Guide des prérequis et objectifs

Appel à Financement relatif à un programme de financement destiné à renforcer la sécurité numérique des établissements de santé - Fonction « Stratégie de continuité et de reprise d'activité »



Historique du document – Suivi des modifications apportées			
Version	Date	Auteur	Commentaires / modifications
V0.0.1	02/07/2024	Équipe programme CaRE	Version initiale
V0.0.2	24/10/2024	Équipe programme CaRE	Version de travail - *avancée*
V0.1.0	19/11/2024	Équipe programme CaRE	Version de travail soumise à concertation des régions et du groupe de travail
V0.1.1	19/12/2024	Équipe programme CaRE	Version de travail soumise à concertation des fédérations hospitalières
V1.0.0	16/07/2025	Équipe programme CaRE	Version publiée
V1.1.1	26/08/2025	Équipe programme CaRE	D2.P1 : Modification de la période durant laquelle la PSSI doit avoir été mise à jour et validée D2.02.A : Modification de la période durant laquelle la politique de sauvegarde et de restauration doit avoir été mise à jour et validée Modification de la date de fermeture du guichet de paiement. Ajout de la partie « Éligibilité des dépenses »

			Ajouts de précisions sur certains éléments du guide (Éléments surlignés ci-dessous)
V1.1.2	04/09/2025	Équipe programme CaRE	Modifications mineures
V1.1.3	29/10/2025	Équipe programme CaRE	Ajouts de précisions sur certains éléments du guide (Éléments surlignés ci-dessous)
V1.1.4	17/12/2025	Équipe programme CaRE	Ajouts de précisions sur certains éléments du guide (Éléments surlignés ci-dessous)
V1.1.5	30/01/2026	Équipe programme CaRE	Modifications mineures
V1.1.6	06/05/2026	Équipe programme CaRE	Ajouts de précisions sur certains éléments du guide (Éléments surlignés ci-dessous)

SOMMAIRE

Sommaire 3

1 Objectif de ce guide 4

2 Prérequis du domaine « Stratégie de continuité et de reprise d'activité » 7

2.1 D2.P1 : Disposer d'une Politique de Sécurité des Systèmes d'Information (PSSI) formalisée et à jour 7

2.2. D2.P2 : Décrire l'organisation prévue pour la mise en œuvre du Plan de Continuité et de Reprise d'Activité 9

3 Eligibilité des dépenses 10

4 Objectifs du Domaine « Stratégie de continuité et de reprise d'activité » 12

D2.O1 – Inclure la gestion de la Continuité et Reprise d'activité dans la gouvernance des établissements 12

D2.O1.A - Mettre en place une gouvernance pour la Continuité et de Reprise d'activité 12

D2.O1.B - Décrire les procédures de réponse à la crise cyber 14

D2.O1.C - Formaliser un plan de continuité d'activité (PCA) et un plan de reprise d'activité (PRA) 16

D2.O1.D - Tester la mise en œuvre d'un Plan de Continuité d'Activité (PCA) dans un exercice terrain 18

4.1 D2.O2 – Définir, documenter et tenir à jour la politique et le(s) plan(s) de sauvegarde et de restauration 21

D2.O2.A - Définir une politique de sauvegarde et de restauration et la maintenir à jour 21

D2.O2.B - Formaliser un/des plan(s) de sauvegarde et de restauration et le(s) maintenir à jour 24

D2.O3 – Construire un système de sauvegarde sécurisé 26

D2.O3.A – Mettre en œuvre une authentification sécurisée pour les infrastructures de sauvegarde .. 26

D2.O3.B – S'inscrire dans une trajectoire pour un cloisonnement de son infrastructure de sauvegarde 28

D2.O3.C – S'inscrire dans une trajectoire pour la mise en œuvre du 3-2-1 30

D2.O3.D – Mettre en place une supervision des sauvegardes 32

D2.O4 – Tester la sauvegarde et la restauration 34

D2.O4 – Tester la sauvegarde et la restauration 34

1 OBJECTIF DE CE GUIDE

L'objectif de ce guide est de détailler les prérequis et objectifs du domaine « Stratégie de continuité et de reprise d'activité ».

Pour rappel et conformément à l'arrêté du 3 juillet 2025 relatif à un programme de financement destiné à renforcer la sécurité numérique des établissements de santé - Fonction « Stratégie de continuité et de reprise d'activité », 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. Les GHT sont toutefois invités à associer les EG médico-sociales rattachées à des EJ sanitaires aux travaux relatifs à la politique et aux plans de sauvegarde prévus dans le domaine, notamment lorsqu'ils reposent sur l'infrastructure commune de l'établissement support. Cependant, ces EG médico-sociales ne sont pas prises en compte dans le calcul du financement attribué à l'établissement candidat.

  - Pour les structures éligibles ne faisant pas partie d'un GHT : la demande de candidature au financement doit être portée par l'entité juridique.

- **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.

Ci-dessous, le tableau récapitulatif des prérequis et objectifs de l'appel à financement « Stratégie de continuité et de reprise d'activité ».

Les prérequis et objectifs fixés dans le cadre de ce domaine doivent être traités, sauf mention contraire, par :

- Tous les établissements parties du Groupement Hospitalier de Territoire (GHT) ;
- Entité Juridique (EJ), pour les candidats hors GHT.

La mention candidat, constitue une mention générique qui traite les deux cas précités de candidats GHT et hors GHT.

Prérequis	Description
D2.P1 : Disposer d'une Politique de Sécurité des Systèmes d'Information (PSSI) formalisée et à jour	Le candidat doit fournir sa politique de sécurité des systèmes d'information (PSSI). Ce document doit être validé et revu entre le 16 juillet 2022 et la date de dépôt de candidature.
D2.P2 : Décrire l'organisation prévue pour la mise en œuvre du Plan de Continuité et de Reprise d'Activité	Le candidat doit décrire l'organisation projet mise en place pour assurer la construction et le maintien dans le temps de son plan de continuité et de reprise d'activité.

