



AGENCE GENERALE DES EQUIPEMENTS ET PRODUITS DE SANTE

7, rue du Fer à Moulin

75221 - PARIS CEDEX 05

Tél. : 01 43 37 95 96

**CAHIER DES CLAUSES TECHNIQUES PARTICULIERES**

**N° 25.31.IT**

Objet : Audit et certification du système de management du système de l’information (SMSI) selon le référentiel de certification HDS (Hébergement de Données de Santé) et la norme ISO/IEC 27001 pour l’Assistance Publique – Hôpitaux de Paris.

Pour une période de trois ans, à compter de la date de notification.

# Sommaire

[Sommaire 2](#_Toc210396342)

[ARTICLE 1 : Périmètre de la consultation 3](#_Toc210396343)

[1. Préambule - L’hébergement de données de Santé 3](#_Toc210396344)

[2. Activités certifiables 3](#_Toc210396345)

[ARTICLE 2 : PRESTATIONS DEMANDEES 5](#_Toc210396346)

[1. L’objet de la prestation 5](#_Toc210396347)

[2. Prestations attendues 5](#_Toc210396348)

[3. Référentiels applicables 6](#_Toc210396349)

[4. Les Phases attendues 7](#_Toc210396350)

[5. Livrables attendus 7](#_Toc210396351)

[6. Résultats attendus 7](#_Toc210396352)

ARTICLE 1 : Périmètre de la consultation

L’Assistance Publique Hôpitaux de Paris (AP-HP) s’est engagée dans une démarche de certification de son système de management de la sécurité de l’information sous la norme ISO 27001 dans le cadre de la certification Hébergement de Données de Santé (HDS – Articles R1111-8 et R1111-9 du code de la santé publique).

L’AP-HP a été certifiée HDS le 08 septembre 2020 et doit renouveler la certification HDS le 08 septembre 2023.

La présente consultation comporte deux lots :

- Lot 1 : Cycle de certification HDS/ISO27001,

- Lot 2 : Audits internes du S.I. de l’AP-HP.

Préambule - L’hébergement de données de Santé

Les modalités d’hébergement de données de santé à caractère personnel sont encadrées par l’article L.1111-8 du code de la santé publique.

Un décret publié au Journal Officiel le 26 février 2018 et entré en vigueur le 1er avril 2018 précise que :

Toute personne physique ou morale qui héberge des données de santé à caractère personnel recueillies à l’occasion d’activités de prévention, de diagnostic, de soins ou de suivi social ou médicosocial pour le compte d’un tiers, doit être certifié ou agrée à cet effet ;

L’obligation de recourir à un hébergeur certifié ou agrée pèse donc sur tout responsable de traitement de données de santé à caractère personnel « recueillies à l’occasion d’activités de prévention, de diagnostic ou de soins ou de suivi social et médico-social » qui souhaiterait en confier la conservation à un tiers.

Les sanctions encourues par un hébergeur hébergeant des données de santé sans agrément ou certificat sont précisées dans les articles L1115-1 et L1115-2 du code de la santé publique et prévoit une peine de trois ans d’emprisonnement et 45 000 € d’amende.

L’hébergement de donnée de santé est encadré par une certification exigible à tout organisme entrant dans les critères exposés dans le référentiel HDS V2 publié le 16/05/2024 :

* <https://esante.gouv.fr/espace-presse/publication-au-journal-officiel-du-referentiel-de-certification-hds-souverainete-des-donnees-et-ameliorations-du-referentiel?position&keys=HDS&pageNumber=1>

Activités certifiables

Prestation d’hébergeurs d’infrastructure physique

• Mise à disposition ou maintien en condition opérationnelle de locaux permettant d’héberger l’infrastructure matérielle du système d’information de santé,

• Mise à disposition ou maintien en condition opérationnelle de l’infrastructure matérielle du système d’information de santé.

Prestation d’hébergeur info géreur

• Mise à disposition ou maintien en condition opérationnelle de la plateforme logicielle (système d’exploitation, middleware, base de données, etc.) du système d’information de santé,

• Mise à disposition ou maintien en condition opérationnelle de l’infrastructure virtuelle du système d’information de santé,

• Infogérance d’exploitation du système d’information de santé,

• Sauvegardes externalisées des données de santé.

