ANNEXE

PLAN D'ASSURANCE SECURITE

SOMMAIRE

1. INTRODUCTION 5
1.1 Objet du plan d'assurance sécurité (PAS) 5
1.2 Glossaire 5
1.3 Documents de référence 7
1.4 Règles de remplissage du document 7
2. DOMAINE D'APPLICATION ET RESPONSABILITES 7
2.1 Présentation des acteurs pour la prestation 7
2.2 Applicabilité 8
2.3 Dérogation à l'application du PAS 8
3. DESCRIPTION DE LA PRESTATION 8
3.1 Nature de la prestation 8
3.2 Besoins de sécurité et Disponibilité de la prestation 9
3.3 Site et SI de réalisation de la prestation 10
3.4 Tiers du Prestataire 10
4. ORGANISATION DE LA SECURITE DE L'INFORMATION (ISO27001-A.5) 11
4.1 Organisation interne 11
4.1.1 Fonctions et responsabilités liées à la sécurité de l'information 11
4.1.2 Séparation des tâches (RACI) 11
4.1.3 Relations avec les autorités 12
4.1.4 Relations avec des groupes de travail spécialisés 12
4.1.5 La sécurité de l'information dans la gestion de projet 12
4.2 Politique en matière d'appareils mobiles 12
5. SECURITE LIEE AUX RESSOURCES HUMAINES [ICP>=3] (ISO27001-A.6) 14
5.1 Sélection des candidats 14
5.2 Conditions d'embauche 14
5.3 Sensibilisation et formations à la sécurité de l'information 14
5.4 Rupture, terme ou modification du contrat de travail 15
6. GESTION DES ACTIFS (ISO27001-A.5.9) 16

Confidentiel

6.1 Responsabilités relatives aux actifs 16
6.1.1 Inventaire et propriété des actifs 16
6.1.2 Utilisation correcte des actifs 16
6.1.3 Restitution des actifs 17

6.2 Classification de l'information 17
6.2.1 Identification des besoins de sécurité de l'information 17
6.2.2 Marquage des informations 17
6.2.3 Manipulation des actifs 18

6.3 Gestion des supports 19
6.3.1 Gestion des supports amovibles 19
6.3.2 Mise au rebut des supports 19
6.3.3 Transfert physique des supports 19

7. CONTROLE D'ACCES (ISO27001-A.5.15) 21

7.1 Exigences métier en matière de contrôle d'accès 21
7.1.1 Politique de contrôle d'accès 21

7.2 Gestion de l'accès utilisateur 21
7.2.1 Enregistrement et désinscription des utilisateurs 21
7.2.2 Distribution des accès aux utilisateurs 22
7.2.3 Gestion des droits d'accès à privilège 22
7.2.4 Gestion des informations secrètes d'authentification des utilisateurs 22
7.2.5 Revue des droits d'accès utilisateurs 22
7.2.6 Suppression ou adaptation des droits d'accès 23

7.3 Contrôle de l'accès au système d'exploitation 23
7.3.1 Sécuriser les procédures de connexion 23
7.3.2 Utilisation de programmes utilitaires 23

8. CRYPTOGRAPHIE (ISO27001-A.8.24) [ICP>=3] 24

8.1 Politique d'utilisation des mesures cryptographiques 24

8.2 Gestion des clefs 25

9. SECURITE PHYSIQUE ET ENVIRONNEMENTALE (ISO27001-A.7) [DICP>=3] 26

9.1 Contrôles physiques des accès et sécurisation des zones 26

9.2 Menaces extérieures et environnementales 26

9.3 Sortie des actifs 27

10. SECURITE LIEE A L'EXPLOITATION (ISO27001-A.8) [DICP>=3] 28

10.1 Procédure et responsabilités liées à l'exploitation 28
10.1.1 Procédures d'exploitation documentées 28
10.1.2 Gestion des changements 28
10.1.3 Dimensionnement 28
10.1.4 Séparation des environnements de développement, de test et d'exploitation 28

10.2 Protection contre les codes malveillants 29
10.2.1 Mesures contre les logiciels malveillants 29

10.3 Sauvegarde 29
10.3.1 Sauvegarde des informations 29

Confidentiel

10.4 Journalisation et surveillance 29
10.4.1 Journalisation des évènements 30
10.4.2 Analyse et corrélation des évènements 30
10.4.3 Protection de l'information journalisée 30
10.4.4 Journaux administrateur et opérateur 31
10.4.5 Synchronisation des horloges 31

10.5 Maitrise des logiciels en exploitation 31
10.5.1 Installation de logiciels sur des systèmes en exploitation 31
10.5.2 Administration 31

10.6 Gestion des vulnérabilités techniques 32
10.6.1 Gestion des vulnérabilités techniques 32
10.6.2 Restrictions liées à l'installation de logiciels 33

10.7 Considérations sur l'audit des systèmes d'information 33
10.7.1 Mesures relatives à l'audit des systèmes d'information 33

11. SECURITE DES COMMUNICATIONS (ISO27001-A.5 ET 8) [DICP>=3] 34

11.1 Cartographie du système d'information 34

11.2 Gestion de la sécurité des réseaux 34
11.2.1 Contrôle des réseaux 34
11.2.2 Cloisonnement des réseaux 35

11.3 Transfert de l'information 35
11.3.1 Politiques d'extraction et de transfert de l'information 35
11.3.2 Engagements de confidentialité ou de non-divulgation 36

12. ACQUISITION, DEVELOPPEMENT ET MAINTENANCE DES SYSTEMES D'INFORMATION (ISO27001-A.5 ET 8) [ICP>=3] 37

12.1 Exigences de sécurité applicables aux systèmes d'information 37
12.1.1 Analyse et spécification des exigences de sécurité 37
12.1.2 Sécurisation des services d'application sur les réseaux publics 37

12.2 Sécurité des processus de développement et d'assistance technique 37
12.2.1 Politique de développement sécurisé 37
12.2.2 Revue technique des applications après changement 38
12.2.3 Principes d'ingénierie de la sécurité des systèmes de développement 38
12.2.4 Environnement de développement sécurisé 38
12.2.5 Développement externalisé 38
12.2.6 Test de la sécurité et de conformité du système 39

12.3 Données de test 39
12.3.1 Protection des données de test 39

13. RELATIONS AVEC LES FOURNISSEURS (ISO27001-A.5.19) [DICP>=3] 39

13.1 Sécurité dans les relations avec les fournisseurs 40
13.1.1 Politique de sécurité de l'information dans les relations avec les fournisseurs 40
13.1.2 La sécurité dans les accords conclus avec les fournisseurs 40
13.1.3 Chaine d'approvisionnement informatique 40

13.2 Gestion des prestations de service des fournisseurs 40
13.2.1 Surveillance et revue des services des fournisseurs 40
13.2.2 Gestion des changements apportés dans les services des fournisseurs 41

Confidentiel

14. GESTION DES INCIDENTS LIES A LA SECURITE DE L'INFORMATION (ISO27001- A.5 ET 6) 42

14.1 Gestion des incidents liés à la sécurité de l'information et améliorations 42
14.1.1 Responsabilités et procédures 42
14.1.2 Signalement des évènements et failles liés à la sécurité de l'information 42
14.1.3 Appréciation des évènements liés à la sécurité de l'information et prise de décision 42
14.1.4 Réponse aux incidents liés à la sécurité de l'information 43
14.1.5 Tirer des enseignements des incidents liés à la sécurité de l'information 44
14.1.6 Collecte de preuves 44

15. GESTION DE LA CONTINUITE DE L'ACTIVITE (ISO27001-A.5.29) [D>=3] 45

15.1 Continuité de la sécurité de l'information 45
15.1.1 Organisation de la continuité de la sécurité de l'information 45
15.1.2 Mise en œuvre de la continuité de la sécurité de l'information 45
15.1.3 Vérifier, revoir et évaluer la continuité de la sécurité de l'information 46

16. CONFORMITE (ISO27001-A.5.31 ET 36) 47

16.1 Conformité aux obligations légales et réglementaires 47

Confidentiel

1. Introduction

1.1 Objet du plan d'assurance sécurité (PAS)

Le Plan d'Assurance Sécurité (PAS) décrit les dispositions et procédures de sécurité mises ou à mettre en œuvre par le Prestataire, et en accord avec la CDC, dans le cadre d'un projet, notamment d'une externalisation. Il décrit les dispositions générales de sécurité.

Conformément à la PSSI (Politique de Sécurité des Systèmes d'Information) de la CDC, le PAS s'appuie principalement sur le référentiel normatif ISO/CEI 27001 – 2022.

Le PAS permet de démontrer la capacité du Prestataire à identifier, prévenir, détecter et répondre aux défaillances puis à se rétablir en réduisant au minimum les impacts négatifs pour la CDC.

1.2 Glossaire

Administrateur – utilisateur disposant de droits privilégiés lui permettant de réaliser les tâches d'administration qui lui sont attribuées.

Administrateur d'infrastructure – administrateur en charge de la gestion et du maintien en conditions opérationnelles et en condition de sécurité de l'infrastructure technique du service.

ANSSI – Agence Nationale de la Sécurité du Système d'Information.

Authentification standard - mode d'authentification impliquant l'utilisation d'un mot de passe conforme aux standards de sécurité SI.

Authentification renforcée - Mode d'authentification impliquant l'utilisation d'un mot de passe renforcé (i.e. d'un niveau de sécurité supérieur à l'authentification standard) en plus d'un second facteur (Token, SMS, *etc*.).

Cloud – modèle permettant un accès aisé, généralement à la demande, et au travers d'un réseau, à un ensemble de ressources informatiques partagées et configurables.

Confidentialité – aptitude du Système d'Information à garantir la protection de l'information contre toute divulgation non autorisée.

Disponibilité : aptitude du Système d'Information à garantir l'accès à une application, un système, une donnée.