Objectifs	Description
D2.O1 : Inclure la gestion de la Continuité et Reprise d'activité dans la gouvernance des établissements	
D2.O1.A - Mettre en place une gouvernance pour la Continuité et de Reprise d'activité	Le candidat doit élaborer un schéma de gouvernance décrivant la démarche mise en place pour la continuité et la reprise d'activité.
D2.O1.B - Décrire les procédures de réponse à la gestion de crise cyber	Le candidat doit : • Intégrer les risques numériques dans le plan blanc. • Formaliser ou revoir les procédures de crise cyber, incluant l'organisation de la cellule de crise et les modalités de signalement.
D2.02.C - Formaliser un plan de continuité d'activité (PCA) et un plan de reprise d'activité (PRA)	Le candidat doit formaliser un Plan de Continuité et de Reprise d'Activité (PCRA) en s'appuyant sur la réalisation de bilans d'impacts sur l'activité, a minima sur les périmètres suivants s'ils existent au sein de la structure du candidat : • Un service de soins ayant un impact majeur sur la prise en charge du patient. • Le processus administratif le plus critique pour l'établissement (exemples paie, comptabilité, gestion des fournisseurs, etc.). • Plateau technique en lien avec le parcours de soins tel que la pharmacie, l'imagerie, la biologie.
D2.O1.D - Tester la mise en œuvre d'un Plan de Continuité d'Activité (PCA) dans un exercice terrain	Le candidat doit : • Effectuer un test pour la mise en œuvre d'au moins un PCA sur un périmètre défini par le candidat dans le cadre d'un exercice terrain adapté pendant la phase opérationnelle. • Etablir un planning de test des autres exercices de PCA.
D2.O2 : Définir, documenter et tenir à jour la politique et le(s) plan(s) de sauvegarde et de restauration	
D2.O2.A - Définir une politique de sauvegarde et de restauration et la maintenir à jour	Le candidat doit fournir sa politique de sauvegarde et de restauration validée. Elle doit pouvoir s'appliquer aux prestations externalisées et aux applications gérées en mode SaaS par le biais de clauses contractuelles avec le prestataire, et doit avoir été mise à jour entre le 16 juillet 2022 et la date de dépôt du dossier d'atteinte des objectifs.
D2.O2.B - Formaliser un/des plan(s) de sauvegarde et de restauration et le(s) maintenir à jour	Le candidat doit fournir les plans de sauvegarde de ses systèmes d'information critiques, tels qu'identifiés dans le sous-objectif D2.O1.C, ainsi que les procédures de leur mise à jour.
D2.O3 : Construire un système de sauvegarde sécurisé	
D2.O3.A – Mettre en œuvre une authentification sécurisée pour les infrastructures de sauvegarde	Le candidat doit disposer d'un système d'authentification indépendant (AD dédié, comptes locaux, …) pour ses infrastructures de sauvegarde.

D2.O3.B – S'inscrire dans une trajectoire pour un cloisonnement de son infrastructure de sauvegarde	Le candidat doit s'inscrire dans une démarche visant à cloisonner les infrastructures de sauvegarde au sein du système d'information et disposer d'une capacité technique d'isolation en cas d'incident (mode « bouton rouge »).
D2.O3.C - S'inscrire dans une trajectoire pour la mise en œuvre du 3-2-1	Le candidat doit s'inscrire dans une démarche pour la mise en œuvre du 3-2-1 avec une trajectoire définie et des jalons clés. Cette démarche vise à mettre en place une copie immuable de ses sauvegardes hors ligne ou hors site (dans deux bâtiments distincts, si applicable par l'établissement, chez un hébergeur tiers, etc.).
D2.O3.D - Mettre en place une supervision des sauvegardes	Le candidat doit instaurer et documenter une organisation pour assurer le suivi efficace des sauvegardes, incluant un plan d'actions pour vérifier leur bonne exécution et des procédures à suivre en cas d'échec.
D2.O4 – Tester la sauvegarde et la restauration	Le candidat doit : • Réaliser au moins un test technique de bon fonctionnement des sauvegardes et de remise en ligne des restaurations dans le système pendant la phase opérationnelle sur un périmètre d'un SI concourant à une des activités identifiées dans le cadre de l'objectif D2.O1.C. • Identifier au minimum un référent ou correspondant métier en prévision de la réalisation des tests fonctionnels sur les applications métiers critiques telles qu'identifiées dans le sous-objectif D2.O1.C.

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 :

- La date de publication de l'arrêté relatif à la fonction « Stratégie de continuité et de reprise d'activité »
- Le dépôt de la déclaration d'atteinte des objectifs par le candidat sur le guichet dédié.

2 PREREQUIS DU DOMAINE « STRATEGIE DE CONTINUITE ET DE REPRISE D'ACTIVITE »

2.1 D2.P1 : Disposer d'une Politique de Sécurité des Systèmes d'Information (PSSI) formalisée et à jour

Domaine	**Domaine « Stratégie de continuité et de reprise d'activité »**
Prérequis	**Disposer d'une Politique de Sécurité des Systèmes d'Information (PSSI) formalisée et à jour**
1. Définition du prérequis	
Définition	Présence d'une PSSI à jour revue et validée.
Valeur cible / seuil d'éligibilité	Le candidat doit disposer d'une PSSI validée et revue entre le 16 juillet 2022 et la date de dépôt de candidature. En fonction de son organisation, ce document peut être fourni par candidat ou par chaque établissement constituant le candidat. Si l'entité juridique ou le GHT ne fournit pas une PSSI unique, l'établissement porteur de la candidature doit s'assurer que chaque établissement dispose de sa propre PSSI, signée par le directeur de l'établissement : - Pour les GHT, ce document peut être fourni au niveau des Entités Juridiques. - Pour les EJ, ce document peut être fourni par Entité Géographique.
Textes de référence	• Guide PSSI *(en cours de construction)* • Guide d'élaboration de PSSI (ANSSI) • Guide pratique organisationnel PGSSI-S

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	• Dépôt des pièces justificatives sur la plateforme de candidature.

Documents justificatifs	• La PSSI validée par le représentant légal du candidat ou, le cas échéant, par chaque établissement du groupement et revue entre le 16 juillet 2022 et la date de dépôt de candidature. OU • Un document de présentation de la PSSI (et non la PSSI complète) selon un formalisme laissé à leur appréciation. Le document de présentation devra néanmoins présenter (i) la date de mise à jour, (ii) le signataire de la PSSI (iii) le périmètre des entités juridiques et/ou géographiques appliquant cette politique et doit être signé par le référent de cette politique.
Opération de contrôle	• Contrôle sur pièces.

