60 jours avant le dernier audit.

OUTIL D'AUDIT À UTILISER

Service Active Directory Security ADS_ORADAD proposé par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)

- **Objectif D1.02 : Maitriser l'exposition internet**
Objectif D1.02.A : Réaliser régulièrement des audits de l'exposition internet



Pourquoi ?

Il est nécessaire de **mesurer régulièrement son niveau d'exposition sur internet** et de déployer des mesures adéquates **pour le maitriser** (correction des vulnérabilités)
 Un audit régulier de l'exposition internet permet de **contrôler les effets des actions de remédiation engagées** et du **maintien du niveau obtenu**.

Détails de l'objectif

Réaliser des audits de l'exposition Internet tous les 60 jours en moyenne durant la phase opérationnelle

- Un audit d'exposition internet doit être réalisé en moyenne tous les 60 jours durant la phase opérationnelle, avec un intervalle d'au plus 100 jours entre deux audits consécutifs, sur l'ensemble de la surface exposée par le candidat



- Pour l'ensemble des ES membres d'un GHT

ES privé (EBNL et lucratif)



- Pour l'ensemble des ES-géographiques d'une EJ candidate

+ *Phase opérationnelle : Phase opérationnelle : Phase débutant sur une date comprise entre la date de publication de l'arrêté portant l'appel à financement et la date de validation de la candidature par l'ARS et finissant au dépôt de la déclaration d'atteinte des objectifs.*

Liste des pièces à fournir

- Liste des domaines exposés
- Liste des adresses IP publiques
- Rapports des audits d'exposition internet réalisés

OUTIL D'AUDIT À UTILISER



Le candidat peut solliciter le service SILENE de l'Agence de Sécurité des Systèmes d'Information - ANSSI (sa souscription doit alors avoir été réalisée dans les 100 premiers jours de la phase opérationnelle). **Ces audits sont disponibles pendant 6 mois et doivent être téléchargés par le candidat.**

Des audits d'exposition industriels peuvent également permettre de justifier de l'atteinte de cet objectif à condition que les prestations délivrées soient conformes au cahier des charges publié par l'ANS (CERT Santé)

- **Objectif D1.O2 : Maitriser l'exposition internet**
Objectif D1.O2.B : Atteindre un niveau de sécurisation minimum de son exposition sur internet



Pourquoi ?

Il est nécessaire de **mesurer régulièrement son niveau d'exposition sur internet** et de déployer des mesures adéquates **pour le maitriser** (correction des vulnérabilités)

Détails de l'objectif

Absence de vulnérabilités critiques sur les 2 derniers audits d'exposition internet

- Un audit d'exposition internet doit être réalisé tous les 2 mois durant la phase opérationnelle.



Absence de vulnérabilités critiques sur les 2 derniers audits successifs d'exposition internet sur l'ensemble du périmètre

Liste des pièces à fournir

- 2 (ou 3) derniers rapports d'audit d'exposition internet (démontrant l'absence de vulnérabilité critique - CVSS supérieur à 9.0 - et des risques de niveau critique et l'application des correctifs de sécurité associés)
- Remarque : le dernier audit doit être réalisé au plus 60 jours avant la soumission du dossier
- Remarque : si l'avant dernier n'est pas à la cible, l'antépénultième audit peut être soumis s'il a été réalisé dans les 60 jours avant le dernier audit

OUTIL D'AUDIT À UTILISER

Des audits d'exposition industriels conformes au cahier des charges publié par l'ANS (CERT Santé)



Les rapports d'audit d'exposition internet réalisés par les industriels doivent être transmis dans le cadre du dossier d'atteinte des objectifs.

- **Objectif D1.03** : Se préparer au risque cyber



Pourquoi ?

Face à la menace, l'amélioration de la résilience numérique par l'entraînement à la gestion de crise cyber n'est plus seulement une opportunité, mais bien une nécessité pour toutes les organisations. A ce titre, il est nécessaire de réaliser un exercice de gestion de crise cyber a minima une fois par an pour tout ES.

Détails de l'objectif

Réaliser un exercice de gestion de crise cyber en utilisant les kits nationaux ANS.