Preuve (ou Traçabilité) : aptitude du Système d'Information à tracer les actions techniques qui sont réalisées par les utilisateurs (et dans une certaine mesure par les machines ou les logiciels) et apporter la preuve non réfutable de ces actions.

Confidentiel

Département de la Cyber Sécurité de la CDC - pilote le programme SSI de la Caisse des Dépôts et coordonne la mise en œuvre des dispositifs destinés à protéger l'exposition des systèmes d'information et des données aux risques cyber.

État de l'art - ensemble des bonnes pratiques, des technologies et des documents de référence relatifs à la sécurité des systèmes d'information publiquement accessibles, et des informations qui en découlent de manière évidente. Ces documents peuvent être mis en ligne sur Internet par la communauté de la sécurité des systèmes d'information, diffusés par des organismes de référence ou encore d'origine réglementaire.

Incident lié à la sécurité de l'information – un ou plusieurs événement(s) liés à la sécurité de l'information, indésirable(s) ou inattendu(s) présentant une probabilité forte de compromettre la sécurité des réseaux et des systèmes d'information, et a une incidence négative sur la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données ou sur les services fournis par la CDC.

Intégrité - aptitude du Système d'Information à assurer l'exactitude et l'intégralité de l'information.

Menace – cause potentielle d'un incident indésirable pouvant nuire à un système ou à un organisme.

Mesure de sécurité – mesure qui modifie la vraisemblance ou la gravité d'un risque. Elle comprend la politique, les procédures, les lignes directrices, et les pratiques ou structures organisationnelles, et peut être de nature administrative, technique, managériale ou juridique.

Prestation Critique ou Importante – Prestations qualifiées (i) de services de Technologie de l'Information et de la Communication qui soutiennent des fonctions critiques ou importantes (« Prestation Critique ou Importante DORA » ou « PCI DORA ») au sens de la section 3 du décret n°2020-94 du 5 février 2020 relatif au contrôle interne et externe de la Caisse des Dépôts et Consignations renvoyant au règlement n°2022/2554 du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier (DORA), et (ii) de « prestations de services ou autres tâches opérationnelles essentielles ou importantes » (« Prestation de Service Essentielle Externalisée » ou « PSEE ») à l'activité de la CDC, au sens du 15° de l'article 8 du décret n°2020-94 du 5 février 2020 relatif au contrôle interne et externe de la Caisse des Dépôts et Consignations..

Prestataire : le Titulaire du Marché.

Risque – effet de l'incertitude sur l'atteinte des objectifs. Il est exprimé en termes de combinaison des conséquences d'un événement et de sa vraisemblance.

Sécurité d'un système d'information – ensemble des moyens techniques et non-techniques de protection permettant à un système d'information d'assurer la disponibilité, l'intégrité et la confidentialité des données, traitées ou transmises, et des services connexes que ces systèmes offrent ou rendent accessibles.

Système d'information – ensemble organisé de ressources (matériels, logiciels, personnels, données et procédures) permettant de traiter et de diffuser de l'information.

Traçabilité – aptitude du Système d'Information à fournir les pistes et les éléments de preuve du service.

Utilisateur – Toute personne disposant d'un compte dans le périmètre du service. Ce terme générique englobe les utilisateurs finaux et les administrateurs.

Utilisateur final – personne jouissant *in fine* du service mis en œuvre. Il peut s'agir du personnel de la CDC dans le cas d'un service interne, ou du personnel des clients ou filiales de la CDC dans le cas d'un service proposé à l'extérieur.

Confidentiel

Vulnérabilité –une faiblesse, une susceptibilité ou un défaut d'un actif, d'un système, d'un processus ou d'un contrôle qui peuvent être exploités. .

1.3 Documents de référence

Les documents de référence pour les exigences de ce document sont :

■ D'une part, les cadres dans lesquels s'insère la prestation :

- Les éléments légaux et règlementaires applicables à la prestation ;
- Les standards en matière de sécurité de l'information (Normes ISO/IEC, PCI-DSS…).
- Les politiques thématiques couvrant la sécurité des systèmes d'information, la poursuite de l'activité, la gestion de crise et la sécurité physique, ainsi que les directives de sécurité émises par la CDC, notamment sur l'authentification, l'aliénation des matériels, ou la protection des données de production lors des test, recette ou formation ; et enfin la charte d'utilisation des ressources des systèmes d'information ;
- Les Référentiels Généraux de Sécurité B1 et B2 de l'ANSSI Ainsi que les Notes Techniques TLS et IPSec ;
- Décret n°2020-94 du 5 février 2020 relatif au contrôle interne et externe de la Caisse des dépôts et consignations, rendant applicable à la CDC des dispositions du règlement européen pour la résilience opérationnelle numérique dit « DORA » (Digtial Operational Resilience Act).

Ces éléments ont été largement déclinés dans la suite du document et n'ont pas vocation à être communiqués. Toutefois, des précisions sur des points particuliers peuvent être adressées au Prestataire qui en ferait la demande.

■ D'autre part, les éléments d'encadrement de la prestation :

- Le cahier des charges de la prestation ;
- Le contrat.

1.4 Règles de remplissage du document

- Pour chaque exigence, le Prestataire doit établir son niveau de conformité lorsque cela est demandé. En cas de non-conformité ou non applicable, le Prestataire doit justifier sa réponse dans la zone commentaire.
- Les chapitres « 3.1 Nature de la prestation » et « 3.2 Besoins de sécurité de la prestation » sont renseignés par la CDC (en particulier le DICP est indiqué dans le chapitre 3.2).
- Certains chapitres ne sont à renseigner que si les critères de DICP retenus par la CDC sont supérieurs à un seuil de valeurs : Ex C>= 3 : à ne traiter que si le critère C « confidentialité » est supérieur ou égale à 3. Max DICP >= 3 : un des critères est supérieur ou égale à 3.

2. Domaine d'application et responsabilités

2.1 Présentation des acteurs pour la prestation

Pour le Prestataire :

Confidentiel

Interlocuteur prestation :
NOM/PRENOM :
FONCTION :
COORDONNEES (téléphone/mail) :

Correspondant sécurité :
NOM/PRENOM :
FONCTION :
COORDONNEES (téléphone/mail) :

Suppléant :
NOM/PRENOM :
FONCTION :
COORDONNEES (téléphone/mail) :

Pour la CDC :
Correspondant métier :
NOM/PRENOM : DONINI JOHANN
FONCTION : Responsable unité expertise moyens de paiement
COORDONNEES (téléphone/mail) : 07 88 24 43 02 / johann.donini@caissedesdepots.fr

Correspondant sécurité (RSSI métier) :
NOM/PRENOM :MAZALTARIM David
FONCTION : Responsable de la Sécurité des Systèmes d'Information
COORDONNEES (téléphone/mail) : 06 43 69 35 10 david.mazaltarim@caissedesdepots.fr

2.2 Applicabilité

Le présent document s'applique au périmètre de la prestation décrite ci-après.
Les dispositions décrites dans le PAS deviennent applicables dès le démarrage de la prestation. Les versions ultérieures du PAS deviennent applicables dès leur validation par la CDC.

2.3 Dérogation à l'application du PAS

Le Prestataire peut demander une dérogation au PAS en transmettant une demande dument justifiée à la CDC.

3. Description de la prestation

3.1 Nature de la prestation

C1	Décrire à quoi consiste la prestation :	Location de scanner de chèques – Les prestations sont décrites dans le CCTP
C2	La prestation est qualifiée de Prestation Critique ou Importante ?	☐ OUI ☒ NON ☐ N/A
C3	Lien avec la continuité de l'activité de la CDC ?	☐ OUI ☒ NON ☐ N/A

Confidentiel

C4	DMIA ?	☐ H+4 ☒ H+8 ☐ J+1 ☐ J+2 ☐ J+5 ☐ J+10
C5	Quelle est la nature de la prestation à externaliser ?	☐ Développement d'applications ☐ Maintenance applicative ☐ Maintenance matérielle ☐ Exploitation informatique ☐ Hébergement de ressources ☐ Hébergement de services ☒ Autre, préciser :

3.2 Besoins de sécurité et Disponibilité de la prestation

Dans le cadre de la prestation, la CDC précise les besoins DICP : **Disponibilité, Intégrité, Confidentialité et Preuve (Traces)** de la prestation en identifiant et qualifiant les données :

DICP et échelle d'exigence

	Disponibilité	Intégrité	Confidentialité	Preuve
1	Pas d'exigence	Pas d'exigence	Public	Pas d'exigence
	Une longue indisponibilité est acceptable.	Pas de disposition particulière exigée.	Les données peuvent être librement diffusées en dehors de l'EP ou du Groupe.	Pas de disposition particulière exigée outre le respect des exigences légales applicables.
2	Reprise à moyen terme	Besoin standard	Interne	Besoin standard
	Indisponibilité de quelques jours sans perte de données.	Utilisation de technologies réputées intègres.	Information non librement diffusable. Ex : documents internes à l'EP, à une direction, un projet mais non confidentiels.	Formalisation du besoin : que doit-on tracer et pour combien de temps ?
3	Reprise à court terme	Besoin renforcé	Confidentiel	Besoin renforcé
	Indisponibilité de l'ordre de 24h.	Mise en œuvre de mécanismes complémentaires et/ou de contrôles métier a posteriori.	Information *confidentielle*, limitée aux personnes ayant besoin d'en connaître.	Mise en œuvre de mécanismes complémentaires.
4	Reprise à très court terme	Parfaitement intègre	Secret	Preuves à valeur probante
	Indisponibilité de quelques heures.	Mise en œuvre de mécanismes garantissant l'intégrité des données.	Actif très sensible, seules certaines personnes identifiées peuvent y accéder.	Mise en œuvre de mécanismes garantissant l'intégrité des preuves de bout en bout.

Remarque : La présence de données à caractère personnel ou soumises au secret professionnel (données médicales ou bancaires) doit être précisée le cas échéant.