2.2. D2.P2 : Décrire l'organisation prévue pour la mise en œuvre du Plan de Continuité et de Reprise d'Activité

Domaine	**Domaine « Stratégie de continuité et de reprise d'activité »**
Prérequis	**Décrire l'organisation prévue pour la mise en œuvre du Plan de Continuité et de Reprise d'Activité**
1. Définition du prérequis	
Définition	Existence d'une organisation pour la mise en œuvre et la gestion du Plan de Continuité et de Reprise d'Activité dans le cadre du présent domaine.
Valeur cible / seuil d'éligibilité	Le candidat doit décrire le schéma d'organisation projet mise en place pour assurer la gestion de la continuité et la reprise d'activité. L'écriture des plans de continuité et de reprise d'activité est exigée dans le cadre de l'objectif D2.O1 du présent domaine. Si l'entité juridique ou le GHT ne fournit pas un document unique décrivant l'organisation projet, l'établissement porteur de la candidature doit s'assurer que chaque établissement constituant le candidat dispose de sa propre organisation projet : • Pour les GHT, ce document peut être fourni au niveau des Entités Juridiques. • Pour les EJ, ce document peut être fourni par Entité Géographique. ***Recommandation concernant le Responsable du Plan de Continuité et de Reprise d'Activité (RPCRA) :*** - Il est recommandé, en particulier pour les établissements avancés en termes de gestion de la continuité et de reprise d'activité, de désigner un RPCRA (Fiche de poste disponible sur le site de l'ANS). Ce responsable est chargé de la construction d'un Système de Management de Continuité d'Activité, du maintien en conditions opérationnelles de ce dispositif, ainsi que de la gestion de crise et de la continuité d'activité. - Il peut s'agir d'une fonction ou d'une mission, et non nécessairement d'un poste dédié. Cette fonction ou mission peut également être externalisée. - **La désignation d'un RPCRA n'est pas obligatoire pour remplir ce prérequis.** L'instruction N° DNS/2025/12 du 22 janvier 2025 exige la désignation d'un responsable PCA/PRA de ce rôle au plus tard fin juin 25. Cependant, lors des travaux de construction du présent domaine, il a été souligné la complexité de cette désignation notamment pour les plus petites structures. Afin que cela ne représente pas de frein pour la candidature de ces établissements, il est attendu que le financement apporté dans le cadre de ce domaine puisse constituer un levier de création de ce rôle de RPCRA pour les établissements qui n'en disposent pas

	lors de la phase de candidature pour une mise en conformité avec l'instruction en vigueur.
Textes de référence	• N/A

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	• Dépôt sur le guichet de candidature des pièces justificatives.
Documents justificatifs	• Document décrivant l'organisation projet avec la constitution de l'équipe projet et d'une gouvernance du projet.
Opération de contrôle	• Contrôle sur pièces.

3 ELIGIBILITE 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 2 sont éligibles à un subventionnement. À titre d'exemple, le recours à la prestation externe, l'acquisition d'un SMCA ou encore la mise en œuvre d'un nouveau système de sauvegarde sécurisée sont éligibles – étant entendu que cette liste n'est pas exhaustive. Il est à noter que l'ensemble des dépenses réalisées durant la phase opérationnelle concourants à l'élaboration du PCRA seront éligibles, y compris si le périmètre dépasse le périmètre minimal défini dans les objectifs tout en restant dans les cibles fixées par ceux-ci. En ce qui concerne les objectifs visant à « s'inscrire dans une démarche », les investissements opérationnels réalisés pour définir cette démarche ou la mettre en œuvre sont bien valorisables au titre de l'AAF domaine 2.

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 au 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),

- ou la mobilisation de personnels disposant des justificatifs nécessaires (lettre de mission, feuille de temps).

Concernant les dépenses éligibles au titre des objectifs de formalisation du PCA/PRA (D2.O1.C) et de la politique de sauvegarde (D2.O2.A) : les dépenses liées à la définition de la stratégie sont prioritaires. Les dépenses de mise en œuvre ne sont éligibles que si elles répondent directement aux éléments formalisés.

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.

Une trame de justification des coûts – similaire dans son formalisme à celle du Domaine 1 – sera également fournie.

4 OBJECTIFS DU DOMAINE « STRATEGIE DE CONTINUITE ET DE REPRISE D'ACTIVITE »

Le pilotage de la réponse au présent domaine et le suivi de l'atteinte de ses objectifs doit être pilotée par l'ES support au niveau du GHT. Une gouvernance transverse du projet doit être mise en place pour l'ensemble du GHT permettant d'atteindre les objectifs.

D2.O1 – Inclure la gestion de la Continuité et Reprise d'activité dans la gouvernance des établissements

D2.O1.A - Mettre en place une gouvernance pour la Continuité et de Reprise d'activité

Domaine	**Domaine « Stratégie de continuité et de reprise d'activité »**
Objectif	**Mettre en place une gouvernance pour la Continuité et de Reprise d'activité**
1. Définition de l'objectif	
Définition	Cet objectif vise à permettre aux établissements de : • **Anticiper** : Contribuer à la politique de réduction des risques. • **Continuer l'activité** : Réduire les conséquences de l'évènement perturbateur. • **Reprendre l'activité** : Garantir une reprise normale des activités.
Valeur cible / seuil d'éligibilité	Le candidat doit élaborer un schéma de gouvernance décrivant la démarche mise en place pour la continuité et la reprise d'activité. Ce document doit être signé par la direction du candidat. Ce schéma doit permettre d'établir une gouvernance pour la continuité et la reprise d'activité incluant notamment la constitution d'un comité de pilotage, l'organisation de réunions régulières pour le suivi du projet. Cette démarche devra s'inscrire dans une logique de pérennité au-delà du présent domaine.
Textes de référence	• Instruction n° DNS/2025/12 du 22 janvier 2025 relative à l'obligation de mettre en œuvre des actions urgentes ou prioritaires au service de la sécurité des systèmes d'information dans les établissements sanitaires

2. Production de l'objectif	
Unité	• Booléen
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	• N/A
Documents justificatifs	Le candidat doit fournir : • Le schéma de gouvernance signé par la direction de l'établissement / GHT explicitant la démarche mise en place pour la continuité et la reprise d'activité (Contexte, prérequis, objectifs, bénéfices attendus, portée / périmètre, équipe / responsables et leurs rôles, comitologie, macro-planning, processus et méthodologie, communication, indicateurs de suivi, etc.) accompagné du • Compte-rendu d'une instance de direction du candidat où le schéma de gouvernance a été présenté et validé (CODIR, COSTRAT, ...).
Opération de contrôle	• Contrôle sur pièces.

