Guide des prérequis et objectifs

Appel à Financement n°1- Fonction « Annuaires techniques et exposition sur internet »

Historique du document – Suivi des modifications apportées			
Version	Date	Auteur	Commentaires / modifications
V1	25/01/2024	Equipe programme CaRE	Version initiale
V1.1	05/02/2024	Equipe programme CaRE	Précision objectif D1.O1.B et D1.O2.A
V1.2	09/02/2024	Equipe programme CaRE	Objectif D1.O1.B : retrait de la notion de vulnérabilité critique sur les AD
V1.3	16/02/2024	Equipe programme CaRE	D1.O2.A : Intégration usage possible de SILENE D1.O1.A : Ajustement de la définition “phase opérationnelle” D1.O1.B : Ajout délai de réalisation du dernier audit AD avant déclaration d’atteinte des objectifs D1.O2.A : Ajustement de la définition “phase opérationnelle” D1.O2.B : Ajout délai de réalisation du dernier audit exposition internet avant déclaration d’atteinte des objectifs D1.O5 : Précision sur la période concernée - *Dernière année clôturée comptablement au moment du dépôt de preuve*
V1.4	04/03/2024	Equipe programme CaRE	Ajout de précisions sur les objectifs D1.O1 et D1.O2
V1.5	26/03/2024	Equipe programme CaRE	Ajout de précisions sur la cible à atteindre dans le cadre de l’objectif D1.O6B

V1.6	09/07/2024	Equipe programme CaRE	Ajout de précisions sur l'année de référence dans le cadre de l'objectif D1.O5
V1.7	31/07/2024	Equipe programme CaRE	Ajout de précisions sur les pièces justificatives pour les objectifs D1.04 et D1.05
V1.8	17/02/2025	Equipe programme Care	D1.O1.A et D1.O2.A : • Nouvelle définition de la phase opérationnelle en lien avec l'arrêté rectificatif du D1 D1.O1.A : • Suppression du NB2 relatif aux AD hébergés par un tiers • Ajout d'un NB2 sur les établissements sans AD • Ajout d'un NB3 sur les établissements ayant un AD de type EntraId sans hybridation D1.O3 : • Modification de la période de réalisation d'un exercice de crise cyber en lien avec l'arrêté rectificatif du D1 • Modification des éléments contrôlés afin qu'ils soient harmonisés avec les documents justificatifs D1.O4 : • Ajout de précisions concernant les éléments contrôlés D1.O6.B • Précision concernant le premier jalon, qui se situe 18 mois après le dépôt d'atteinte des objectifs • Précision sur l'exemple de la cible de convergence
V1.9	18/03/2025	Equipe programme CaRE	D1.O2.A • Précision quant au respect de l'objectif dans le cas où l'établissement candidat sollicite le service SILENE (ANSSI) D1.O1.B et D1.O2.B • Ajout NB 3

SOMMAIRE

1 OBJECTIF DE CE GUIDE

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

	N°	Intitulé prérequis			Détails
Prérequis	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)
	N°	Intitulé objectifs	N°	Intitulé sous-objectifs	Détails
Objectifs	D1.O1	Maitriser l'annuaire d'établissement	D1.O1.A	Réaliser régulièrement des audits de tous les AD	• Réaliser des audits des AD tous les 2 mois durant la phase opérationnelle
			D1.O1.B	Atteindre un niveau de sécurisation minimum des AD	• Atteindre un score supérieur ou égal à 2 sur les 2 derniers audits de chaque AD
	D1.O2	Maitriser l'exposition internet	D1.O2.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.O2.B	Atteindre un niveau de sécurisation minimum de son exposition sur internet	• Absence de vulnérabilités critiques sur les 2 derniers audits d'exposition internet
	D1.O3	Se préparer au risque cyber			• Réaliser un exercice de gestion de crise cyber en utilisant les kits nationaux ANS
	D1.O4	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.O5	Calculer le budget dédié au numérique			• Calculer la part du budget dédiée au numérique dans le budget général de l'ES
	D1.O6 GHT	Renforcer la convergence des GHT *(spécifique ES publics)*	D1.O6.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.O6.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