	Besoins de sécurité				
Données	**D**	**I**	**C**	**P/T**	**Commentaires / justifications**
	2	3	3	4	

Confidentiel

3.3 Site et SI de réalisation de la prestation

C6	Site de la prestation	☐ Site de la CDC ☐ site du Prestataire ☐ Cloud
C7	Locaux	☐ Dédiés à la prestation ☐ Mutualisés avec d'autres Clients
C8	Système d'information	☐ Dédiés à la prestation ☐ Mutualisés.
C9	Si Cloud	Nom hébergeur : Adresse sociale : Adresse du site : Type de cloud : ☐ Public ☐ Privé ☐ Hybride Certification :

3.4 Tiers du Prestataire

Dans le cadre de la prestation, le Prestataire fait-il à son tour intervenir des prestataires ou des partenaires :
☐ OUI ☐ NON ☐

Si OUI préciser la RAISON SOCIALE DU TIERS :
LOCALISATION DU LIEU DE DELIVRANCE DES SERVICES :
NATURE DE LA PRESTATION :

Confidentiel

4. Organisation de la sécurité de l'information (ISO27001-A.5)

4.1 Organisation interne

4.1.1 Fonctions et responsabilités liées à la sécurité de l'information

Le Prestataire doit documenter et mettre en œuvre une organisation interne de la sécurité pour assurer la définition, la mise en place et le suivi du fonctionnement opérationnel de la sécurité de l'information au sein de son organisation.
Le Prestataire désigne un responsable de la sécurité des systèmes d'information et un responsable de la sécurité physique.

	Identification des acteurs et instances de pilotage	Réponse
D1	Un interlocuteur privilégié est désigné par le Prestataire pour tenir le rôle de responsable de l'application des obligations du présent Plan d'Assurance Sécurité et traiter les sujets relatifs à la sécurité au sein de la prestation dans le cadre de comités de pilotage a minima annuels (semestriels si PCI), dédiés ou non.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
	Documentation de sécurité	**Réponse**
D2	Une politique de sécurité du système d'information précisant notamment la gouvernance en matière de sécurité est formalisée. Elle est diffusée au sein de son organisation, revue régulièrement et déclinée d'un point de vue opérationnel.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
	Indicateurs de sécurité	**Réponse**
D3	Des indicateurs de sécurité sont produits périodiquement et adressés à la CDC. Les indicateurs attendus par La CDC sont à définir dans le contrat.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
	Sous-traitants et autres tiers du Prestataire	**Réponse**
D4	Les sous-traitants et tiers du Prestataire intervenant sur le périmètre de la prestation sont assujettis aux mêmes règles et conditions imposées par la CDC. Ces règles doivent faire l'objet d'une formalisation contractuelle et d'un contrôle par le Prestataire. En outre, leur intervention doit faire l'objet d'un accord avec la CDC.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

4.1.2 Séparation des tâches (RACI)

Confidentiel

	Séparation des tâches (RACI)	Réponse
D5	Le Prestataire doit identifier les risques associés à des cumuls de responsabilités ou de tâches, les prend en compte dans l'appréciation des risques et met en œuvre des mesures de réduction de ces risques.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

4.1.3 Relations avec les autorités

Il est recommandé que le Prestataire mette en place des relations appropriées avec les autorités compétentes en matière de sécurité de l'information et de données à caractère personnel et, le cas échéant, avec les autorités sectorielles selon la nature des informations confiées par la CDC au Prestataire. Exemple : ACPR, AMF, CNIL, *etc*. En tout état de cause, en cas d'audit et de contrôle de l'autorité de régulation, le Prestataire s'engage à coopérer pleinement avec la CDC.

Un incident de sécurité donnant lieu à une enquête des autorités judiciaires françaises est considéré comme un incident critique et doit activer la cellule de crise chez le Prestataire.

Dans le cadre de la prestation, préciser ce que le Prestataire met en œuvre :	

4.1.4 Relations avec des groupes de travail spécialisés

Il est recommandé que le Prestataire entretienne des contacts appropriés avec des groupes de spécialistes ou des sources reconnues, notamment pour prendre en compte de nouvelles menaces et les mesures de sécurité appropriées pour les contrer. Exemple : inter-cert, ANSSI, *etc*.

Dans le cadre de la prestation, préciser ce que le Prestataire met en œuvre (CERT, veille juridique et règlementaire, revue de presse, publications, listes de diffusion internes).	

4.1.5 La sécurité de l'information dans la gestion de projet

	La sécurité de l'information dans la gestion de projet	Réponse
D6	Le Prestataire doit documenter une estimation des risques préalablement à tout projet pouvant avoir un impact sur le service. Il doit informer la CDC des mesures mises en place pour réduire ces impacts ainsi que des risques résiduels le concernant.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

4.2 Politique en matière d'appareils mobiles

Confidentiel

	Politique en matière d'appareils mobiles, principales mesures :	Réponse
D7	- Interdiction des équipements non fournis par le Prestataire - Chiffrement des ordinateurs portables et supports de stockage amovibles, - Authentification sur tous les terminaux, - Protection contre le vol, - Sécurisation des accès réseaux.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

Confidentiel

5. Sécurité liée aux ressources humaines [ICP>=3] (ISO27001-A.6)

5.1 Sélection des candidats

	Sélection des candidats	Réponse
E1	Le Prestataire doit documenter et mettre en œuvre une procédure de vérification des informations concernant son personnel conforme aux lois et règlements en vigueur. Ces vérifications s'appliquent à toute personne impliquée dans la fourniture du service et doivent être proportionnelles à la sensibilité ou à la spécificité des informations de la CDC confiées au Prestataire ainsi qu'aux risques identifiés.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
E2	Le Prestataire doit renforcer ces vérifications lorsqu'il s'agit de personnels disposant de privilèges d'administration élevés sur les composants logiciels et matériels de l'infrastructure du service. Il est entendu par « privilèges d'administration élevés », toutes actions permettant l'élévation de privilèges ou la possibilité de réaliser des actions sans traces techniques ou de désactiver, altérer les traces techniques.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

5.2 Conditions d'embauche

	Conditions d'embauche	Réponse
E3	Le Prestataire fait signer une charte d'éthique à l'ensemble des personnes impliquées dans la fourniture du service.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
E4	Le Prestataire précise dans le contrat de travail des personnels disposant de privilèges d'administration élevés, un engagement de responsabilité avec un renvoi aux clauses du code du travail sur la protection du secret des affaires et de la propriété intellectuelle.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
E5	Le Prestataire doit, sur demande de la CDC, rendre accessible à la CDC son règlement intérieur et sa charte d'éthique.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

5.3 Sensibilisation et formations à la sécurité de l'information

		Réponse
E6	Le Prestataire sensibilise à la sécurité de l'information et aux risques liés à la protection des données l'ensemble des personnes impliquées dans la fourniture du service. Il doit leur communiquer les mises à jour des politiques et procédures pertinentes dans le cadre de leurs missions.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
E7	Le Prestataire documente et met en œuvre un plan de formation concernant la sécurité de l'information adapté au service et aux missions des personnels.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

Confidentiel

E8	Le responsable de la sécurité des systèmes d'information du Prestataire valide formellement le plan de formation concernant la sécurité de l'information.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

5.4 Rupture, terme ou modification du contrat de travail

		Réponse
E9	Le Prestataire documente et met en œuvre un processus disciplinaire applicable à l'ensemble des personnes impliquées dans la fourniture du service ayant enfreint la politique de sécurité.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
E10	Le Prestataire doit, sur demande de la CDC, lui rendre accessible les sanctions encourues en cas d'infraction à la politique de sécurité.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
E11	Au départ d'un collaborateur impliqué dans la fourniture du service, les mesures suivantes sont mises en œuvre a minima : - Suspension de comptes sur les serveurs, - Restitution du matériel et preuve de restitution du matériel, - Procédures de formatage de l'ordinateur.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

Confidentiel

6. Gestion des actifs (ISO27001-A.5.9)

6.1 Responsabilités relatives aux actifs

6.1.1 Inventaire et propriété des actifs

		Réponse
F1	Le Prestataire tient à jour l'inventaire de l'ensemble des équipements mettant en œuvre le service.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
F2	Cet inventaire précise pour chaque équipement : - Les informations d'identification (Nom, @IP, @MAC, etc.) ; - La fonction de l'équipement ; - Le modèle de l'équipement ; - La localisation de l'équipement ; - Le propriétaire de l'équipement ; - Le besoin de sécurité des informations (au sens du chapitre 6.2.1).	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
F3	Le Prestataire tient à jour l'inventaire de l'ensemble des logiciels mettant en œuvre le service. Cet inventaire identifie pour chaque logiciel, sa version et les équipements sur lesquels le logiciel est installé.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
F4	Le Prestataire s'assure de la validité des licences des logiciels tout au long de la prestation.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

6.1.2 Utilisation correcte des actifs

		Réponse
F5	Le Prestataire est doté d'une charte d'utilisation du système d'information et d'une charte éthique afin de : - Définir les conditions d'une bonne utilisation des ressources partagées, dans le respect des lois et de l'éthique, - Porter à la connaissance des utilisateurs, en parfaite transparence, les dispositifs mis en place pour garantir la sécurité des systèmes.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
F6	Ces chartes s'appliquent à toute personne se servant des outils informatiques et des moyens de communication du Prestataire quel que soit son statut, notamment : salarié, mandataire social, intérimaire, prestataire et ses éventuels sous-traitants, stagiaires, personnels et/ou membres des structures hébergées par le Prestataire, ainsi que les utilisateurs occasionnels.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

Confidentiel

6.1.3 Restitution des actifs

		Réponse
F7	Le Prestataire documente et met en œuvre une procédure de restitution des actifs permettant de s'assurer que chaque personne impliquée dans la fourniture du service restitue l'ensemble des actifs en sa possession à la fin de sa période d'emploi ou de son contrat.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
F8	Il est interdit de réaffecter un poste de travail sans un formatage bas niveau.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