D2.O1.B - Décrire les procédures de réponse à la crise cyber

Domaine	**Domaine « Stratégie de continuité et de reprise d'activité »**
Objectif	**Décrire les procédures de réponse à la gestion de la crise cyber**
1. Définition de l'objectif	
Définition	La sécurité des systèmes d'information et la gestion des incidents sont devenues une priorité pour les pouvoirs publics. Les attaques peuvent menacer directement non seulement le système d'information des établissements, mais aussi la prise en charge des patients. Ces attaques peuvent paralyser les communications internes et externes de l'établissement de santé et perturber jusqu'à l'interruption de l'offre de soins. Il est donc essentiel que les établissements s'engagent dans la définition et la mise en œuvre d'un plan de réponse aux incidents numériques de manière générale, et en particulier des cyberattaques.
Valeur cible / seuil d'éligibilité	Le candidat doit : • Intégrer les risques numériques dans le plan blanc. • Formaliser ou revoir les procédures de crise cyber, incluant l'organisation de la (les) cellule(s) de crise et les modalités de signalement. Remarque : il est recommandé que le plan blanc (ou son extrait) puisse permettre d'identifier : • la prise en compte explicite du risque numérique comme un type de crise à part entière ; • les conditions de déclenchement d'une gestion de crise cyber ; • l'organisation de la cellule de crise en cas d'incident numérique (rôles, pilotage, articulation avec la direction et le SI) ; • les principes généraux de gestion de la crise (coordination, communication, signalement).
Textes de référence	• N/A

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	• Dépôt des pièces justificatives sur la plateforme de candidature.

Documents justificatifs	• Plan blanc (ou extrait du plan blanc) du candidat (ou des établissements constituant le candidat) intégrant les modalités de gestion des risques numériques et décrivant notamment l'organisation de la / les cellules de crise. Un candidat peut soumettre un « plan blanc » couvrant plusieurs entités juridiques ou géographiques, en veillant à ce que le document soumis précise son périmètre d'application et intègre – le cas échéant – les spécificités des différentes structures. • Procédure décrivant les modalités de signalement (montante et descendante) en place. Remarque : les modalités de signalement montantes correspondent aux processus organisant la remontée vers les autorités externes compétences en cas d'incident. Les modalités de signalement descendantes correspondent aux processus organisant la prise en compte et le traitement d'une alerte reçue.
Opération de contrôle	• Contrôle sur pièces.

D2.O1.C - Formaliser un plan de continuité d'activité (PCA) et un plan de reprise d'activité (PRA)

Domaine	**Domaine « Stratégie de continuité et de reprise d'activité »**
Objectif	**Formaliser un plan de continuité d'activité (PCA) et un plan de reprise d'activité (PRA)**
1. Définition de l'objectif	
Définition	Pour aider les établissements à renforcer leur résilience, il est important de mettre en œuvre des mesures permettant de réagir efficacement en cas de crise majeure. Cela inclut la préservation des activités critiques et la garantie de la reprise rapide de leurs activités.
Valeur cible / seuil d'éligibilité	Le candidat doit formaliser un Plan de Continuité et de Reprise d'Activité (PCRA) en s'appuyant, dans la mesure du possible, sur les kits nationaux mis à disposition par l'Agence du Numérique en Santé. L'attendu minimal porte sur la formalisation de chaque activité critique ayant fait l'objet d'un BIA. La réalisation d'un PCRA cadre est vivement recommandée mais n'est pas exigée dans le cadre de l'atteinte de l'objectif. Le PCA et le PRA portent sur les aspects métiers et organisationnels de l'établissement, au-delà de l'aspect informatique seul. Il est fortement recommandé de traiter les 4 scénarios d'indisponibilités listés dans le kit PCA / PRA proposé par l'ANS : indisponibilité des ressources humaines, indisponibilité bâtimentaires, indisponibilité des fournisseurs et indisponibilité informatique. Toutefois, seul le traitement du scénario d'indisponibilité des systèmes d'information et d'un second scénario au choix sont obligatoires pour atteindre la cible. Lors de la rédaction du projet PCRA, un bilan d'impacts sur les activités (BIA) doit être réalisé pour analyser la criticité et l'impact temporel d'une perturbation sur l'établissement. L'établissement devra réaliser un BIA sur a minima 3 services critiques devant inclure : • Un service de soins ayant un impact majeur sur la prise en charge du patient. • Un plateau technique en lien avec le parcours de soins tel que la pharmacie, l'imagerie, la biologie. • Le processus administratif/support le plus critique pour l'établissement (exemple : paie, comptabilité, gestion des fournisseurs, blanchisserie, restauration, etc.). Le candidat est libre du choix de ce second scénario d'indisponibilité, qui peut être différent pour chaque périmètre. Il est suggéré pour les établissements possédant des activités de recours, d'inclure l'une de celle-ci dans les BIA demandés. Le candidat pourra alors définir un PCRA sur la base des conclusions des BIA réalisés.

	Remarque : pour les candidats ne disposant pas d'un plateau technique, il est demandé de remplacer le BIA/PCRA attendu au titre du plateau technique par : - La réalisation d'un BIA/PCRA sur un 2nd service de soins ; - Si le candidat dispose d'un unique service de soins, il est invité à réaliser un BIA/PCRA sur un 2nd service administratif / support Pour les GHT avec plusieurs entités juridiques (FINESS EJ) - Les BIA et les PCRA doivent être formalisés pour un nombre d'EJ représentant au moins 66% de l'activité combinée du candidat. Pour les candidats hors GHT ayant plusieurs entités géographiques (FINESS EG) - Les BIA et les PCRA doivent être formalisés pour un nombre d'EG représentant au moins 66% de l'activité combinée du candidat. Remarque : un candidat peut traiter de manière unique les BIA et le PCRA d'un SI mutualisé* dans le cadre du risque numérique uniquement. Il pourra soumettre un unique document, en portant une vigilance quant à l'analyse des impacts en termes de processus et à l'applicabilité des mesures de continuité d'activités aux différentes entités utilisant le SI mutualisé*. Les BIA et le PCRA soumis devront clairement préciser le périmètre des entités (juridiques ou géographiques) couvertes par ces documents. Si un des périmètres retenus conformément à la liste dessus est applicable aux établissements constituant le candidat, alors le BIA peut être fourni à l'échelle du candidat. * Un SI est considéré comme mutualisé lorsqu'il repose sur une instance unique, ou lorsque le même applicatif est déployé dans plusieurs établissements avec la même version, le même paramétrage et la même organisation.
Textes de référence	• Guide 2024 de la HAS pour la certification des établissements de santé pour la qualité des soins. • Kit PCA-PRA de l'ANS • Guide la continuité d'activité, SGDSN

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	• Dépôt des pièces justificatives sur la plateforme de candidature.
Documents justificatifs	• Bilans d'impacts sur l'activité - BIA (Autant de BIA que de périmètres à minima) • Document énumérant les activités critiques sur les périmètres à minima de chaque établissement. • Si un ou plusieurs BIA non réalisés : Motif(s) de non-présence du document. • Plans de Continuité d'Activité / Plans de Reprise d'Activité sur les activités critiques identifiées ayant fait l'objet d'un BIA
Opération de contrôle	• Contrôle sur pièces.

