

« Guide des prérequis et objectifs

Appel à Financement n°1bis - Fonction « Annuaire techniques et exposition sur internet » - périmètre complémentaire



Historique du document – Suivi des modifications apportées			
Version	Date	Auteur	Commentaires / modifications
V1	02/02/2026	Equipe programme CaRE	Version initiale

SOMMAIRE

1	Objectif de ce guide	3
2	Prérequis du domaine 1.....	5
2.1	D1.P1 : Atteindre les prérequis de sécurité des systèmes d'information prévus par le programme SUN-ES	5
3	Eligibilité des dépenses.....	7
4	Objectifs du domaine 1	8
4.1	D1.O1 – Maitriser l’annuaire d’établissement	8
	<i>D1.O1.A - Réaliser régulièrement des audits de tous les AD</i>	<i>8</i>
	<i>D1.O1.B - Atteindre un niveau de sécurisation minimum des AD.....</i>	<i>10</i>
	D1.O2 – Maitriser l’exposition internet.....	12
	<i>D1.O2.A - Réaliser régulièrement des audits de l’exposition internet.....</i>	<i>12</i>
	<i>D1.O2.B – Atteindre un niveau de sécurisation minimum de son exposition sur internet</i>	<i>14</i>
	D1.O3 – Se préparer au risque cyber	16
	D1.O4 – S’auto-évaluer en matière de maturité vis-à-vis des risques cyber	17
	D1.O5 – Calculer le budget dédié au numérique.....	18
	D1.O6 – Renforcer la convergence des GHT	20
	<i>D1.O6.A - Piloter au niveau du GHT la réponse au programme et le suivi de l’atteinte des objectifs..</i>	<i>20</i>
	<i>D1.O6.B - Formaliser la stratégie du GHT en matière de convergence des AD</i>	<i>22</i>
5	atteinte partielle et des objectifs et financements associés.....	24

1 OBJECTIF DE CE GUIDE

L'objectif de ce guide est de détailler les prérequis et objectifs du domaine « Annuaire techniques et exposition sur internet » - périmètre complémentaire.

Pour rappel et conformément à l'arrêté du 27 janvier 2026 relatif à un programme de financement destiné à renforcer la sécurité numérique des établissements de santé - Fonction « Annuaire techniques et exposition sur internet » - périmètre complémentaire (l'Arrêté dans la suite du guide), les structures autorisées à déposer des candidatures au financement pour le compte des établissements éligibles sont définies en fonction du statut des établissements éligibles :

- **Pour établissements éligibles publics** : dans le cadre d'un GHT, l'établissement support du GHT candidate pour l'ensemble des EJ sanitaires du groupement dans le respect de la convention constitutive du GHT présentant ses compétences et ses instances décisionnelles, ou le cas échéant, avec une autorisation octroyée lors d'une instance décisionnelle.
- **Pour les établissements privés (lucratifs et à but non lucratif)**, la demande de candidature au financement doit être portée par l'entité juridique pour l'ensemble de ses établissements géographiques.

Les prérequis et objectifs fixés dans le cadre de ce domaine doivent être traités, sauf mention contraire, par les candidats indépendamment de leur statut. La mention candidat, constitue une mention générique qui traite l'ensemble des cas précités.

Ci-dessous, le tableau récapitulatif des prérequis et objectifs de l'appel à financement « Annuaire techniques et exposition sur internet ».

L'objectif de ce guide est de présenter de manière détaillée les prérequis et objectifs du domaine 1 bis dont le récapitulatif est précisé dans le tableau ci-dessous :

Prérequis	N°	Intitulé prérequis		Détails	Détails
	D1.P1	Atteindre les prérequis de sécurité des systèmes d'information prévus par le programme SUN-ES			Les prérequis Cyber figurant dans SUN-ES sont atteints (prérequis PS2.1 et PS2.2)
Objectifs	N°	Intitulé objectifs	N°	Intitulé sous-objets	Détails
	D1.01	Maîtriser l'annuaire d'établissement	D1.01.A	Réaliser régulièrement des audits de tous les AD	Réaliser des audits AD tous les 2 mois durant la phase opérationnelle
			D1.01.B	Atteindre un niveau de sécurisation minimum des AD	Atteindre un score supérieur ou égale à 2 sur les 2 derniers audits de chaque AD
	D1.02	Maîtriser l'exposition internet	D1.02.A	Réaliser régulièrement des audits de l'exposition internet	Réaliser des audits de l'exposition internet tous les 2 mois durant la phase opérationnelle
			D1.02.B	Atteindre un niveau de sécurisation minimum de son exposition internet	Absence de vulnérabilité critiques sur les 2 derniers audits d'exposition internet
	D1.03	Se préparer au risque cyber			Réaliser un exercice de gestion de crise cyber en utilisant les kits nationaux ANS
	D1.04	S'auto-évaluer en matière de maturité vis-à-vis des risques cyber			Remplir tous les volets de l'oSIS pour alimenter l'OPSSIES
D1.05	Calculer le budget dédié au numérique			Calculer la part du budget dédié au numérique dans le budget général de l'ES	

	D1.06 <i>GHT</i>	Renforcer la convergence des GHT <i>(spécifique ES publics)</i>	D1.06.A	Piloter au niveau du GHT la réponse au programme et le suivi de l'atteinte des objectifs	Désigner un responsable de projet au niveau du GHT avec formalisation d'une lettre de mission.
			D1.06.B	Formaliser la stratégie du GHT en matière de convergence AD	Intégrer dans le schéma directeur de convergence des SI du GHT les sujets AD comprenant les volets organisationnel et technique.