6.2 Classification de l'information

6.2.1 Identification des besoins de sécurité de l'information

		Réponse
F9	Le Prestataire identifie et catégorise les niveaux de classification nécessaires aux différents besoins de sécurité des informations relatives au service.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
F10	Lorsque la CDC confie au Prestataire des données soumises à des contraintes légales, réglementaires ou sectorielles spécifiques, le Prestataire identifie les besoins de sécurité spécifiques associés à ces contraintes et définie les règles de classification *adhoc*.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

6.2.2 Marquage des informations

	Classification des données	Réponse
F11	Toute donnée manipulée dans le cadre de la prestation fait l'objet d'une classification de sécurité compatible avec la classification faite par la CDC. C***1. Public*** C***2. Interne*** C***3. Confidentiel*** C***4. Secret***	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
	Marquage des ressources	**Réponse**
F12	Tous les actifs (support IT, documents, ...) utilisés dans le cadre de la prestation font l'objet d'un marquage précisant notamment le niveau de classification et sont inventoriés.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

Confidentiel

Définitions des niveaux de marquages de données à la CDC :

C1 - Public	C2 - Interne	C3-Confidentiel	C4-Secret
Données et documents d'information à destination du **grand public**, que l'on peut trouver sur le site web de la CDC par exemple.	Données et documents pouvant être partagés **en interne de l'établissement public**, mais également avec nos partenaires, clients, fournisseurs, etc.	Données et documents contenant des **informations sensibles pour la CDC**, dont la diffusion doit être limitée à un cercle clos et défini : une même équipe, un même département ou un même projet.	Données et documents contenant des **informations très sensibles pour la CDC** à destination d'interlocuteurs ciblés et de confiance devant avoir accès à ces informations.

6.2.3 Manipulation des actifs

L'ensemble des données relatives au projet doivent être stockées sur un espace accessible aux seuls membres autorisés du projet. En cas de besoin de confidentialité accrue, ceux-ci doivent être stockés sur un serveur dédié, ou chiffrés dans des répertoires d'accès strictement limités aux seules personnes autorisées.

	Protection des données stockées	Réponse
F13	Les **données C2** stockées sont *a minima* protégées par un **contrôle d'accès.**	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
F14	Les **données C3 et C4** stockées sont *a minima* protégées par un **chiffrement et un contrôle d'accès.** Indiquer en commentaire le mécanisme de chiffrement utilisé.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
	Transmission à l'oral de l'information	**Réponse**
F15	La transmission à l'oral d'informations jugées confidentielles ou équivalent fait l'objet de certaines restrictions.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
	Protection des informations au format papier	**Réponse**
F16	L'usage de documents papier classifiés C3 ou C4 est encadré par des règles et usages tenant compte de leur niveau de confidentialité, notamment concernant : • Leur impression, protégée par authentification ou surveillance visuelle ; • Leur stockage dans des espaces sécurisés ; • Leur partage suivant le principe du droit d'en connaître.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
	Protection des transferts de données	**Réponse**
F17	Les données C3 et C4 sont systématiquement chiffrées avant toute transmission (il peut s'agir d'une protection du flux ou de la donnée elle-même).	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

Confidentiel

F18	Aucune donnée relative à la prestation ne transite sur un cloud géré par un tiers sans autorisation explicite de la CDC.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
F19	Un dispositif de Data Loss Prevention (DLP) permettant d'identifier, de contrôler et de protéger les données est déployé, notamment sur les canaux de communication du type courrier électronique.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

6.3 Gestion des supports

Le Prestataire documente et mette en œuvre une procédure pour la gestion des supports, conformément au besoin de sécurité défini au chapitre 6.2.1 (notamment gestion de la mise au rebut et transfert physique des supports). Sur demande, cette procédure devra être communiquée à la CDC.

6.3.1 Gestion des supports amovibles

	Les principales restrictions appliquées sont :	Réponse
F20	Les supports amovibles sont utilisés uniquement pour transférer des informations, un média amovible n'étant pas un support de stockage définitif.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
F21	Les supports amovibles sont chiffrés ou leur contenu est chiffré dès lors qu'ils contiennent des données sensibles.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

6.3.2 Mise au rebut des supports

	Suppression des informations sensibles et ressources supports	Réponse
F22	Tous les supports numériques ou papier liés à la prestation font l'objet d'une procédure de destruction logique et/ou physique dès lors qu'ils sont mis au rebus, mis en maintenance, recyclés ou lorsque leur propriétaire est modifié. Une preuve est fournie à la CDC pour toute destruction de données. Pour les données C1 à C2, la destruction logique est effectuée par formatage à zéro. Pour les données C3 et C4, la destruction logique est effectuée par formatage à zéro en un nombre de passes suffisant pour que les données soient rendues irrécupérables par des moyens communs.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

6.3.3 Transfert physique des supports

Si le projet nécessite le transfert d'un support physique entre la CDC et le Prestataire, les règles suivantes seront mises en œuvre :

- Utilisation d'un coursier validé entre la CDC et le Prestataire (pas de transmission *via* des services ouverts (ex : La Poste)),
- Mise en place d'un acquittement de réception,

Confidentiel

- En fonction de la nature des actifs, chiffrement des données.

	Remise de supports de stockage (disques durs, clé USB, *etc.*) contenant des informations sensibles	Réponse
F23	**Tout échange de supports de stockage** est effectué au travers d'un processus dont le niveau de sécurité est adapté au niveau de confidentialité des informations impliquées. Notamment les échanges : • Internes au SI du Prestataire ; • Entre le Prestataire et la CDC ; • Entre le Prestataire et ses sous-traitants.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

Confidentiel

7. Contrôle d'accès (ISO27001-A.5.15)

Sauf mention explicite, ce chapitre concerne le contrôle d'accès et la gestion des identités des utilisateurs :

- Placés sous la responsabilité du Prestataire (ses employés et éventuellement ceux des tiers participant à la fourniture du service) ;
- Placés sous la responsabilité de la CDC, mais pour lesquels le Prestataire met en œuvre les moyens de contrôle d'accès (en fournissant notamment à la CDC une interface de gestion des comptes et des droits d'accès).

Les utilisateurs pour lesquels la CDC met en œuvre les moyens de contrôle d'accès et de gestion des identités sont hors du champ d'application de ce référentiel.

7.1 Exigences métier en matière de contrôle d'accès

7.1.1 Politique de contrôle d'accès

	Politique de contrôle d'accès :	Réponse
G1	Le Prestataire documente et met en œuvre une politique de contrôle d'accès sur la base du résultat de son appréciation des risques et du partage des responsabilités.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
G2	Le Prestataire révise annuellement la politique de contrôle d'accès et à chaque changement majeur pouvant avoir un impact sur le service.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
G3	Le Prestataire défini une liste de droits d'accès incompatibles entre eux. Il doit s'assurer, lors de l'attribution de droits d'accès à un utilisateur qu'il ne possède pas de droits d'accès incompatibles entre eux au titre de la liste précédemment établie.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

7.2 Gestion de l'accès utilisateur

7.2.1 Enregistrement et désinscription des utilisateurs

		Réponse
G4	Le Prestataire documente et met en œuvre une procédure d'enregistrement et de désinscription des utilisateurs s'appuyant sur une interface de gestion des comptes et des droits d'accès. Cette procédure doit indiquer quelles données doivent être supprimées au départ d'un utilisateur.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
G5	Le Prestataire met en œuvre des moyens permettant de s'assurer que la désinscription d'un utilisateur entraîne la suppression de tous ses accès aux ressources du système d'information du service, ainsi que la suppression de ses données, conformément à la procédure d'enregistrement et de désinscription.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

Confidentiel

7.2.2 Distribution des accès aux utilisateurs

		Réponse
G6	Les comptes utilisateurs doivent être tous nominatifs et l'usage des comptes génériques est proscrit dans les tâches courantes d'administration ou d'utilisation d'une application. Si ce n'est pas le cas, l'usage de comptes génériques est associé à un tableau de correspondances, recensant nominativement les utilisateurs de ces comptes.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

7.2.3 Gestion des droits d'accès à privilège

		Réponse
G7	Les utilisateurs de postes de travail ne sont pas autorisés à avoir des privilèges d'administration sur leur poste. Les profils administrateurs sont réservés aux personnels habilités à la gestion des socles matériels et logiciels. Le principe du moindre privilège doit être appliqué (absence des accès "lire", "écrire" et/ou "exécuter" si non nécessaire).	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
G8	Lorsque des comptes techniques/applicatifs, non nominatifs, sont nécessaires, le Prestataire met en place des mesures obligeant les utilisateurs à s'authentifier avec leur compte nominatif avant de pouvoir accéder à ces comptes techniques.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

7.2.4 Gestion des informations secrètes d'authentification des utilisateurs

	Les règles de gestion des informations secrètes d'authentification :	Réponse
G9	- Un mot de passe doit être composé de lettres (majuscule et minuscule), et chiffres ou caractères spéciaux, et avoir une longueur minimale de 9 caractères (15 pour les comptes à privilège). - Le changement du mot de passe est obligatoire lors de la première connexion de l'utilisateur sauf impossibilité technique dûment justifiée et formalisée. - Le changement du mot de passe doit être obligatoire tous les 6 mois pour les comptes à privilège. - Blocage d'un compte après un nombre limité de tentatives infructueuses.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
G10	- Une authentification multi facteurs ou authentification transparente (SSO) doit être mise ne place pour tout accès à une information C3/C4. Indiquer en commentaire le mécanisme utilisé.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

7.2.5 Revue des droits d'accès utilisateurs

Confidentiel

		Réponse
G11	Le Prestataire doit réviser semestriellement les droits d'accès des utilisateurs sur son périmètre de responsabilité.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
G12	Le Prestataire doit mettre à disposition de la CDC un outil facilitant la revue des droits d'accès des utilisateurs placés sous la responsabilité du Prestataire.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

7.2.6 Suppression ou adaptation des droits d'accès

		Réponse
G13	Lors du départ d'un collaborateur impliqué dans la fourniture du service, le Prestataire a la charge de s'assurer que les droits d'accès sont révoqués.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

7.3 Contrôle de l'accès au système d'exploitation

7.3.1 Sécuriser les procédures de connexion

		Réponse
G14	Tous les équipements sont protégés par des mots de passe à tous les niveaux (BIOS, écran de veille, ouverture de session).	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
G15	L'accès aux postes de travail n'est permis qu'à la condition de disposer *a minima* d'un identifiant personnel ainsi que d'un mot de passe pour ouvrir une session Windows.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

7.3.2 Utilisation de programmes utilitaires

		Réponse
G16	L'utilisation de programmes utilitaires (ex. prise de contrôle à distance) permettant de contourner les mesures de sécurité d'un système ou d'une application doit être limitée et étroitement contrôlée.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

Confidentiel

8. Cryptographie (ISO27001-A.8.24) [ICP>=3]

8.1 Politique d'utilisation des mesures cryptographiques

Chiffrement des données stockées

Le Prestataire doit définir et mettre en œuvre un mécanisme de chiffrement empêchant la récupération des données de la CDC en cas de réallocation d'une ressource ou de récupération du support physique.