De même que dans les programmes HOP'EN et SUN-ES, ils 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)

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	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 : • 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	**Pour les GHT**, il est nécessaire que • Ce prérequis soit atteint par '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. **Pour les établissements publics hors GHT**, il est nécessaire que ce prérequis soit atteint par : • L'entité juridique (FINESS EJ) porteuse de la candidature. **Pour les établissements privés (à but non lucratif et lucratif),** il est nécessaire que : • 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	• N/A
Période	• Au moment de la candidature

Fréquence	• N/A

3. Restitution de l'objectif	
Remontée de l'information	Pour les établissements ayant une candidature validée au programme SUN-ES : • Aucune remontée nécessaire : données consolidées déjà disponibles au niveau national Pour les établissements n'ayant pas une candidature validée au programme SUN-ES : • Dépôt des pièces justificatives sur la plateforme de candidature
Documents justificatifs	Pour les établissements ayant une candidature validée au programme SUN-ES : • Aucun document Pour les établissements n'ayant pas une candidature validée au programme SUN-ES : • Liste des documents exigées pour les prérequis PS2.1 et PS2.2 de SUN-ES : o 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) o Procédure de remontée des incidents de sécurité (Art. L.1111- 8-2 CSP). o Organigramme mettant en évidence le positionnement du RSSI, préconisé en dehors de la DSI" par exemple rattaché à la cellule qualité. o 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 o 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
Opération de contrôle	• Contrôle sur pièces

3 OBJECTIFS DU DOMAINE 1

3.1 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	Un audit ADS (porté par l'ANSSI) doit être réalisé pour l'ensemble des annuaires des établissements du candidat tous les 2 mois durant la phase opérationnelle. 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 courant 2024 par l'ANSSI d'un outil adapté aux AD hébergés complétement dans le cloud, ces annuaires hébergés dans le cloud sont également concernés par cet objectif. 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. 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. 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. • Le démarrage de la phase opérationnelle doit être compris entre la date de publication de l'arrêté du 18 mars 2024 (22 mars 2024) et le 20 septembre 2024. 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	Nombre d'audits réalisés sur chaque AD : • Du GHT pour les établissements publics membres d'un GHT • De l'entité juridique pour les établissements publics hors GHT et les établissements privés
Textes de référence	Le service ADS

2. Production de l'indicateur	
Unité	Booléen

Modalité de calcul	Pour chaque annuaire d'établissement : • L'intervalle entre 2 audits doit être de 60 jours maximum
Période	• Sur la durée de l'appel à financement (phase opérationnelle)
Fréquence	• Une fois lors du dépôt de preuve

3. Restitution de l'objectif	
Remontée de l'information	• Dépôt sur le guichet de déclaration d'atteinte des objectifs
Documents justificatifs	• Description exhaustive des infrastructures AD et de leurs interconnexions • Rapports des audits ADS réalisés
Opération de contrôle	Eléments contrôlés : • 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.O1.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	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. Un score supérieur ou égal à 2 doit être obtenu pour les deux derniers audits ADS des différents AD. Il est cependant rappelé que les préconisations de l'ANSSI recommandent l'atteinte d'un score de 3 a minima.

Valeur cible / seuil d'éligibilité	**Cible à atteindre :**
	
	Un score supérieur ou égal à 2 doit être obtenu pour les 2 derniers audits ADS des différents AD, selon les règles ci-dessous :
	
	Pour les GHT :
	• Score des 2 derniers audits successifs ADS ≥ 2 pour tous les AD de l'établissement support
	ET
	• Si le GHT à plusieurs entités juridiques (FINESS EJ)
	  ○ 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
	NB : Une entité juridique (EJ) est considérée « à la cible » à condition que l'ensemble de ses infrastructures AD ait un score ≥ 2
	
	Pour les établissements publics hors GHT et pour les établissements privés :
	• Score des 2 derniers audits successifs ≥ 2 pour tous les AD de l'entité juridique (FINESS EJ)
	ET
	• Si l'EJ à plusieurs entités géographiques (FINESS EG)
	  ○ 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