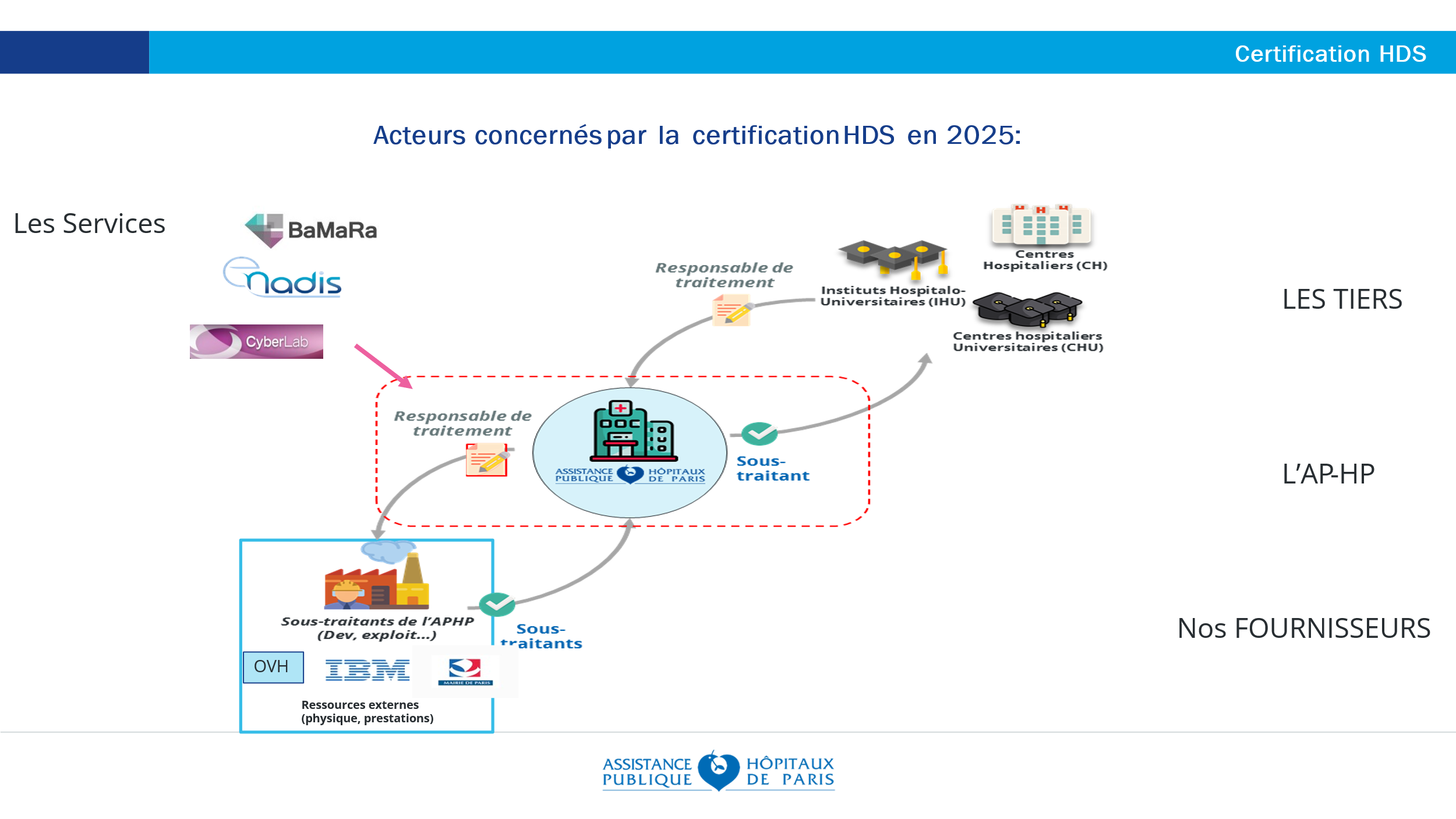
Contexte

L'AP-HP est certifiée ISO 27001 pour son système de management de l'information et certifiée HDS Hébergement de Données de Santé. L'AP-HP est certifiée HDS depuis le 20 octobre 2020

Périmètre de certification

L’AP-HP héberge des données de santé à caractère personnel pour le compte de tiers qui nous fournissent des outils (logiciels) à installer sur notre infrastructure et qui stockent des données de santé à caractère personnel.