D2.O1.D - Tester la mise en œuvre d'un Plan de Continuité d'Activité (PCA) dans un exercice terrain

Domaine	**Domaine « Stratégie de continuité et de reprise d'activité »**
Objectif	**Tester la mise en œuvre d'un Plan de Continuité d'Activité (PCA) dans un exercice terrain**
1. Définition de l'objectif	
Définition	Les exercices sont **essentiels** pour **tester la mise en œuvre et l'efficacité des solutions de continuité d'activité définies.** Ils permettent de clarifier les missions spécifiques de chaque fonction en cas d'événement perturbateur, et d'assurer une gestion globale efficace de ce dispositif. Un test PCA ou exercice terrain simule en temps réel l'indisponibilité d'une ou plusieurs ressources critiques et teste la mise en œuvre des solutions de continuité d'activité à l'échelle des services de soins (niveau opérationnel). Il est également possible d'y éprouver la coordination et la conduite (niveau tactique) ainsi que le pilotage (niveau stratégique). Remarque : le test constitue une simulation d'arrêt (d'un service, d'une ressource ou d'un périmètre défini), réalisée de manière contrôlée. Ces exercices permettent de recueillir des retours d'expérience et de définir un plan d'actions visant à maintenir le Système de Management de la Continuité d'Activité.
Valeur cible / seuil d'éligibilité	Le candidat doit : • Effectuer un test pour la mise en œuvre d'au moins un PCA sur un périmètre défini par le candidat* et sur un scénario donné dans le cadre d'un exercice terrain adapté pendant la phase opérationnelle**. • Planifier les autres exercices de PCA. Il est fortement recommandé de réaliser un test portant sur les 4 scénarios d'indisponibilités listés dans le kit PCA / PRA proposé par l'ANS : indisponibilité des ressources humaines, indisponibilité bâtimentaires, indisponibilité des fournisseurs et indisponibilité

	informatique. Toutefois, seul le test d'un scénario à choisir par le candidat est obligatoire. Pour les GHT avec plusieurs entités juridiques (FINESS EJ) : - Le test de PCA doit être réalisé pour un nombre d'EJ représentant au moins 66% de l'activité combinée du candidat. Pour les candidats hors GHT ayant plusieurs entités géographiques (FINESS EG) : - Le test de PCA doit être réalisé pour un nombre d'EG représentant au moins 66% de l'activité combinée du candidat. **Attention :** • Les exercices PCRA ne peuvent pas se substituer à l'exercice annuel de crise cyber obligatoire. • Il est en revanche possible de réaliser simultanément un exercice de cybercrise (dans le format connu, et notamment exigé au titre du Domaine 1) et un exercice de continuité d'activité au sein des services. **Spécificités pour les SI mutualisés*** :** • Réaliser un test d'un PCA au niveau du candidat sur un périmètre inclus dans le SI mutualisé sur un scénario choisi par l'établissement. Le test doit être réalisé à l'échelle d'un service : si les services d'une entité A et d'une entité B s'appuient sur un même SI mutualisé, alors le test doit être réalisé sur chacun des services des deux entités. Le scénario de test doit être identique et il est recommandé de le réaliser simultanément sur les sites concernés * En fonction de ses priorités et de sa capacité opérationnelle avec à minima un service / périmètre testé. ** Phase opérationnelle : phase comprise entre : • La publication de l'arrêté relatif à la fonction « Stratégie de continuité et de reprise d'activité » • Le dépôt de la déclaration d'atteinte des objectifs par le candidat sur le guichet dédié. *** Un SI est considéré comme mutualisé lorsqu'il repose sur une instance unique, ou lorsque le même applicatif est déployé dans plusieurs établissements avec la même version, le même paramétrage et la même organisation.
Textes de référence	

2. Production de l'objectif	
Unité	• Booléen
Modalité de calcul	• N/A
Période	• Sur la durée de l'appel à financement (pendant la phase opérationnelle).

Fréquence	•	Une fois lors du dépôt de preuve.

3. Restitution de l'objectif		
Remontée de l'information	•	N/A
Documents justificatifs	•	PCA utilisé dans le cadre de l'exercice sur une des activités critiques (sauf si celui-ci a déjà été fourni dans l'objectif O1.C). Scénario de test du PCA. RETEX se basant sur le rapport à la suite de l'exercice et incluant un plan d'amélioration du PCA. Planning de réalisation des autres exercices
Opération de contrôle	•	Contrôle sur pièces.

4.1 D2.O2 – Définir, documenter et tenir à jour la politique et le(s) plan(s) de sauvegarde et de restauration

D2.O2.A - Définir une politique de sauvegarde et de restauration et la maintenir à jour

Domaine	**Domaine « Stratégie de continuité et de reprise d'activité »**
Objectif	**Définir une politique de sauvegarde et de restauration et la maintenir à jour**
1. Définition de l'objectif	
Définition	La sauvegarde des systèmes d'information opérée par un établissement, initialement utile dans le cas d'incidents opérationnels tels que les pannes matérielles, est désormais indispensable pour répondre efficacement aux incidents de sécurité et d'assurer la continuité et la reprise d'activité. La politique de sauvegarde est un ensemble de directives et de règles établies au sein d'un établissement pour protéger l'ensemble de ses données. Elle vise à garantir que toutes les données importantes soient sauvegardées régulièrement et de manière sécurisée, en fonction de la criticité des activités qu'elles soutiennent. La politique de sauvegarde et de restauration énonce le cadre général tandis que les plans de sauvegarde et les procédures de restauration décrivent les processus pour suivre les règles décrites dans la politique.
Valeur cible / seuil d'éligibilité	Le candidat doit fournir sa politique de sauvegarde et de restauration validée. Elle doit pouvoir s'appliquer aux prestations externalisées et aux applications gérées en mode SaaS par le biais de clauses contractuelles avec le prestataire, et doit avoir été mise à jour entre le 16 juillet 2022 et la date de dépôt du dossier d'atteinte des objectifs. La politique de sauvegarde et de restauration doit inclure, a minima, les éléments suivants : • Les types de données à sauvegarder (base de données, applications, serveurs, documents, ...). • Hiérarchisation des données en fonction de leur criticité. • La fréquence des sauvegardes en fonction de la criticité des données. • Le délai de rétention en fonction de la typologie des données. • La planification des sauvegardes en fonction de l'activité. • Les responsabilités des personnels impliqués dans le processus des sauvegardes. • Les exigences de conformité légale et réglementaire (RGPD, CNIL, ...). • Les procédures de mise à jour de la politique de sauvegarde. • Les mesures de sécurisation des sauvegardes (chiffrement, contrôle d'accès, ...). • Les mesures sur la confidentialité et l'intégrité des données.