Dans le cas d'un service SaaS, cet objectif pourra être atteint en utilisant un chiffrement applicatif dans le périmètre du Prestataire, avec au moins une clé par client.

Le Prestataire doit utiliser une méthode de chiffrement des données respectant les règles de [CRYPTO_B1] de l'ANSSI.

Le Prestataire doit mettre en place un chiffrement des données sur les supports amovibles et les supports de sauvegarde amenés à quitter le périmètre de sécurité physique du système d'information du service, en fonction du besoin de sécurité des données.

Chiffrement des flux

Lorsque le Prestataire doit mettre en œuvre un mécanisme de chiffrement des flux réseau, celui-ci doit respecter les règles de [CRYPTO_B1].

Lorsque le protocole TLS est mis en œuvre, le Prestataire doit respecter les recommandations de [NT_TLS] de l'ANSSI.

Lorsque le protocole IPsec ou SSH est mis en œuvre, le Prestataire doit respecter les recommandations de [NT_IPSEC] de l'ANSSI.

Hachage des mots de passe

Le Prestataire ne doit stocker que l'empreinte des mots de passe des utilisateurs et des comptes techniques.

Le Prestataire doit mettre en œuvre une fonction de hachage respectant les règles de [CRYPTO_B1].

Le Prestataire doit générer les empreintes des mots de passe avec une fonction de hachage associée à l'utilisation d'un sel cryptographique respectant les règles de [CRYPTO_B1].

Non répudiation

Lorsque le Prestataire met en œuvre un mécanisme de signature électronique, celui-ci doit respecter les règles de [CRYPTO_B1].

Confidentiel

	Politique d'utilisation des mesures cryptographiques	Réponse
H1	Respect des recommandations CRYPTO B1 de l'ANSSI	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
H2	Respect des recommandations NT IPSec de l'ANSSI	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
H3	Respect des recommandations NT TLS de l'ANSSI	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

	Gestion des mécanismes de chiffrement	Réponse
H4	Les mécanismes de chiffrement utilisés dans le cadre de la prestation sont **définis comme robustes par les autorités en la matière** (ANSSI, NIST, etc.).	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
H5	La génération, la distribution et l'expiration des clés et des certificats sont **gérées par le Prestataire.**	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
H6	L'accès aux secrets de chiffrement n'est rendu possible qu'aux rôles et personnes ayant besoin d'en connaître. Les secrets de chiffrement sont stockés chiffrés.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

8.2 Gestion des clefs

Le Prestataire doit mettre en œuvre des clés cryptographiques respectant les règles de [CRYPTO_B2] de l'ANSSI.

Le Prestataire doit protéger l'accès aux clés cryptographiques et autres secrets utilisés pour le chiffrement des données par un moyen adapté : conteneur de sécurité (logiciel ou matériel) ou support disjoint.

Le Prestataire doit protéger l'accès aux clés cryptographiques et autres secrets utilisés pour les tâches d'administration par un conteneur de sécurité adapté, logiciel ou matériel.

Sur l'infrastructure technique, le Prestataire doit utiliser exclusivement des certificats de clé publique issus d'une autorité de certification d'un état membre de l'Union européenne. Les cérémonies de génération des clés maîtresses doivent avoir lieu dans un pays membre de l'Union européenne et en présence du Prestataire.

	Politique de la gestion des clefs	Réponse
H7	Respect des recommandations CRYPTO B2 de l'ANSSI	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

Confidentiel

9. Sécurité physique et environnementale (ISO27001-A.7) [DICP>=3]

	Politique de sécurisation des zones sensibles*	Réponse
I1	Des mesures de protection physiques et de contrôle d'accès doivent être mises en œuvre pour protéger les sites. Elles doivent notamment inclure : un accueil et une gestion des visiteurs sur le site, le port d'un badge obligatoire, un système de vidéosurveillance, un processus sécurisé de réception des plis et colis, une zone de livraison dédiée et protégée.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

9.1 Contrôles physiques des accès et sécurisation des zones

	Politique de sécurisation des zones sensibles*	Réponse
I2	Le Prestataire définit et documente les plages horaires et conditions d'accès aux zones sensibles en fonction des profils des intervenants.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
I3	Le Prestataire documente et met en œuvre des mécanismes de surveillance et de détection des accès non autorisés aux zones sensibles.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
I4	Le Prestataire met en place une journalisation des accès physiques aux zones sensibles. Il doit effectuer une revue de ces journaux au moins mensuellement.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
I5	Le Prestataire met en œuvre les moyens garantissant qu'aucun accès direct n'existe entre une zone publique et une zone sensible.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

* Les zones sensibles sont celles réservées à l'hébergement du système d'information de production du service hors postes d'administration, d'exploitation et de supervision.

9.2 Menaces extérieures et environnementales

	Protection contre les risques environnementaux	Réponse
I6	Les locaux abritant la prestation doivent être protégés contre les menaces environnementales. Doivent *a minima* être identifiés et mises en œuvre des mesures de réduction des risques suivants : • Locaux en zone inondable / tempête / mouvement de terrain • Présence d'établissements industriels dangereux (Seveso) à proximité (rayon de 2 km) • Locaux à proximité établissement sensibles (étatique) ou quartier sensible	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

Confidentiel

9.3 Sortie des actifs

	Procédure de transfert hors site de données de la CDC	Réponse
I7	Le Prestataire met en œuvre les moyens permettant de garantir que le niveau de protection en confidentialité et en intégrité des actifs durant leur transport est équivalent à celui sur site.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

Confidentiel

10. Sécurité liée à l'exploitation (ISO27001-A.8) [DICP>=3]

10.1 Procédure et responsabilités liées à l'exploitation

10.1.1 Procédures d'exploitation documentées

		Réponse
J1	Le Prestataire documente les procédures d'exploitation, les tient à jour et les rend accessibles au personnel concerné.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

10.1.2 Gestion des changements

		Réponse
J2	Le Prestataire documente et met en œuvre une procédure permettant, en cas d'opérations réalisées par le Prestataire et pouvant avoir un impact sur la sécurité ou la disponibilité du service, de communiquer au plus tôt à la CDC les informations suivantes : - La date et l'heure programmées du début et de la fin des opérations ; - La nature des opérations ; - Les impacts sur la sécurité ou la disponibilité du service ; - Le contact au sein du Prestataire.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

10.1.3 Dimensionnement

		Réponse
J3	L'utilisation des ressources est surveillée et ajustée par le Prestataire et des projections sur les dimensionnements futurs sont effectuées pour garantir les performances exigées du service.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

10.1.4 Séparation des environnements de développement, de test et d'exploitation

		Réponse
J4	Le Prestataire documente et met en œuvre les mesures permettant de séparer physiquement ou logiquement les environnements liés à la production du service des autres environnements, dont les environnements de développement.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

Confidentiel

10.2 Protection contre les codes malveillants

10.2.1 Mesures contre les logiciels malveillants

		Réponse
J5	Le Prestataire documente et met en œuvre les mesures de détection, de prévention et de restauration pour se protéger des codes malveillants. Le périmètre d'application de cette exigence est l'ensemble des systèmes utilisés dans la cadre de la prestation (dont les postes utilisateurs et les flux entrants).	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
J6	Le Prestataire documente et met en œuvre une sensibilisation de ses employés aux risques liés aux codes malveillants et aux bonnes pratiques pour réduire l'impact d'une infection.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

10.3 Sauvegarde

10.3.1 Sauvegarde des informations

		Réponse
J7	Le Prestataire documente et met en œuvre une politique de sauvegarde et de restauration des données sous sa responsabilité dans le cadre du service. Cette politique doit prévoir une sauvegarde quotidienne de l'ensemble des données (informations, logiciels, configurations, *etc.*) sous la responsabilité du Prestataire dans le cadre du service.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
J8	Le Prestataire documente et met en œuvre des mesures de protection des sauvegardes conformément à la politique de contrôle d'accès. Cette politique doit prévoir une revue mensuelle des traces d'accès aux sauvegardes.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
J9	Le Prestataire documente et met en œuvre une procédure permettant de tester régulièrement la restauration des sauvegardes.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
J10	Le Prestataire localise les sauvegardes à une distance suffisante des équipements principaux en cohérence avec les résultats de l'appréciation de risques et permettant de faire face à des sinistres majeurs. Le ou les sites de sauvegarde sont assujettis aux mêmes exigences de sécurité que le site principal. Les communications entre site principal et site de sauvegarde doivent être protégées par chiffrement.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