L’AP-HP sous-traite une partie de son infrastructure salle machine auprès d’organismes externes : Datacenter IBM ou Datacenter Mairie de Paris ou OVH.



Référentiels applicables

Le titulaire du marché devra appuyer sur sa méthode sur l’IAF International Accréditation Forum et répondre aux règles internationales en vigueur relatives aux processus.

[Le référentiel de Certification](https://esante.gouv.fr/services/hebergeurs-de-donnees-de-sante/les-referentiels-de-la-procedure-de-certification) :

<https://esante.gouv.fr/services/hebergeurs-de-donnees-de-sante/les-referentiels-de-la-procedure-de-certification>

ARTICLE 2 : PRESTATIONS DEMANDEES

L’objet de la prestation

Lot 1 : Audits de certification HDS

Les prestations attendues consistent pour l’organisme retenu à auditer le système de management du système de l’information sous la norme ISO 27001 et de certification HDS Hébergement de Données de Santé.

Le processus de certification initial devra être bâti sous la norme ISO 27001-2023 et le référentiel HDS V2 et également aider à conduire une philosophie d’amélioration continue au sein de l’organisation.

Ce lot comprend l’audit de **certification initiale**, les **audits de suivi des 1ère et 2ème année** et en compléments des **extensions de périmètre pour la 1ere année et la 2eme année** pour adapter le périmètre de la certification si cela est nécessaire.

Lot 2 : Audits internes du SI de l’AP-HP

Les prestations attendues consistent pour l’organisme retenu à effectuer annuellement un audit interne de conformité HDS V2 en amont des audits de certification.

Ce lot comprend les **audits internes de conformité HDS V2** annuels et en complément des **audits internes d’extension du périmètre** pour adapter le périmètre de la certification si cela est nécessaire, et des **audits spécifiques du SI**.