- L'ensemble des établissements au sens FINESS PMSI devront avoir réalisé un exercice entre le **1^{er} janvier 2025** et la **date de dépôt** de la déclaration d'atteinte des objectifs :



100 % des entités juridiques ont réalisé un exercice de crise

ES privé (EBNL et lucratif)



100 % des entités géographiques ont réalisé un exercice de crise

Liste des pièces à fournir

- Rapport de réalisation de l'exercice sur la base du modèle fourni dans les kits ANS ou une attestation de réalisation par le prestataire, l'ARS ou le GRADeS

OUTIL À UTILISER

CLICK 

Exercice peut être réalisé sur la base des kits mis à disposition par l'ANS, qui s'appuient notamment sur la norme relative aux exercices (ISO 22398:2013).



- **Objectif D1.04** : S'auto-évaluer en matière de maturité vis-à-vis des risques cyber



Pourquoi ?

L'objectif est de donner aux établissements **les moyens de s'auto-évaluer** afin de leur permettre **d'identifier les actions prioritaires à mener** et de mieux orienter et piloter leur feuille de route, suivre les évolutions réglementaires et leurs impacts pour les établissements (directive NIS 2...)

Détails de l'objectif

Remplir tous les volets de l'oSIS pour alimenter l'OPSSIES

- 100 % des établissements du candidat (au sens FINESS PMSI) ont renseigné l'oSIS sur les champs suivants :
 - ▶ Part du budget numérique dans le budget global de l'ES
 - ▶ 90% des 43 mesures prioritaires doivent être complétées

Liste des pièces à fournir

- Aucun document.

OUTILS À UTILISER

- **oSIS** (Observatoire des Systèmes d'Information de Santé) pour la saisie des informations par les ES



- **Objectif D1.05** – Calculer la part du numérique dans le budget



Pourquoi ?

Dans les établissements de santé, le budget moyen dédié au numérique est de 1,6%, dont une proportion est ensuite dédiée à la sécurité des SI. Afin de permettre la planification et la réalisation d'actions efficaces au service de la sécurité des systèmes d'information, il est indispensable de consacrer une part suffisante du budget au numérique et à la sécurité des SI.

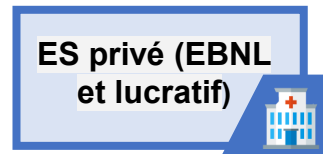
Détails de l'objectif

Calculer la part du budget dédiée au numérique dans le budget général des établissements et le nombre d'ETP dédié à la SSI (ces ETP incluent les ressources de la DSI ainsi que le RSSI)

La Part du budget dédiée au numérique et les ETP doivent être restitués au niveau d'une entité juridique (EJ) :



Les valeurs sont à renseigner pour chaque entité juridique constituant le GHT



Les valeurs sont à renseigner pour chaque entité géographique

Liste des pièces à fournir

- Aucun document.

OUTILS À UTILISER

- oSIS (Observatoire des Systèmes d'Information de Santé) pour la saisie des informations par les ES (mesures prioritaires 9 et 10)
- [Note d'information n° DGOS/PF2/2019/207 du 26 septembre 2019 relative à la définition et au suivi des ressources et des charges des systèmes d'information hospitaliers](#)



- **Objectif D1.O6: Renforcer la convergence des GHT**
Objectif D1.O6.A : Piloter au niveau du GHT la réponse au programme et le suivi de l'atteinte des objectifs



Pourquoi ?

Dans le cadre de la création des GHT prévue par la loi de modernisation de notre système de santé de 2016, il est prévu la mise en place de fonctions mutualisées obligatoires, dont la gestion commune d'un SI hospitalier convergent.

Détails de l'objectif

- **Le GHT doit mettre en place une organisation centralisée permettant d'atteindre les objectifs du programme.**
- **Intégrer dans le schéma directeur de convergence des SI du GHT les sujets AD comprenant les volets organisationnels et techniques.**

Le GHT doit :

- Désigner un référent du projet, nommé par le directeur de l'établissement support de GHT, dont le rôle sera de :
 - Suivre la bonne réalisation des audits AD et d'exposition internet
 - Veiller à la bonne exécution de l'exercice de gestion de crise
 - Veiller au bon remplissage de l'oSIS dont notamment la part du numérique dans le budget
- Mettre en place une équipe opérationnelle unique pour la gestion des AD au niveau du GHT en charge de la réalisation des audits et des actions de remédiation associées
- Mettre en place la gouvernance transverse du projet CaRE l'ensemble du GHT, assurant notamment la coordination du référent, de la DSI, du RSSI et de l'équipe opérationnelle

Liste des pièces à fournir

- Constitution de l'équipe projet
- Schéma de le gouvernance mise en place

- **Objectif D1.O6: Renforcer la convergence des GHT**
Objectif D1.O6.B : Formaliser la stratégie du GHT en matière de convergence des AD



Pourquoi ?

