RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Agence Régionale de Santé Auvergne-Rhône-Alpes

Appel à candidature

Renforcement de la Cybersécurité des Organismes Gestionnaires médico-sociaux de la région Auvergne Rhône-Alpes

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Agence Régionale de Santé Auvergne-Rhône-Alpes

Sommaire

1 Contexte national et stratégie régionale pour les établissements et services médico-sociaux

La transformation numérique du secteur social et médico-social, s'accompagne d'une exposition croissante au risque cyber. **Le risque est avéré** pour les ESMS et les personnes accompagnées.

Au premier semestre 2023, le chantier national **cybersécurité social et médico-social** a permis de mener :

- Une concertation auprès **de 60 organismes gestionnaires**
- **8 ateliers de co-construction** avec les acteurs du secteur
- Un **plan d'action 2023/2027 ambitieux, adapté, et cohérent** avec la feuille de route sanitaire.

Parallèlement à ceci**, l'observatoire des SI MS** a établi une grille pour évaluer la maturité numérique des établissements. Sur la base de différentes questions et de facteurs de pondérations, un score est produit qui détermine un niveau de et les actions nécessaires pour améliorer sa maturité numérique. A terme, cette grille devra être remplie par l'ensemble des organismes gestionnaires.

Le financement d'actions de cybersécurité est en construction au niveau national (Plan Care). L'Agence Régionale de Santé, souhaite dès à présent pouvoir engager un appel à candidature afin de :

- Déterminer la capacité des établissements à pouvoir renseigner eux-mêmes des grilles d'évaluation
- Evaluer d'un point de vue méthodologique l'accompagnement à réaliser auprès des établissements dans leur diagnostic et mise en œuvre de plan d'action pour améliorer leur maturité en matière de cybersécurité.

Cet appel à candidature a pour objectifs de :

1) Procéder à la sélection d'une dizaine d'organismes gestionnaire dans la perspective de faire réaliser par un prestataire un audit de maturité numérique

2) Financer la mise en œuvre d'actions de remédiations de vulnérabilités failles évaluées comme critiques.

L'audit et le plan d'action seront financés sur des fonds régionaux dans le cadre du présent programme

2 Calendrier de l'appel à candidature

L'appel à candidature est ouvert jusqu'au **15 octobre 2023 à minuit.**

Tout dossier déposé après la date de clôture de l'appel à candidature sera considéré comme non recevable.

Les candidatures seront instruites au fil de l'eau.

3 Comment déposer sa candidature ?

La personne morale gestionnaire qui souhaite candidater doit remplir le questionnaire suivant et joindre les pièces complémentaires avant le 15 octobre à minuit.

Les pièces à fournir concernant cet appel à projet sont les suivantes :

- Une note de présentation expliquant la motivation de l'organisme gestionnaire à présenter sa candidature (obligatoire).
- Une lettre d'engagement signée, précisant que l'organisme gestionnaire s'engage à se rendre disponible (ainsi que les professionnels identifiés) pour la bonne réalisation des audits et de la mise en place des actions, sous respect d'un délai de prévenance de 15 jours à minima par le prestataire (obligatoire).

4 Déroulé du projet

A. Audits de l'organisme gestionnaire

Les candidats retenus dans le cadre de cet appel à candidature se verront contacter par un prestataire dans l'objectif de réaliser un audit sur site à partir d'outils préétablis (grille Maturin SMS, et guide de maturité cyber en 13 questions[1]).

Un entretien préalable sera réalisé afin d'identifier les documents et procédures existantes ainsi que de déterminer les personnes à rencontrer et sites à visiter sur cet audit.

L'audit ne dépassera pas 1 journée et demie.

Au terme de cet audit, le prestataire émettra un rapport d'audit ainsi qu'un plan d'action à mettre en oeuvre par l'organisme gestionnaire afin de pallier aux risques ou failles considérées comme les plus critiques. Ces éléments seront présentés lors d'un entretien à l'organisme gestionnaire qui sera amené à se positionner sur sa capacité à mettre en œuvre les actions préconisées.