	NB : Une entité géographique (EG) est considérée « à la cible » à condition que l'ensemble de ses infrastructures AD ait un score ≥ 2 NB 2 : Au moment de la déclaration d'atteinte des objectifs sur le guichet dédié, le dernier audit ADS réalisé devra dater d'un mois maximum NB 3 : Le dernier audit doit être conforme aux objectifs fixés, et il doit y avoir eu un autre audit datant d'au moins 45 jours et d'au plus 60 jours, également conforme aux objectifs.
Textes de référence	Le service ADS

2. Production de l'indicateur	
Unité	Booléen
Modalité de calcul	Pour chaque annuaire d'établissement soumis par l'EJ candidat : • Score audit ADS ≥ 2 sur les 2 derniers audits successifs
Période	• Sur la durée de l'appel à financement (phase opérationnelle)
Fréquence	• Une fois lors du dépôt de preuve

3. Restitution de l'objectif	
Remontée de l'information	• Dépôt sur le guichet de déclaration d'atteinte des objectifs
Documents justificatifs	• 2 derniers rapports des audits ADS pour l'ensemble des AD du candidat
Opération de contrôle	Eléments contrôlés : • Vérification de l'atteinte du score cible sur les deux derniers audits pour tous les AD • 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	Un audit d'exposition internet doit être réalisé tous les deux mois durant la phase opérationnelle. 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. • Le démarrage de la phase opérationnelle doit être compris entre la date de publication de l'arrêté du 18 mars 2024 (22 mars 2024) et le 20 septembre 2024. 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. Pour réaliser cet audit, il est possible de solliciter : • 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 de modalités de restitution des résultats.
Valeur cible / seuil d'éligibilité	Nombre d'audits d'exposition internet de l'ensemble des domaines et adresses IP publics : • Du GHT pour les établissements publics membres d'un GHT • De l'entités juridique pour les établissements publics hors GHT et les établissements privés
Textes de référence	Le cahier des charges audit d'exposition internet de l'ANS Le service SILENE

2. Production de l'indicateur	
Unité	Booléen
Modalité de calcul	Par candidature : • 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 le 20/11/2024, la réalisation régulière des audits d'exposition internet sera considérée respectée (la **date du 20/09 étant la date limite de début de la phase opérationnelle, la date du 20/11 est implicitement la date butoir** pour que chaque candidat ait réalisé un premier audit d'exposition internet, cf. arrêté rectificatif du 22 janvier).

	• Dans le cas où l'établissement sollicite une plateforme d'audit industrielle, l'intervalle entre 2 audits doit être de 60 jours maximum. ET • Nombre de mois phase opérationnelle / Nombre d'audits réalisé ≤ 2
Période	• Sur la durée de l'appel à financement (phase opérationnelle)
Fréquence	• Une fois lors du dépôt de preuve

3. Restitution de l'objectif	
Remontée de l'information	• Dépôt sur le guichet de déclaration d'atteinte des objectifs
Documents justificatifs	• Liste des domaines exposés • Liste des adresses IP publiques • Rapports d'audit d'exposition internet réalisés
Opération de contrôle	Eléments contrôlés : • 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.O2.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	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. 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.
Valeur cible / seuil d'éligibilité	**Pour les GHT, les établissements publics hors GHT et les établissements privés :** : • Absence de vulnérabilités critiques sur les 2 derniers audits successifs d'exposition internet sur l'ensemble du périmètre 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. NB 2 : Au moment de la déclaration d'atteinte des objectifs sur le guichet dédié, le dernier audit réalisé devra dater d'un mois maximum NB 3 : Le dernier audit doit être conforme aux objectifs fixés, et il doit y avoir eu un autre audit datant d'au moins 45 jours et d'au plus 60 jours, également conforme aux objectifs.
Textes de référence	Le cahier des charges audit d'exposition internet de l'ANS

2. Production de l'indicateur	
Unité	Booléen
Modalité de calcul	Pour chaque établissement : • Nombre de vulnérabilités critiques sur les 2 derniers audits successifs d'exposition internet = 0
Période	• Sur la durée de l'appel à financement (phase opérationnelle)
Fréquence	• Une fois lors du dépôt de preuve