Cet objectif doit permettre à court terme de fédérer à travers une approche globale et la mise en place de bonnes pratiques, puis dans un second temps (au-delà du domaine 1), de poser les enjeux de financement pour mener à bien ce projet.

Détails de l'objectif

- **La trajectoire de convergence du GHT doit intégrer les modalités de travail et actions permettant d'aboutir au schéma de convergence défini au niveau du GHT.**

Le GHT doit formaliser, présenter et faire valider par le comité stratégique du GHT :

- Un document précisant les modalités de convergence de l'infrastructure AD du GHT
- Ce document est élaboré au niveau du GHT et validé par la Direction de l'établissement support du GHT et la DSI de l'établissement support du GHT
- Ce document comprend un planning projet prévoyant une trajectoire de convergence de l'infrastructure AD à une échéance maximale de 18 mois post appel à financement D1, les modalités organisationnelles devant être mises en œuvre (existence d'un responsable et mutualisation des équipes SI dédiées à ces sujets) et le budget prévisionnel nécessaire au projet.
- Ce document est transmis pour permettre de prendre en compte le projet décrit par le GHT et de définir avec l'établissement les modalités de mise en œuvre.

Liste des pièces à fournir

- Trajectoire de convergence des AD qui adresse l'ensemble des établissements du GHT

• Synthèse des coûts éligibles

Dépenses non éligibles

Type de dépense	Intitulé	Remarque
Frais de déplacement	Frais liés aux déplacements des professionnels au sein des établissements du candidat : forfait kilométrique, ticket de péage, facture d'essence, note de restaurant, etc.	
Formation des collaborateurs	Frais associés à la réalisation de formations générales en cybersécurité	Non éligible si ces formations ne contribuent pas directement à l'atteinte des objectifs..
Dépenses liées à l'organisation d'évent. / com.	Frais d'impression, de réalisation de campagnes de communication et/ou d'achats de prestation de restauration	
Achat de matériel informatique courant	Frais d'achats de matériel informatique courant : ordinateur, téléphone, borne wifi, imprimante, etc.	
Frais récurrent de fonctionnement	Dépenses et abonnements récurrents permettant le fonctionnement nominal de la structure : abonnement internet, coûts d'électricité, etc.	
Coûts de convergence des AD	Dépenses et investissements engagés pour mettre en œuvre la convergence des AD (pour les GHT)	Seuls les frais de définition de la stratégie sont éligibles.

Dépenses éligibles

Type de dépense	Intitulé	Remarque
Prestations externes	Ensemble des frais de prestations intellectuelles externes permettant d'accompagner le candidat dans l'atteinte des objectifs et la production des documents.	
Remédiation des niveaux de sécurité de l'AD / exposition internet	Ensemble des coûts mis en œuvre (prestations, acquisition ou investissement logiciel) pour remédier à un niveau de sécurité inférieur aux objectifs fixés dans le domaine, ou soutenir la convergence des AD	Si et seulement si ces coûts s'inscrivent dans le respect des objectifs définis pour le domaine.
Investissement logiciel	Ensemble des coûts d'investissement logiciel, y compris des frais d'abonnement, acquittés pour contribuer à l'atteinte des objectifs (hors objectif D6)	Les dépenses préexistantes au lancement du dispositif ne sont pas éligibles.
Coûts internes	Ensemble des coûts induits par la mobilisation de personnels de l'établissement pour permettre l'atteinte des objectifs.	