	Spécificités pour les SI mutualisés : • Les candidats multi-établissements doivent élaborer une politique de sauvegarde et de restauration visant à harmoniser les pratiques avec un planning prévisionnel sur les 18 mois post appel à financement domaine stratégie de continuité et de reprise d'activité. • Pour les GHT dont un ou plusieurs établissements parties comptent des EG médico-sociales, celles-ci peuvent être intégrées dans cette politique visant à harmoniser les pratiques au sein du GHT. Il est entendu par le terme « harmonisation » une stratégie de sauvegarde cohérente entre établissements pour les SI sous-tendant une même activité, un cadre documentaire partagé, etc. Il n'est pas attendu une unification du système de sauvegarde par exemple.
Textes de référence	• PGSSI-S • Clausier de sécurité numérique du Club RSSI Santé

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 des pièces justificatives sur la plateforme de candidature.
Documents justificatifs	• Politique de sauvegarde et de restauration conforme aux exigences de la cible. **Spécificités pour les SI mutualisés :** • Un planning prévisionnel sur 18 mois post appel à financement domaine « stratégie de continuité et de reprise d'activité » pour l'harmonisation des pratiques de sauvegarde et de restauration. ***Documents à fournir par le prestataire pour la sauvegarde en cas de SI métier externalisé ou sauvegarde externalisée sur le périmètre propre au candidat :*** • Inventaire complet des applications en mode SaaS, précisant pour chaque application si un PAS a été obtenu, et si un contrat de service a été obtenu • Contrat de service : Document définissant les niveaux de services attendus, les responsabilités de chaque partie, les délais de récupération des données, notamment ; et ce pour deux applications inventoriées.

	• Plan d'Assurance Sécurité (PAS) du prestataire pour deux des applications inventoriées : Si ce document est disponible : o PAS ou attestation du candidat de la présence de ce document. Si ce document est incomplet et ne peut pas être mis à jour immédiatement : o Documents disponibles. o Attestation ou justification des démarches engagées. o Liste exhaustive des prestataires concernés. Si ce document est non disponible : o Motif(s) de non-présence du document : élément(s) de preuve du refus du prestataire ou de l'absence du document. o Nom du prestataire et de la solution.
Opération de contrôle	• Contrôle sur pièces.

D2.O2.B - Formaliser un/des plan(s) de sauvegarde et de restauration et le(s) maintenir à jour

Domaine	**Domaine « Stratégie de continuité et de reprise d'activité »**
Objectif	**Formaliser un/des plan(s) de sauvegarde et de restauration et le(s) maintenir à jour**
1. Définition de l'objectif	
Définition	Alors que la politique de sauvegarde définit les grandes lignes, le plan de sauvegarde détaille les procédures à suivre pour mettre en œuvre ces directives. Un plan de sauvegarde détaille la manière dont les sauvegardes seront effectuées en pratique. Son objectif est de mettre en œuvre la politique de sauvegarde et de garantir une récupération rapide des données perdues ou corrompues.
Valeur cible / seuil d'éligibilité	Le candidat doit produire ou mettre à disposition les plans de sauvegarde de ses systèmes d'information critiques, tels que identifiés dans le sous-objectif D2.O1.C, et les procédures de leur mise à jour. Pour rappel, un plan de sauvegarde doit contenir a minima les éléments techniques suivants : • Les logiciels, matériels. • Supports utilisés (Serveurs de sauvegarde, stockage dédié, cloud (préciser les types de flux utilisés), bande, ...). • Les types de sauvegardes (complète, incrémentielle, différentielle, ...). • La fréquence de réalisation des sauvegardes et les heures d'exécution. • Le délai de réplication. • Le délai de rétention détaillé lié aux plans de sauvegarde. • Les procédures à suivre en cas d'échec. • Les procédures de mise à jour des plans de sauvegarde. **Spécificités pour les SI mutualisés** : • Les candidats multi-établissements, conformément à l'objectif D2.O2.A, doivent intégrer un projet d'harmonisation sur 18 mois post appel à financements, des plans de sauvegarde et de restauration au niveau du candidat. • Les GHT dont un ou plusieurs établissements parties comptent des EG médico-sociales, peuvent inclure ces EG médico-sociales dans le projet d'harmonisation des plans de sauvegarde au niveau du GHT.
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 des pièces justificatives sur la plateforme de candidature.
Documents justificatifs	• Plan(s) de sauvegarde à jour et la procédure de leur mise à jour pour tous les éléments* des SI critiques (tels que identifiés dans le sous-objectif D2.O1.C). ** Éléments : Bases de données, serveurs, serveurs de fichiers* • Pour les SI mutualisés : Un projet d'harmonisation des plans de sauvegarde et de restauration. ***Documents à fournir par le prestataire pour la sauvegarde en cas de SI externalisé ou sauvegarde externalisée :*** ○ Le calendrier des tests de sauvegarde ou à défaut les éléments contractuels définissant les Contrats de Niveau de Service (CNS/SLA) en place.
Opération de contrôle	• Contrôle sur pièces.

D2.O3 – Construire un système de sauvegarde sécurisé

D2.O3.A – Mettre en œuvre une authentification sécurisée pour les infrastructures de sauvegarde

Domaine	**Domaine « Stratégie de continuité et de reprise d'activité »**
Objectif	**Mettre en œuvre ou une authentification sécurisée pour les infrastructures de sauvegarde**
1. Définition de l'objectif	
Définition	Il est nécessaire que les établissements puissent mettre en œuvre une authentification sécurisée sur leurs infrastructures de sauvegarde.
Valeur cible / seuil d'éligibilité	Le candidat doit disposer d'un système d'authentification indépendant (AD dédié, comptes locaux, ...) pour ses infrastructures de sauvegarde (baies, serveurs, lecteurs de bande, etc.). Le candidat doit s'assurer : - D'une gestion fine des rôles pour l'accès à la sauvegarde, avec un rôle minimisé au strict nécessaire pour l'opérateur de sauvegarde. - De l'utilisation d'une authentification à double facteurs si la solution de sauvegarde le permet. En cas d'un système d'authentification porté par un Active Directory indépendant, un audit ADS (réalisé par l'outil ORADAD porté par l'ANSSI) doit être réalisé sur l'AD utilisé pour l'administration de la sauvegarde durant la phase opérationnelle et un score minimum de 3 doit être obtenu à la fin de la période opérationnelle.
Textes de référence	• Le service ADS • Les fondamentaux de l'ANSSI – Sauvegarde des systèmes d'information • Fiches pratiques du CERT-Santé : o Schéma d'architecture : Fiche technique ANS : Formaliser un schéma d'architecture o Matrice de flux : Fiche technique ANS : Formaliser une matrice de flux