Dans la suite du document, les prérequis et objectifs sont décrits dans des fiches synthétiques composées :

- D'une définition.
- De la méthode de production de l'indicateur.
- Des modalités de restitution (pour vérifier leur bonne atteinte).

La phase opérationnelle est la phase comprise entre :

- Une date déterminée par l'établissement comprise entre (i) la date de publication de l'Arrêté, et (ii) la date de validation de la candidature par l'Agence Régionale de Santé du candidat ;
- Le dépôt de la déclaration d'atteinte des objectifs par le candidat sur le guichet dédié.

2 PREREQUIS DU DOMAINE 1

2.1 D1.P1 : Atteindre les prérequis de sécurité des systèmes d'information prévus par le programme SUN-ES

Domaine	Domaine 1
Prérequis	Atteindre les prérequis de sécurité des systèmes d'information prévus par le programme SUN-ES
1. Définition du prérequis	
Définition	<p>L'établissement de santé (ES) doit avoir validé les 2 prérequis liés à la sécurité des systèmes d'information qui figurent dans le programme SUN-ES :</p> <ul style="list-style-type: none"> • Prérequis PS2.1 - Présence d'une politique de sécurité et plan d'action SSI réalisé, existence d'un responsable sécurité (reprise à l'identique du P2.4 HOP'EN) • Prérequis PS2.2 - Cybersécurité : réalisation d'un audit externe de cybersurveillance (extension du P2.5 HOP'EN)
Valeur cible / seuil d'éligibilité	<p>Pour les GHT, il est nécessaire que</p> <ul style="list-style-type: none"> • Ce prérequis soit atteint par l'établissement support du GHT (FINESS EJ) ; • Les établissements du GHT (FINESS EJ) qui ont validé les prérequis PS2.1 et PS2.2 représentent au moins 90% de l'activité combinée du GHT. <p>Pour les établissements privés (à but non lucratif et lucratif), il est nécessaire que :</p> <ul style="list-style-type: none"> • Les établissements (FINESS EG) qui ont validé les prérequis PS2.1 et PS2.2 représentent au moins 90% de l'activité combinée de l'entité juridique porteuse de la candidature.
Textes de référence	Guide des prérequis - Programme SUN-ES - volet 1 et 2

2. Production de l'objectif

Unité	Booléen (O/N)
Modalité de calcul	<ul style="list-style-type: none"> • N/A
Période	<ul style="list-style-type: none"> • Au moment de la candidature
Fréquence	<ul style="list-style-type: none"> • N/A

3. Restitution de l'objectif

<p>Remontée de l'information</p>	<p>Pour les établissements ayant une candidature validée au programme SUN-ES :</p> <ul style="list-style-type: none"> • Aucune remontée nécessaire : données consolidées déjà disponibles au niveau national <p>Pour les établissements n'ayant pas une candidature validée au programme SUN-ES :</p> <ul style="list-style-type: none"> • Dépôt des pièces justificatives sur la plateforme de candidature
<p>Documents justificatifs</p>	<p>Pour les établissements ayant une candidature validée au programme SUN-ES :</p> <ul style="list-style-type: none"> • Aucun document <p>Pour les établissements n'ayant pas une candidature validée au programme SUN-ES :</p> <ul style="list-style-type: none"> • Liste des documents exigées pour les prérequis PS2.1 et PS2.2 de SUN-ES : <ul style="list-style-type: none"> ○ Document présentant la politique de sécurité décrivant notamment l'analyse des risques détaillée, l plan d'action associé en lien avec le plan d'action SSI de l'instruction 309 du 14 octobre 2016 (datant de moins de 3 ans) et la fonction de responsable sécurité des SI (RSSI) ○ Procédure de remontée des incidents de sécurité (Art. L.1111- 8-2 CSP). ○ Organigramme mettant en évidence le positionnement du RSSI, préconisé en dehors de la DSI" par exemple rattaché à la cellule qualité. ○ Fourniture d'une attestation de la tenue d'au moins 2 rendez-vous annuels RSSI/Direction de l'établissement avec à l'ordre du jour a minima : le suivi du plan d'actions SSI et le suivi de la remontée des incidents de sécurité ○ Fourniture d'une attestation de réalisation de l'audit de cybersurveillance (exposition sur internet) par le prestataire et signée par le directeur d'établissement et datant de moins de 2 ans
<p>Opération de contrôle</p>	<ul style="list-style-type: none"> • Contrôle sur pièces

3 ELIGIBITE DES DEPENSES

Les subventions allouées à travers le présent dispositif ont pour objectif de concentrer le soutien financier sur des actions concourant à des objectifs précis favorisant la sécurité des SI des établissements de santé, dont l'atteinte est mesurée par des indicateurs. Les subventions sont allouées après vérification par l'ANS de l'atteinte de ces indicateurs et du respect des modalités administratives et ne font pas l'objet d'un amorçage.