- Ressources à mobiliser : Accompagnement par vos CRRC

Les CRRC proposent des services mutualisés et personnalisables, pour mieux prévenir et gérer la cybersécurité des établissements de santé



Objectifs et services du CRRC pour les structures :



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












Nous vous invitons à vous rapprocher de vos CRRC pour vous faire accompagner sur le domaine 1 bis

[Ressources et mutualisation | e-santé](#)

- Ressources à mobiliser

Une sélection de ressources documentaires est mise à disposition des candidats dans le cadre du domaine 1 bis du programme CaRE

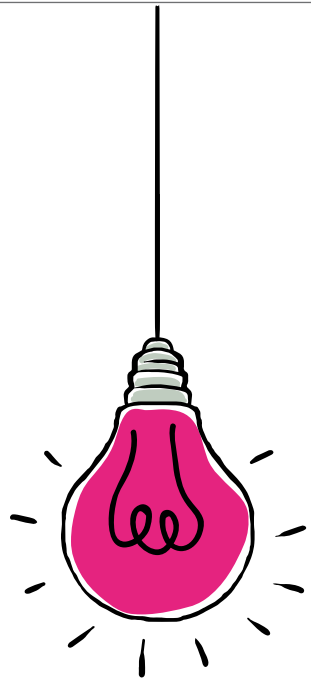
-  [Arrêté du 27 janvier 2026](#)
-  [Replay du webinaire du 11/04/2025](#)
-  [Base des ES recensés](#)
-  [Guide des prérequis et objectifs du domaine 1 bis](#)
-  [Catalogue des offres cyber](#)
-  [Fiche de présentation ADS](#)
-  [Fiche de présentation SILENE](#)
-  [Site ANS : Ressources et Mutualisation \(CRRC\)](#)
-  [Cahier des charges pour l'audit d'exposition internet](#)



Pour toute demande autour du programme, les établissements sont invités à utiliser le support mis en place par l'ANS.

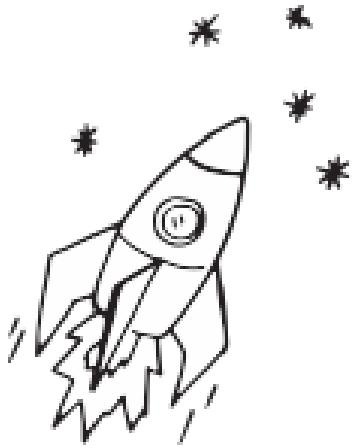


Page web dédiée au Programme CaRE sur le site de l'ANS : <https://esante.gouv.fr/strategie-nationale/CaRE>



Ce webinaire est enregistré et le replay sera mis à disposition sur la chaîne Youtube de l'ANS





**MERCI POUR VOTRE ATTENTION
ET A BIENTÔT SUR LE PROGRAMME**

Annexes



- Ajustements des modalités de contrôle et dispositif d'atteinte partielle des objectifs

Un **ajustement des modalités de contrôle** et un **dispositif d'atteinte partielle** ont été mis en place dans le cadre du domaine 1 afin de prendre en compte les éventuelles difficultés opérationnelles ou divergence d'interprétation des règles définies au lancement du domaine. Cet ajustement et ce dispositif **s'appliquent également au Domaine 1bis**.

Une note explicative est disponible au lien [suivant](#).

Le barème de cette décote est le suivant, considérant que la décote appliquée au montant plafond des candidats est cumulative selon le nombre d'objectif non-atteint :

Objectif / Sous-objectif	% de décote en cas de non-atteinte
D1.O1. A : Réaliser régulièrement des audits de tous les AD (objectif sur la fréquence)	10%
D1.O1.B : Atteindre un niveau de sécurisation minimum des AD	100% (pas de subvention)
D1.O2.A : Réaliser régulièrement des audits d'exposition sur internet (objectif sur la fréquence)	10%
D1.O2.B : Atteindre un niveau de sécurisation minimum de son exposition sur internet	
Pour un nombre d'établissements représentant entre 90% et 66% de l'activité combinée	15%
Pour un nombre d'établissements représentant moins que 66% de l'activité combinée	100% (pas de subvention)
D1.O3 : Se préparer au risque Cyber (exercice de crise)	10%
D1.O4 : S'autoévaluer en matière de maturité vis-à-vis des risques cyber (remplissage Osis)	2,5%
D1.O5 : Calculer le budget dédié au numérique	2,5%
D1.O6 : Renforcer la convergence des GHT	5% pour un candidat GHT Non applicable pour les autres candidats



esante.gouv.fr

Le portail pour accéder à l'ensemble des services et produits de l'Agence du Numérique en Santé et s'informer sur l'actualité de la e-santé.

 **[@esante_gouv_fr](https://twitter.com/esante_gouv_fr)**

 **linkedin.com/company/agence-du-numerique-en-sante**