3. Restitution de l'objectif	
Remontée de l'information	• Dépôt sur le guichet de déclaration d'atteinte des objectifs
Documents justificatifs	• 2 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)
Opération de contrôle	Eléments contrôlés : • Vérification de l'atteinte du score cible sur les deux derniers audits ; • 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	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). Objectif : Un premier exercice de crise cyber doit être réalisé au sein de tous les établissements du candidat (au sens FINESS PMSI) **entre le 1er janvier 2023 et la date de dépôt de la déclaration d'atteinte des objectifs** par l'établissement sur le guichet dédié.
Valeur cible / seuil d'éligibilité	L'ensemble des établissements au sens FINESS PMSI devront avoir réalisé un exercice : • 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	• 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	• N/A
Période	• Sur la durée de l'appel à financement (phase opérationnelle)
Fréquence	• Une fois lors du dépôt de preuve

3. Restitution de l'objectif	
Remontée de l'information	• Saisie de la donnée dans l'oSIS par l'établissement
Documents justificatifs	• 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 :

	• 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 les champs suivants : • Part du budget numérique dans le budget global de l'ES • 43 mesures prioritaires
Textes de référence	• Document "Référentiel des mesures prioritaires" publié par le Ministère

2. Production de l'objectif	
Unité	Booléen (O/N)
Modalité de calcul	• N/A
Période	• Sur la durée de l'appel à financement (phase opérationnelle)
Fréquence	• Une fois lors du dépôt de preuve

3. Restitution de l'objectif	
Remontée de l'information	• Saisie dans l'oSIS
Documents justificatifs	• Une capture d'écran d'oSIS peut être communiquée
Opération de contrôle	Eléments contrôlés : • 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	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 nécessaire de disposer au sein des budgets des ES d'une part suffisante dédiée au numérique et à la sécurité des SI. 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)
Valeur cible / seuil d'éligibilité	La Part du budget dédiée au numérique et les ETP doivent être restitués au niveau d'une entité juridique (EJ) : • Pour les GHT : les valeurs sont à renseigner pour chaque entité juridique constituant le GHT
Textes de référence	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 **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. **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).

2. Production de l'indicateur	
Unité	• Part du numérique dans le budget : Pourcentage • ETP : nombre de personnels
Modalité de calcul	• Numérateur = total des dépenses liées aux comptes couvrant le champ du numérique | Dénominateur = total des dépenses tous comptes confondus

	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).
Période	• 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	• Une fois lors du dépôt de preuve

3. Restitution de l'objectif	
Remontée de l'information	• Saisie dans l'oSIS
Documents justificatifs	• Une capture d'écran d'oSIS peut être communiquée
Opération de contrôle	Eléments contrôlés : • 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 publics hors GHT et 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	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. 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.

Valeur cible / seuil d'éligibilité	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 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	• N/A
Période	• Sur la durée de l'appel à financement (phase opérationnelle)
Fréquence	• Une fois lors du dépôt de preuve

3. Restitution de l'objectif	
Remontée de l'information	• Dépôt sur le guichet de déclaration d'atteinte des objectifs

Documents justificatifs	• Constitution de l'équipe projet • Schéma de le gouvernance mise en place
Opération de contrôle	Eléments contrôlés : • Désignation du chef de projet en charge du domaine • Composition équipe en charge de la gestion des AD au niveau du GHT

D1.O6.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	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. 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. 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.
Valeur cible / seuil d'éligibilité	Le GHT doit formaliser, présenter et faire valider par le comité stratégique du GHT : • 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. 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.
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	• N/A

Période	• Sur la durée de l'appel à financement (phase opérationnelle)
Fréquence	• Une fois lors du dépôt de preuve

3. Restitution de l'objectif	
Remontée de l'information	• Dépôt sur le guichet de déclaration d'atteinte des objectifs
Documents justificatifs	• Trajectoire de convergence des AD qui adresse l'ensemble des établissements du GHT
Opération de contrôle	Eléments contrôlés : • Trajectoire de convergence et planning associé • Modalités organisationnelles à mettre en œuvre