10.4 Journalisation et surveillance

Confidentiel

10.4.1 Journalisation des évènements

		Réponse
J11	Le Prestataire documente et met en œuvre une politique de journalisation incluant au minimum les éléments suivants : - La liste des sources de collecte ; - La liste des événements à journaliser par source ; - L'objet de la journalisation par événement ; - La fréquence de la collecte et base de temps utilisée ; - La durée de rétention locale et centralisée ; - Les mesures de protection des journaux (dont chiffrement et duplication) ; - La localisation des journaux.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
J12	Le Prestataire génère et collecte les événements suivants : - Les activités des utilisateurs liées à la sécurité de l'information ; - La modification des droits d'accès dans le périmètre de sa responsabilité ; - Les événements issus des mécanismes de lutte contre les codes malveillants (voir chapitre 10.2) ; - Les exceptions ; - Les défaillances ; - Tout autre événement lié à la sécurité de l'information.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
J13	Le Prestataire conserve les événements issus de la journalisation pendant une durée minimale de six mois, sous réserve du respect des exigences légales et réglementaires.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
J14	Le Prestataire fournit, sur demande de la CDC, l'ensemble des événements le concernant.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

10.4.2 Analyse et corrélation des évènements

		Réponse
J15	Le Prestataire documente et met en œuvre une infrastructure permettant l'analyse et la corrélation des événements enregistrés par le système de journalisation afin de détecter les événements susceptibles d'affecter la sécurité du système d'information du service, en temps réel ou *a posteriori* pour des événements remontant jusqu'à six mois.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
J16	Le Prestataire doit acquitter les alarmes remontées par l'infrastructure d'analyse et de corrélation des événements au moins quotidiennement.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

10.4.3 Protection de l'information journalisée

Confidentiel

		Réponse
J17	Le Prestataire protège les équipements de journalisation et les événements journalisés contre les atteintes à leur Disponibilité, Intégrité ou Confidentialité.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
J18	Le stockage des journaux doit se faire sur une machine physique distincte de celle qui les a générés et un réseau distinct.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

10.4.4 Journaux administrateur et opérateur

		Réponse
J19	Le Prestataire s'assure que les activités de l'administrateur système sont journalisées, protégées et vérifiées régulièrement.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

10.4.5 Synchronisation des horloges

		Réponse
J20	Le Prestataire documente et met en œuvre une synchronisation des horloges de l'ensemble des équipements sur une ou plusieurs sources de temps internes cohérentes entre elles. Ces sources pourront elles-mêmes être synchronisées sur plusieurs sources fiables externes, sauf pour les réseaux isolés.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
J21	Le Prestataire met en place l'horodatage de chaque événement journalisé.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

10.5 Maitrise des logiciels en exploitation

10.5.1 Installation de logiciels sur des systèmes en exploitation

		Réponse
J22	Le Prestataire met en œuvre des procédures afin de contrôler l'installation de logiciel sur ses systèmes en exploitation, ainsi que de leur maintien en condition de sécurité.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

10.5.2 Administration

Confidentiel

		Réponse
J23	Le Prestataire documente et met en œuvre une procédure obligeant les administrateurs sous sa responsabilité à utiliser des terminaux dédiés pour la réalisation exclusive des tâches d'administration. Il doit les maîtriser et les maintenir à jour.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
J24	Le Prestataire met en place des mesures de durcissement de la configuration des terminaux utilisés pour les tâches d'administration.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

10.6 Gestion des vulnérabilités techniques

10.6.1 Gestion des vulnérabilités techniques

		Réponse
J25	Le maintien du niveau de sécurité des équipements et logiciels utilisés dans le cadre de la prestation est assuré par le Prestataire au travers d'un processus formalisé couvrant la veille, l'évaluation des vulnérabilités, le test et le déploiement des correctifs. Les vulnérabilités identifiées sont traitées dans les délais prévus dans la grille de criticité ci-dessous.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

Grille de délais de traitement des vulnérabilités
Niveau des vulnérabilités techniques

Niveau	Conséquences possibles si celle-ci était exploitée	Critère CVSS
Critique	Remet en cause la sécurité globale de la cible. Des actions de correction à très court terme sont requises.	9 ≤ CVSS
Haute	Des mesures sont à prendre rapidement afin de garantir un niveau de sécurité maximal.	7 ≤ CVSS < 9
Moyenne	Les risques modérés requièrent des actions planifiées dans le temps et l'implémentation de mesures de sécurité à moyen terme.	4 ≤ CVSS < 7
Faible	Les risques faibles requièrent des actions planifiées dans le temps et l'implémentation de mesures de sécurité à long terme.	CVSS < 4

Délai maximum de traitement des vulnérabilités techniques

Niveau	Critère
Critique	Le plus rapidement possible, sans excéder 7 jours
Haute	Avant 3 mois
Moyenne	Avant 6 mois
Faible	Avant 1 an

Confidentiel

10.6.2 Restrictions liées à l'installation de logiciels

		Réponse
J26	Le Prestataire document et met en œuvre des règles d'installation de logiciels par les utilisateurs.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

10.7 Considérations sur l'audit des systèmes d'information

10.7.1 Mesures relatives à l'audit des systèmes d'information

Le Prestataire s'assure que les exigences et activités d'audit impliquant des vérifications sur les systèmes en exploitation sont prévues avec soin et validées afin de réduire au minimum les perturbations subies par les processus métiers et activités de la CDC.

	Audits de sécurité du SI	Réponse
J27	Un audit de sécurité annuel du SI du Prestataire est assuré. Il est effectué par le Prestataire ou un tiers qu'il aura désigné et couvre *a minima* les exigences du présent Plan d'Assurance Sécurité sur le périmètre de la prestation. Préciser en commentaire : le type d'audit (test d'intrusion, audit de configuration, audit documentaire, *etc.*) et la fréquence.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
J28	Le Prestataire doit documenter et mettre en œuvre un programme d'audit sur trois ans définissant le périmètre et la fréquence des audits en accord avec la gestion du changement, les politiques, et les résultats de l'appréciation des risques.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

Confidentiel

11. Sécurité des communications (ISO27001-A.5 et 8) [DICP>=3]

11.1 Cartographie du système d'information

Le Prestataire établi et tient à jour la cartographie du SI impliquée dans le cadre de la prestation, en lien avec l'inventaire des actifs (voir chapitre 6), comprenant au minimum les éléments suivants :

- La liste des ressources matérielles ou virtualisées ;
- Les noms et fonctions des applications, supportant le service ;
- Le schéma d'architecture réseau au niveau 3 du modèle OSI sur lequel les points névralgiques sont identifiés :
  - Les points d'interconnexions, notamment avec les réseaux tiers et publics,
  - Les réseaux, sous-réseaux, notamment les réseaux d'administration,
  - Les équipements assurant des fonctions de sécurité (filtrage, authentification, chiffrement, *etc.*),
  - Les serveurs hébergeant des données ou assurant des fonctions sensibles ;
  - La matrice des flux réseau autorisés en précisant :
    - Leur description technique (services, protocoles et ports) ;
    - La justification métier ou d'infrastructure technique ;
    - Le cas échéant, lorsque des services, protocoles ou ports réputés non sûrs sont utilisés, les mesures compensatoires mises en place, dans la logique de défense en profondeur.

	Cartographie	Réponse
K1	Le Prestataire établit, tient à jour et révise au moins annuellement la cartographie décrit ci-avant.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

11.2 Gestion de la sécurité des réseaux

11.2.1 Contrôle des réseaux

Le Prestataire documente et met en œuvre un dispositif où les réseaux sont gérés et contrôlées de façon à protéger l'information contenue dans les systèmes et les applications.

Le Prestataire doit disposer une ou plusieurs sondes de détection d'incidents de sécurité sur le système d'information du service. Ces sondes doivent notamment permettre la supervision de chacune des interconnexions du système d'information du service avec des systèmes d'information tiers et des réseaux publics. Ces sondes doivent être des sources de collecte pour l'infrastructure d'analyse et de corrélation des événements (voir chapitre 10.4.2).

	Gestion sécurisée des flux	Réponse
K2	Toute nouvelle demande d'ouverture de flux, sur le périmètre de la prestation, fait l'objet d'une validation de la part de la CDC, d'une expression de besoin fonctionnel ainsi qu'une date de validité ou de revue.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

Confidentiel

K3	Filtrage des adresses : seuls les protocoles et les ports définis sont autorisés à se connecter aux adresses réseaux recensées sur le périmètre de la prestation.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
K4	L'ensemble des flux identifiés sur le périmètre de la prestation fait l'objet d'une matrice de flux validée entre la CDC et le Prestataire.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

11.2.2 Cloisonnement des réseaux

Le Prestataire documente et met en œuvre, pour le système d'information du service, les mesures de cloisonnement (logique, physique ou par chiffrement) pour séparer les flux réseau selon :

- La sensibilité des informations transmises ;
- La nature des flux (production, administration, supervision, *etc.*) ;
- Le domaine d'appartenance des flux (des clients – avec distinction par client ou ensemble de clients, du Prestataire, des tiers, *etc.*) ;
- Le domaine technique (traitement, stockage, *etc.*).