Prestations attendues

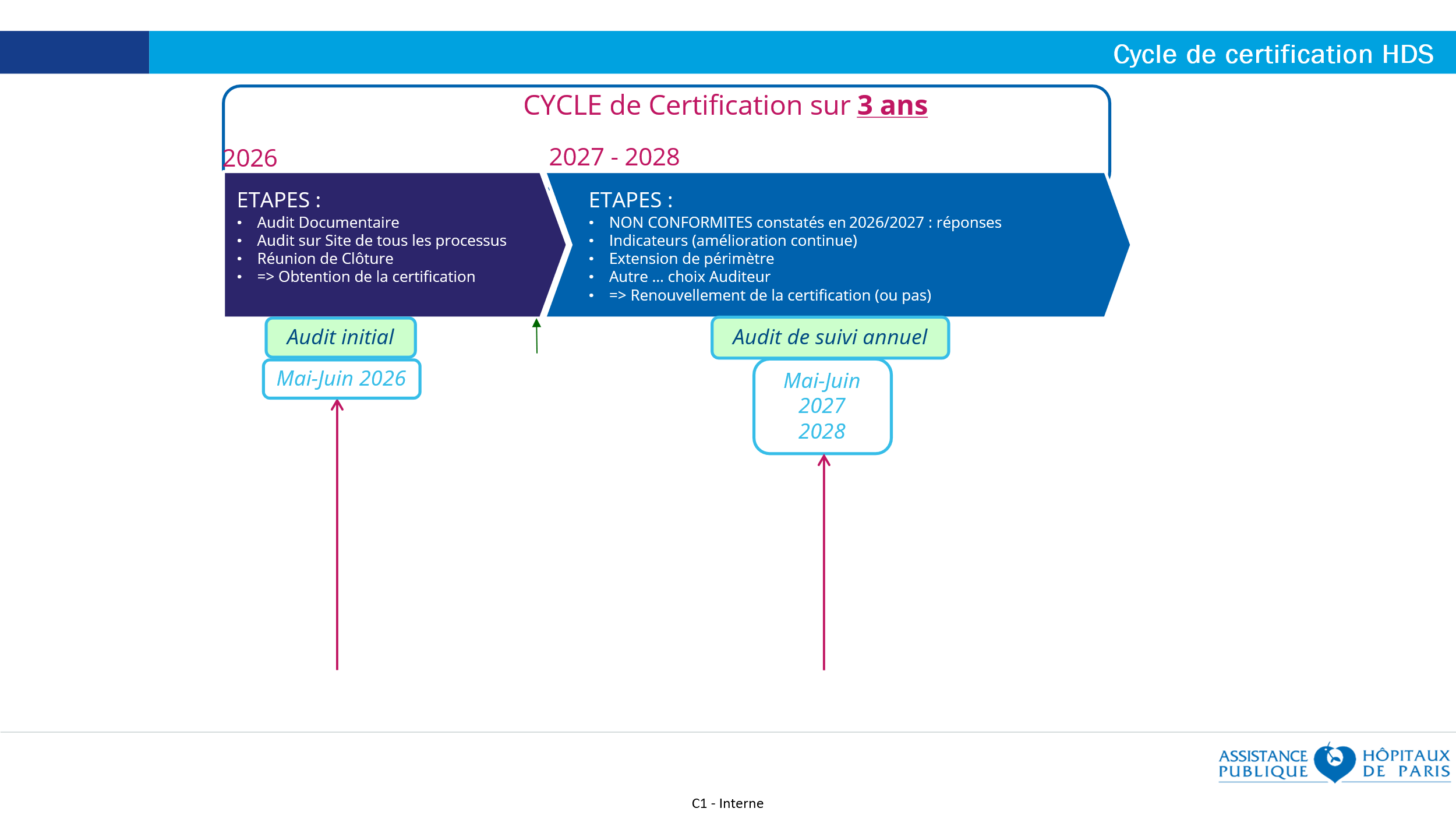
La durée du cycle de certification est bâtie sur un cycle complet de 3 ans

La prestation comprend pour **le lot 1** :

* Un audit Initial de certification (année 1) incluant notamment :
  + La revue documentaire.
  + Un audit de conformité.
* Un audit de suivi annuel (années 2 et 3) permettant une mise à jour des données de l’AP-HP en matière de certification
* Elle devra inclure :
  + Le temps d’audit
  + La rédaction finale du rapport

La prestation comprend pour **le lot 2** :

* Des audits internes annuelsde conformité HDS V2 :
  + La revue documentaire.
  + Un audit de conformité.
* Elle devra inclure :
  + Le temps d’audit
  + La rédaction finale du rapport



Exigences calendaires

Les nouveaux certificats ISO 27001 et HDS doivent démarrer le 08 septembre 2026 pour une durée de 3 ans, en conséquence l’Audit Initial du cycle de certification doit démarrer en Mai 2026.

LOT 1 :

Les étapes principales sont :

Démarrage de l’audit de certification : Mai 2026

Audit initial (2026) ou Audits de suivis (2027 et 2028) :

ETAPE 1 (Documentaire) : Mai de chaque Année

ETAPE 2 (Audit sur site) : Mai de chaque Année

Remise des rapports d’Audit : Juin de chaque Année

LOT 2 :

Audit interne de vérification : Février de chaque Année

Audit interne d’extension de périmètre : à la demande

Audit spécifique : à la demande

Ce planning et les échéances précisées sont à respecter tous les ans à la même période pendant la durée du marché.

