MINISTÈRE
DE LA SANTÉ
ET DE LA PRÉVENTION
Liberté
Égalité
Fraternité

CAPSI
Cellule d'Appui à la Protection des Systèmes d'Information

AGENCE
DU NUMÉRIQUE
EN SANTÉ

Programme CaRE

Le mémo

Axe 4 : Sécurité opérationnelle
Domaine 1 - Audits techniques : annuaires techniques et exposition sur internet

Objectif

Cet appel à financement vise à permettre aux établissements de rattraper le retard sur les périmètres identifiés, à savoir l'exposition internet et les Active Directory.

Qui peut candidater ?

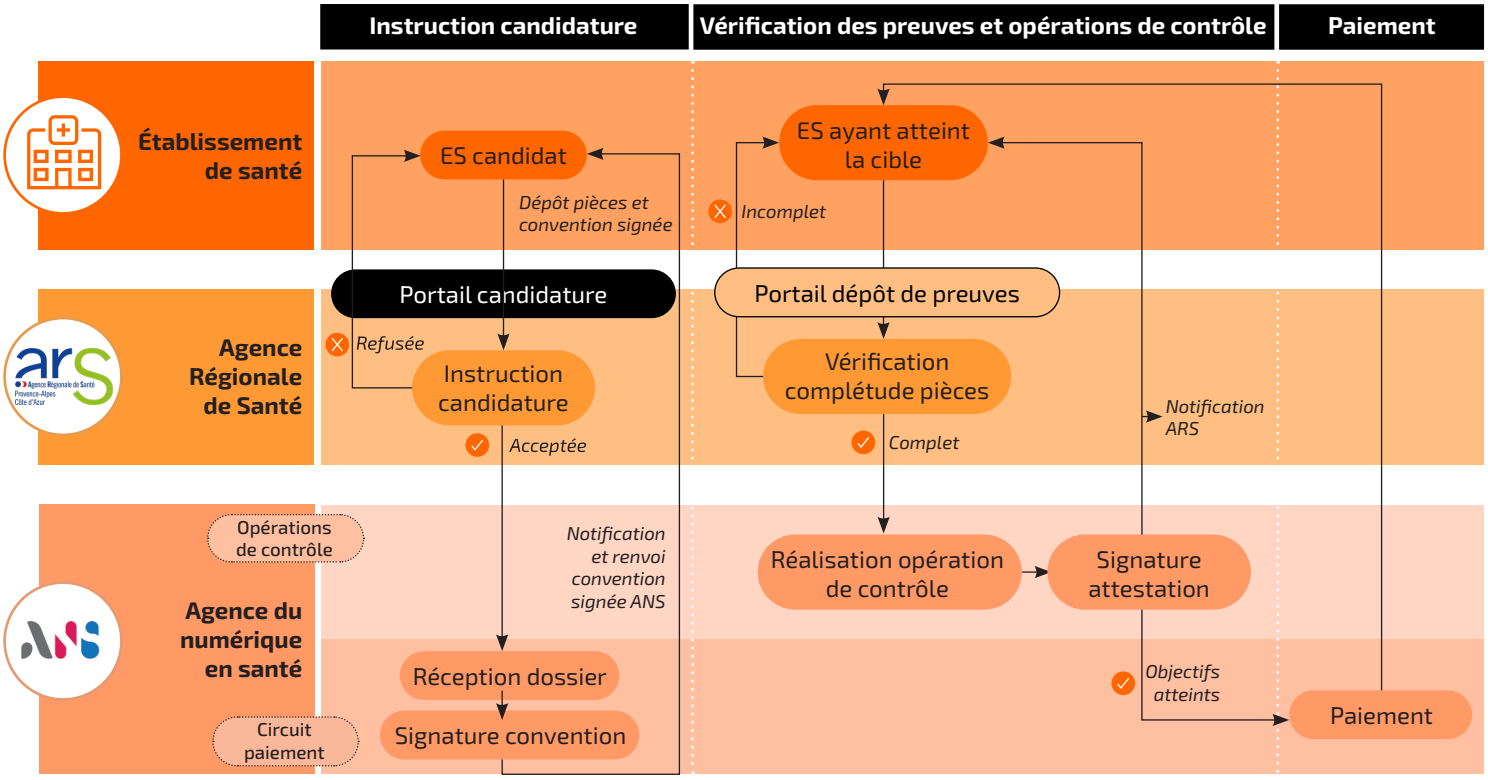
Tous les établissements ayant validé les prérequis SUN-ES sur les exigences de sécurité.