L'ensemble des dépenses réalisées pendant la phase opérationnelle pour contribuer à l'atteinte des objectifs du Domaine 1bis sont éligibles à un subventionnement. A titre d'exemple, le recours à la prestation externe, les coûts engendrés par la réalisation d'audit, et les coûts induits pour remédier aux failles de sécurité identifiées sont éligibles. Il est à noter que l'ensemble des dépenses réalisées durant la phase opérationnelle et concourant à l'atteinte des objectifs du domaines sont éligibles à un financement.

Les coûts associés à la mobilisation des ressources humaines du candidat sont également éligibles. Néanmoins, il est à souligner que ces coûts doivent être explicitement justifiés au regard des activités du programme. À ce titre, il est recommandé aux établissements de privilégier :

- les dépenses associées à un recrutement spécifique dans le cadre du programme,
- la formation des professionnels si les actions de formation ont permis de contribuer directement à l'atteinte d'un objectif du présent domaine (par exemple, la formation spécifique d'un professionnel de l'établissement disposant d'une lettre de mission),

Il est rappelé que les subventions allouées dans le cadre du programme doivent nécessairement couvrir des dépenses nouvelles. Les établissements ne peuvent donc pas valoriser des dépenses déjà engagées ou financées par d'autres dispositifs. En particulier, les établissements déjà financé au titre de l'appel à financement « Annuaire techniques et exposition sur internet » (domaine n°1) créé par l'arrêté du 18 mars 2024 ne pourront redéclarer des actions et dépenses sur les composants déjà mis en conformité avec les objectifs dans le cadre de ce précédent dispositif.

Une trame de justification des coûts sera également fournie.

4 OBJECTIFS DU DOMAINE 1

4.1 D1.O1 – Maitriser l’annuaire d’établissement

D1.O1.A - Réaliser régulièrement des audits de tous les AD

Domaine	Domaine 1
Objectif	Réaliser régulièrement des audits de tous les AD
1. Définition de l’objectif	
Définition	<p>Un audit ADS (porté par l'ANSSI) doit être réalisé pour l’ensemble des annuaires des établissements du candidat en moyenne tous les 60 jours durant la phase opérationnelle.</p> <p>NB : Les annuaires AD locaux ou en mode hybride (AD local avec recopie dans le cloud) sont concernés par cet objectif. Sous réserve de la mise à disposition par l'ANSSI d'un outil adapté aux AD hébergés complètement dans le cloud, ces annuaires hébergés dans le cloud sont également concernés par cet objectif.</p> <p>NB 2 : Pour les établissements ne possédant pas AD, et ayant un projet d'implémentation, au début de la phase opérationnelle, ceux-ci doivent se signaler auprès de leur ARS. Ils devront s'inscrire au plus tôt au club SSI de l'ANSSI pour réaliser des audits réguliers de l'AD.</p> <p>NB 3 : Pour les établissements possédant un AD de type EntraID sans hybridation et en fonction de la disponibilité de l'outil ORADAZ adapté ceux-ci devront s'inscrire à ce service au plus tôt auprès de l'ANSSI pour réaliser des audits réguliers de l'AD après s'être signalés auprès leur ARS.</p> <p>NB 4 : Les résultats des audits ADS réalisés par l'ANSSI sont disponibles pendant 6 mois suite à leur réalisation. Les candidats sont invités à télécharger régulièrement les résultats d'audits sur la plateforme de l'ANSSI pour pouvoir les déposer dans le guichet de dépôt d'atteinte des objectifs.</p> <p>Phase opérationnelle : Phase opérationnelle : La phase opérationnelle est la période pendant laquelle l'établissement doit respecter la fréquence imposée par les objectifs O1.A et O2.A.</p> <ul style="list-style-type: none"> Le démarrage de la phase opérationnelle doit être compris entre (i) la date de publication de l'Arrêté et (ii) la date de validation de la candidature par l'Agence Régionale de Santé du candidat. Elle est déterminée par l'ES selon l'avancement de ses travaux La phase opérationnelle s'achève au dépôt de la déclaration d'atteinte des objectifs par l'établissement sur le guichet dédié.
Valeur cible / seuil d'éligibilité	<p>Nombre d'audits réalisés sur chaque AD :</p> <ul style="list-style-type: none"> Du GHT pour les établissements publics membres d'un GHT De l'entité juridique pour les établissements privés
Textes de référence	Le service ADS

2. Production de l'indicateur

Unité	Booléen
Modalité de calcul	<p>Pour chaque annuaire d'établissement :</p> <ul style="list-style-type: none"> L'intervalle entre 2 audits doit être en moyenne de 60 jours maximum L'intervalle entre 2 audits consécutifs doit être inférieur à 100 jours.
Période	<ul style="list-style-type: none"> Sur la durée de l'appel à financement (phase opérationnelle)
Fréquence	<ul style="list-style-type: none"> Une fois lors du dépôt de preuve

3. Restitution de l'objectif

Remontée de l'information	<ul style="list-style-type: none"> Dépôt sur le guichet de déclaration d'atteinte des objectifs
Documents justificatifs	<ul style="list-style-type: none"> Description exhaustive des infrastructures AD et de leurs interconnexions Rapports des audits ADS réalisés
Opération de contrôle	<p>Eléments contrôlés :</p> <ul style="list-style-type: none"> Contrôle de l'exhaustivité de la déclaration des annuaires AD en lien avec les rapports fournis Vérification de la réalisation d'audits à la fréquence cible.