Référentiels applicables

Le titulaire du marché devra appuyer sa méthode :

* Sur l’IAF International Accréditation Forum et répondre aux règles internationales en vigueur relatives aux processus.
* Sur les référentiels de l’ANS (Ex ASIP Santé) relatifs à la certification HDS :
  + Annexe 4 du CCTP : [Référentiel\_accréditation\_HDS - FR - V2](https://esante.gouv.fr/sites/default/files/media_entity/documents/referentiel_accreditation_hds---fr---v2.pdf)
  + Annexe 5 du CCTP : [Référentiel\_certification\_HDS - FR -V2](https://esante.gouv.fr/sites/default/files/media_entity/documents/referentiel_certification_hds---fr--v2.pdf)
* Norme NF EN ISO/IEC 27001 JUILLET 2023, vision auditeur selon le site   [:](https://www.google.com/aclk?sa=L&ai=DChsSEwiM07vWgIiQAxUF_XkEHfWOEwoYACICCAEQARoCd2Y&co=1&gclid=CjwKCAjw6P3GBhBVEiwAJPjmLomxWp5ITtNVdb4rKExVx9CMbKPi6VQwN0orOwCC20DJpPQHyRvukxoC1AEQAvD_BwE&cce=2&sig=AOD64_3pc9OTprLtpiRSb0ezpjD2cOtdCQ&authuser=1&q&adurl&ved=2ahUKEwjC9LXWgIiQAxUtNPsDHcpTMawQ0Qx6BAgKEAE) [[Certification ISO/IEC 27001 - Sécurité des systèmes d'information](https://www.google.com/aclk?sa=L&ai=DChsSEwiM07vWgIiQAxUF_XkEHfWOEwoYACICCAEQARoCd2Y&co=1&gclid=CjwKCAjw6P3GBhBVEiwAJPjmLomxWp5ITtNVdb4rKExVx9CMbKPi6VQwN0orOwCC20DJpPQHyRvukxoC1AEQAvD_BwE&cce=2&sig=AOD64_3pc9OTprLtpiRSb0ezpjD2cOtdCQ&authuser=1&q&adurl&ved=2ahUKEwjC9LXWgIiQAxUtNPsDHcpTMawQ0Qx6BAgKEAE)](https://certification.afnor.org/numerique/certification-iso-27001)

Les Phases attendues

LOT 1 :

La durée du cycle de certification doit être bâti sur un cycle complet décomposé comme suit :

* Un Audit de certification initial en mai 2026.
* Un Audit de Suivi annuel permettant une mise à jour des données de l’AP-HP en matière de certification
* En complément : Un audit d’extension de périmètre pour adapter le périmètre de la certification si cela est nécessaire. (Sur la base d’ajout d’un périmètre applicatif)

Le plan de charge présenté doit en outre inclure :

* Le temps d’audit
* La rédaction finale du rapport sur site

LOT 2 :

La durée des audits internes doit être bâti sur un cycle décomposé comme suit :

* Un Audit interne de vérification annuel.
* Un audit interne de vérification de l’extension de périmètre pour préparer les étapes de certification de mai/juin de chaque année à partir de la deuxième année.
* Audit des 3 datacenters de l’AP-HP sur l’ensemble du cycle à raison d’un datacenter par an (Clichy, La Chapelle, Bicêtre)
* En complément : un audit interne spécifique sur un périmètre restreint suite à une demande de vérification.

Le plan de charge présenté doit en outre inclure :

* Le temps d’audit
* La rédaction finale du rapport sur site

Livrables attendus

* LOT 1, Cycle de certification HDS, chaque année :
  + Présentation de synthèse et rapport de l’audit à blanc
  + Plan d’audit détaillé
  + Pack Documentaire Sécurité de l’Information HDS
  + Présentation de synthèse des audits en réunion de clôture
  + Rapport d’audit
  + Certificats ISO 27001 & HDS.
* LOT 2, Pour chaque audit :
  + Plan d’audit détaillé ;
  + Bilan des entretiens en fin de chaque journée d’audit sur site ;
  + Présentation de synthèse en réunion de clôture ;
  + Rapports d’audits détaillé avec propositions de maîtrise des constats.

Résultats attendus

L’organisme certificateur doit délivrer un certificat valable sous format papier et numérique avant la date anniversaire de la certification comme décrite à l’article 1 du présent CCTP.