2. Production de l'indicateur	
Unité	• Booléen (O/N)
Modalité de calcul	En cas d'un système d'authentification indépendant / distinct porté par un Active Directory : • Un niveau supérieur ou égal à 3 à l'audit ADS obtenu à la fin de la période opérationnelle.
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	Le candidat doit fournir les documents suivants : • Document décrivant le rôle de l'opérateur de sauvegarde et de l'administrateur. • Document décrivant la gestion des rôles pour l'accès à la sauvegarde. • Selon la gestion de l'authentification à double facteur, le candidat doit fournir un des documents suivants : o Si l'interface d'administration permet une authentification forte, un document décrivant la mise en œuvre de l'authentification (procédure, impressions d'écran). o Si l'interface d'administration permet une authentification forte mais qu'elle n'est pas activée, un document justificatif des raisons de sa non mise en œuvre. o Si l'interface d'administration ne permet pas une authentification forte, un document précisant le nom de la solution de sauvegarde et sa version. <u>Cas d'un candidat disposant d'un AD indépendant dédié à l'administration de la sauvegarde :</u> • Score audit ORADAD supérieur ou égal à 3 réalisé dans les 60 jours précédant le dépôt de la déclaration d'atteinte des cibles. <u>Cas d'une infrastructure de sauvegarde externalisée :</u> • Documents décrivant les moyens d'accès aux sauvegardes fournis par le prestataire. • Plan d'Assurance Sécurité (PAS) du prestataire : Si ce document est disponible : o Extraits du PAS relatifs à la sauvegarde ou attestation du candidat de la présence de ce document Si ce document est non disponible : o Motif(s) de non-présence du document : élément(s) de preuve du refus du prestataire ou de l'absence du document. o Nom du prestataire et de la solution.
Opération de contrôle	• Contrôle sur pièces.

D2.O3.B – S'inscrire dans une trajectoire pour un cloisonnement de son infrastructure de sauvegarde

Domaine	**Domaine « Stratégie de continuité et de reprise d'activité »**
Objectif	**S'inscrire dans une trajectoire pour un cloisonnement de son infrastructure de sauvegarde**
1. Définition de l'objectif	
Définition	Il est nécessaire que les établissements puissent s'inscrire dans une démarche permettant un cloisonnement de leurs infrastructures de sauvegarde.
Valeur cible / seuil d'éligibilité	Le candidat doit s'inscrire dans une démarche visant à cloisonner les infrastructures de sauvegarde au sein du système d'information et disposer d'une capacité technique d'isolation en cas d'incident (mode "bouton rouge"). Il s'agit de les positionner au sein du système d'administration ou, au minimum, dans une zone réseau distincte de celle des serveurs de production avec une fonction de filtrage autorisant uniquement les flux strictement nécessaires qui doivent circuler. Les flux de sauvegarde doivent être à l'initiative du serveur vers les clients sauvegardés. Cette action doit être simple, immédiate et sans ambiguïté, permettant de séparer rapidement les serveurs de sauvegarde du reste du système d'information, sur décision du RSSI ou de ses équipes.

Textes de référence	• Les fondamentaux de l'ANSSI – Sauvegarde des systèmes d'information
	• Fiches pratiques du CERT-Santé :
	  ○ Schéma d'architecture : Fiche technique ANS : Formaliser un schéma d'architecture
	  ○ Matrice de flux : Fiche technique ANS : Formaliser une matrice de flux

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	Le candidat doit fournir les documents suivants : • Schéma technique et fonctionnel d'architecture actuel ou cible détaillant la matrice des flux techniques. • Pour les établissements s'inscrivant dans la démarche, un planning prévisionnel pour atteindre ce schéma cible, dans un délai inférieur à trois ans dans un souci de mise en conformité avec la directive NIS2.

	• Procédure permettant l'isolation ou l'arrêt des serveurs de sauvegarde en cas d'incident en preuve. Document en plus dans le cas d'applications externalisées / d'infogérance / exploitation externalisée : • Plan d'Assurance Sécurité (PAS) du prestataire : Si ce document est disponible : o Extraits du PAS relatifs à la sauvegarde ou attestation du candidat de la présence de ce document. Si ce document est non disponible : o Motif(s) de non-présence du document : élément(s) de preuve du refus du prestataire ou de l'absence du document. o Nom du prestataire et de la solution.
Opération de contrôle	• Contrôle sur pièces.

D2.O3.C – S'inscrire dans une trajectoire pour la mise en œuvre du 3-2-1

Domaine	**Domaine « Stratégie de continuité et de reprise d'activité »**
Objectif	**S'inscrire dans une trajectoire pour la mise en œuvre du 3-2-1**
1. Définition de l'objectif	
Définition	Il est nécessaire que les établissements puissent s'inscrire dans une trajectoire pour la mise en œuvre du 3-2-1 pour une sauvegarde intègre et immuable de l'ensemble des données nécessaires à la continuité des activités critiques. Une sauvegarde est considérée immuable si, une fois écrit, son contenu ne peut plus être modifié ni supprimé (volontairement ou involontairement) pendant une durée définie*. Cette immuabilité doit être garantie par la "technologie" (certifiée ou non / Implémentation de mécanismes internes ou produit déjà packagé), et non seulement par des procédures organisationnelles. En résumé : l'externalisation ou la redondance ne suffisent pas ; seule une contrainte technique empêchant toute modification/suppression prématurée (volontaire ou non) permet de qualifier la sauvegarde d'immuable. * La durée d'immuabilité souhaitée propre à définir par chaque candidat au regard de son contexte spécifique et de ses besoins
Valeur cible / seuil d'éligibilité	Le candidat doit s'inscrire dans une démarche pour la mise en œuvre du 3-2-1* avec une trajectoire définie et des jalons clés. Cette démarche vise à mettre en place une copie immuable de ses sauvegardes hors ligne ou hors site (dans deux bâtiments distincts, si applicable par l'établissement, chez un hébergeur tiers, etc.). Dans le cas de la matérialisation des sauvegardes sur des supports physiques, la protection physiques de ces éléments doit être assurée. À titre d'exemple, l'achat d'un robot cassette pour avoir « une copie hors ligne » est bien valorisable tant qu'il est réalisé pendant la phase opérationnelle. L'ensemble doit être documenté au sein d'un document d'architecture. Remarques : • Les données du serveur de production peuvent être considérées comme l'une des 3 copies de données. • Une réplication n'est pas une copie de sauvegarde. **Définition disponible dans le glossaire en annexe du présent guide des prérequis et objectifs.**