D1.01.B - Atteindre un niveau de sécurisation minimum des AD

Domaine	Domaine 1
Objectif	Atteindre un niveau de sécurisation minimum des AD
1. Définition de l'objectif	
Définition	<p>L'audit des AD se traduit par l'évaluation du niveau de sécurité de la configuration de l'Active Directory, via une échelle de 1 à 5. Le niveau obtenu dépend de la gravité des vulnérabilités trouvées, le niveau 1 correspondant au niveau de plus forte criticité et le niveau 5 correspondant au niveau à l'état de l'art. Chaque niveau donne accès à une liste de recommandations adaptées pour corriger les problèmes importants (vulnérabilité critiques) et autres points d'attention à intégrer. L'application de l'ensemble des recommandations portant sur les points importants d'un niveau permet de passer au niveau supérieur et d'accéder à une collection complémentaire de recommandations.</p> <p>Un score supérieur ou égal à 2 doit être obtenu pour les deux derniers audits ADS des différents AD.</p> <p>Il est cependant rappelé que les préconisations de l'ANSSI recommandent l'atteinte d'un score de 3 a minima.</p>
Valeur cible / seuil d'éligibilité	<p>Cible à atteindre :</p> <p>Un score supérieur ou égal à 2 doit être obtenu pour les 2 derniers audits ADS des différents AD, selon les règles ci-dessous :</p> <p>Pour les GHT :</p> <ul style="list-style-type: none"> • Score des 2 derniers audits successifs ADS ≥ 2 pour tous les AD de l'établissement support <p>ET</p> <ul style="list-style-type: none"> • Si le GHT à plusieurs entités juridiques (FINESS EJ) <ul style="list-style-type: none"> ○ Score des 2 derniers audits successifs ADS ≥ 2 pour tous les AD d'au moins 2 établissements (FINESS EJ) pour un nombre d'établissements représentant au moins 66% de l'activité combinée du GHT <p>NB : Une entité juridique (EJ) est considérée « à la cible » à condition que l'ensemble de ses infrastructures AD ait un score ≥ 2</p> <p>Pour les établissements privés :</p> <ul style="list-style-type: none"> • Score des 2 derniers audits successifs ≥ 2 pour tous les AD de l'entité juridique (FINESS EJ) <p>ET</p> <ul style="list-style-type: none"> • Si l'EJ à plusieurs entités géographiques (FINESS EG) <ul style="list-style-type: none"> ○ 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 <p>NB : Une entité géographique (EG) est considérée « à la cible » à condition que l'ensemble de ses infrastructures AD ait un score ≥ 2</p>

	<p>NB 2 : Au moment de la déclaration d'atteinte des objectifs sur le guichet dédié, le dernier audit ADS réalisé devra dater de 60 jours</p> <p>NB 3 : Dans le cas où l'avant-dernier audit n'est pas à la cible, il n'est pas pris en compte dans la validation de l'atteinte de l'objectif. L'antépénultième audit est alors considéré si et seulement s'il a été réalisé moins de 60 jours avant la réalisation du dernier audit.</p>
Textes de référence	Le service ADS

2. Production de l'indicateur

Unité	Booléen
Modalité de calcul	<p>Pour chaque annuaire d'établissement soumis par l'EJ candidat :</p> <ul style="list-style-type: none"> Score audit ADS ≥ 2 sur les 2 derniers audits successifs, ou pour le dernier et l'antépénultième audit si l'avant-dernier audit n'est pas à la cible.
Période	<ul style="list-style-type: none"> Sur la durée de l'appel à financement (phase opérationnelle)
Fréquence	<ul style="list-style-type: none"> Une fois lors du dépôt de preuve

3. Restitution de l'objectif

Remontée de l'information	<ul style="list-style-type: none"> Dépôt sur le guichet de déclaration d'atteinte des objectifs
Documents justificatifs	<ul style="list-style-type: none"> 2 (ou 3) derniers rapports des audits ADS pour l'ensemble des AD du candidat
Opération de contrôle	<p>Eléments contrôlés :</p> <ul style="list-style-type: none"> Vérification de l'atteinte du score cible sur les deux derniers audits pour tous les AD, ou le dernier et l'antépénultième audit Contrôle du pourcentage de l'activité combinée couverte par l'ensemble des AD ayant atteint l'objectif ; Contrôle des rapports détaillés.