		Réponse
K5	Le Prestataire met en œuvre des mesures de cloisonnement appropriées entre ses Clients.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
K6	Le Prestataire doit cloisonner, physiquement ou par chiffrement, tous les flux de données internes au système d'information du service vis-à-vis de tout autre système d'information. Lorsque ce cloisonnement est réalisé par chiffrement, il est réalisé en accord avec les exigences du chapitre 8.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
K7	Dans le cas où le réseau d'administration de l'infrastructure technique ne fait pas l'objet d'un cloisonnement physique, les flux d'administration doivent transiter dans un tunnel chiffré, en accord avec les exigences du chapitre 8.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
K8	Le Prestataire met en place et configure un pare-feu applicatif pour protéger les interfaces d'administration destinées à ses clients et exposées sur un réseau public.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
K9	Le Prestataire met en œuvre sur l'ensemble des interfaces d'administration et de supervision de l'infrastructure technique du service un mécanisme de filtrage n'autorisant que les connexions légitimes identifiées dans la matrice des flux autorisés.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

11.3 Transfert de l'information

11.3.1 Politiques d'extraction et de transfert de l'information

Confidentiel

		Réponse
K10	Des politiques, des procédures et des mesures de transfert formelles sont mises en place par le Prestataire pour protéger / sécuriser les transferts d'information transitant par tous types d'équipements de communication : transfert de données vers des tiers, protection de l'information transitant par messagerie. Préciser en commentaire : quels sont les solutions utilisées pour sécuriser les transferts de données, que ce soit ou non par messagerie (plateforme d'échange sécurisée, API, protection des PJ sur les mails), en accord avec la politique de classification des données.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
K11	Toute extraction de données de la CDC depuis l'environnement de production est par défaut interdite. Si elle est nécessaire, elle devra être effectuée selon une procédure dérogatoire et formalisée, renseignée dans le plan d'assurance qualité.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

11.3.2 Engagements de confidentialité ou de non-divulgation

		Réponse
K12	Les exigences en matière d'engagement de confidentialité ou de non-divulgation, doivent être identifiées, vérifiées régulièrement et documentées.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

Confidentiel

12. Acquisition, développement et maintenance des systèmes d'information (ISO27001-A.5 et 8) [ICP>=3]

12.1 Exigences de sécurité applicables aux systèmes d'information

12.1.1 Analyse et spécification des exigences de sécurité

Les exigences liées à la sécurité de l'information doivent être intégrées aux exigences des nouveaux systèmes d'information ou des améliorations de systèmes d'information existants.

		Réponse
L1	La Prestataire doit assurer la prise en compte de la sécurité des systèmes d'information dès la conception d'applications nouvelles ou lors de la modification d'applications existantes. Il doit intégrer la sécurité dans les projets (notion de *security by design* voire, en présence de données à caractère personnel, de *privacy by default*).	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

12.1.2 Sécurisation des services d'application sur les réseaux publics

Les informations liées aux services d'application transmises sur les réseaux publics doivent être protégées contre les activités frauduleuses, les différents contractuels, ainsi que la divulgation et la modification non autorisées.

		Réponse
L2	Dès lors que le service utilise des flux sur les réseaux publics (*ex.* : services dans le Cloud et/ou exposés sur l'internet), l'utilisation de ces services doit faire l'objet : - De connexions chiffrées, - D'une Authentification renforcée.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

12.2 Sécurité des processus de développement et d'assistance technique

12.2.1 Politique de développement sécurisé

.		Réponse
L3	Le Prestataire documente et met en œuvre des règles de développement sécurisé des logiciels et des systèmes, et les appliquer aux développements internes.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
L4	Le Prestataire documente et met en œuvre une formation adaptée en développement sécurisé aux employés concernés.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

Confidentiel

12.2.2 Revue technique des applications après changement

Le Prestataire documente et met en œuvre une procédure permettant de tester, préalablement à leur mise en production, l'ensemble des applications afin de vérifier l'absence de tout effet indésirable sur l'activité ou sur la sécurité du service.

	Revue technique	Réponse
L5	À la suite de tout changement ou migration technique impactant le service, le Prestataire réalise une mise à jour des plans de tests d'intégration et de recette, suite aux évolutions applicatives, y compris la partie sécurité.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

12.2.3 Principes d'ingénierie de la sécurité des systèmes de développement

		Réponse
L6	Des principes d'ingénierie de la sécurité des systèmes de développement doivent être établis, documentés, tenus à jour et appliqués à tous les travaux de mise en œuvre des systèmes d'information. Exemple : Framework OWASP.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

12.2.4 Environnement de développement sécurisé

		Réponse
L7	Le Prestataire met en œuvre un environnement sécurisé de développement permettant de gérer l'intégralité du cycle de développement du système d'information du service.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
L8	Le Prestataire prend en compte les environnements de développement dans l'appréciation des risques et en assurer la protection conformément au présent référentiel.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

12.2.5 Développement externalisé

Confidentiel

		Réponse
L9	Le Prestataire documente et met en œuvre une procédure permettant de superviser et de contrôler l'activité de développement externalisé des logiciels et des systèmes. Cette procédure doit s'assurer que l'activité de développement externalisé soit conforme à la politique de développement sécurisé du Prestataire et permette d'atteindre un niveau de sécurité du développement externe équivalent à celui d'un développement interne.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

12.2.6 Test de la sécurité et de conformité du système

Le Prestataire doit soumettre les systèmes d'information, nouveaux ou mis à jour, à des tests de conformité et de fonctionnalité de sécurité pendant le développement.

		Réponse
L10	Des tests de sécurité (revue de code, tests automatisés de sécurité) des applications sont effectués tout au long du cycle de développement, préalablement à la mise en production. Ils s'appuieront sur des jeux de données de test n'utilisant pas de données réelles issues de la production. Indiquer en commentaire : les outils utilisés pour réaliser ces tests. Ex. : solutions IAST, DAST, SAST.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
L11	Les plans de remédiation issus de ces tests devront être portés à la connaissance de la CDC et faire l'objet d'un suivi formel pouvant être intégré au suivi de la prestation.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
L12	Si la prestation est qualifiée de Prestation Critique ou Importante, les tests doivent être pilotés par la menace (TLPT – conformément au règlement DORA).	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

12.3 Données de test

12.3.1 Protection des données de test

Le Prestataire documente et met en œuvre une procédure permettant d'assurer l'intégrité des données de tests utilisés en pré-production.

		Réponse
L13	Si le Prestataire souhaite utiliser des données de la CDC issues de la production pour réaliser des tests, le Prestataire doit préalablement obtenir l'accord de la CDC et les anonymiser. Le Prestataire doit assurer la confidentialité des données lors de leur anonymisation.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

13. Relations avec les fournisseurs (ISO27001-A.5.19) [DICP>=3]

Confidentiel

13.1 Sécurité dans les relations avec les fournisseurs

13.1.1 Politique de sécurité de l'information dans les relations avec les fournisseurs

Des exigences de sécurité de l'information pour limiter les risques résultant de l'accès des sous-traitants du Prestataire aux actifs de la CDC doivent être acceptées par le Prestataire et documentées.

		Réponse
M1	Le Prestataire doit tenir à jour une liste exhaustive des tiers participant à la mise en œuvre du service. Cette liste doit préciser la contribution du tiers au service et au traitement des données à caractère personnel. Elle doit tenir compte des cas de sous-traitance à plusieurs niveaux.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

13.1.2 La sécurité dans les accords conclus avec les fournisseurs

		Réponse
M2	Le Prestataire doit exiger des tiers participant à la mise en œuvre du service, dans leur contribution au service, un niveau de sécurité au moins équivalent à celui qu'il s'engage à maintenir dans sa propre politique de sécurité. Il doit le faire au travers d'exigences, adaptées à chaque tiers et à sa contribution au service, dans les cahiers des charges ou dans les clauses de sécurité des accords de partenariat. Le Prestataire doit inclure ces exigences dans les contrats conclus avec les tiers.	☐ Conforme ☐ Non conforme ☐ N/A
M3	Le Prestataire doit contractualiser, avec chacun des tiers participant à la mise en œuvre du service, des clauses d'audit permettant à la CDC, au Prestataire ou à un organisme de qualification, à la demande du Prestataire ou à la demande de la CDC, de vérifier que ces tiers respectent les exigences du présent référentiel.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
M4	Le Prestataire doit documenter et mettre en œuvre une procédure permettant de réviser au moins annuellement les exigences en matière d'engagements de confidentialité ou de non-divulgation vis-à-vis des tiers participant à la mise en œuvre du service.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

13.1.3 Chaine d'approvisionnement informatique

		Réponse
M5	Les accords conclus avec les fournisseurs doivent inclure des exigences sur le traitement des risques liés à la sécurité de l'information associé à la chaine d'approvisionnement des produits et des services informatiques.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

13.2 Gestion des prestations de service des fournisseurs

13.2.1 Surveillance et revue des services des fournisseurs

Confidentiel

		Réponse
M6	Le Prestataire doit documenter et mettre en œuvre une procédure permettant de contrôler régulièrement les mesures mises en place par les tiers participant à la mise en œuvre du service.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

13.2.2 Gestion des changements apportés dans les services des fournisseurs

		Réponse
M7	Le Prestataire doit documenter et mettre en œuvre une procédure de suivi des changements apportés par les tiers participant à la mise en œuvre du service susceptibles d'affecter le niveau de sécurité du système d'information du service.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
M8	Dans la mesure où un changement de tiers participant à la mise en œuvre du service affecte le niveau de sécurité du service, le Prestataire doit en informer la CDC sans délais et mettre en œuvre les mesures permettant de rétablir le niveau de sécurité précédent.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

Confidentiel

14. Gestion des incidents liés à la sécurité de l'information (ISO27001-A.5 et 6)

14.1 Gestion des incidents liés à la sécurité de l'information et améliorations

14.1.1 Responsabilités et procédures

		Réponse
N1	Le Prestataire doit documenter et mettre en œuvre une procédure traitant de la détection, de l'évaluation, de la qualification et de la remédiation des incidents de sécurité et d'y apporter des réponses rapides et efficaces. Ces procédures doivent définir les moyens et délais de communication des incidents de sécurité à la CDC.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
N2	Le Prestataire doit informer ses employés et l'ensemble des tiers participant à la mise en œuvre du service de cette procédure de détection, d'évaluation, de qualification et de remédiation des incidents de sécurité.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

14.1.2 Signalement des évènements et failles liés à la sécurité de l'information

		Réponse
N3	Le Prestataire doit communiquer sans délai à la CDC, à l'adresse cert@caissedesdepots.fr, les incidents de sécurité et les préconisations associées pour en limiter les impacts. La communication doit comporter au moins : • La nature de l'incident ; • Sa gravité (échelle, voir tableau ci-dessous) ; • Les mesures prises du côté du Prestataire ou tiers ; • Toutes autres informations utiles : lien GAE, les noms de domaines potentiellement concernés, les adresses de messagerie concernées, *etc.* Il doit permettre à la CDC de choisir les niveaux de gravité des incidents pour lesquels il souhaite être informé.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
N4	Le Prestataire doit communiquer les incidents de sécurité aux autorités compétentes conformément aux exigences légales et réglementaires en vigueur. Toute violation de données à caractère personnel doit être notifiée à la CNIL si elle présente un risque pour les droits et libertés des personnes concernées.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

14.1.3 Appréciation des évènements liés à la sécurité de l'information et prise de décision

		Réponse

Confidentiel

N5	Le Prestataire doit apprécier les événements liés à la sécurité de l'information et décider s'il faut les qualifier en incidents* de sécurité. Pour l'appréciation, il doit s'appuyer sur une ou plusieurs échelles (estimation, évaluation, etc.) partagées avec la CDC. * Les incidents de sécurité incluent les violations de données à caractère personnel.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

Dans le cadre du projet, le niveau de gravité de l'incident peut être défini en prenant comme valeur le niveau de gravité le plus élevé des quatre critères DICP : Disponibilité, Intégrité, Confidentialité, Preuve.
L'échelle de gravité peut s'appuyer sur la norme ISO27035. Pour faciliter la compréhension, ces termes ont été convertis en Limité, Important, Grave, Critique, plus communément usités.
La correspondance est indiquée ci-dessous et précise les critères.