Textes de référence	• Le service ADS
	• Les fondamentaux de l'ANSSI – Sauvegarde des systèmes d'information
	• Fiches pratiques du CERT-Santé :
	  ○ Schéma d'architecture : Fiche technique ANS : Formaliser un schéma d'architecture
	  ○ Matrice de flux : Fiche technique ANS : Formaliser une matrice de flux

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	Le candidat doit fournir les documents suivants : <u>Cas d'une infrastructure internalisée :</u> • Schéma technique et fonctionnel d'architecture actuel détaillant la matrice des flux techniques (seuls les flux strictement nécessaires doivent circuler). • Pour les établissements s'inscrivant dans la démarche, un schéma directeur / trajectoire ou schéma technique et fonctionnel d'architecture cible vers une mise en place du 3-2-1 avec les principaux jalons identifiés. Remarque : il n'est pas attendu du candidat de démontrer l'immuabilité de sa sauvegarde, mais uniquement de présenter la cible attendue (i.e. schéma technique et fonctionnel cible) et la trajectoire définie. <u>Cas d'un hébergeur tiers et sur le périmètre propre au candidat :</u> • Éléments contractuels explicitant les Contrats de Niveau de Service (CNS/SLA) en application. • Plan d'Assurance Sécurité (PAS) du prestataire : Si ce document est disponible : o Extraits du PAS relatifs à la sauvegarde ou attestation du candidat de la présence de ce document. Si ce document est non disponible : o Motif(s) de non-présence du document : élément(s) de preuve du refus du prestataire ou de l'absence du document. o Nom du prestataire et de la solution.
Opération de contrôle	• Contrôle sur pièces.

D2.O3.D – Mettre en place une supervision des sauvegardes

Domaine	**Domaine « Stratégie de continuité et de reprise d'activité »**
Objectif	**Mettre en place une supervision des sauvegardes**
1. Définition de l'objectif	
Définition	La sauvegarde des données est essentielle, mais la supervision de ces activités est tout aussi indispensable pour assurer la restauration des données, en particulier celles critiques, à la suite d'un incident, attaque ou perte informatique. La supervision doit s'appuyer a minima sur les outils de sauvegarde existants, permettant de générer des rapports de suivi de la réalisation des sauvegardes.
Valeur cible / seuil d'éligibilité	Le candidat doit instaurer une organisation pour assurer le suivi efficace des sauvegardes, incluant un plan d'actions pour vérifier leur bonne exécution et des procédures à suivre en cas d'échec. **<u>Spécificités pour les GHT :</u>** • Le GHT, conformément à sa feuille de route décrite dans l'objectif D2.O2.A, doit mettre en place une gouvernance de contrôle, centraliser les alertes et permettre au Responsable de la Sécurité des Systèmes d'Information (RSSI) d'effectuer les contrôles nécessaires. • Le GHT doit avoir une procédure formalisée pour traiter les alertes non résolues par un ou plusieurs établissements. Les coûts de mise en œuvre pour répondre à ce sous-objectif sur la durée de la phase opérationnelle peuvent être valorisés.
Textes de référence	• N/A

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	Le candidat doit fournir les documents suivants : *<u>En cas d'internalisation :</u>* • Exemple d'états produits ou générés par les solutions de sauvegarde / tableaux de bord produits par les outils de sauvegarde (extraction de l'outil, impressions d'écran, etc.).

	• Procédures associées pour le contrôle des incidents de sauvegarde et le plan de traitement des alertes telles que décrites dans la politique de sauvegarde. **<u>Spécificités pour les GHT :</u>** - Documents décrivant la gouvernance de contrôle de la réalisation des sauvegardes. *<u>En cas d'externalisation :</u>* • Les procédures pour la gestion des incidents remontés par la supervision et à défaut éléments contractuels explicitant les Contrats de Niveau de Service (CNS/SLA) en application.
Opération de contrôle	• Contrôle sur pièces.

D2.O4 – Tester la sauvegarde et la restauration

D2.O4 – Tester la sauvegarde et la restauration

Domaine	**Domaine « Stratégie de continuité et de reprise d'activité »**
Objectif	**Tester la sauvegarde et la restauration**
1. Définition de l'objectif	
Définition	La réalisation de tests réguliers des sauvegardes permet aux établissements de vérifier leur capacité à restaurer les données et d'autre part, à évaluer leur capacité de réaction en situation de crise, assurant ainsi la continuité et la reprise des activités.
Valeur cible / seuil d'éligibilité	Lors de la phase opérationnelle, le candidat doit : 1. Réaliser des tests techniques de : • Bon fonctionnement des sauvegardes ; • Remise en marche du système suite à la restauration. Ces tests techniques doivent porter sur la restauration d'une machine virtuelle ou d'une base de données sur un périmètre d'un SI concourant à une des activités identifiées dans le cadre de l'objectif D2.O1.C. Au moins un des tests menés doit concerner un environnement de production. Celui-ci doit concerner un système dont la criticité pour l'activité de l'établissement est établie. 2. Identifier au minimum un référent ou correspondant métier sur les applications métier critiques telles qu'identifiées dans le sous-objectif D2.O1.C. Ces référents sont identifiés en prévision de la réalisation des tests fonctionnels (non demandés dans le cadre de cet objectif). Les coûts de mise en œuvre pour répondre à cet objectif sur la durée de la phase opérationnelle peuvent être valorisés. Dans le cadre de services centralisés (groupes nationaux) la réalisation d'un test central embarquant l'ensemble des établissements du groupe est acceptée si les mesures de sauvegarde sont identiques dans l'ensemble des établissements. Le justificatif soumis devra préciser le périmètre d'applicabilité du test.
Textes de référence	• N/A

2. Production de l'indicateur	
Unité	• Booléen
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	• Document précisant le périmètre des tests. • Cahier de tests de l'opération de restauration (contenant à minima la vérification du bon démarrage pour une VM ou l'exécution d'au moins une requête basique pour une BDD). • Identification (non nominative) des référents ou correspondants métiers pour la réalisation des tests sur les applications métier sur les systèmes critiques (tels que identifiés dans le sous-objectif D2.O1.C).
Opération de contrôle	• Contrôle sur pièces.