D1.O2 – Maitriser l'exposition internet

D1.O2.A - Réaliser régulièrement des audits de l'exposition internet

Domaine	Domaine 1
Objectif	Réaliser régulièrement des audits de l'exposition internet
1. Définition de l'objectif	
Définition	<p>Un audit d'exposition internet doit être réalisé tous les deux mois durant la phase opérationnelle.</p> <p><u>Phase opérationnelle</u> : Phase opérationnelle : La phase opérationnelle est la période pendant laquelle l'établissement doit respecter la fréquence imposée par les objectifs O1.A et O2.A.</p> <ul style="list-style-type: none"> Le démarrage de la phase opérationnelle doit être comprise entre (i) la date de publication de l'Arrêté, et (ii) la date de validation de la candidature par l'Agence Régionale de Santé du candidat. Elle est déterminée par l'ES selon l'avancement de ses travaux ; La phase opérationnelle s'achève au dépôt de la déclaration d'atteinte des objectifs par l'établissement sur le guichet dédié. <p>Pour réaliser cet audit, il est possible de solliciter :</p> <ul style="list-style-type: none"> Le service SILENE (ANSSI) Une plateforme d'audit industrielle chargée de produire les rapports conclusifs (D1.O2.B). Cette plateforme respectera le cahier des charges mis à disposition par l'Agence du Numérique en Santé (CERT Santé) qui décrit les attendus de cet audit en termes d'éléments contrôlés et de modalités de restitution des résultats. <p>NB : Les résultats des audits SILENE réalisés par l'ANSSI sont disponibles pendant 6 mois suite à leur réalisation. Les candidats sont invités à télécharger régulièrement les résultats d'audits sur la plateforme de l'ANSSI pour pouvoir les déposer dans le guichet de dépôt d'atteinte des objectifs.</p>
Valeur cible / seuil d'éligibilité	<p>Nombre d'audits d'exposition internet de l'ensemble des domaines et adresses IP publics :</p> <ul style="list-style-type: none"> Du GHT pour les établissements publics membres d'un GHT De l'entités juridique pour les établissements privés
Textes de référence	<p>Le cahier des charges audit d'exposition internet de l'ANS</p> <p>Le service SILENE</p>
2. Production de l'indicateur	
Unité	Booléen
Modalité de calcul	<p>Par candidature :</p> <ul style="list-style-type: none"> Dans le cas où l'établissement sollicite le service SILENE (ANSSI) et à condition que l'inscription au club SSI ait été réalisée au plus tard 100 jours après le début de la phase

	<p>opérationnelle, la réalisation régulière des audits d'exposition internet sera considérée respectée (la date de validation de la candidature par l'ARS étant la date limite de début de la phase opérationnelle).</p> <ul style="list-style-type: none"> • Dans le cas où l'établissement sollicite une plateforme d'audit industrielle, l'intervalle en 2 audits doit être inférieur à 60 jours en moyenne <p>ET</p> <ul style="list-style-type: none"> • L'intervalle maximum entre 2 audits consécutifs doit être inférieur à 100 jours.
Période	<ul style="list-style-type: none"> • Sur la durée de l'appel à financement (phase opérationnelle)
Fréquence	<ul style="list-style-type: none"> • Une fois lors du dépôt de preuve

3. Restitution de l'objectif

Remontée de l'information	<ul style="list-style-type: none"> • Dépôt sur le guichet de déclaration d'atteinte des objectifs
Documents justificatifs	<ul style="list-style-type: none"> • Liste des domaines exposés • Liste des adresses IP publiques • Rapports d'audit d'exposition internet réalisés
Opération de contrôle	<p>Eléments contrôlés :</p> <ul style="list-style-type: none"> • Contrôle de l'exhaustivité de la déclaration des adresses IP publiques et noms de domaine exposés et accessible depuis internet (réalisation d'une recherche type OSINT). • Vérification de la réalisation d'audits à la fréquence cible.

D1.02.B – Atteindre un niveau de sécurisation minimum de son exposition sur internet

Domaine	Domaine 1
Objectif	Atteindre un niveau minimum de sécurisation de son exposition sur internet
1. Définition de l'objectif	
Définition	<p>Lors de chaque audit de l'exposition internet, le niveau de sécurité des services exposés sur Internet est traduit par la détection de vulnérabilités classifiées par niveau de gravité. L'administrateur réseau peut alors démontrer de manière objective et factuelle que les actions menées améliorent significativement le niveau de sécurité des services exposés sur Internet, et par conséquent la difficulté pour des acteurs malveillants de pouvoir accéder au SI de l'organisation.</p> <p>L'Agence du Numérique en Santé (CERT Santé) a produit un cahier des charges permettant de décrire précisément le périmètre de l'audit, la restitution des résultats et la cotation des vulnérabilités détectées. Les outils utilisés par les établissements de santé pour tester leur exposition internet devront respecter ce cahier des charges.</p>
Valeur cible / seuil d'éligibilité	<p>Pour les GHT et les établissements privés :</p> <ul style="list-style-type: none"> Absence de vulnérabilités critiques sur les 2 derniers audits successifs d'exposition internet sur l'ensemble du périmètre <p>NB 1 : Ces deux derniers audits devront impérativement être réalisés par une plateforme d'audit industrielle respectant le cahier des charges mis à disposition par l'Agence du Numérique en Santé (CERT Santé). SILENE n'est pas une solution répondant au cahier des charges élaboré par l'ANS.</p> <p>NB 2 : Au moment de la déclaration d'atteinte des objectifs sur le guichet dédié, le dernier audit réalisé devra dater de moins de 60 jours.</p> <p>NB 3 : Dans le cas où l'avant-dernier audit n'est pas à la cible, il n'est pas pris en compte dans la validation de l'atteinte de l'objectif. L'antépénultième audit est alors considéré si et seulement si il a été réalisé moins de 60 jours avant la réalisation du dernier audit.</p> <p>NB 4 : L'objectif est considéré atteint dans le cas où l'absence de vulnérabilité critique est observée pour un nombre d'établissements représentant au moins 90% de l'activité combinée du candidat.</p> <p>Complémentaire, dans le cas où la condition précédente ne serait pas satisfaite et en l'absence de vulnérabilité critique pour un nombre d'établissements représentant 66 à 90% de l'activité combinée du candidat, alors l'objectif est considéré comme partiellement atteint.</p>
Textes de référence	Le cahier des charges audit d'exposition internet de l'ANS