Gravité	Définition des impacts
1- LIMITE	Impact nul ou quasi-nul : Les enjeux sont faibles et les risques sont maitrisés (préjudice commercial faible, pas d'impact social, peu voire pas d'action exigée, …).
2 -IMPORTANT	Impact sensible : Les enjeux sont modérés car les risques sont maitrisés et peuvent causer un tort limité à l'entreprise (incidents, pertes de business, image de marque, actif important ou ordinaire, impact social, …).
3- GRAVE	Impact fort : Les enjeux sont importants et correspondent à des menaces dont les effets doivent être limités (dysfonctionnement, préjudice commercial et financier grave, impact social important, …) pour ne pas menacer la vie de l'entreprise. Déclenche la procédure d'escalade.
4- CRITIQUE	Impact critique : Les enjeux sont très élevés (voire vitaux) et correspondent à des risques inadmissibles qui peuvent menacer l'entreprise ou l'une de ses activités (pertes financières directes ou indirectes, actif primordial, image de marque altérée, moyens humains subissant des dommages, impact social majeur, retards importants, préjudice irréparable ou sans alternative, …). Déclenche la procédure d'escalade.

14.1.4 Réponse aux incidents liés à la sécurité de l'information

Si ces mesures s'avèrent insuffisantes et/ou si la situation n'est pas maitrisée et/ou si le niveau d'impact de l'incident le justifie, au regard des critères d'évaluation, la cellule de crise est activée.

Confidentiel

	Dispositif de gestion de crise	Réponse
N6	Un dispositif de gestion de crise devra être mis en œuvre. Il s'appuie notamment sur une politique de gestion de crise et de gestion de communication de crise : • Un schéma d'escalade doit faire apparaitre les relations avec la CDC, et les acteurs associés ; • Les canaux de communication doivent être formalisés ; • Le niveau de disponibilité du dispositif et des acteurs doit être cohérent avec les exigences de la CDC.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
	Maintien du dispositif de gestion de crise	**Réponse**
N7	Le dispositif de gestion de crise devra être connu et maintenu : • Les collaborateurs impliqués doivent être formés ; • Des exercices de crises doivent être planifiés, et les résultats faire l'objet d'analyses et d'éventuels plans d'actions.	☐ Conforme ☐ Non conforme ☐ N/A

Il est recommandé que le Prestataire fasse appel à un prestataire de réponse aux incidents de sécurité [PRIS] qualifié pour traiter les incidents de sécurité nécessitant une expertise supplémentaire.

14.1.5 Tirer des enseignements des incidents liés à la sécurité de l'information

		Réponse
N8	Le Prestataire doit documenter et mettre en œuvre un processus d'amélioration continue afin de diminuer l'occurrence et l'impact de types d'incidents de sécurité déjà traités.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

14.1.6 Collecte de preuves

		Réponse
N9	Le Prestataire doit documenter et mettre en œuvre une procédure permettant d'enregistrer les informations relatives aux incidents de sécurité et pouvant servir d'éléments de preuve.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

Confidentiel

15. Gestion de la continuité de l'activité (ISO27001-A.5.29) [D>=3]

15.1 Continuité de la sécurité de l'information

15.1.1 Organisation de la continuité de la sécurité de l'information

	Identification des acteurs et instances de pilotage	Réponse
O1	Un interlocuteur privilégié doit être désigné pour toutes les questions relatives à la poursuite de l'activité et gestion de crise. Ses coordonnées, ainsi que celles de son suppléant, devront être communiquées à la CDC afin de faciliter les échanges entre acteurs de la continuité globale de la CDC et du Prestataire. Il devra traiter les sujets relatifs de poursuite de l'activité et gestion de crise dans le cadre de comités de pilotage *a minima* annuels (semestriels si la prestation est qualifiée de Prestation Critique ou Importante).	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

15.1.2 Mise en œuvre de la continuité de la sécurité de l'information

	Documentation de poursuite de l'activité et de gestion de crise	**Réponse**
O2	Une politique formalisant les processus et mesures de poursuite d'activité et de gestion de crise est disponible et diffusée au sein de l'organisation. Le responsable de la gouvernance de cette politique doit être identifié et procède à une revue de cette dernière *a minima* annuellement.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
O3	Le Prestataire doit documenter et mettre en œuvre un plan de secours informatique contenant les procédures permettant de maintenir ou de restaurer l'exploitation du service et d'assurer la disponibilité des informations au niveau et dans les délais pour lesquels le Prestataire s'est engagé contractuellement vis-à-vis de la CDC.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
O4	Le personnel du Prestataire et celui de ses sous-traitants doit être sensibilisé et formé à la poursuite de l'activité, ainsi qu'à la gestion de crise.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
O5	Les DIMA (Durée d'Interruption Maximale Admissible) et PDMA (Pertes de Données Maximales Admissibles) liées à la prestation et définies au plan d'assurance qualité ou dans d'autres documents contractuels seront respectées par le Prestataire. En outre, Les durées maximales de reprise technique doivent être en cohérence avec la DIMA.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
	Couverture du Plan d'Urgence et de Poursuite de l'activité (PUPA)	Réponse
O6	Un Plan d'Urgence et de Poursuite de l'Activité doit être mis en œuvre en cas d'indisponibilité d'un bâtiment, du SI ou du personnel susceptible d'impacter le service. Le PUPA doit couvrir *a minima* les scénarios suivants : • Indisponibilité durable d'un site hébergeant du personnel ; • Défaillance des systèmes d'information et/ou des systèmes techniques ; • Absentéisme majeur de collaborateurs ; • Prestataires essentiels indisponibles. Il met en œuvre les moyens de reprise et solutions de secours permettant de respecter les Durées d'Interruption Maximale Admissible (DIMA) définies contractuellement.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

Confidentiel

	Sous-traitants ou autres tiers du Prestataire	Réponse
O7	La relation avec les sous-traitants, ou autres tiers autorisés doit être maîtrisée. Ces derniers doivent être assujettis aux même règles et conditions que le Prestataire, et doivent avoir des pratiques de Plan d'Urgence et de Poursuite de l'Activité de niveau équivalent à celles attendues par la CDC.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

15.1.3 Vérifier, revoir et évaluer la continuité de la sécurité de l'information

Le Prestataire doit documenter et mettre en œuvre une procédure permettant de tester le Plan d'Urgence et de Poursuite de l'Activité afin de s'assurer qu'il est pertinent et efficace en situation de crise.

	Maintien en condition opérationnel du PUPA	Réponse
O8	Des procédures de maintien en condition opérationnelle du Plan d'Urgence et de Poursuite de l'Activité doivent être mises en œuvre. Ces procédures doivent être révisées, mises à jour et régulièrement testés. Les résultats de ces tests et plans d'actions en découlant doivent être communiqués à la CDC. Cette dernière, à sa demande, doit également pouvoir y participer sur le périmètre de son activité externalisée.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
	Test du PUPA	**Réponse**
O9	Le Prestataire fait une série de tests de son PUPA : bascule partielle, bascule complète, tests de connaissance des équipes, repli sur site secondaire, déclenchement d'une crise).	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

Confidentiel

16. Conformité (ISO27001-A.5.31 et 36)

16.1 Conformité aux obligations légales et réglementaires

		Réponse
P1	Le Prestataire doit identifier les exigences légales, réglementaires et contractuelles en vigueur applicables au service. En France, le Prestataire doit considérer au minimum les textes suivants : - Les données à caractère personnel [LOI_IL], [RGPD] ; - Le secret professionnel [CP_ART_226_13], le cas échéant sans préjudice de l'application de l'article 40 alinéa 2 du code de procédure pénale relatif au signalement à une autorité judiciaire ; - L'abus de confiance [CP_ART_314-1] ; - Le secret des correspondances privées [CP_ART_226-15] ; - L'atteinte à la vie privée [CP_ART_226-1] ; - L'accès ou le maintien frauduleux à un système d'information [CP_ART_323-1].	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
P2	Le Prestataire doit, selon son rôle dans les traitements de données à caractère personnel (responsable de traitement, sous-traitant ou co-responsable) justifier et documenter les choix de mesures techniques et organisationnelles réalisés en vue de répondre aux exigences de protection des données à caractère personnel du présent référentiel.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
P3	Le Prestataire doit documenter et mettre en œuvre les procédures permettant de respecter les exigences légales, réglementaires et contractuelles en vigueur applicables au service, ainsi que les besoins de sécurité spécifiques. Le Prestataire doit, sur demande de la CDC, lui rendre accessible l'ensemble de ces procédures.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :
P4	Le Prestataire doit documenter et mettre en œuvre un processus de veille actif des exigences légales, réglementaires et contractuelles en vigueur applicables au service.	☐ Conforme ☐ Non conforme ☐ N/A Commentaire :

Confidentiel