Qui porte la cadidature ?

Pour les GHT l'établissement support porte la candidature pour l'ensemble des entités juridiques du groupement.

Pour les établissement publis hors GHT et les établissements privés, l'entité juridique porte la candidature pour l'ensemble des entités géographiques.

Processus de candidature et de paiement



Calendrier prévisionnel

18/03 : Ouverture des candidatures
19/04 : Fin des candidatures
21/05 : Fin de la période d'instruction des candidatures par l'ARS

21/05/2024 au 28/03/2025 : Déclaration de l'atteinte des objectifs par les établissements
10/06/2024 au 25/10/2025 : Paiement des établissements

Comment candidater ?

Rendez-vous sur le portail de connexion, Convergence, pour saisir le dossier de candidature.

Les prérequis SUN-ES à valider

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

Vous souhaitez vérifier si votre établissement rempli les prérequis SUN-ES et est donc éligibilible à la candidature ? **Téléchargez le guide.**

Les objectifs du Domaine 1

[D1.01] Maîtrise de l'annuaire d'établissement

Consulter la présentation du service ADS (Active Directory Security) : Service gratuit de l'ANSSI ouvert aux ES privés et publics qui candidatent au programme CaRE permettant de faire un audit de son AD.

[D1.01.A] Réaliser régulièrement des audits de tous les Active Directory (AD)
Un audit Active Directory Sécurity (porté par l'ANSSI) doit être réalisé pour l'ensemble des établissements du candidat tous les 2 mois durant la phase opérationnelle.

Valeur cible : nombre d'audits réalisés sur chaque AD.

[D1.01.B] Atteindre un niveau de sécurisation minimum des Active Directory (AD)
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.

Valeur cible : un score supérieur ou égal à 2 doit être obtenu pour les 2 derniers audits ADS des différents AD.

[D1.02] Maîtrise de l'exposition internet

Consulter la présentation du service SILENE : Service gratuit de l'ANSSI permettant de réaliser son audit d'exposition : SILENE.

[D1.02.A] Réaliser régulièrement des audits de l'exposition internet
Un audit d'exposition internet doit être réalisé tous les deux mois durant la phase opérationnelle.

Valeur cible : nombre d'audits réalisés de l'ensemble des domaines et adresses IP publics.

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

Valeur cible : absence de vulnérabilités critiques sur les 2 derniers audits successifs d'exposition internet sur l'ensemble du périmètre.

[D1.03] Exercices Cyber

Se préparer au risque cyber en réalisant un exercice de crise cyber
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.

Valeur cible : l'ensemble des établissements au sens FINESS PMSI devront avoir réalisé un exercice, soir 100% des EJ pour les ES publics et 100% des EG pour les ES privés.

[D1.04] Auto-évaluation en matière de maturité visà-vis des risques cyber

S'auto-évaluer en matière de maturité vis-à-vis des risques cyber en remplissant tous les volets de l'oSIS
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 : 100 % des établissements (au sens FINESS PMSI) ont renseigné l'oSIS sur la part du budget numérique dans le budget global de l'ES et les 43 mesures prioritaires.

[D1.05] Calculer la part du numérique dans le budget

Calculer la part du budget dédiée au numérique dans le budget général de l'ES
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).

Valeur cible : la Part du budget dédiée au numérique et les ETP doivent être restitués au niveau d'une EJ. Pour les GHT, les valeurs sont à renseigner pour chaque EJ constituant le GHT.

[D1.06] Renforcer la convergence des GHT (spécifique GHT)

[D1.06.A] Piloter au niveau du GHT la réponse au programme et le suivi de l'atteinte des objectifs
Le GHT doit mettre en place une organisation centralisée permettant d'atteindre les objectifs du programme CaRE.

Valeur cible : Désigner un référent projet, mettre en place une équipe opérationnelle unique pour la gestion des AD en charge de la réalisation des audits, mettre en place la gouvernance transverse du projet CaRE pour l'ensemble du GHT.

[D1.06.B] Formaliser la stratégie du GHT en matière de convergence des AD
La trajectoire de convergence des SI du GHT doit intégrer les modalités de travail et actions permettant d'aboutir au schéma de convergence défini au niveau du GHT.

Valeur cible : 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.

Liens utiles

Le plan d'action du programme CaRE

Le guide des prérequis et objectifs du domaine 1

Le webinaire ANS de présentation du Domaine 1