2. Production de l'indicateur

Unité	Booléen
Modalité de calcul	<p>Pour chaque établissement :</p> <ul style="list-style-type: none"> • Nombre de vulnérabilités critiques sur les 2 derniers audits successifs (ou le dernier et l'antépénultième audit le cas échéant) d'exposition internet = 0
Période	<ul style="list-style-type: none"> • Sur la durée de l'appel à financement (phase opérationnelle)
Fréquence	<ul style="list-style-type: none"> • Une fois lors du dépôt de preuve

3. Restitution de l'objectif

Remontée de l'information	<ul style="list-style-type: none"> • Dépôt sur le guichet de déclaration d'atteinte des objectifs
Documents justificatifs	<ul style="list-style-type: none"> • 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) ou sur le dernier audit et l'antépénultième audit le cas échéant.
Opération de contrôle	<p>Eléments contrôlés :</p> <ul style="list-style-type: none"> • Vérification de l'atteinte du score cible sur les deux derniers audits (ou le dernier audit et l'antépénultième) ; • Contrôle des rapports détaillés

D1.O3 – Se préparer au risque cyber

Domaine	Domaine 1
Objectif	Se préparer au risque cyber
1. Définition de l'objectif	
Définition	<p>Face à une menace informatique toujours croissante et en mutation, 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. Cet exercice doit mobiliser la cellule de crise décisionnelle de l'établissement et est à réaliser sur la base des kits mis à disposition par l'ANS, qui s'appuient notamment sur la norme relative aux exercices (ISO 22398:2013).</p> <p>Objectif : Un premier exercice de crise cyber doit être réalisé au sein de tous les établissements du candidat (au sens FINESS PMSI) entre le 1^{er} janvier 2025 et la date de dépôt de la déclaration d'atteinte des objectifs par l'établissement sur le guichet dédié.</p>
Valeur cible / seuil d'éligibilité	<p>L'ensemble des établissements au sens FINESS PMSI devront avoir réalisé un exercice :</p> <ul style="list-style-type: none"> • Pour les établissements publics : 100 % des entités juridiques (FINESS EJ) ont réalisé un exercice de crise • Pour les établissements privés : 100 % des entités géographiques (FINESS EG) ont réalisé un exercice de crise
Textes de référence	<ul style="list-style-type: none"> • INSTRUCTION N° SHFDS/FSSI/2023/15 du 30 janvier 2023 relative à l'obligation de réaliser des exercices de crise cyber dans les établissements de santé et à leur financement • Kit ANS exercice de gestion de crise cyber publié sur le site de l'ANS

2. Production de l'indicateur

Unité	Booléen (O/N)
Modalité de calcul	<ul style="list-style-type: none"> • N/A
Période	<ul style="list-style-type: none"> • Sur la durée de l'appel à financement (phase opérationnelle)
Fréquence	<ul style="list-style-type: none"> • Une fois lors du dépôt de preuve

3. Restitution de l'objectif

Remontée de l'information	<ul style="list-style-type: none"> • Saisie de la donnée dans l'oSIS par l'établissement
Documents justificatifs	<ul style="list-style-type: none"> • 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
Opération de contrôle	Eléments contrôlés :

	<ul style="list-style-type: none"> • Rapport de réalisation de l'exercice ou attestation de réalisation par le prestataire, l'ARS ou le GRADeS avec indication du FINeSS juridique de l'établissement candidat ou d'un élément permettant l'identification de l'ES.
--	--

D1.O4 – S'auto-évaluer en matière de maturité vis-à-vis des risques cyber

Domaine	Domaine 1
Objectif	S'auto-évaluer en matière de maturité vis-à-vis des risques cyber
1. Définition de l'objectif	
Définition	L'Observatoire Permanent de la Sécurité des Systèmes d'Information des Établissements de Santé (OPSSIES), prévu dans le Plan de Renforcement Cyber, s'appuie, entre autres, sur les résultats des audits de maturité de la sécurité des systèmes d'information (SSI) : les audits ADS de l'ANSSI et les audits cybersurveillance menés par le CERT Santé, ainsi que sur les données saisies dans oSIS (Observatoire des Systèmes d'Information de Santé).
Valeur cible / seuil d'éligibilité	100 % des établissements (au sens FINeSS PMSI) ont renseigné l'oSIS sur le champ suivant : part du budget numérique dans le budget global de l'ES ET 100 % des établissements (au sens FINeSS PMSI) ont renseigné l'oSIS pour au moins 90% des champs relatifs aux 43 mesures prioritaires
Textes de référence	<ul style="list-style-type: none"> • Document "Référentiel des mesures prioritaires" publié par le Ministère

2. Production de l'objectif	
Unité	Booléen (O/N)
Modalité de calcul	<ul style="list-style-type: none"> • N/A
Période	<ul style="list-style-type: none"> • Sur la durée de l'appel à financement (phase opérationnelle)
Fréquence	<ul style="list-style-type: none"> • Une fois lors du dépôt de preuve

3. Restitution de l'objectif	
Remontée de l'information	<ul style="list-style-type: none"> • Saisie dans l'oSIS
Documents justificatifs	<ul style="list-style-type: none"> • Une capture d'écran d'oSIS peut être communiquée
Opération de contrôle	Eléments contrôlés : <ul style="list-style-type: none"> • La complétude des informations est requise, sans qu'un niveau à atteindre ne soit défini.