Au terme de l'ensemble des audits des OG candidats, l'ARS et le GRADeS évalueront l'ensemble des actions proposées par les prestataires et la criticité des remédiations relevées lors des audits. Un certain nombre d'actions seront sélectionnées et proportionnées au financement pour mise en œuvre au sein des organismes gestionnaires.

Il est précisé que chaque organisme gestionnaire audité ne se verra pas obligatoirement proposer d'actions financées.

[1] La Cybersécurité pour le social et le médico-social en 13 questions - Agence du Numérique en Santé https://esante.gouv.fr/sites/default/files/media_entity/documents/ANS_GUIDECYBER_PHASE%201-EXE%20-V2.pdf

B. Mise en œuvre du plan d'action

Pour les actions de remédiations retenues[2] dans le cadre de la mise en œuvre par un prestataire, l'organisme gestionnaire sera contacté afin de pouvoir lui mettre à disposition les ressources (humaines et matérielles) nécessaires.

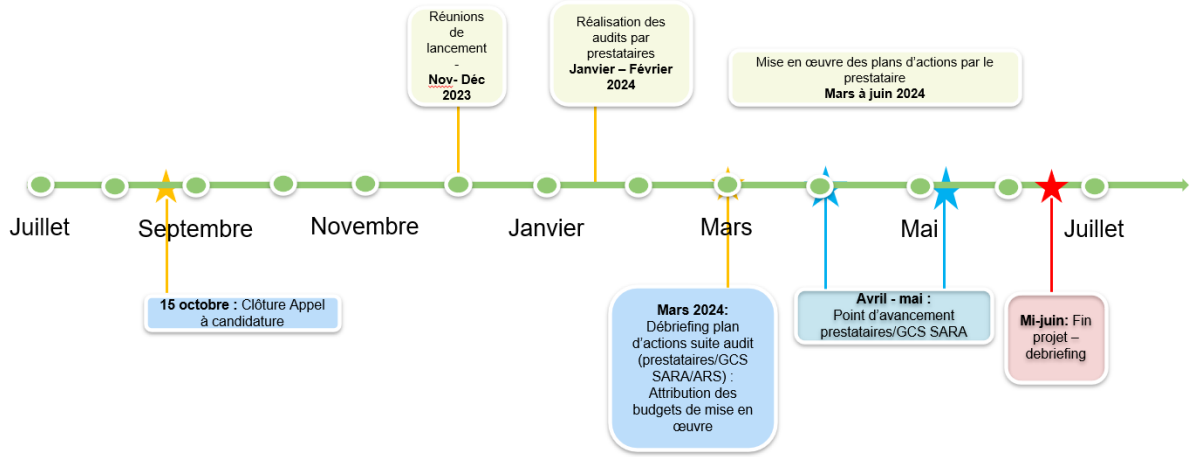
Le prestataire devra rendre compte des actions mises en œuvre au sein des organismes gestionnaires et de l'amélioration de la sécurité des SI au terme du projet.

C. Prestataires

Les audits et l'accompagnement à la mise en œuvre des actions seront réalisés par des prestataires spécialisés en cybersécurité et certifiés PASSI.

Ils sont retenus dans le cadre d'un marché public dont le GCS SARA est le pouvoir adjudicateur.

D. Planning prévisionnel



Nota : les projets déposés avant le 15 octobre peuvent voir leur planning anticipé.

5 Priorisation des projets

L'ARS Auvergne-Rhône-Alpes priorisera les dossiers selon les éléments remplis dans les éléments de candidature et permettant d'évaluer les facteurs de risques de l'organisme gestionnaire.

[2] N.B. : Les actions financées par l'ARS ne pourront pas dépasser 5 jours de prestation par organisme gestionnaire.

6 Contacts

Pour toute information complémentaire, veuillez contacter :

- M. Hervé BLANC, Directeur des projets eSanté - ARS Auvergne-Rhône-Alpes
  herve.blanc@ars.sante.fr

- M. Thierry NAVARRETE, Chef de projet Cybersécurité - GCS SARA
  ssi@sante-ara.fr

  Mme Priscilla OHLING, Responsable programmes ESMS - GCS SAR
  priscilla.ohling@sante-ara.fr