D1.O5 – Calculer le budget dédié au numérique

Domaine	Domaine 1
Objectif	Calculer le budget dédié au numérique
1. Définition de l'objectif	
Définition	<p>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.</p> <p>Afin de permettre la planification et la réalisation d'actions efficaces au service de la sécurité des systèmes d'information, il est nécessaire de disposer au sein des budgets des ES d'une part suffisante dédiée au numérique et à la sécurité des SI.</p> <p><u>Objectif</u> : 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)</p>
Valeur cible / seuil d'éligibilité	<p>La Part du budget dédiée au numérique et les ETP doivent être restitués au niveau d'une entité juridique (EJ) :</p> <ul style="list-style-type: none"> • Pour les GHT : les valeurs sont à renseigner pour chaque entité juridique constituant le GHT
Textes de référence	<p>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</p> <p>Note [a] : l'annexe 2 de la note d'information précise les modalités du recueil des informations associées à l'objectif. Etablissements publics, ESPIC et EBNL sont invités à exploiter directement les données soumises via la plate-forme ANCRE (intégrant la segmentation des classes 2 et 6) pour le calcul de la part du budget dédiée au numérique (poids des dépenses de fonctionnement et d'investissement du champ numérique dans le budget global de l'hôpital) et à reporter celle-ci dans le dispositif de renseignement de l'OPSSIES.</p> <p>Note [b] : oSIS V2 intègre un module RH dédiées au SI. Dans le cadre du présent arrêté, il est demandé de lister de façon exhaustive les métiers et d'indiquer pour chacun d'eux le nombre d'ETP (Equivalents Temps Plein) au sein de la direction des systèmes d'information ou de la direction des services numériques, cellule ou service Sécurité des Systèmes d'information incluse (si celle-ci en est détachée, en comptabiliser les ETP) dans le dispositif de renseignement de l'OPSSIES. Les personnels détachés sur un projet SI, hors de la DSI/DSN, ainsi que les personnes associées au PMSI ne sont pas à comptabiliser (ces informations sont à indiquer dans le module RH).</p>
2. Production de l'indicateur	
Unité	<ul style="list-style-type: none"> • Part du numérique dans le budget : Pourcentage • ETP : nombre de personnels
Modalité de calcul	<ul style="list-style-type: none"> • Numérateur = total des dépenses liées aux comptes couvrant le champ du numérique Dénominateur = total des dépenses tous comptes confondus

	<p>Note : des travaux sont en cours pour actualiser la segmentation des achats relatifs au numérique. Il en résultera de nouvelles clés de répartition des dépenses associées à des éléments de nomenclature facilitant leur analyse sous l'angle des chantiers numériques (chantiers en cybersécurité inclus). Dans l'attente de l'achèvement de ces travaux, il est demandé d'évaluer le plus précisément possible les dépenses associées aux comptes couvrant ou intégrant le champ informatique hors rémunération des personnels (annexes 1a et 1b de la note d'information n° DGOS/PF2/2019/207 du 26 septembre 2019 pour les établissements publics, ESPIC et EBNL).</p>
Période	<ul style="list-style-type: none"> L'année de référence pour le calcul de la part du numérique dans le budget de l'ES est l'année 2023 pour tous les ES candidats.
Fréquence	<ul style="list-style-type: none"> Une fois lors du dépôt de preuve

3. Restitution de l'objectif

Remontée de l'information	<ul style="list-style-type: none"> Saisie dans l'oSIS
Documents justificatifs	<ul style="list-style-type: none"> Une capture d'écran d'oSIS peut être communiquée
Opération de contrôle	<p>Eléments contrôlés :</p> <ul style="list-style-type: none"> Contrôle exhaustivité des données

D1.O6 – Renforcer la convergence des GHT

Les deux objectifs ci-dessous concernent uniquement les GHT et ne sont donc pas applicables aux établissements privés.

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

Domaine	Domaine 1
Objectif	Piloter au niveau du GHT la réponse au programme et le suivi de l'atteinte des objectifs
1. Définition de l'objectif	
Définition	<p>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.</p> <p>Dans le cadre du domaine 1 du programme CaRE, le GHT doit mettre en place une organisation centralisée permettant d'atteindre les objectifs du programme.</p>
Valeur cible / seuil d'éligibilité	<p>Le GHT doit :</p> <ul style="list-style-type: none"> • Désigner un référent du projet, nommé par le directeur de l'établissement support de GHT, dont le rôle sera de : <ul style="list-style-type: none"> ○ 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 pour l'ensemble du GHT, assurant notamment la coordination du référent, de la DSI, du RSSI et de l'équipe opérationnelle
Textes de référence	Guide méthodologique « Stratégie, optimisation et gestion commune d'un système d'information convergent d'un GHT »

2. Production de l'indicateur	
Unité	Booléen (O/N)
Modalité de calcul	<ul style="list-style-type: none"> • N/A
Période	<ul style="list-style-type: none"> • Sur la durée de l'appel à financement (phase opérationnelle)
Fréquence	<ul style="list-style-type: none"> • Une fois lors du dépôt de preuve

3. Restitution de l'objectif	
Remontée de l'information	<ul style="list-style-type: none"> • Dépôt sur le guichet de déclaration d'atteinte des objectifs

Documents justificatifs	<ul style="list-style-type: none">• Constitution de l'équipe projet• Schéma de le gouvernance mise en place
Opération de contrôle	Eléments contrôlés : <ul style="list-style-type: none">• Désignation du chef de projet en charge du domaine• Composition équipe en charge de la gestion des AD au niveau du GHT

D1.06.B - Formaliser la stratégie du GHT en matière de convergence des AD

Domaine	Domaine 1
Objectif	Formaliser la stratégie du GHT en matière de convergence des AD
1. Définition de l'objectif	
Définition	<p>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. A ce titre, les GHT doivent disposer d'un schéma directeur de convergence des SI du GHT.</p> <p>Dans le cadre du domaine 1 du programme CaRE, cette trajectoire de convergence doit intégrer les modalités de travail et actions permettant d'aboutir au schéma de convergence défini au niveau du GHT.</p> <p>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 gros projet.</p>
Valeur cible / seuil d'éligibilité	<p>Le GHT doit formaliser, présenter et faire valider par le comité stratégique du GHT :</p> <ul style="list-style-type: none"> • Un document précisant les modalités de convergence des infrastructures AD du GHT (définissant le plan de convergence de la gestion des annuaires et des forêts selon les recommandations ANSSI) • La définition de la cible de convergence à atteindre (par exemple : gestion centralisée des AD) est à la charge du GHT car dépendante des situations locales • 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 dont un premier jalon de mise en œuvre est fixé à 18 mois après le dépôt d'atteinte des objectifs, 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. <p>NB : dans le cadre de cet appel à financement, il est attendu une définition de trajectoire et non la mise en œuvre effective de la convergence.</p>
Textes de référence	Guide méthodologique « Stratégie, optimisation et gestion commune d'un système d'information convergent d'un GHT »
2. Production de l'indicateur	
Unité	Booléen (O/N)
Modalité de calcul	<ul style="list-style-type: none"> • N/A

Période	<ul style="list-style-type: none"> Sur la durée de l'appel à financement (phase opérationnelle)
Fréquence	<ul style="list-style-type: none"> Une fois lors du dépôt de preuve

3. Restitution de l'objectif

Remontée de l'information	<ul style="list-style-type: none"> Dépôt sur le guichet de déclaration d'atteinte des objectifs
Documents justificatifs	<ul style="list-style-type: none"> Trajectoire de convergence des AD qui adresse l'ensemble des établissements du GHT
Opération de contrôle	<p>Eléments contrôlés :</p> <ul style="list-style-type: none"> Trajectoire de convergence et planning associé Modalités organisationnelles à mettre en œuvre

5 ATTEINTE PARTIELLE ET DES OBJECTIFS ET FINANCEMENTS ASSOCIES

Un dispositif d'atteinte partielle des objectifs est introduit et permet au candidat de percevoir un financement quand bien même il n'aurait pas atteint certains objectifs du domaine.

Cette **atteinte partielle est conditionnée à la validation des objectifs D1.O1.B et D1.O2.B qui sont considérés comme le socle minimal de cyber-résilience du domaine 1**. En effet, l'exposition internet constitue une porte d'entrée privilégiée dans le système d'information par les attaquants et la compromission des annuaires techniques représente le premier vecteur de propagation. Tout candidat n'ayant pas atteint ces deux objectifs ne reçoit aucun financement dans le cadre du présent domaine.

Sous réserve de la validation des D1.O1.B et D1.O2.B, **un candidat n'ayant pas atteint l'ensemble des objectifs du domaine voit son montant plafond être décoté**. 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)	15% pour les autres candidats
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

A titre illustration :

- Un candidat GHT ayant atteint les objectifs du domaine à l'exception du D1.O2.A et du D1.O3 pourra percevoir un financement au titre de l'atteinte partielle des objectifs. Le montant plafond de financement d'atteinte partielle est fixé à 80% du montant plafond initial du candidat.
- Un candidat « privé » composé de plusieurs entités géographiques ayant atteint les objectifs du domaine à l'exception du D1.O2.A et du D1.O2.B pour lequel une atteinte partielle est prononcée (i.e. pour un nombre d'entités représentant entre 66% et 90% de l'activité combinée du candidat) est éligible à l'atteinte partielle des objectifs. Le montant plafond de financement d'atteinte partielle est fixé à 75% du montant plafond initial du candidat.
- Un candidat « privé » ayant atteint les objectifs du domaine à l'exception du D1.O1.A et du D1.O3 est éligible à l'atteinte partielle des objectifs. Le montant plafond de financement d'atteinte partielle est fixé à 75% du montant plafond initial du candidat